Technische Universität Berlin

Forschungsberichte
der Fakultät IV – Elektrotechnik und Informatik

Information Security and Knowledge Management: Solutions Through Analogies?

Timo Glaser, Frank Pallas

Bericht-Nr. 2007 - 18

ISSN 1436 - 9915

Impressum

Herausgeber:
Die Professoren der Fakultät IV – Elektrotechnik und Informatik
der Technischen Universität Berlin

Geschäftsführender Herausgeber:
PD Dr.-Ing. Horst Zuse •
Sekretariat FR 5-3 • Franklinstraße 28/29 • D-10587 Berlin
Internet: http://www.cs.tu-berlin.de/~zuse
E-Mail: zuse@cs.tu-berlin.de
Phone: +49 30 314 24788

Druck und Vertrieb:
Fakultätsdruckerei

Information Security and Knowledge Management: Solutions Through Analogies?

Timo Glaser[1,2] and Frank Pallas[1]

[1] Technical University of Berlin
Computers and Society

[2] Peritor Wissensmanagement GmbH

timo.glaser@peritor.com, pallas@cs.tu-berlin.de

Abstract. Information Security Management and Knowledge Management show a couple of intriguing similarities. This paper identifies some of these similarities and highlights abstract problems arising from them in both areas. Those analogies motivate to look for possibilities to transfer solutions from one area to the other.

1 Introduction

In our current world of postindustrial value generation, knowledge has become one of the most significant production resources. The existence and success of a growing number of organizations strongly depends on their capability of exclusively using their knowledge for profit generation.

Such *exclusively usable knowledge* can appear in various forms. Intermediary and final results from research and development departments possess the highest value for an organization as long as they are unknown by rivals. Knowledge about customers is one of the most valuable assets of many businesses and represents a larger benefit if its use is restricted to the business itself. Consulting firms act as aggregators of knowledge and are able to offer this knowledge at the market as long as it can be used by them exclusively.[3] Even the business models of many open source firms are primarily built upon this principle. Their extensive knowledge about a certain product predestines them as preferred provider of respective complementary products like consulting services, training etc.[4]

As efficient utilization of exclusively usable industrial facilities and human working power was the delimiting factor for the wealth and and growth of an

[3] See, for example, Birkenkrahe (2002, p. 5): *"In consulting, there is nothing but knowledge to sell."*

[4] See, for example, Hars and Ou (2001, p. 3): *"[C]ompanies like RedHat have begun to offer commercial consulting, training, distribution, support, and implementation services."* See also Grand, von Krogh, Leonard, and Swap (2004, p. 599): *"These firms do not realize returns from selling proprietary software protected by commercial licenses but by distributing and adding services to software protected under the OS license."*

organization in the former days of industrial production, efficient utilization of exclusively usable knowledge has, in many cases, become the delimiting factor nowadays. To ensure success, organizations therefor try to maximize the level of exclusively usable knowledge inside the organization.

Currently, this aim is addressed by two main fields of activity: Knowledge Management and Information Security Management.

Knowledge Management has been defined as *"[...] the capability by which communities capture the knowledge that is critical to their success, constantly improve it, and make it available in the most effective manner to those who need it [...]"* (Birkenkrahe, 2002, p. 5). According to Liebowitz (1999, p. iii f.), Knowledge Management is dealing *"with the process of creating value from an organization's intangible assets"* and is about *"the conceptualization, review, consolidation and action phases of creating, securing, combining, coordination and retrieving knowledge"*.

Information Security, on the other hand, is usually outlined as the *"preservation of confidentiality, integrity and availability of information"* while *"other properties such as authenticity, accountability, non-repudiation and reliability can also be involved"* (ISO / IEC, 2005, p. 2). There are a number of alternative definitions, but in any case, confidentiality, integrity and availability of information play an outstanding role and can thus be identified as the core of Information Security. Information Security Management can thus be defined as the management of activities being aimed at the confidentiality, integrity and availability of organization-internal information.

This article identifies several similarities between the fields of Knowledge Management and Information Security Management inside organizations and ascribes well-known challenges from daily practice to some common abstract problems. It then introduces a couple of well known strategies and activities from both areas which overcome some of the known problems at least within one of the two fields. In a final step, established solutions from one field are transferred to the other field to suggest possible new approaches for supporting Knowledge Management and Information Security Management inside organizations.

2 Similarities

Both fields, Knowledge Management and Information Security Management, are rated highly important by organizations and have been strongly present to IT-departments and top management over the past few years. These two fields share—from an abstract point of view—some common characteristics that suggest translating established solutions from one area to the other:

2.1 Dependence on People

First, in both disciplines success heavily depends on *people*. In Knowledge Management, people have to share their individual—tacit as well as explicit—knowledge with others to form and establish a comprehensive body of knowledge

which can be used (and thus profited from) all over the organization. This body of knowledge has in turn to be capitalized by other members of the organization.

The same is true for Information Security. After decades of mainly technical approaches to Information Security, it is now widely accepted that *"people are the cornerstone of [information] security"* (Bishop and Frincke, 2005, p. 49). To make Information Security work, people have to behave in a secure manner, must not circumvent established security mechanisms and procedures, and should develop a sense for making the right decision in case of unforeseen events.

Thus, a strong dependence on people's behavior can be identified as a first similarity between Knowledge Management and Information Security Management.

2.2 Production of Public Goods

The second similarity is that both areas are aimed at the production of what economists call *public goods*. In economic theory, public goods are defined as being non-rival in consumption, which means that any usage of the good does not decrease its value or availability for others, and non-excludable, meaning that nobody can be barred from making use of the good.[5] At least for the scope of the organization, these characteristics apply to Knowledge Management as well as to Information Security Management.[6]

As mentioned above, Knowledge Management is conducted to create and sustain a body of knowledge that can be used all over the organization to generate profit. Making use of this existing knowledge results in a higher working efficiency. It would therefore be counterproductive for an organization to exclude any of its members from using an existing body of knowledge for daily work, resulting in non-exclusive treatment of knowledge.[7]

The principle of non-rivalry, in turn, results from the non-physical nature of knowledge. As an information good, knowledge can—once it has been produced—be used repeatedly at minimal or even at zero costs[8] leading to non-scarcity. If one member uses existing knowledge, this does in no way limit or constrain its utility for other members.

The same is true for Information Security. Once a solution for enhancing Information Security has been established, the usual case is that there is no

[5] See, for example, Mankiw and Taylor (2006, p. 208).

[6] This limitation to the scope of the organization could encourage using the term of *club goods* instead of *public goods* because of the exclusion of non-members of the organization. Nonetheless, as this article solely takes an internal view of the organization and ignores external circumstances, we will keep using the term of *public goods*.

[7] A possible exclusion of individual members from certain kinds of information, for example to prevent information overload, does not affect this basic principle. It is therefore not further considered herein.

[8] See, for example, Shapiro and Varian (1999, p. 21): *"Information is costly to produce but cheap to reproduce."*

rivalry in making use of it.[9] Information Security does not decrease for any individual member of an organization as a result of another member making use it.[10]

Non-exclusion is also present for organizational Information Security. With Information Security being a fundamental (and non-rival) requirement for smooth operations, it would make no sense for an organization to exclude any member from taking advantage of it. In fact, the opposite is true: If an organization would intentionally hinder any of its members from having a certain level of Information Security, this would impose possible weaknesses since most Information Security problems are weakest-link problems[11]. Consequently, non-exclusion of single members is the usual case for organizational Information Security.

In sum, Knowledge Management and Information Security Management share a second similarity, being aimed at the production of organization-internal public goods.

2.3 Positive Effect on Exclusively Usable Knowledge

A *positive effect* on the *exclusively usable knowledge* of an organization is a third similarity of Knowledge Management and Information Security Management.

Knowledge Management is aimed at enhancing visibility and accessibility of an organization's existing knowledge for every member. Individual knowledge has to be divulged organization-wide to increase the amount of organization-internal knowledge that can be used by any individual (to generate profit for the organization as a whole). For organizations, this profit-increasing effect is most significant for internal knowledge not being available to rivals and thus representing a competitive advantage.

In short, knowledge that can be used by all members of an organization promises higher profits than individual knowledge and knowledge that remains secret from competitors promises higher profits than knowledge that is publicly available. Knowledge Management is thus aimed at expanding the body of exclusively usable knowledge.

As mentioned above, confidentiality, integrity and availability of information are the classical main goals of Information Security. By applying these goals to the body of exclusively usable knowledge, it becomes clear that Information Security Management is not directly aimed at increasing this body, but rather at *preventing its decrease*. Confidentiality decreases the risk of business secrets

[9] The underlying scale effects of Information Security have, for example, been mentioned by Biri and Trenta (2004, p. 15). See also CSI / FBI (2005, p. 7): *"[T]here are strictly increasing economies of scale when it comes to information security"*.

[10] In fact, there might be cases where this only holds true up to a certain level of available capacity. As a vivid example, one could think of a content-scanner being built into a corporate firewall, which might be unable to scan huge amounts of traffic. The same would be true for security trainings and several other measures. But, as a matter of principle, Information Security is still non-rival in most cases.

[11] See, for example, Schneier (2004, p.xxii).

getting known by rivals and thus assures exclusiveness, integrity prevents knowledge from being manipulated and availability is targeted against cases of existing knowledge not being usable for the organization's members. Thus, Information Security Management is, similar to Knowledge Management, aimed at having a positive effect on the body of exclusively usable knowledge.

2.4 Optimization Challenge

As a final major similarity, Knowledge Management and Information Security Management both represent *optimization challenges*. As Björck (2001, p. 1) stated, *"[t]oo much business security [...] increase[s] [...] costs and reduce[s] [...] potential revenue streams substantially"*. Even if many Information Security investments might have a positive payoff, there will always be a point from where on additional security investments will result in a negative payoff due to two main reasons:

First, with every investment in Information Security the remaining risks decrease (at least, they should . . .) and become more costly to decrease further. At some state, a point is reached where the expected loss resulting from a risk not being eliminated is lower than the costs of eliminating it. And second, if there is "too much security" in place, working gets less efficient due to a growing number of restrictions and constraints, leading to substantial losses of profits that would otherwise have been possible. Thus, the optimization challenge for Information Security Management is to find the level of security where the marginal benefit of an additional countermeasure equals its marginal costs.

For Knowledge Management, the optimization challenge is similar. Up to a certain point, the refurbishment of existing knowledge and creation of new knowledge results in an overall benefit for the organization, exceeding the costs that have to be borne due to a loss of "productive" working time. As it is the case for Information Security, there will always be a point where the marginal benefit of additional knowledge management efforts is lower than the resulting marginal cost. In both fields, the optimization challenge is finding the point from where on additional efforts would be counterproductive.

2.5 Summary

So far, we have identified four major similarities between the areas of corporate Information Security Management and Knowledge Management: The *strong involvement of and dependence on people*, the *aim of producing an organization-internal public good*, a *positive effect on the exclusively usable knowledge of the organization* and the *underlying optimization problem* of finding the optimal level from where on additional costs and inefficiencies outreach additional benefits. Further similarities could be identified. However, we will focus on the mentioned four. Resulting from these abstract similarities, there are some mutual abstract problems being known from daily practice of Knowledge Management and Information Security Management.

3 Abstract Problems

Based on the four similarities of Information Security Management and Knowledge Management we just identified, we can draw two common goals.

1. Producing and protecting an organization-internal public good mostly relying on people.
2. Finding the optimal level from where on additional costs and inefficiencies outreach additional benefits.

Those two goals entail a couple of *abstract problems* that are similar for Information Security Management and Knowledge Management.

3.1 Production of Public Goods and Misaligned Incentives

Since Information Security and Knowledge are both considered *public goods*, they can be described using the economic model of *externalities*. If an individual user behaves in a secure manner or generates publicly available knowledge, he creates a benefit for the organization as a whole while solely bearing the costs—a *positive externality*. The creation of those public goods by individuals is being impeded by three central problems which we will analyze in the following.

Misaligned and Negative Incentives: As we have described in our analysis of similarities between Information Security Management and Knowledge Management, both activities highly depend on *people*. Companies face the problem that the company's motivation for the creation of public goods, like Information Security and publicly available knowledge, is not valid for individuals who have to bear the costs of production. Those individuals have no or even negative incentives to support their companies' ambitions.

There is no obvious direct "Return on Investment" for an individual if he behaves in a secure manner.[12] To the contrary, the deployment of security solutions and processes builds working barriers and costs in intangibles like *"time, convenience, flexibility, or privacy"* (Schneier, 2006, p. 8), that have to be borne by the individual. Those trade-offs can therefore be regarded as *negative incentives*. Another barrier is the bad image that is being attached to security. If the company does not manage to implement a corporate *security culture*, people are often said to be *paranoid* if they have strong passwords and *not-trusting* if they don't want to share them with their colleagues.[13]

[12] Furthermore, employees are normally not being held fully accountable for their actions. See Anderson and Moore (2006, p. 610): *"Network insecurity is somewhat like air pollution or traffic congestion, in that people who connect insecure machines to the Internet do not bear the full consequences of their actions."*

[13] See, for example, Sasse, Brostoff, and Weirich (2001, p. 127): *"People who exhibit good password behaviour are often described as 'paranoid', 'pedantic' or 'the kind of person who doesn't trust anybody'"*.

Very similar problems arise in knowledge management. The devotion of time to generate knowledge, especially in companies with strict deadlines and a lot of pressure, is unlikely to happen as long as the company does not create other incentives for doing so. Employees who use knowledge management systems intensively are regarded as having too much spare time or wanting to make a good impression in front of their superiors.

Since knowledge is being regarded as power[14] people are motivated to acquire knowledge generated by others but it is unlikely that they share their knowledge altruistically on pure basis of their *intrinsic motivation*. The result are *free riders* who use public resources (knowledge or security) generated by others but do not participate in the creation themselves.

Short-term Orientation: Not only the individual who has to create the public good, but also his direct superior and sometimes even the CEO of a company have individual incentives that are misaligned with the company's needs.

Since many managers are evaluated on basis of their quarterly or yearly results—from the perspective of a company very short-termed—they often act in an inconsiderate manner. This is being worsened because measures have to be in place for some time to see a benefit resulting from the ongoing efforts.[15] Sustainable, *long-term oriented* corporate governance is therefore hard to achieve, especially if a company is partially owned by external investors looking for short-term profits.

This lack of incentives for *long-term orientation* in corporate governance hinders managers to develop and implement Information Security or Knowledge Management concepts. Even if there are concepts and measures already in place, if the management is not convinced that the organization will benefit from them and if it does not have any other personal incentives to support those measures, it will not behave as a good example. Hence, their subordinates will not act according to corporate policies and principles because they follow the behavior of the management.

Short-term orientation and *misaligned incentives* for management and other employees leads to another problem. A critical mass of users must adopt the system before others are being sensitized and see a benefit from using it.[16] The building up of this critical mass is countervailed by an effect which was described by Anderson and Moore (2006, p. 611) as the *bootstrapping problem*—the focus of our next paragraph.

---

[14] *"[K]nowledge itself is a power"* (Bacon, 1996, p.71)

[15] But even then, security is extremely hard to measure. See, for example, Schneier (2006, p. 5 f.): *"Most of the time, we hear about security only when it fails. [...] we might conclude that the security expenditures are wasteful, because the successes remain invisible."*

[16] Even if this critical mass has been reached, the costs borne by the individual for producing the public good are still higher than the resulting benefits—unless there are other advantages for him.

Critical Mass and Bootstrapping: If there is only one user who got a secure password and sticks to security procedures, the organization is still insecure because an intruder can just pick another employee's account to enter the system. As more and more employees' behavior complies with the company's security policy, the risk is being reduced because the attacker has fewer potential accounts he can crack and a *security culture* might start to be established within the company. Other employees will be influenced by the majority of people complying with defined procedures and newcomers are likely to adopt the new corporate culture.[17]

Anderson and Moore (2006, p. 611) describe the underlying problem, which can be called a *bootstrapping problem*, as follows:

> *"if everyone waits for others to go first, the technology [or process, corporate culture, ...] never gets deployed."*

The same principle applies to Knowledge Management. Sharing tacit knowledge makes sense right from the start, even if only two employees decide to do so. For explicit knowledge, often stored in knowledge management systems, the value of the system increases with the number of users actively using it. Managing tacit knowledge by making it explicit, for example by letting employees fill out profiles with their special abilities and interest, does not make sense and will not be used by others unless there is a critical amount of information already in the system.

3.2 The Optimization Problem

The last problem we would like to discuss is the challenge of finding the optimal Information Security or Knowledge Management investment.

In Information Security Management, the *annual loss expectancy* must be balanced with security investments, which consist of spending on information security measures and indirect costs[18]. Most of those resulting costs, caused indirectly by implementing new security measures, are due to a decline of work efficiency. New security measures often imply additional barriers for users.[19] Calculating those overall security investments (direct costs and resulting costs) is therefore a complex task. Another complex problem is to determine the *annual loss expectancy*. As a part of risk management, it requires an assessment of all

[17] Some people will argue that one employee who does not behave in a secure manner is enough for the attacker to get into the corporate system (weakest link principle). It is true that in Knowledge Management free riders, who do not participate in building up the public good but "consume" it (of course without decreasing it), can more easily be accepted than in Information Security Management. But, as soon as more and more people stick to policies, the security awareness of all other employees is automatically being increased as well—which is one of the main goals of Information Security Management

[18] See: Schneier (2004, p. 301 f.)

[19] E.g. lower usability, connectivity and flexibility.

corporate assets, their categorization and valuation.[20] Most companies already fail in identifying their assets. The annual loss expectancy is being calculated based on the value of a company's assets and the risk of disclosure, manipulation and loss or temporary unavailability. Determining the expected loss is highly complex because all secondary losses resulting from an initial security breach must be included as well. Examples are the loss of goodwill (e.g. corporate image and trust of suppliers, partners and customers) and loss of working and production time due to unavailable information or resources. Calculating the *Return on Security Investment* (ROSI) is the term used by security professionals for describing this task.

Determining the *Return on Investment* (ROI) is also the primary problem behind optimizing Knowledge Management activities. Up to a certain point, investing resources (time and money[21]) in knowledge management activities generates a benefit for the organization as a whole. Explicit knowledge can be searched more efficiently if it is stored in a structured way, accessible through a user-friendly interface. Tacit knowledge can be utilized if communication within the company is enhanced by measures like the implementation of an expert directory, organizational measures and the establishment of a corporate culture that supports knowledge exchange. Spending further resources after passing the optimal investment leads to a situation where additional costs outweigh additional benefits. Individuals might still experience beneficial situation for themselves but those benefits are generated at the expense of the organization as a whole. An example is the knowledge acquisition of a particular employee, through training and study during working time, in fields unrelated to his actual work.

Calculating *Return on Security Investment* (Information Security spending) and *Return on Investment* for Knowledge Management activities are major problems that have neither been solved satisfactorily by research nor business.[22]

3.3 Summary

The creation and protection of the public goods Information Security and Knowledge is hindered by an initial bootstrapping problem and by misaligned and negative incentives. No single employee wants to start investing in those activities if he does not see any benefits for himself, as long as nobody else supports those activities as well. Even if a critical mass of users is being reached, people have negative incentives, like loss of time, convenience, flexibility and privacy, to generate those public goods.

---

[20] The implicitness of this widely accepted approach can be questioned. If the calculation of an *annual loss expectancy* is too complex to achieve, one could look for other approaches. Due to the complexity of Return on Investment estimation, *self-optimization* without any direct human interaction would be ideal.

[21] Well, time is money ;-)

[22] Deficiencies in calculating a Return on Investment further leads to very practical problems for managers in charge of Information Security or Knowledge Management. Receiving budgets for implementing new measures, especially organizational ones, is extremely hard because they cannot provide a list of direct monetary benefits.

From a company's perspective, another problem is finding the optimal investment in Information Security and Knowledge Management. Calculating a Return on Investment for those activities is extremely complex and results are very hard to measure.

Today, in a world that has undergone a substantial shift from industrial to knowledge-based societies, both activities are absolutely essential. Business and research proposed solutions for solving the problems we just described. In the following, we will present a couple of those solutions that and discuss the question if Knowledge Management can adopt measures present in Information Security Management, as well as vice versa.

4 Solutions through Analogies

As it has been shown so far, Knowledge Management and Information Security Management share some common abstract properties and are facing the same two abstract problems resulting from these. Any substantial improvement in either of those areas has to take into account the identified abstract problems and must provide partial solutions to at least one of them.

Thus, one possible method for the identification of new approaches for enhancing Knowledge Management and Information Security Management inside organizations would be to find abstract solutions for the abstract problems and then derive applicable solutions from them.

An alternative way, which is pursued herein, is identifying existing solutions that are established and are considered as being effective and efficient for one of the two areas and then transferring these solutions to the other area. A solution being established in the area of Knowledge Management to meet the problem of underproduction of the "public good" might, for example, provide promising approaches for tackling the same abstract problem in the area of Information Security Management.

4.1 General Similarities in Solutions

Before transferring solutions from one field to the other, we would like to highlight some general similarities that currently established strategies to improving Information Security and Knowledge Management inherit.

1. Multi-layered Solutions:
   Concepts were not always multi-layered. In Information Security, for example, early strategies tried to solve problems through technical measures alone. But today, Information Security Management and Knowledge Management both focus on three different layers within the organization: *technology*, *organization* and *people*.
2. From Management by Incidents to Management by Objectives:
   In both fields, measures were for a long time only implemented when incidents occurred. Without a security breach or knowledge management in-

cidents[23], budget was not allocated to Information Security or Knowledge Management. Additionally, even if there was budget available, the measures that were implemented focused on solving problems that recently occurred. Only recently, management realized that they should favor proactive management, management by objectives (MBO), over reactive management, management by incidents.[24]

3. PDCA or Deming Cycle:
   Since both fields require a continuous process of adaption to changing requirements, their management can be described as a Deming Cycle, consisting of *plan, do, check and act*. For Information Security Management, the cycle is composed of: *Establish ISMS*[25] (plan), *Implement and operate the ISMS* (do), *Monitor and review the ISMS* (check) and *Maintain and improve the ISMS* (act).[26] The corresponding steps in Knowledge Management are: *Analysis and conceptualization* (plan), *Implementation of measures and change management* (do), *Review and success measurement* (check) and *Improve concept by adapting to new requirements and results from review* (act).

4.2 Transferring Solutions from Information Security Management to Knowledge Management

We begin with the direction of transferring established solutions for Information Security Management to the field of Knowledge Management. In doing so, we refer to the standard ISO/IEC 27001:2005 to identify widely accepted solutions. In the standard's annex (pp. 13–29), there are a couple of *control objectives and controls* of which we chose a small subset for exemplary transfer to the field of Knowledge Management. For every chosen control, we give a brief description and link it to the above-mentioned abstract problems the control is being aimed at. Finally, we derive ideas for transferring the control to the area of Knowledge Management.

A.5.1 Security Policy: The first group of controls being mentioned in the standard refers to information security policies. Such a policy should be in place, widely communicated throughout the organization, be approved by the management and regularly updated. These controls are mainly aimed at the abstract problem of *misaligned or negative incentives*. Especially by prescribing a certain kind of behavior and introducing sanctions for non-compliance, policies introduce negative incentives for selfish behavior and thereby readjust individual incentives. The same type of solution could be applied to Knowledge Management by introducing a *knowledge sharing policy* that forces the members of the

[23] Companies often buy out entire management levels from their competitor, which results in a profound loss of knowledge. Another problem is a natural, but extraordinary high fluctuation of employees.

[24] Probst, Raub, and Romhardt (2006, p. 55), ISO / IEC (2005)

[25] ISMS: Information Security Management System

[26] ISO / IEC (2005, p. vi)

organization to share their knowledge with others and enables sanctions in case of non-sharing.

A.7.2 Information Classification: Another group of Information Security controls addresses the classification of different types of information in matters of its value, sensitivity or criticality for the organization. Information shall be labeled in terms of this qualitative classification and shall be handled accordingly. This group of controls is primarily aimed at the *optimization problem*, as it encourages non-uniform treatment of information and thereby allows to restrict measures with high indirect costs to highly sensitive information while keeping indirect costs lower for less critical information. Transfer of this principle to Knowledge Management could, for example, be realized through a similar *classification of different kinds of knowledge* according to its ascribed importance for the organization. By doing so, an organization could diversify Knowledge Management investments and accept higher indirect costs for pivotal knowledge while limiting them for rather nonsignificant domains.

A.8.2 Human Resources Security During Employment: The human dimension is also represented by an own group of controls in ISO 27001. Management has to make sure that employees as well as third parties follow established policies and procedures and a formal process for sanctions shall be in place. These controls are aimed at the enforcement of an established policy and are therefrom targeted at the abstract problem of *misaligned incentives*. They could similarly be applied to the enforcement of a knowledge sharing policy.

Additionally, this group of controls refers to security awareness, education and training. Usual realizations of this measure go far beyond the suggested training sessions and include awareness posters or regular columns and articles in company magazines, just to name a few examples. Such awareness and training initiatives are primarily aimed at the abstract problems of *short-term orientation* and the *bootstrapping problem*. They shall lead to well-informed and less short-sighted users and provide an opportunity for reaching a critical mass by establishing a *security culture*. The same approaches can be pursued for Knowledge Management. Training on different aspects of Knowledge Management can be conducted and even the idea of awareness campaigns is transferable. Think, for example, of *knowledge sharing initiatives* including posters reminding employees to share their knowledge with others, regular columns in corporate magazines introducing selected articles from a Knowledge Management System etc.

Similar considerations could be made for many other Information Security measures. However, our goal was to give a few examples, hoping to have illustrated how established approaches from Information Security Management can be transferred to Knowledge Management to generate new ideas for creative solutions.

We will now follow the same approach in the opposite direction, applying established approaches from Knowledge Management to Information Security Management.

4.3 Transferring Solutions from Knowledge Management to Information Security Management

For the transfer from Knowledge Management to Information Security Management, we chose to follow the structure proposed by the *European Committee for Standardization* (CEN). During a workshop in 2004, they developed, together with participating member states, a framework they called *European Guide to good Practice in Knowledge Management*[27]. We will just pick a few ideas from the standard and try to translate them into Information Security measures.

Part 2 – 5.4 Motivation: For overcoming the problem of misaligned incentives, the European best practice guide suggests a couple of methods and especially focusses on rewarding employees who engage in Knowledge Management activities. It differentiates between *social rewards* and *financial rewards*.

Examples for social rewards in Knowledge Management are *recognition* by colleagues, managers and subordinates, or *improved power* (bigger choice of action, larger field of responsibilities, ...).

The current way of "motivating" employees to stick to information security policies is by putting pressure on them if they don't. Using positive, instead of negative incentives might make sense in Information Security Management as well. Giving positive feedback to employees who behave in a very secure manner or suggest ideas how to reduce risks, can be extremely motivating for them. [28]

Financial rewards are another way to create positive incentives, instead of solely relying on pressure. In Knowledge Management, financial incentive systems are pretty common. One possible way is to reward staff on basis of the number of articles created for or commented in a Knowledge Management system if those articles were useful for others. Practice shows that this way many employees start using a system without any pressure from management. There are odds related to this method though. If such an incentive system is being used for a long period of time, the extrinsic motivation of bonuses is likely to reduce the employees' intrinsic motivation. Therefore, it should only be used at the beginning, to reach a *critical mass* of users and to overcome the *bootstrapping problem*.[29] A similar system might make sense in Information Security Management. At the beginning, after a new policy has been released, employees who stick to those policies or suggest improvements could get financially rewarded. If

[27] See European Commitee for Standardization (2004)

[28] However, one should keep in mind that the choice of measures and their success highly depends on regional and corporate cultures and will therefore vary from company to company.

[29] If the critical mass has been reached, secure behavior has become the *norm*. Behavior outside of the norm should be punished. See Ellickson (1991, p. 125 f.)

secure behavior becomes the norm, the company can shift to negative incentives again, punishing those who do not stick to the policy.

Part 3 – 6.2.7 Pilot Implementation and Feedback of Results:

> "In an ideal situation, instead of implementing the project immediately across the whole organization, a pilot implementation should be carried out, during which it should be possible to learn from the process and to avoid the pitfalls encountered when extending the implementation process across the whole organization."[30]

In Knowledge Management, this approach is being followed very often. Small measures, taken out of a complex concept, are being implemented first. The acceptance and upcoming problems are analyzed and the concept is being adjusted, either by replacing or modifying the measure, or by coming up with new incentives that support the implementation of the concept. This pilot project can also be implemented within a small group, maybe a department or a branch of the organization. This reduces the costs of adjusting to problems that were not anticipated at the beginning.

Information Security managers, on the other hand, develop a security concept and normally try to roll-out their entire concept, including all measures, at once. Without prior probing the acceptance and analyzing resulting costs in intangibles, late changes are likely and costly. In software development, the roll-out of Knowledge Management activities would be called *agile programming or extreme programming*, Information Security projects rather follow the classical *waterfall* approach. It seems to be beneficial to transfer agile implementation methods from Knowledge Management to Information Security Management: probing small parts of the concept within a small test group first, listening to feedback and adjusting concepts accordingly.

For analyzing problems and preventing mistakes to be made twice, knowledge managers use a method called *lessons learned*, which is being described in section 7.2.1 of the CEN Workshop Agreement (CWA). Even if an adoption of *lessons learned* for Information Security aspects has already happened, it is normally not being institutionalized.

Part 4 – Measuring: Part 4 of the workshop agreement ("Guidelines for Measuring KM") does not provide Knowledge Management practitioners with an ultimate tool to measure the outcome of Knowledge Management activities. It therefore cannot fully solve the problem of calculating a return on investment. Nevertheless, it introduces a couple of tools that help managers to keep various perspectives of their Knowledge Management activities in mind. By using a tool, like a balanced score card, those perspectives can be described in performance figures. Implementing one of the tools being used in Knowledge Management can help Information Security managers to broaden their horizon and to continuously evaluate all effects of their activities.

[30] See European Commitee for Standardization (2004, part 3, p. 30)

5 Conclusion and Outlook

As we have seen, Information Security Management and Knowledge Management share some natural similarities. These similarities lead to to common problems that can be tackled in similar ways. We have shown that it is possible to identify new approaches for solving currently unsolved problems from one field by looking at established solutions from the other one. As fields can be considered analogous to a certain extent, solutions might be similar, too.

This analogy opens a wide field of opportunities for future action. Practitioners could expand the exemplary transfer of measures to further ones in order to derive practical solutions. Researchers, on the other hand, might rather be interested in abstract solutions for the identified abstract problems. These may lead to innovative approaches for the world of practice in a later step, too.

Interestingly, Information Security Management and Knowledge Management are not the only areas of the same nature. To the contrary, the identified similarities are not even restricted to microeconomics. Environmental protection, for instance, is a macroeconomic problem that also relies on individuals—companies or even states in that case—who have to build or rather avoid the corrosion of a public good. Established practices from environmental protection could thus provide further inspiration for Knowledge Management and Information Security Management.

Further research might also consider organizational forms differing from established ones. The concept of a "body of *exclusively* usable knowledge" might, for example, not hold true for organizations following an approach of "open innovation" leading to more "porous" (Chesbrough, 2003, p. 37) boundaries between "internal" and "external" and thereby possibly eliminating the necessity of exclusiveness considered herein. It would be interesting to analyze the resulting implications for Knowledge Management as well as for Information Security Management.

Another starting point for future research might be the ongoing shift of organizational forms. Thomas W. Malone (2004), for example, identified an ongoing shift from independent entities over hierarchical organizations to more networked structures. Generally speaking, top-down governance will not work anymore in such organizations and is likely to be replaced by more market-driven approaches. It would be interesting to identify possibilities for realizing organizational Information Security and Knowledge Sharing on the basis of market forces.

Such approaches might provide advanced solutions for the *optimization problem*, which is currently tackled by using economic calculus based upon extensive data aggregation. As F. A. Hayek already stated—even though in a different context and more than sixty years ago: "the 'data' from which the economic calculus starts are never [...] 'given' to a single mind which could work out the implications and can never be so given."

Bibliography

Anderson, R. J. and T. Moore (2006). The economics of information security. *Science 314*(5799), 610–613.

Bacon, F. (1996). *Meditations Sacrae and Human Philosophy*. Kessinger Publishing, LLC.

Biri, K. and G. M. Trenta (2004). Corporate information security governance im schweizerischen privatbankengeschäft. Diploma Thesis, Executive MBA, University of Zurich.

Birkenkrahe, M. (2002). How large multi-nationals manage their knowledge. *University of Auckland Business Review 4*(2), 2–12.

Bishop, M. A. and D. Frincke (2005). A human endeavor – lessons from shakespeare and beyond. *IEEE Security & Privacy 3*(4), 49–51.

Björck, F. (2001). Security scandinavian style.

Chesbrough, H. W. (2003). The era of open innovation. *MIT Sloan Management Review 44*(3), 35–41.

CSI / FBI (2005). Computer crime and security survey 2005. Available via University of Maryland.

Ellickson, R. C. (1991). *Order Without Law: How Neighbors Settle Disputes*. Cambridge: Harvard University Press.

European Commitee for Standardization (2004). *CWA 14924: European Guide to Good Practice in Knowledge Management*.

Grand, S., G. von Krogh, D. Leonard, and W. Swap (2004). Resource allocation beyond firm boundaries: A multi-level model for open source innovation. *Longe Range Planning 37*, 591–610.

Hars, A. and S. Ou (2001). Working for free? - motivations of participating in open source projects. *hicss 07*, 7014.

Hayek, F. A. (1945). The use of knowledge in society. *The American Economic Review 35*(4), 519–530.

ISO / IEC (2005). Iso / iec 27001:2005(e) – information technology – security techniques – information security management systems – requirements. International Organization for Standardization and International Electrotechnical Commission. First edition - 2005-10-15.

Liebowitz, J. (1999). *Knowledge Management Handbook*. CRC.

Malone, T. W. (2004). *The Future of Work: How the New Order of Business Will Shape Your Organization, Your Management Style, and Your Life*. Boston, Massachusetts: Harvard Business School Press.

Mankiw, N. G. and M. P. Taylor (2006). *Economics*. London: Thomson Learning.

Probst, G. J. B., S. Raub, and K. Romhardt (2006). *Wissen managen. Wie Unternehmen ihre wertvollste Ressource optimal nutzen*. Gabler.

Sasse, M., S. Brostoff, and D. Weirich (2001). Transforming the 'weakest link': A human/computer interaction approach to usable and effective security. *BT Technology Journal 19*(3), 122–131.

Schneier, B. (2004). *Secrets and Lies: Digital Security in a Networked World*. Indianapolis, Indiana: Wiley.

Schneier, B. (2006). *Beyond Fear. Thinking Sensibly About Security in an Uncertain World*. Springer, Berlin.

Shapiro, C. and H. R. Varian (1999). *Information Rules. A Strategic Guide to the Network Economy*. Boston, Massachusetts: Harvard Business School Press.