Mikko Kuhalampi

IMPACT OF DETERRENCE THEORY METHODS ON EMPLOYEES’ INFORMATION SECURITY BEHAVIOR

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2017

TIIVISTELMÄ

Kuhalampi, Mikko
Peloteteorian keinojen vaikutus työntekijöiden tietoturvakäyttäytymiseen
Jyväskylä: Jyväskylän yliopisto, 2017, 29 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Moilanen, Panu

Peloteteoria (Deterrence theory) on alun perin psykologiassa ja kriminologiassa käytetty termi, ja sen mukaan rangaistuksen pelko estää yksilöä toimimasta vastoin lakia ja sääntöjä. Digitalisoituvassa maailmassa on viimeisen kahdenkymmenen vuoden aikana tehty paljon tutkimusta, jossa peloteteoriaa on sovellettu tietojärjestelmien sekä tietoturvakäyttäytymisen kontekstiin. Tutkielma käsittelee käytössä olevia peloteteorian keinoja tässä kontekstissa sekä niiden vaikutuksia työntekijöiden tietoturvakäyttäytymiseen.

Tutkielma on toteutettu kirjallisuuskatsauksena ja sen tarkoitus on määritellä peloteteorian käsitettä tietojärjestelmien ja tietoturvakäyttäytymisen kontekstissa sekä tutkia olemassa olevia keinoja ja niiden vaikutuksia. Tutkimuksen tuloksina voidaan todeta, ettei ole olemassa absoluuttista totuutta peloteteorian keinojen vaikutuksista työntekijöiden käyttäytymiseen. Tämä johtuu siitä, että tuloksiin vaikuttavat myös esimerkiksi yksilön ominaisuudet, toimintaympäristö ja kulttuuri. Peloteteoria on edelleen tutkituimpia teorioita työntekijöiden tietoturvakäyttäytymisen kontekstissa, ja aiheen tutkimus jatkuu varmasti myös tulevaisuudessa.

Asiasanat: peloteteoria, informaatioturvallisuus, ohjeidenmukaisuus, käyttäytyminen

ABSTRACT

Kuhalampi, Mikko
Impact of deterrence theory methods on employees' information security behavior
Jyväskylä: University of Jyväskylä, 2017, 29 p.
Information Systems, Bachelors thesis
Supervisor(s): Moilanen, Panu

Deterrence theory is originally a term used in psychology and criminology. According to the theory sanction fear prevents individuals from committing illicit acts against the rules. As the corporate world digitalizes, there has been a lot of research on the topic in the context of information systems and security policy compliance in the last 20 years. This study examines the deterrence theory methods and their impacts in employees' information security behavior.

This study is implemented as a literary review and its purpose is to define deterrence theory in the context of information systems and information security compliance as well as study the existing methods and their impacts on employee behavior. The results of the study suggest that there is no absolute truth about the impacts of the deterrence theory methods in the information security behavior of the employees. This is because there are other variables that influence the results, such as qualities of the employees, working environment and culture. Deterrence theory is one of the most-used theories in the context of information security behavior, and research on the topic will surely continue in the future.

Keywords: deterrence, information security, compliance, behavior

FIGURES

CONTENTS

1 INTRODUCTION

During this era of digitalization almost every job includes the use of a digital device, usually a computer or a smartphone. Employees are handling confidential information about their work, their enterprise and their customers. Every individual deserves their own privacy and it is illegal to give customer information to third parties without a permission, for example. Of course, this does not happen intentionally, but lack of information security and information security policies can make the systems vulnerable and cause them to lose crucial information that is not meant for any third party to read.

Nowadays almost every company has their own information security technologies and applications in use. Unfortunately, successful information security is not reached by technological actions alone. According to Herath and Rao (2009a) "End-user security behaviors are an important part of enterprise-wide information security". Security breaches are hard to discover and a major part of security incidents are never revealed (Hoffer & Straub, 1989). As every industry digitalizes their operations, it affects the employees' everyday working life.

This phenomenon seems largely underrated, as users are a big part of the organization's information security. Puhakainen (2006) posits that information security compliance among employees is one of the biggest information security problems in organizations. According to a research, over a half of security incidents are caused by actions within the organization (Ernst and Young, 2003). Therefore, organizations should go through their information security policies and constantly remind their employees about them.

In this study, this problem is approached from the point of view of deterrence theory. Both procedural and technical countermeasures can be seen as deterrent and as factors increasing the perceived certainty and severity of punishment for misuse of information systems (Straub & Welke 1998, Tittle 1980). Former research on deterrence theory state, that the certainty and severity of countermeasure actions caused by an illicit act, have an impact on the individuals (Gibbs, 1975). However, as this is a general conclusion, further research about deterrence in this context is demanded.

Studying this subject is important from the point of view of individuals, enterprises and organizations, because enterprise employees are handling private information about their customers. If they risk that information because of their own security behavior, it does not give a very good image of the firm. According to Richardson (2007), organizations often refuse to publish information about their security flaws or breaches, because they fear it might damage their organization's image and even the stock price. For these reasons, this is a very interesting subject to study. This study searches for existing actions that can be done to lower the number of security breaches that are caused from within. Considering deterrence theory in this context is important, because it is a very important way of impacting the behavior of individuals. However, the theory methods can be easily used wrong. In this case, the effects might even make the security situation worse.

The main point of this study is to evaluate deterrence theory's feasibility in the context of information systems. Nowadays every organization has its own information security policies, and this way they might already be using methods that can be described as "deterrent", without consciously knowing it. If there is not any kind of sanction when employees cause security breaches, what motivates them to act safely while using the information systems? However, the sanctions can't be the only motivator for employees to obey the rules that are given. Therefore, I am also considering neutralization techniques and employee motivation. Needless to say, every organization should have clear security policies that the employees should follow.

In this study, I am searching answers for the following research questions:

- What does deterrence theory mean?
- What does deterrence mean in the context of information systems?

Going deeper into the topic, this study also looks for answers to following additional questions: What are the existing deterrence theory methods to prevent information system misuse, and what kind of impacts do these methods have.

This study looks for answers to earlier presented questions, and is implemented as a literary review. The process consists of reading trustable articles related to the topic, collecting information of them and making conclusions based on the information gathered. The sources used are mainly research- or conference articles considering the topic. First, thorough research on deterrence theory was searched for. After having the needed theoretical basis on the topic, deterrence theory studies within information systems context were looked for and analyzed. A lot of research has been done on the topic, and they have reached different results. Therefore, it was important to go deeper to the reasons why the results are contradictory.

Content of this study is the following: In the second chapter I am going through the definition of deterrence theory and its relation to the context of information systems and why is it an important part of information security. Also, few techniques strongly related to deterrence are considered, such as neutralization techniques and employee motivation. They are taken into consideration because they are important factors in the efficiency of this theory, since they are closely related to deterrence in general. The third chapter is about the existing deterrence methods to prevent illicit acts among employees. These methods are analyzed in the information systems context, because their usability and suitability in practice needs to be evaluated. Also, the management's actions are evaluated and their role in the process is discussed. The fourth chapter consists of going through the impacts of the methods used to prevent information systems misuse. This includes looking in the previous research methods on the impacts of these countermeasures. After that, positive and negative impacts are discussed, because it is important to realize the risks the theory brings even though usually the results are positive. This chapter also aims at explaining the contradictory results of former research. In the last chapter I go through the gathered answers to the research questions and discuss the key findings of this study. Also, few possible topics for further studies are presented.

2 DETERRENCE THEORY

This chapter is about deterrence theory in general and its suitability to information systems context to prevent information security flaws. The first chapter is about the history of deterrence and how it has ended in this context. The second chapter, deterrence theory is presented in the context of information systems. The third chapter is about neutralization techniques, which are an individual's way of justifying their own actions. They are closely related to deterrence, because the neutralization techniques must be counteracted to reach efficient results with deterrence (Siponen & Vance, 2010). In the fourth chapter, employees' motivation and the factors that have an influence on it are discussed, as deterrence methods are proven to have an influence on the personnel's motivation. The fifth chapter briefly discusses the possible downsides and risks of this theory, as they should always be taken into consideration while using the methods. Avoidance of these negative consequences is a continuous objective.

2.1 History of Deterrence theory

Deterrence theory is originally a theory from psychology that is about controlling behavior of individuals through the fear of punishment (Gibbs, 1975). It also has a long history in the context of international relations and war. For the first time, it was used during the cold war to cause uncertainty and fear in the other countries. It was believed, that by showing off the level of weaponry to other countries they would be able to deter the opponent from taking actions against them. It was also assumed, that the enemy would act rationally and try to minimize the possibilities of severe losses. (Sagan, 1991)

Deterrence theory is later strongly associated in criminology, and it is a method used in criminal justice systems in multiple countries (Zimring, Hawkins & Vorenberg, 1973). It was originally developed into criminology to control criminal behavior by preventing them from committing crimes (Higgins, Wilson & Fell, 2005). According to this theory individual's fear of punishment has a negative impact on the intention to commit crimes (Gibbs 1975, Tittle 1980). Later, it was noticed that deterrence would be helpful in organizations which needed to control their employees' behavior. Deterrence had evidence of its operability and there was a need for strategies that could prevent individuals from preventing illicit acts within an organization (Nagin & Pogarsky, 2001, Gibbs, 1975, Tittle 1980).

As the industry of computing started to realize the importance of security behavior of the employees and the possible risks they might cause, several studies started to examine deterrence theory to be used in this context (D'Arcy & Herath, 2011). Straub and Nance (1990) found that detection and punishment of violators lowers the amount of computer abuse. Straub (1990) also found that deterrents such as raising awareness, information about sanctions and acceptable system use as well as clear statements about penalties had a significant impact on the number of misuses. Deterrence theory is one of the most used theories in information system security research concerning employee behavior (D'Arcy & Herath, 2011). Nowadays the information security in organizations is continuously highlighted. In the research, deterrence theory has been used to predict users' behaviors in different circumstances. Behaviors are seen to be either supportive or disruptive of information security and its variables (D'Arcy & Herath, 2011).

Despite the positive results of research the theory has also received a lot of criticism for feasibility in certain contexts. In this study, deterrence is studied in the context of information systems. There has been a lot of research on the topic in the last 20 years and there still seems to be a demand for further research. Assuming that by applying deterrence theory in this context it is possible to strengthen the information security of an organization, this study aims at finding the right methods to use to find beneficial results.

2.2 Deterrence in the context of information systems

In this thesis, deterrence is seen as a typical method to prevent information systems misuse in organizations. Information system misuse means that an individual (Herath & Rao, 2009a) breaks the given information security policies even though it is not permitted. Deterrence theory is one of the most-used theories in literature concerning information system security policy compliance (Siponen & Vance 2010, D'Arcy & Herath 2011). According to this theory, the more likely it is to get punished and the stronger the sanctions are, the better they behave (Herath & Rao, 2009a). This way the number of policy violations should be smaller. An individual estimates the likelihood of getting caught and the hardness of the punishment before making the decision whether or not to break the rules (D'Arcy et al. 2009). In this study, the hypothesis is that the certainty of sanctions and severity of sanctions have a negative effect on information system misuse.

One of the biggest problems in proving that deterrence methods have beneficial effects in information security behavior among employees, is that the results are very hard to evaluate and monitor (Herath & Rao 2009a, Herath & Rao 2009b). Monitoring the employees can be very costly and complicated. For example, following the information system use of many employees demands a lot of time and money. Also, employees might find it confusing to know that all their actions are surveilled (D'Arcy, Hovav & Galletta, 2009).

Regardless of the problematics in monitoring the results, deterrence theory is widely used in organizations to prevent information system misuse even though the research results have been contradictory (Herath & Rao, 2009a). This might originate from differences in the organizations and populations that are tested. However, there is not a lot alternative theories to control security behavior. Therefore, deterrence is still seen as the strongest theory to go with in this context. Many theories relate to deterrence and work as supportive actions to enhance the results of deterrence, such as neutralization theory. According to Siponen and Vance (2010) preventing employees from using neutralization techniques to justify their actions has a significant impact on security compliance.

2.3 Neutralization techniques

In the context of information systems, neutralization theory is strongly connected to deterrence theory. According to Siponen and Vance (2010) employees often use neutralization techniques that stand in the way of given sanctions to have the hoped impact on behavior. Neutralization techniques are means that humans use to justify their own actions, such as not following the given procedures about information security. Siponen and Vance (2010) present six techniques that fit in the context of information systems and information security: Denial of Responsibility, denial of injury, defense of necessity, condemnation of the condemners, appeal to higher loyalties and metaphor of the ledger. These techniques are presented next. Examples of the techniques retell the views of Siponen and Vance (2010). The use of the presented techniques should be prevented to enhance the information security policy compliance among employees. Preventing these techniques from happening can also enhance the efficiency of deterrence. (Siponen & Vance, 2010)

2.3.1 Denial of responsibility

Denial of responsibility means, that personnel might question the importance of information security. They don't see themselves to be responsible for the outcomes of their actions. Puhakainen (2006) found that employees did not see themselves responsible for following a policy that was unclear for them.

Therefore, going through the information security policies with the staff should prevent the denial of responsibility among them.

According to Piquero, Tibbets and Blankenship (2005), an individual rationalizes that the outcomes and consequences are out of his control, and they are going to happen even though the individual would not act against the rules. This way, the individual does not feel that he should feel guilty of what happens.

2.3.2 Denial of injury

Denial of injury means, that employees undermine the causes their actions lead to. They might think that it is permissible to violate the given rules and directives about information security if no harm is caused to the organization they work for. Parker (1998) discovered that computer criminals often deny the damage they have done to their victims. For example, criminals argue that breaking into a computer does not harm the user itself in any way.

Despite of the consequences, they still break the given rules and privacy of the user. Violator convinces himself to think that there is no reason for any shame or guilt about what is done. Another example of denial of injury is that employees use weak passwords because they don't think that anyone can do anything severe with their account, for instance. In this case, individual thinks that the benefit of using a strong password is not worth the effort. (Barlow, Warkentin, Ormond & Dennis, 2013)

2.3.3 Defense of necessity

Defense of necessity technique means, that personnel explain their non-compliance by pleading to its necessity, for example tight schedules (Puhakainen, 2006). So, for example employees claim that this was the only choice to do in this situation or a time frame (Siponen & Vance, 2010).

Usually an individual rationalizes that he does not have a choice so he does not have to feel guilty of acting against the rules. An employee might also think that he can easily defend himself against sanctions with this reason so that the management would not have a reason to punish him for the violations. The employee would just explain that they give him too much work so he has to break the rules in order to succeed with the given tasks. (Barlow et al. 2013)

2.3.4 Condemnation of the condemners

The technique called "Condemnation of the condemners" means, that the employees blame the unreasonable demands of the information security policies or the people who set them. According to Parker (1998) the people that commit computer crimes often say that the law was unfair. By thinking that the given rules are unreasonable, the individual rationalizes that it is fine to act against the rules. So, in this context for example, it means that employees break the security policies because they think that the rules are too strict. (Siponen & Vance, 2010)

2.3.5 Appeal to higher loyalties

Technique of appealing to the higher loyalties means that employees appeal to the fact that they must violate the given rules or policies if they want to get the job done (Siponen & Iivari, 2006). In this case, there might be a need for the organization to modify their habits to prevent these conflicts from happening. According to Piquero et al. (2005) the employees may also appeal to the hierarchy of the firm or organizational values. This way an individual usually thinks he can get away unpunished even though he broke the given rules.

2.3.6 Metaphor of the ledger

Using the metaphor of the ledger means that employees accept their own information systems misuses by thinking that a small violation does not make a difference when they usually follow the given policies (Siponen & Vance, 2010). For example, an employee thinks that even though he would make one mistake, his actions for the firm are clearly positive in average. So, they rationalize that enough good deeds allow them to do one that is bad. (Barlow et al. 2013)

2.4 Employee motivation

Motivating the personnel is an essential way to enhance the behavior of them. Deterrence can have an impact on both intrinsic an extrinsic motivation. Intrinsic motivation is a stimulation that makes a human being act a certain way for his or her own internal satisfaction. Extrinsic motivation refers to change in an individuals' motivation caused by external factors. Deterrence methods mainly influence the extrinsic motivation, since security policies and rules are given by the management. (Son, 2011)

Deterrence methods are not always seen as the best solution to prevent certain unhoped behavior. Sanctions and surveillance do not make a positive effect on the employees' opinions about the information security policies, and they might even have a negative effect on compliance (Son, 2011). Surveillance does not make the employees to do the maximum effort, it only motivates them to do the demanded minimum (Leach, 2003). This means that organizations have to consider, which is the right amount to "threaten" the employees, to avoid having a negative effect on employees' motivation. Harrington (1996) states that rules and punishments are not seen only as deterrence methods, but they are an important way to an organization to have clear procedures against the individuals who break the rules, which makes them an important way of motivating the employees to obey the rules.

Multiple studies exist about motivating the personnel, but the results seem to be a little bit contradictory. According to intrinsic motivation model individuals' innate preferences have a larger impact on human behavior than the results of the actions; rewards and sanctions, for example (Son, 2011). For example, Deci, Koestner and Ryan (1999) have proven, that any tangible reward that is given for performance of an individual undermines the intrinsic motivation, even though Eisenberger and Cameron (1996) claimed exactly the opposite only a few years earlier. Therefore, it is a little challenging for a reader to find which studies represent the situation they are looking for. Ryan and Deci (2000) found that there is a difference between intrinsic and extrinsic motivators and their results. In this psychological study, they came up with self-determination theory, which is about motivation, well-being and psychological needs of a human being.

There are many factors that have an influence on an individual's behavior. Son (2011) has studied this issue in the context of information systems, and in his study, he approaches the subject by adding both extrinsic and intrinsic motivation models in to the same figure. Son (2011) found, that intrinsic motivators had a bigger impact on employee behavior than extrinsic motivators. However, it seems that both are needed to have a significant impact on employee behavior.

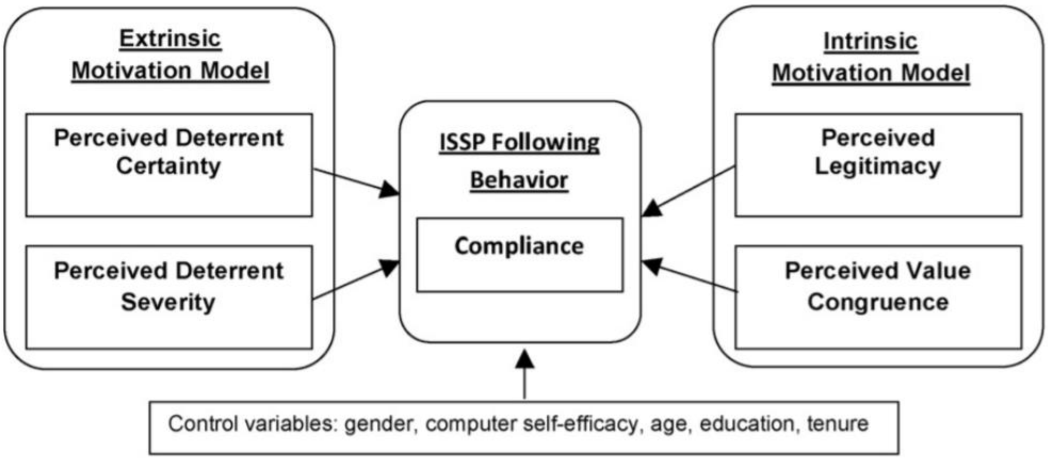
Extrinsic Motivation Model
Perceived Deterrent Certainty
Perceived Deterrent Severity
ISSP Following Behavior
Compliance
Intrinsic Motivation Model
Perceived Legitimacy
Perceived Value Congruence
Control variables: gender, computer self-efficacy, age, education, tenure

Figure 1 - Factors that have an influence on information security policy compliance. (Son, 2011).

Figure 1 consists of extrinsic and intrinsic motivators and control variables. All of them have are supposed to have an impact on information system security policy (ISSP) compliance. Son (2011) found that both extrinsic and intrinsic motivators do have an impact on policy compliance. However, it seems that intrinsic motivators have a significantly bigger effect on information system security policy compliance. The study found that the deterrence methods such as severity of sanctions and certainty of sanctions had actually smaller impact on employee behavior than the intrinsic motivators. According to Son (2011) a positive intrinsic motivation can be reached by combining the employees' values and the main points of the information security policy. Son (2011) also posits certain variables in an individual to have an influence in the information security compliance, such as gender, computer self-efficacy, age, education and tenure. Several studies suggest these variables to have an impact on the results of deterrence methods used (D'Arcy et al. 2009, Hovav & D'Arcy 2012). However, as this study concentrates on the deterrence theory methods to prevent information system misuse, these variables are not widely discussed in this text.

2.5 Potential downsides and risks

Deterrence theory has proven to be effective in certain situations, but has also downsides and risks that need to be avoided. An organization must evaluate which is the amount of resources they can use to evaluate the results of methods used. To develop the information security behavior in the long run, the results must be evaluated to identify the possibilities to improve the results achieved. (Herath & Rao 2009a, Herath & Rao 2009b)

Monitoring the employees' information security behavior itself is costly, and this is a clear downside particularly for smaller companies, because they have less resources to put into information security in general (Herath & Rao 2009a, Kankanhalli et al. 2003). Another downside is that the monitoring of all the desired actions of an employee is practically impossible (Herath & Rao, 2009a). For example, password security flaws such as password sharing and reusing is very hard to evaluate. Surveillance might also confuse the employees and make them feel like they are not trusted, and thus lower the intrinsic motivation of the employees to comply with the given policies (Son, 2011).

3 EXISTING METHODS

Deterrence theory includes multiple methods, but not all of them are effective in the context of information systems (Herath & Rao, 2009b). In this chapter, the most influential ones in the information system context are presented: Surveillance, education, management's actions, certainty of sanctions and severity of sanctions. Certainty and severity of sanctions are the most popular methods in this context. In this study, surveillance is considered as a method since it can take many forms and has a direct impact on employees' behavior. Education refers to raising the personnel's awareness about information security and to influence the employees' intrinsic motivation. Also, actions to raise the security compliance in an organization are discussed. Management needs a strategy or a model to work with to reach wanted results. Therefore, information security cycle is considered which works as a tool for management to implement deterrence methods.

Gibbs (1975) states that the stronger the severity and certainty of sanctions are for certain behavior; the more individuals are deterred by it. However, this is not thoroughly proven in the context of information systems. Certainty of sanctions stands for the probability of getting punished and severity of sanctions stands for the degree of the punishment (Tittle, 1980). Skinner and Fream (1997) found that in the information system context, the severity of sanctions was more influential than certainty of sanctions. These results were discovered by studying college students' intentions to illegally access other students' accounts.

Nagin and Pogarsky (2001) state, that deterrence studies have frequently shown that the fear of possible sanctions prevent deviant behaviors, such as information system misuse. However, there are studies that also claim, that deterrence-based controlling actions do not have any deterrent effect regarding to misuse of information systems (D'Arcy, Hovav & Galletta, 2009). Whitman, Townsend and Alberts (2001) claim that on the operational level, given security policies define guidelines for appropriate information system use. Guidelines can be seen as deterrent if there are widely-known sanctions that follow illicit acts.

There are also variables that might influence the success of an organization's information security, such as qualities of the employees and size of the company. For example, Kankanhalli et al. (2003) found, that large companies are more likely to use deterrent methods, as they usually have the needed resources and expertise to engage these actions. However, this study concentrates on the actual deterrent methods that are used, and does not take these variables into consideration.

3.1 Surveillance

Monitoring the employees' information security behavior demand surveillance. Surveillance is an important part of managing information security compliance. Individuals who know that they are working under surveillance tend to obey the given rules. To ensure the liable information security among employees, an organization should have certain evaluation procedures to control the behavior (Vroom & Von Solms, 2004). According to Herath and Rao (2009a) surveillance is proven to have a positive effect on personnel's information security policy compliance. The amount of surveillance done in an organization also has a direct impact on the probability of given sanctions (Herath & Rao 2009a, Herath & Rao 2009b).

3.1.1 Surveillance techniques

According to Bennet and Reagan (2004) surveillance control techniques are getting more and more usual, for example in working environments. In the context of information systems, a comprehensive surveillance is hard to implement and demands a lot of resources. Even with a high use of resources the thorough surveillance of information security related actions is nearly impossible. However, surveillance is an efficient way of getting to know what the employees are up to. Network monitoring to control online behaviors and camera surveillance to overlook for physical information security behavior are techniques that are considered as helpful in this context (Herath & Rao, 2009a). Network monitoring helps to see if an employee uses services unrelated to their work, for instance. Computer monitoring consists of tracking internet use, recording network activities and performing security audits (D'Arcy et al. 2009). It can also help to prevent employees from downloading untrusted software to the computer. With camera surveillance, it is possible to see if they use any untrusted devices, such as their own USB-memory sticks (Bennet & Reagan, 2004). These actions can be interfered and this way one can track down the employees who commit illicit acts in the information systems.

3.2 Education and awareness

Raising the awareness about information security is an important part of managing the employees' security behavior. Security awareness programs can be seen as deterrent countermeasures, because educating the personnel has major benefits. Both the employees and the superiors must be educated (Straub & Welke, 1998). Raising the knowledge about risks in company's everyday business helps in detecting the possible security breaches. The action that makes education a deterrent method, is that the actions of the firm in the case of information system misuse is highlighted. Possible threats and sanctions are revealed, and they prevent the employees from committing illicit acts.

D'Arcy et al. (2009) state that by security education and awareness programs the misuse of information systems can be reduced within an organization. The goal of information security education and raising awareness is to make the employees cognizant about the possible risks and possible consequences of their actions (Bulgurcu, Cavusoglu & Benbasat, 2010). In their study, general information security awareness means employees' overall knowledge and understanding of the information security risks and potential issues. It consists of general awareness and information security policy awareness. Individuals in an organization have different backgrounds, and that causes different views about information security. Bulgurcu et al. (2010) posit that earlier life experiences concerning information security such as getting attacked by a virus has an impact on the security policy compliance. Lee and Lee (2002) also found that providing wide knowledge about the given policies and unacceptable actions increases the amount of threat perceived in an individual.

In the context of information systems, security education, training and awareness (SETA) programs directly impacts the perceived certainty and perceived severity of sanctions. Thus, these consequences have a direct influence on intention to information system misuse (D'Arcy et al. 2009). SETA programs' deterrent effects are achieved through security briefings and courses and emphasizing the probable consequences following the misuse. In SETA programs, security policies are often used as main training tools (Peltier, 2005).

3.3 Management's ways to act

Every method presented in this study are ways for management to control employees' security policy compliance. In addition to the employees, it is also important to consider the security policies of the management. Managing the information security behavior of the employees is not just a set of different actions; there must be a strategy how to implement it. It is important that the organization management leads by example and therefore convinces the employees about the importance of information security to the organization. (Herath & Rao, 2009a)

Straub and Welke (1998) presented a model called information security cycle (See Figure 2) in their study. They found empirical evidence about information security having a lowering impact on systems risk. According to Nance and Straub (1988) an important application of deterrence theory is based on the relationship between managers and computer abusers and their activities. The set of possible security actions and their interrelationships are presented next in Figure 2. Based on this model, information security management should aim at maximizing the deterred and prevented illicit acts and minimizing the detected and punished ones (Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005).

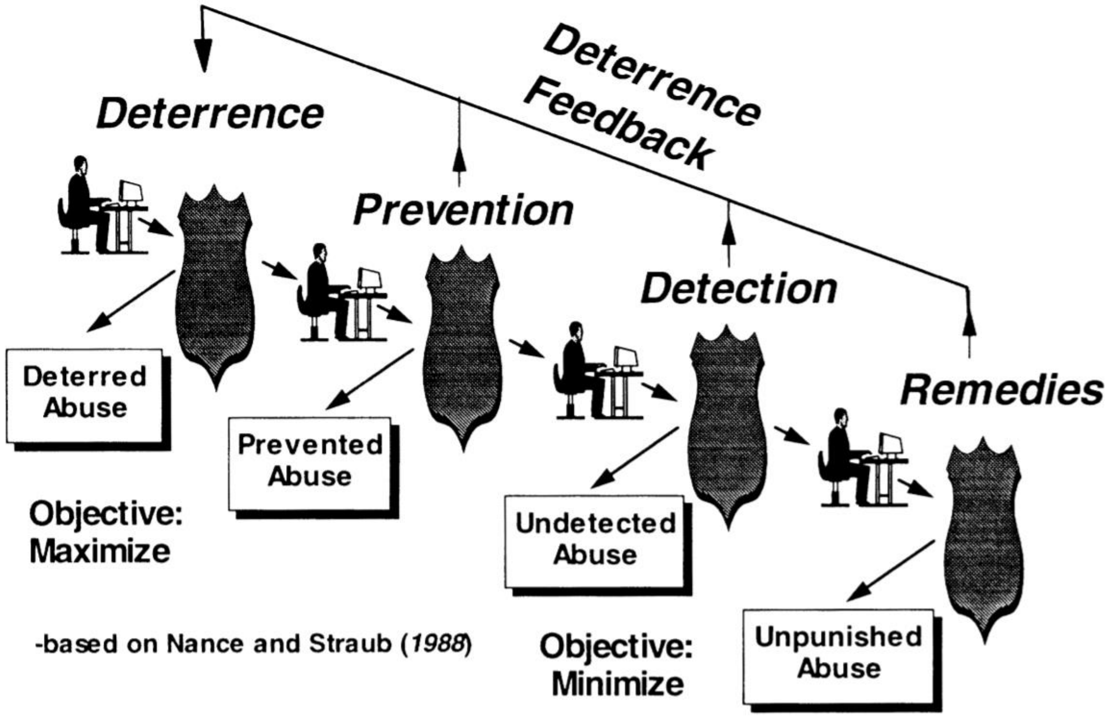

Figure 2 - Information security cycle (Straub & Welke, 1998).

According to this model, managers themselves are the main factors to manage in deterring, preventing, and detecting abuse. Also, possible remedies or possible punishments are under the impact of the managers. Deterrence techniques such as policies and commands given to employees to change their password in a certain time frame. These techniques' success lay only on the shoulders of the employee, whether they are decided to comply with. When employees decide not to comply with these deterrents, the next step is preventives. Preventives are active actions to increase security, such as installing physical locks or taking password access controls into use (Straub & Welke, 1998).

If these first two security steps are penetrated, organization needs capability of detecting the misuse. Some active actions can be done, such as system audits and virus scans. These techniques are needed when a security breach has already happened. Detection aims at gathering evidence of information system misuse and identifying the individual responsible for the situation (Straub & Welke, 1998). After these steps, a sufficient information security program should remedy the negative effects caused by the illicit act and the perpetrator should be punished. Also, the situation should be discussed widely and internal warnings about the problem should be done to raise the awareness concerning the cause. The deterrence feedback loop demonstrates that the more these defensive methods are used in the right way, the more deterred the employees are and their behavior becomes better.

Earlier presented organizational actions will have an impact on the employee deterrence in the future. Straub & Welke (1998) found, that technical remedies do not help in deterring the future abuse of information systems, but the four defense methods can have a significant impact on it. By setting an example of the security policy and action process management gives a straight message to the employees to act within the given rules (Straub & Welke, 1998).

3.4 Certainty and severity of sanctions

According to Hollinger and Clark (1983) the certainty of sanctions, of all the deterrence theory methods, has the strongest effect on behavior of an individual. It makes individuals to avoid taking risks of getting caught. Multiple studies suggest that severity and certainty of sanctions have a negative effect on intention to commit illicit acts (Nagin & Pogarsky 2001, Tittle 1980, Gibbs, 1975). However, in the context of information systems there are studies that present the subject differently. For example, D'Arcy et al. (2009) reported that personnel's information system misuse is influenced only by the perceived severity of sanctions, and that the certainty did not have a significant effect. However, Kankanhalli, Hock-Thai, Tan & Wei (2003) found that deterrent severity did not have a strong influence on information system security effectiveness. Both separately might not have a significant effect on information system security behavior, but they are important parts of general information security. Dissimilar views on the subject in the context of information systems makes the inspection of the effects slightly challenging.

Certainty and severity of sanctions is strongly related to the methods presented earlier, especially surveillance and education. These methods raise the level of perceived certainty and severity of sanctions (Tittle 1980, Nagin & Pogarsky 2001). The higher the amount of perceived certainty of sanctions and severity of sanctions is among employees, the more deterred by the sanctions they get and it affects the intention to commit illicit acts (D'Arcy et al. 2009).

4 IMPACTS OF THE COUNTERMEASURES

In this chapter, impacts of the countermeasures are considered and evaluated. In this study, countermeasures refer to any action done to prevent information system misuse. First, research methods of previous research are discussed. Comparison of different research methods used in various studies is needed, because the studies seem to use different kinds of approaches to the topic. In the second chapter, positive impacts of these countermeasures are presented and examples of hoped consequences are discussed. Third chapter is about the negative impacts of presented countermeasures. It is discussed, why in certain situations the results are negative or why the methods do not have an effect at all. Fourth chapter considers the contradictory results of research on the topic. It is important to evaluate the factors that leads to various studies to end in different conclusions.

Research on this topic suggest that deterrence theory methods have a negative impact on individuals' intention to break the rules or commit illicit acts (Gibbs 1975, Tittle 1980). However, in the context of information systems, successful use of deterrence methods seems to be more complicated. Conflicting research results are a proof of the complication of the topic (Herath & Rao, 2009a).

Different variables were mentioned earlier as a possible factor of security compliance. Even though this study does not examine them, deterrence methods have an impact on these variables. Sanctions are seen to have an indirect influence on multiple variables, such as attitude and perceived behavioral control (Liao, Gurung, Luo & Li 2009, Bulgurcu et al. 2010). On the other hand, few variables are seen to have an influence on security compliance itself. Son (2011) suggested that variables such as age, gender, education, tenure and computer self-efficacy have a direct impact on security compliance and behavior.

High level of information security brings new kinds of obstacles to its success. Post and Kagan (2006) found that employees find strict information security rules as negative factors on their work efficiency. Deterrence methods aim to overcome this kind of obstacles. For example, by educating the employees about the importance of information security they might understand that the rules are reasonable and worth doing (D'Arcy et al. 2009).

4.1 Research methods of former studies

As mentioned earlier, there is a lot of research done on this topic mainly in the last 20 years. In this chapter, different approaches to this topic are presented and evaluated. D'Arcy et al. (2009) suggested that the differences in research results originate from the different starting points and perspectives in the studies. This is a realistic perception that holds true. Studies on this topic have different types of research methods as well as different objectives. This is explicable by the fact that monitoring the results of deterrence methods is challenging and costly (Herath & Rao, 2009a).

D'Arcy et al. (2009) presented an extended model of general deterrence theory and collected data through a survey to find out the level of perceived certainty and severity, moral commitment and misuse intention. They also divided information system misuse to four categories to get results that are more precise. Herath and Rao (2009a) collected tested data from different existing studies to reach reliable results. The research methods of these studies varied which might have helped to reach consensus on the topic. Lee, Lee and Yoo (2004) used a scale to measure variables and used path analysis approach to summarize data collected by a survey. They also presented few questions twice to ensure reliability. Liao, Gurung, Luo and Li (2009) also used their own research model to evaluate impacts of punishments, while applying information from prior studies.

These studies mentioned had differences in results regarding to the effectivity of deterrence methods and procedures. The problem seems to be that even though there are a lot of research on the topic, their objectives vary and their approach to the subject is different. There is a possibility that this influences the results and partly explains the differences in the results.

4.2 Positive impacts

Positive impacts refer to beneficial results of information system misuse countermeasures from the perspective of the organization and its management. According to research punishment severity has a significant influence on software piracy intentions and attitudes in an organization. This result can also be applied to information security compliance, as penalties can work as deterrent to employees. It is important to notice, that only having the rules within an organization has a little impact. Therefore, the rules need to be enforced to receive results. (Peace, Galletta & Thong, 2003)

Surveillance has a direct impact to severity and certainty of sanctions perceived by an employee. Therefore, it affects the security compliance and the intention to follow the given policies (D'Arcy et al. 2009). Successful surveillance naturally consists of both physical and technical methods. Skinner and Fream (1997) found that both severity and certainty of sanctions had a negative impact on intentions to illegally using other students' accounts. This result can be adapted to employee behavior in an organization as a proof of the potential of these methods.

D'Arcy et al. (2009) found, that awareness of the security and SETA programs have an impact on employees' security compliance. They reduce the information system misuses significantly. Bulgurcu et al. (2010) suggest that security awareness programs have an indirect impact on policy compliance through influencing the individual's beliefs about information security. Bulgurcu et al. (2010) also suggest, that security training should be arranged to employees to ensure that they know exactly what they should be doing. This has a positive impact on security compliance.

Several studies found that certainty of sanctions has a positive impact on employees' intentions to comply with security policies (Herath & Rao 2009a, Nagin & Pogarsky 2001, Herath & Rao 2009b, Kankanhalli et al., 2003) There seems to be a lot better results on certainty of sanctions than severity of sanctions.

4.3 Negative impacts

Negative impacts refer to unhoped results of information system misuse countermeasures from the perspective of the organization and its management. Usually the hypothesis of deterrence theory studies is that they have a beneficial impact on security policy compliance, but several studies have found results suggesting the opposite.

Herath and Rao (2009a) found that severity of sanctions had a negative impact on security behavior intentions. Son (2011) also found that severity was negatively associated with intention to comply. Oliver (1980) agrees that sanctions have a positive effect on motivating the individuals, but on the other hand, the methods can generate hostilities against the rules and their authors. Herath and Rao (2009b) found that the more efforts the security policies demand from an employee, the more their attitude against the policy is negatively affected.

As deterrence theory methods have an impact on employees' extrinsic motivation, on the other hand, they can negatively affect the employees' intrinsic motivation at the same time. For example, if the employee feels that the demands are too high, it can affect their attitude negatively towards the management and the policies. Also, if an employee feels that he as an individual can't make a difference on general information security, it can lower the motivation to comply with the rules. (Herath & Rao, 2009b)

4.4 Contradictory results of research

This chapter aims at explaining the contradictory results of research on this topic. As mentioned earlier, not all the deterrence methods have an influence in this context. Previously different research methods were discussed and it is possible that differences the previous researches' methods have an influence on the results.

The circumstances in an organization can differ, which can possibly make the studies find different results. Hovav and D'Arcy (2012) found that effectiveness of deterrence methods varied in different national cultures. They also highlighted the importance of other variables such as morale and awareness as a factor in the information system behavior.

Notable difference in former studies is that some of them take individuals' variables into consideration in their studies and some leave them out entirely to focus on deterrence methods. Most of the studies take few variables into consideration, but they hardly ever are the exact same ones. Some studies have added variables such as age, gender and education to the research (Herath & Rao 2009a, Herath & Rao 2009b). Siponen and Vance (2010) approached intention to violate information security policies by adding variables such as work experience, gender, age, realism, sample organization and scenario type. D'Arcy et al. (2009) suggested contingency variables, such as moral beliefs, virtual status, self-control and employee position.

Based on these perceptions, when studying this subject, it should include a large group of individuals from different companies and organizations, representing different cultures. Pahnila, Siponen & Mahmood (2007) suggest that sanctions do not have a remarkable influence on the employees' intentions to comply with information security policies. Pahnila et al. (2007) also posit that further research on the topic is needed and the tests should be done with different population.

5 CONCLUSION

The purpose of this study was to study deterrence theory in the context on information systems, find the existing methods and evaluate them as well as their consequences. The study itself was done as a literature review based on earlier research on the subject. Despite of the long history of deterrence theory itself, it fits well in the context of information systems. Several key findings are presented next.

Deterrence theory's basic idea is that an individual's behavior can be influenced by having sanctions that follow illicit acts. Therefore, an individual knows what happens if he does not follow the rules, and is deterred by that. In the context of information systems, this means punishing employees for actions that might weaken the organization's information security, such as using the same passwords at work accounts and employees' own accounts. One of the biggest problem concerning deterrence in this context is, that the monitoring of the results is complicated and costly. Therefore, it is hard to evaluate the efficiency of these methods and the results.

Deterrence theory has multiple methods to influence the behavior of an individual. This study presented the mostly-used ones in the context of information systems: Surveillance, education, management's actions, as well as certainty and severity of sanctions. These methods raise the employee's perceived severity and certainty, and therefore cause the employees to fear the consequences. Notable perception was that not all the normally accepted deterrence theory methods have a scientifically proven impact on employee behavior in this context. Multiple studies suggested that raising the awareness of information security and information security policies lower the intention to misuse information systems. Achieving the deterrence on information misuse demands a set of both procedural and technical controls, for example security policies and monitoring software.

Deterrence theory itself is strongly related to psychology, motivation of the employees also has an influence on the efficiency of the methods used. Both intrinsic and extrinsic motivation have an impact on an individual's information security compliance. Deterrence theory methods mainly affect the individual's extrinsic motivation as the sanctions are set by someone else. However, as this study sees education as a deterrence method, also intrinsic motivation is affected. The more the employees feel that they can have an impact on the organization's security, the more likely it is for them to comply with the given policies.

Considering the contradictory results of research on the topic, it appears that some of the methods' impacts remain unclear. However, with only one of these methods it is unlikely for an organization to achieve beneficial results in policy compliance. Therefore, to reach beneficial results, several methods and countermeasures should be implemented at the same time. This naturally demands an up-to-date information security policy and a deterrence plan as a part of general information security plan to achieve the highest efficiency. This plan would ensure the rationality of the implementation phase and it would consider all the possible downsides and risks of deterrence. A widely-known tool for information security management is Information security cycle, which demonstrates the operating model. The main point of management's role based on this model, is to maximize the acts deterred and prevented, and therefore minimize the actions detected and punished.

After going through the former research on the topic and evaluating the possible factors that have an impact on deterrence methods' efficiency, there is not absolute truth about whether the theory works in this context or not. Several studies have achieved both positive and negative results. Some also suggest, that few methods do not have an influence at all. There are certain variables that are believed to have an impact on the efficiency, such as age, gender and education of an individual. Also, same methods seem to work differently in different cultures and organizations. Therefore, there is no one right way to implement these methods.

As the results of deterrence methods in this context remain unclear, there is a need for further research on the topic. Research is needed to perceive all the variables that have an impact on information security compliance. After that it would be possible to study if all the existing methods combined have a significant impact on security compliance. Having these results, should the studies concentrate on excluding the ones that do not have any kind of impact. This would of course demand a lot of results, since the research demands a large group of test subjects from different cultures and organizations. Also, as this research did not consider the impacts of rewards, there is a demand for research on reward systems as a way to enhance existing policy compliance.

REFERENCES

Barlow, J.B., Warkentin, M., Ormond, D. & Dennis, A.R. (2013). Discouraging neutralization to reduce IT policy violation, Computers & Security (2013).

Bennet, C.J. & Regan, P.M. (2004). Editorial: Surveillance and Mobilities, Surveillance & Society, 1 (4), (pp. 449-455).

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly. Vol. 34, No. 3 (September 2010), (pp. 523-548).

D'Arcy, J. & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. European Journal of Information Systems (2011) 20, (pp. 643–658).

D'Arcy, J., Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, Articles in advance, (pp. 1-20).

Eisenberger, R., & Cameron, J. (1996). Detrimental effects of reward: Reality of myth? American Psychologist, 51, (pp. 1153-1166).

employee misuse: does punishment matter? Journal of Computer

Ernst and Young. (2003). Global Information Security Survey.

Gibbs, J.P. (1975). Crime, punishment and deterrence.

Harrington, S. J. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions, MIS Quarterly (20:3), (pp. 257-278).

Herath, T. & Rao, H.R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 2009 – Elsevier

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

Higgins, G.E., Wilson, A.L. & Fell, B.D. (2005). An Application of Deterrence Theory to Software Piracy. Journal of Criminal Justice and Popular Culture, 12 (3), 166-184.

Hoffer, J.A. & Straub, D.W. (1989). The 9 to 5 underground: are you policing computer crimes? - MIT Sloan Management Review, 1989, 35.

Hollinger, R.C. & Clark, J.P. (1983). Deterrence in the Workplace: Perceived Certainty, Perceived Severity, and Employee Theft. Social Forces.

Hovav, A. & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. Information & Management, 49, 2012, (pp. 99–110)
Information Systems 50(2), (pp.49–59).

Kankanhalli, A., Hock-Thai, T., Tan, B.C.Y. & Wei, K.W. (2003) An integrative study of information systems security effectiveness

Leach, J. (2003). Improving user security behaviour. Computers & Security, 22(8), 685-692.

Lee, J. & Lee, Y. (2002). A holistic model of computer abuse within organizations. Inform. Management Comput. Security 10(2) (pp. 57–63).

Lee, S.M., Lee, S.G. & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management 41 (2004) (pp. 707–718).

Liao, Q., Gurung, A., Luo, X. & Li, L. (2009). Workplace management and

Nagin, D.S. & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. Criminology, Volume 39, number 4.

Nance, W.D. & Straub, D.W. (1988). An investigation into the use and usefulness of security software in detecting computer abuse. International Conference on Information Systems, 1988.

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. Proceedings of the 40th Hawaii International Conference on System Sciences.

Parker, D. B. (1998). Fighting Computer Crime: A New Framework for Protecting Information, New York: John Wiley & Sons.

Peace, A.G., Galletta, D.F. & Thong, J.Y.L. (2003). Software Piracy in the Workplace: A Model and Empirical Test. Journal of Management Information Systems, 20:1, (pp. 153-177).

Peltier, T. R. (2005). Implementing an information security awareness program. Information Systems Security 14(2). (pp. 37–49).

Piquero, N.L., Tibbets, S.G. & Blankenship, M.B. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime. Deviant behavior, Volume 26, pp. 159-188.

Post, G.V. & Kagan, A. (2007). Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks, Computers & Security. Volume 26, Issue 3, May 2007, (pp. 229–237).

Puhakainen, P. (2006). A Design Theory for Information Security Awareness, Oulu, Finland: University of Oulu. (pp. 70-80).

Richardson, R. (2007). CSI/FBI Computer Crime and Security Survey. Computer Security Institute, San Francisco.

Ryan, R.M. & Deci, E.L. (2000). Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being. January 2000, American Psychologist. Vol. 55, No. 1, (pp. 68-78) DOI: 10.1037110003-066X.55.1.68.

Sagan, S.D. (1991). Review: History, Analogy, and Deterrence Theory. The Journal of Interdisciplinary History, Vol. 22, No. 1 (Summer, 1991), pp. 79-88.

Siponen, M. & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Quarterly, Vol. 34, No. 3 (September 2010), (pp. 487-502).

Siponen, M., and Iivari, J. (2006). IS Security Design Theory Framework and Six Approaches to the Application of IS Security Policies and Guidelines. Journal of the Association for Information Systems (7:7), (pp. 445-472).

Skinner, W.F. & Fream, A.M. (1997). A Social Learning Theory Analysis of Computer Crime among College Students. Journal of Research in Crime and Delinquency. Vol 34, issue 4, 1997.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management, 48(7), (pp. 296-302).

Straub, D.W. & Nance, W.D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. MIS Quarterly.

Straub, D.W. & Welke, R.J. (1998). Coping with systems risk: security planning models for management decision making, MIS quarterly, Vol. 22, No. 4. (Dec., 1998), pp. (441-469).

Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2005). The insider threat to Information Systems and the effectiveness of ISO 17799. Computers & Security, Volume 24, Issue 6, September 2005, (pp. 472–484).

Tittle, C.R. (1980). Sanctions and social deviance: The question of deterrence.
Vol. 14, No. 1 (Mar., 1990), (pp. 45-60).
Vol. 62, No. 2 (Dec., 1983), (pp. 398-418).

Vroom, C. & Von Solms, R. (2004) Towards information security behavioural compliance. Computers & Security (2004) 23, (pp. 191-198).

Whitman, M. E., Townsend, A.M., Alberts, R.J. (2001). Information systems security and the need for policy. M. Khosrowpour, ed. Information Security Management: Global Challenges in the New Millennium. Idea Group Publishing, Hershey, PA, 9–18

Zimring, F.E., Hawkins, G. & Vorenberg, J. (1973). Deterrence: The legal threat in crime control. (pp. 20-40).