Battling insider attacks:
Deterring improper security behaviour

"Information security is becoming a big problem here.
Do you still have my Captain Crunch decoder ring, Ma?"

Nanno Zegers, 260234
E-mail: nannozegers@gmail.com

Bachelor Thesis Informatics & Economics
Faculty of Economics, Erasmus University Rotterdam

Supervisor: Dr. Ir. Jan van den Berg
Department of Computer Science
Faculty of Economics, Erasmus University Rotterdam

Table of contents

Introduction

i.1 Inducement

Our society depends more and more on computer systems, which are used in everyday life. Since a single attack on these computer systems can take down an entire sector in a matter of hours, securing those systems has become very important. The information security professionals securing our systems are confronted with a great deal of issues, none of which is as perplexing as insider attacks. In the field of information security significant advances in e.g. intrusion detection, encryption and access control mechanisms have been made, which are all focused on repelling external threats, yet there are minimal advances in coping with the phenomenon of internally initiated attacks (Schultz, 2002). On top of that, most organizations spend their money on improving the technological side of security and they pay relatively little attention to the human factor in security incidents (Briney, 2001). The violation of safeguards by trusted personnel of an organization is emerging as a primary reason for information security concerns (Dhillon, 2001).

i.2 Definition

Since this thesis is on insider attacks, a clear definition of that term will be given here. Insider attacks are defined here as "acts associated in any way with computers and/or networks where a victim suffered, or could have suffered, a loss and a perpetrator made, or could have made, a gain and said perpetrator is authorized to use the aforementioned computers and networks" (adapted from Lee & Lee, 2002; Schultz, 2002). This definition is specifically not limited to intentional attacks only. The fact is that most of the inside security breaches are unintentional (e.g. Vroom & Von Solms, 2004).

i.3 Research method

The method of research used for this bachelor thesis is a combination of literature research followed by a short survey.

In this thesis I will try to shed some light on the phenomenon of insider attacks, how it is influenced by user behaviour and security awareness, and what can be done to prevent, or minimise, insider attacks. To do this, various models and theories will be discussed to achieve some insights in the subject matter. From this literature several hypotheses are derived.

These hypotheses are used later on in a short survey, which is used to find out how companies deal with insider attacks and information security. Furthermore, the hypotheses (and consequently the survey questions) are linked to a framework which is

loosely based on the People Capability Maturity Model (P-CMM 2.0; Curtis, Hefley and Miller, 2001).

i.4 Problem statement

To analyse the topics mentioned above, the following problem statement has been defined:

What are the reasons for/motivations behind insider attacks, what has already been tried to deter these insider attacks and what can organizations do further to efficiently reduce/prevent the occurrence of insider attacks?

i.5 Thesis lay-out

This bachelor thesis is laid out as follows:

Chapter one will provide a brief overview of the phenomenon of insider attacks. Furthermore, some myths and misconceptions will be discussed. Finally, some FBI/CSI-statistics on information and computer security will be treated.

In chapter two several theories and models on human behaviour are discussed, to gain insight in the motivations behind improper security behaviour, and specifically insider attacks. The theories and models discussed include, among others, a theory on cost-benefit trade-offs and a holistic model on computer abuse.

Chapter three deals with some models that can be used to prevent or detect an insider threat to the organization. The models discussed are by Parker (1998), Wood (2000) and Schultz (2002).

In the fourth chapter I will shed some light on several main-stream mechanisms used for preventing insider attacks, and discuss a new 'human factor' focused approach that can be used to deter the insider threat, namely a change in culture.

Chapter five contains the results of a short survey on companies' computer and information security related to the insider threat. The questions used in this survey are based on hypotheses derived from the reviewed literature. They are then linked to a framework, the Insider Security CMM, which is loosely based on the People CMM (Curtis *et al.*, 2001), to analyze at which security maturity level (ranging from one to five) the surveyed companies are.

Finally, chapter six contains a short summary of what's been covered in this thesis, followed by some recommendations for future research, as well as a short conclusion in which the main problem statement will be answered.

1. The phenomenon of insider attacks

1.1 Introduction

In this chapter a closer look at the phenomenon of insider attacks is taken. The definition of insider attacks used in this thesis, as mentioned before in the introduction, is repeated here.

> *Insider attacks are "acts associated in any way with computers and/or networks where a victim suffered, or could have suffered, a loss and a perpetrator made, or could have made, a gain and said perpetrator is authorized to use the aforementioned computers and networks" (adapted from Lee & Lee, 2002; Schultz, 2002).*

Some other definitions of insider attacks are given below (as stated in Schultz, 2002):

> *- "Inside attackers are those who are able to use a given computer system with a level of authority granted to them and who in so doing violate their organization's security policy" (Tuglular & Spafford, 1997)*
>
> *- "an insider attack can be defined as the intentional misuse of computer systems by users who are authorized to access those systems and networks" (Schultz & Shumway, 2001)*
>
> *- An internal attacker is "someone with authorized access who instead of fulfilling assigned responsibilities, manipulates access to a system to exploit it" (Einwechter, 2002)*

The last two definitions differ substantially from the first two, in that they only focus on intentional inside attacks. The first two definitions on the other hand, also comprise unintentional inside attacks, which can result from e.g. naïve mistakes from employees with low technical expertise and/or computer knowledge (Stanton *et al.*, 2005).

1.2 The phenomenon

The role of computers in organizations has changed over the years. Business transactions and information processing are becoming ever more vulnerable (a single attack can even immobilize an entire business sector within hours (Besnard & Arief, 2004)) and for this reason, information security has become critically important to almost any business (Vroom & Von Solms, 2004;). In this computer dependant society, information security professionals are confronted with many issues, but they seem to have substantial problems in dealing with so called insider attacks. In recent years they have made substantial advances in enhancing perimeter security, intrusion detection, encryption, access control mechanisms, etcetera, which are all focussed on fending off externally-initiated attacks, such as viruses, trojans, worms and of course hackers and crackers. On

the other hand, little advances have been made in dealing with attacks that occur from the inside (Schultz, 2002). There are many reasons for this lack of progress, e.g. "there's much thinking and discussion on insider attacks, but only little understanding of the nature of the subject" (which leads to certain myths surrounding it) (Schultz, 2002), "technical experts do not understand the computer abusers' ingenuity and perseverance or the weaknesses of the human factors in our systems" (Parker, 1998). As McCollum (1997) pointed out: "… technology is not the whole solution. It involves effectively managing people". This remark hits the spot: the problem should not only be approached from a technical perspective, but also from one that comprises the human factors involved (e.g. organizational, behavioural and managerial perspectives) (Vroom & Von Solms, 2004; McCollum, 1997).

Another problem with inside attacks is that an insider has legitimate access to certain systems and networks, which gives an insider with malicious intents a major advantage over e.g external hackers, since an insider should always be able to have at least a point of entry within one or more computer systems. So an insider usually needs less time and effort to obtain additional privileges as an external attacker does, which in turn means that insiders are less likely to get caught by implemented security measures (Magklaras & Furnell, 2005).

1.3 Myths on insider attacks

There are several myths, or misunderstandings, surrounding the topic of inside attacks that need to be addressed (Schultz, 2002; Randazzo et al., 2004).

First, there is still a general belief that by far most computer abuse is done by outsiders, e.g. hackers. Although most attacks on computer systems do originate from external sources (Annual FBI and CSI survey on computer crime, 2004), that as much, or more, security breaches (that is, successful attacks) originate from inside the organization (FBI/CSI, 2004; Furnell, 2004; Schultz, 2002; Vroom & Von Solms, 2004). Furthermore, insider attacks cause the bulk of the financial losses caused by security breaches (Carr, 2002; Furnell & Phyo, 2003) and Gartner research indicates that insiders cause 70 percent of the "cyber" attacks that cost the victim $20,000 or more in 2002 (Carr, 2002). This has to do with the sophistication of systems that repel external attacks, e.g. intrusion detection systems and access control mechanisms, on one hand, and the still rather meagre understanding of insider attacks within most organizations on the other. Or, as Schultz (2002) stated in his paper: "… many organizations' network security amounts to a hard outer coating, but a soft-chewy middle …".

Secondly, some people sincerely believe that the attack patterns of insider attacks are mainly similar to those of externally-initiated attacks. Fact is, most insiders usually don't show the same so called attack signatures that external attackers do. First off, insiders

can have physical access to certain systems they want to victimize. This physical access causes the need for more specialized methods of attack. On top of that, insiders will generally be more careful not to trigger any alarms, e.g. other people seeing them physically attacking systems or extracting certain classified data. Intrusion detection systems will probably not detect insider attacks, due to the difference in attack patterns between insider attacks and external attacks (Schultz, 2002).

Thirdly, there is the belief that responding to an inside attack is just like responding to an externally-initiated one. However, the response to both is substantially different. Inside attacks can be traced in other ways than computers alone, since the attackers identity is available through other sources (like, for example, a company database). Profiling insiders is very useful in reverse engineering an insider attack, while using this method on outside attacks would be pointless. (Schultz & Shumway, 2001)

Another myth is that insider attacks require technical sophistication. This is only partly true and applies mostly to intentional inside attackers, who aim at large-scale effects of their actions (see the second myth). The reality is that most insider incidents, whether intentional or unintentional, require minimal technical skills and take advantage of non-technical vulnerabilities, e.g. holes in business practice. In the study by Randazzo *et al*. it became clear that in almost 9 out of 10 cases of insider incidents, insiders used easy, legitimate user commands to trigger an incident. There is no standard profile of an inside attacker. Only 23% of them hold technical positions and most of them have no history of hacking whatsoever (Randazzo *et al.*, 2004).

The fifth myth states that insider attacks are unpredictable. Actually, most inside attacks are planned in advance and thus can be prevented. In practice, specific signs that are signalling an attack usually go unnoticed or are ignored. Fact is, a large number of cases show planning behaviour or frustration on the part of employees beforehand and many of the (intentional malicious) inside attackers had committed less serious violations prior to their actual attack.

Sixth, insider attacks are supposedly motivated by revenge. This assumption is commonly made because it used to be true and because most insider attacks do cause damage, which makes them look malicious. Most inside attacks are motivated by financial gain. Four out of five cases in the Secret Service/CERT study (Randazzo *et al.*, 2004) involved employees who had financial motives for their acts.

Finally, most organizations believe that their current (technical) security measures are able to stop most insider attacks. These organizations need a reality check: a security program/policy can reduce the risk of an insider attack to an adequate level, but only if the employees have a certain level of security awareness (Randazzo *et al.*, 2004).

Hypothesis 1a: Companies, in practice, do not use different methods and/or measures to repel inside attacks when compared to external attacks.

Looking back at the general beliefs and myths surrounding the subject of insider attacks that circulate(d) in the information security world, it comes as no surprise that this phenomenon continues to manifest itself. There certainly seems to be a lack of understanding of the insider attack phenomenon, which partly explains its continuing existence.

Hypothesis 1b: Companies tend to ignore the overall threat of insider attacks to computer and information security and instead focus largely, or even solely, on attacks initiated from outside the organisation.

1.4 Facts and figures on security

In this paragraph some facts and figures on computer and information security are discussed. This information is extracted from the 2004 Annual FBI and Computer Security Institute survey on computer crime.

The overall frequency of successful attacks on computer systems declined in 2004, a continuing a trend that began in 2001 (see Figure A1.1, Appendix A.1). Last year the percentage of respondents (i.e. of the FBI/CSI survey) answering that their organization experienced unauthorized use of computer systems in the last 12 months declined to 53 percent, the smallest percentage since this question first appeared in the survey in 1999. Furthermore, the percentage of respondents answering that there was no unauthorized use of their organization's computer systems increased to 35 percent, as the respondents not knowing if such unauthorized use occurred dropped to a low of 11 percent.

Cybersecurity breaches are declining (see Figure A1.2, Appendix A.1), and the source of the breaches seem to be reasonably evenly split between those originating from the inside and those originating outside the organization. The percentage of respondents estimating that their firm experienced between six and ten computer security incidents within the previous year seems to have levelled off at 20 percent, while the percentage of respondents estimating that their organization experienced between one and five computer security incidents increased to 47 percent. 2004 showed the lowest percentage of respondents estimating that their organization experienced over ten computer security incidents during the past year.

Attacks of computer systems, or detected misuse of these systems, has been gradually, but quite steadily decreasing over many years in nearly all categories (see Figure A1.3, Appendix A.1). As seen in the figure, there has been a remarkable drop in reports of

system penetrations, insider abuse, and theft of proprietary information. Though the occurrence of insider abuse has dropped significantly, it is still at 59%, remaining one of the bigger problems in computer security.

> *Hypothesis 1c: The occurrence of insider attacks is declining, but it remains an issue in computer and information security.*

1.5 Summary

This chapter discussed some basics on the phenomenon of insider attacks in information and computer security. A few different definitions were stated, most of which amount to more or less the same. Several myths concerning security, specifically on insider attacks, were defaced. It seems that a lot of people have marginalized the insider threat over the years, but some have come to see that the threat poses one of the greatest risks to information and computer security. Finally, several recent statistics on computer security were discussed, from which it was apparent that inside abuse was on the decline, but far from eradicated. Still nearly 60% of respondents to the 2004 FBI/CSI survey reported insider abuse over the preceding twelve months.

In chapter two, several theories and models on human behaviour are discussed, in order to get a better understanding of the reasons behind improper security behaviour, which can be applied to, for example, insider attacks.

2. Causes of improper security behaviour

2.1 Introduction

In this chapter some theories and a model will be analyzed, to achieve some insights in the reasons and motivations behind the way people act. The behavioural reasoning mentioned in these theories can be directly linked to employees' security behaviour (one already is: Besnard & Arief, 2004) and why they display security breaking behaviour, whether intentional and unintentional.

The theories that will be analyzed are the General Deterrence Theory, social bond theory, social learning theory (all three of them adapted from Lee and Lee, 2002) and a theory on cost-benefit trade-offs (Besnard & Arief, 2004). Lee and Lee (2002) created a 'holistic' model of computer abuse, based on the combination of the three theories in their paper. This holistic model is described in paragraph 2.6 (see Appendix A.2 for a depiction of this model). Furthermore, a model by Stanton *et al.* on end user security behaviour is discussed in this chapter.

2.2 Cost-benefit trade-offs

2.2.1 Security trade-offs

There are conflicting objectives held by some of the actors of a single system, namely attackers and legitimate users. It follows that depending on the goal that an actor is pursuing (attack or legal use), the use of a given computer system will differ dramatically (Besnard & Arief, 2004).

Since Simon introduced his concept of bounded rationality in 1957, we have come to understand that human actions do not seek perfection but an acceptable level of performance with respect to their objectives and what the cognitive resources allow. Cognitive acts are an instinctive and implicit trade-off, balancing cost and efficiency (e.g. Bainbridge, 1998). People intuitively evaluate the efficiency of their decisions before they implement them. Just like in other activities, trade-offs introduce a risk (e.g. Hoc & Amalberti, 1994) by not taking into account some possible outcomes resulting from the chosen actions. When it comes to IT security, the combination of trade-offs and risk can implement a threat (Besnard & Arief, 2004). Following the cognitive approach, Besnard and Arief (2004) propose that almost every decision is a matter of trade-off. Human flexibility means that people perform instinctive trade-offs between some kind of costs and some kind of benefits. Costs and benefits are not to be seen in purely economical terms. Costs can encompass such things as time and effort that someone puts in, benefits can encompass things such as an improved image among peers and even self-satisfaction. Thus, the terms costs and benefits need to be seen in their broadest context when applied to the theory of cost-benefit trade-offs.

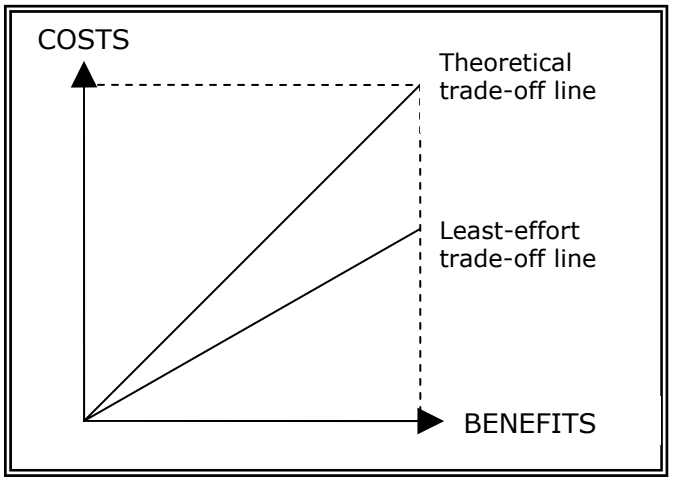


Figure 2.1 Cost/benefit trade-off lines (adapted from Besnard and Arief, 2004)

Figure 2.1 represents the cost/benefit trade-off graphically. In the area above the theoretical trade-off line the costs exceed the benefits, below the line it's vice versa. Since humans lack the ability to always act logically, they sometimes seek cheap actions with the highest possible benefits. This is represented by the least-effort trade-off line in Figure 2.1. This has certain consequences, as decisions that people make will become more dependant on benefits, which means that when applied to the trade-off between security (seen as "costs") and usability (seen as "benefits"), usability may come first, leaving security as a side issue.

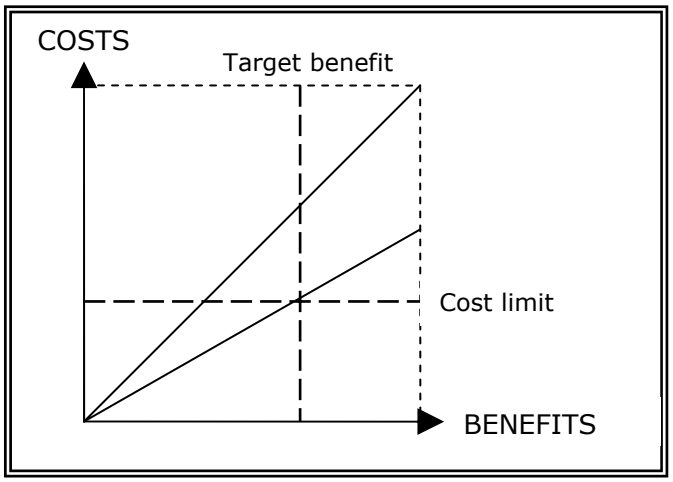


Figure 2.2 Cost/benefit-driven strategies (adapted from Besnard and Arief, 2004)

Sometimes there are explicit boundaries to human decision making. Decisions may be cost-driven or benefit-driven, as depicted in Figure 2.2. Whatever may be the case, the course of action never follows the straight trade-off line, but will instead vary over time

depending on given phases of the work (Besnard & Arief, 2004). This means that sometimes a costly action can be carried out if it has high future benefits.

Typically, attackers are said to exploit security holes left open because of a poor design and/or insecure practices. In other words, the malicious intentions of the attackers are, to some extent, facilitated by the behaviour of some legitimate users (Besnard & Arief, 2004). This all has to do with the trade-offs those legitimate users have made between usability and security, where usability usually has top-priority with those users, as mentioned before.

In practice, both administrators as well as end-users take their actions based on an economic trade-off between security and usability: they weight out the benefits versus the costs involved, where added security (costs) normally leads to reduced usability (benefits). This behaviour leads to threats in computer systems that can be exploited by attackers. System designers should keep the security/usability trade-off in mind when designing security products, so that those products become more user-friendly, thus limiting trade-offs.

> *Hypothesis 2a: In most cases, legitimate users (and companies themselves) will prioritise usability over security (i.e. with regard to systems, software, etc.).*

2.2.2 Acceptable losses

When setting up protections, there are some tolerable losses that humans implicitly take into account. This trade-off entails the cost of protection and the cost of loss (Flechais and Sasse, 2003). The underlying evaluation of the required level of protection is believed to be done in an intuitive manner most of the time. Besnard and Arief (2004) propose that it guides, to some degree, the security policies implemented by organisations.

Since not all data can be protected, some of it is unavoidably left susceptible to attack. This can be a reasonable decision if loss or disclosure of that data is acceptable. Besnard and Arief (2004) suggest that protecting a system is an implicit dialogue between both security officers and attackers. They believe security policies to define the nature of this dialogue before any attack takes place, going against the widespread belief that ‘‘attackers play first’’.

The cost of losing valuable data or service may well be one of the apparent motivations for designing and applying security protections. But seemingly unimportant data, can be damaging as well, particularly at the hands of so-called social engineers.

IT security shares similarities with many domains and risk taking is one of them. Risk and risk management can be both inevitable and implicit (Evans *et al.*, 1995). For example, not plugging a server into a network is a fairly secure condition, but the service

it can provide will not be delivered. This is just the reason why some risk has to be accepted for practically any piece of equipment to properly fulfil its function. There will always be various factors, which can't be influenced, that will impact a piece of equipment's level of safety, but with proper risk management they should not withhold that piece of equipment from operating.

In certain situations, humans perceive risks as being very low and implicitly adapt their protection level accordingly. The smaller the perceived risk, the lower the level of protection. Nevertheless, people are typically prejudiced at perceiving actual levels of risk and rarely have an exhaustive knowledge of the systems they interact with (Redmill, 2002). From this observation, it follows that end-users cannot possibly accurately assess the impact a given practice has on the security of a system. Hence intuitive, heuristic risk evaluations, do not always exactly capture the criticality of specific threats. This lack of accuracy thus degrades the identification and compensation of security breaches, which ultimately can depend on subjective, biased decisions (Besnard & Arief, 2004).

Finally, humans tend to act risky. Major security incidents are not caused by a sudden change in security policy. It's caused by a steady build up of numerous small insecure increments, which are hardly noticeable by themselves, that gradually deteriorate the level of security. This situation often occurs in large industrial systems (Mancini, 1987).

2.2.3 Antagonism among security actors

As we have seen, legitimate users perform trade-offs in the way they use computer systems. It seems likely attackers make a same sort of trade-off. They also compare the costs of their actions to the benefits they expect from those actions.

However, as Besnard and Arief (2004) suggest, there are fundamental differences in the nature of the trade-offs between attackers and legitimate users, because their motivations are very different. Attackers attack because they get a reward of some sort (e.g. peer-recognition, money), legitimate users protect themselves out of necessity. This significant difference in motivations and thus trade-offs, may lead to threats. If attackers have identified a target, they may get focussed solely on the damaging effect of their actions and do not think much about the costs involved. Legitimate users on the other hand, may prioritise usability with little worry for security, which is a common case of usability-driven behaviour.

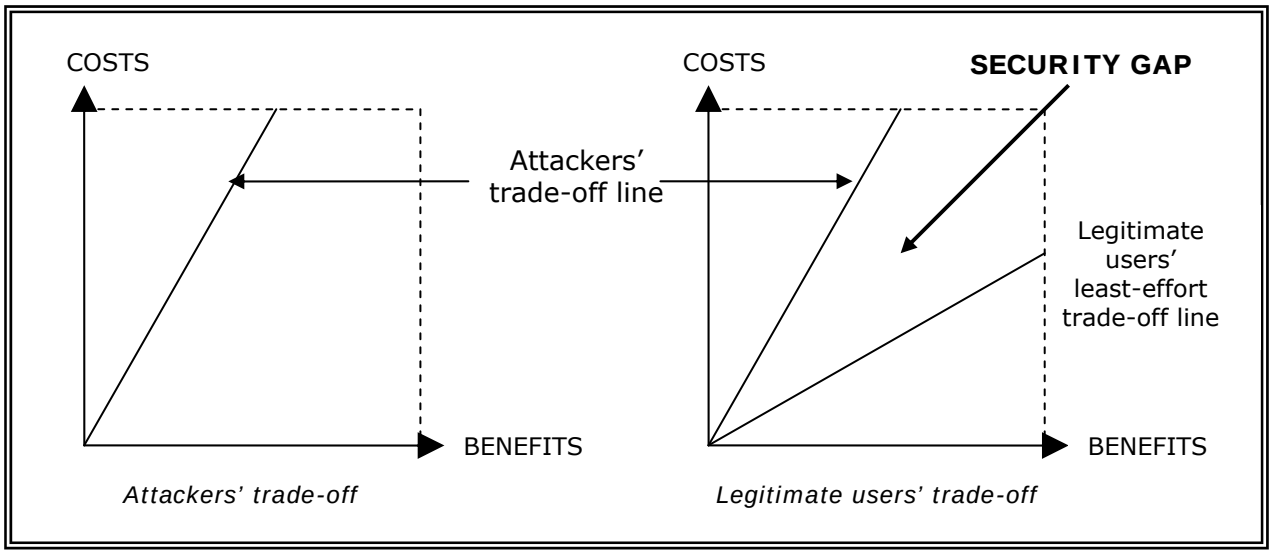


Figure 2.3 Different trade-off strategies (adapted from Besnard and Arief, 2004)

Besnard and Arief (2004) represent this inconsistency as a gap between attackers' and legitimate users' trade-off strategies (see Figure 2.3). They propose that this security gap gives some advantage to attackers and the larger the gap, the more successful and easier an attack could be. The main point is that legitimate users, sometimes being unaware of it, prioritise usability at the cost of security, which creates such a gap in security. As a result, "a successful attack can be expressed in terms of a malicious action whose degree of refinement is higher than the degree of protection of the target system" (Besnard & Arief, 2004).

2.3 General Deterrence Theory

General Deterrence Theory (GDT) assumes that the deviant behaviour can be deterred if the potential deviants fear detection and prosecution (Parker, 1998). It assumes that individuals make rational decisions based on maximizing their benefits and minimizing the costs. Therefore, someone will make a criminal decision when the expected benefits from the criminal act exceed the cost of punishment for that act. GDT has been used to analyze computer abuse behaviour of corporate employees in the information system industry over the past 15 years (see e.g. some papers by Straub: 1990, 1991, 1998). The theory focuses on the mechanisms designed to increase the perceived cost of the crime, thus lowering the odds of people making criminal decisions. Examples of such mechanisms are policies, systems and awareness programs.

In practice however, these mechanisms failed to considerably reduce the criminal intentions and/or behaviours of employees. For example, security policies are supposed to deter computer abuse and deviant behaviour by clearly defining unacceptable or illegal conduct, thereby increasing the perceived threat of punishment. This should clearly lead to reduced criminal intentions and behaviour. However, it turns out that security policies

are unexpectedly ineffective even though over 80 percent of US organizations enforce such security policies. Some possible reasons for this lack of effectiveness are: enforcement of improper security policies, light punishment of deviants and differences in punishment based on rank or privilege of the deviant (e.g. Zajac, 1988; Skinner at al., 1997; Hoffer et al., 1989).

Security systems are expected to be effective tools against computer abuse because they reduce the vulnerability of an organization's information system and increase the computer abusers' fear of detection (Hoffer et al., 1989). Nonetheless, these security systems often proved inadequate in extenuating security abuse, because organizations failed to invest enough in developing and maintaining them. Another reason is that most organizations invested in commercial off-the-shelf products that did not tie into their existing IT systems (Baskerville, 1993).

Security awareness programs are expected to reduce criminal behaviour by passing more security knowledge on to employees, thereby increasing the supposed cost of a criminal decision. It turns out that employees see security knowledge as hard to learn, tiresome, and limiting their freedom, rendering most security awareness programs rather ineffective in practice (Parker, 1998).

It is clear that the abovementioned GDT-mechanisms can be far more effective when deployed correctly. Nevertheless, while GDT provides a reasonable theory, it falls short on some points. The theory clearly does not cover all the factors that come in to play when it comes to criminal intentions and behaviour, computer abuse in particular (Lee & Lee, 2002).

> *Hypothesis 2b: GDT-mechanisms such as off-the-shelf security systems and hard to learn security awareness programs still prevail in most organisations, thus unnecessarily limiting the level of computer and information security.*

2.4 Social bond theory

The social bond theory (Hirschi, 1969) assumes that when social bonds are weak or totally absent, thus giving a deviant the freedom to be criminal, that deviant will commit a crime. The theory assumes all people have a natural tendency towards committing crimes if there are no "social bonds", i.e. strong control mechanisms, present. This means the probability that people will commit a crime will be greater when social bonds are low. To validate this theory empirically, the effect of social bonds on the following four factors was measured: attachment, commitment, involvement and belief.

The results of this study indicated that social bond factors have a positive influence on the reduction of deviant (criminal) behaviour. Criminal acts can be prevented when

people believe that engaging in some sort of criminal behaviour will hamper their chances of success and weaken their self-image (Tesser, 1988).

Agnew (1995) describes the noteworthy effect of involvement in deterring criminal behaviour. He notes that the more people are busy with conventional activities with conventional people, the lower the chance they engage in criminal acts. He also suggested that when people have a positive perception of some kind of deviant (criminal) behaviour, they might engage in that behaviour despite a high risk of retribution.

Finally, the effect of belief on criminal behaviour is described by Le Blanc and Kaspy (1998):

> *"The delinquent may be influenced more by a sense of fairness than by the likelihood of being caught and the costs and immediacy of formal punishment."*

2.5 Social learning theory

The social learning theory (Akers, 1985; 1997) assumes that a person commits a crime because he has been associating with peers exhibiting criminal behaviour. These peers convey delinquent values, reinforce criminal behaviour and they serve as delinquent role models. In his latest work, Akers (1997) characterizes the social learning theory as follows:

> *"The probability that people will engage in criminal and deviant behaviour is increased and the probability of their conforming to the norm is decreased when they differentially associate with others who commit criminal behaviour and espouse definitions favourable to it, are relatively more exposed in-person or symbolically to salient criminal/deviant models, define it as desirable or justified in a situation discriminative for the behaviour, and have received in the past and anticipate in the current or future situation relatively greater reward than punishment for the behaviour. "*

For the purpose of testing the social learning theory on an empirical basis, four main constructs were proposed by researchers (Lee & Lee, 2002):

- *Differential association*. This is the process whereby one is exposed to normative definitions favourable or unfavourable to criminal behaviour.
- *Differential reinforcement/punishment*. This refers to the balance of anticipated or actual rewards and punishments that follow or are consequences of certain behaviour.
- *Definitions*. These are orientations, rationalizations, definitions of the situation, and other evaluative and moral attitudes that define the commission of an act as right or wrong, good or bad, desirable or undesirable, justified or unjustified.

- ∇ *Imitation (e.g. Akers, 1997)*. This refers to the engagement in behaviour after the observation of similar behaviour by others (e.g. peers).

Previous studies based on these measures found that highly positive relations exist between the sort of peers (e.g. colleagues) one has and criminal behaviour (e.g. Akers et al., 1979). Furthermore, association with delinquents increases the motive toward crime, which in turn increases the likelihood of delinquency (Tittle et al., 1986). In another study, Agnew (1995) discovered that:

> *"Friends' delinquency is a very strong predictor of the individual's delinquency, and this relationship may account for the continued appeal of differential association and other learning theories of delinquency."*

Other studies clearly demonstrated a modest to strong relationship between association with deviant peers and deviant behaviour and revealed that the four main constructs of social learning theory (differential association, differential reinforcement, definitions, and imitation) all notably influence computer delinquency (Skinner & Fream, 1997; Krohn et al., 1985). This can of course also work the other way around. Employees see how their colleagues' behaviour is rewarded and thus tend to behave in the same way so that they could be rewarded equally (Thomson & Von Solms, 1998). This way a culture of information security would be fostered within the organisation.

2.6 A holistic model of computer abuse

Holism puts the emphasis on totality, connection and the cooperation of the various parts and processes. The holistic model of computer abuse, as described in Lee and Lee (2002), is based on the combination of several behavioural theories, namely the General Deterrence Theory (GDT), social bond theory (SBT), social learning theory (SLT) and the Theory of Planned Behaviour (TPB). Since the TPB has not been previously described in this thesis, a short explanation is given here.

The Theory of Planned Behaviour model has been broadly and successfully applied to give an explanation for the causal relation underlying different human behaviours (Ajzen, 1985; 1991). The TPB model's key assumption is that behavioural intent is a key factor in predicting someone's behaviour. Intentions are shaped by the attitude towards the behaviour, subjective norms (social factors), and perceived behavioural control[1] (control factors).

[1] "The attitude towards the behaviour is the degree to which the person has a favourable or unfavourable evaluation of the behaviour in question. The subjective norm is the social pressure to perform or not to perform the behaviour. The perceived behavioural control (PBC) is the perceived ease or difficulty of performing the behaviour" (Beck & Ajzen, 1991, p. 286).

In practice, the TPB model has been used with success in predicting different types of abusive behaviour (see e.g. Banerjee *et al.*, 1998; Beck & Azjen, 1991).

Lee and Lee (2002) propose that factors from the GDT, SBT and SLT can affect the intentions from the TPB (see Appendix A.2). This general proposition is based on three "sub-propositions". The first one suggests that social bond factors (e.g. attachment and commitment) negatively affect the attitude towards abusive/criminal behaviour. For example, someone who defines spamming with a corporate email address as wrong behaviour is likely to refrain him- or herself from actually doing so. Secondly, they propose that social learning factors (e.g. definitions and imitation) have a positive effect on the subjective norm for abusive/criminal behaviour. For example, if someone spends a lot of time with peers that display criminal behaviour, that person might come to view that behaviour as acceptable and may finally imitate that behaviour. Finally, they suggest that general deterrence factors (e.g. security policies and security awareness programs) have a negative impact on the perceived behavioural control. For example, if criminal behaviour is more severely punished, if organizations invest more in security systems adapted to their current IT infrastructure (and maintain them) and security awareness programs get more effective, people will notice that the resources and capabilities needed to commit criminal behaviour are becoming scarcer. This will ultimately discourage actual criminal behaviour.

2.7 Two-factor taxonomy of end user security behaviour

As early as one and a half decades ago attempts were made to categorize threats to information systems security (see e.g. Loch et al., 1992). Now, Stanton *et al*. (2005) have undertaken efforts to catalog, characterize, organize and analyze a range of end user security behaviours in organizations. They developed a six-element taxonomy of security behaviour that varies along two dimensions, namely intentionality and technical expertise. Intentionality is used to categorize behaviour as intentionally malicious, intentionally beneficial, or somewhere in between those two. The six categories of security-related behaviour are described below (Stanton *et al.*, 2005).

- *Aware assurance* - high technical expertise, beneficial intentions. This behaviour requires technical expertise together with a strong intent to do the right thing by preserving and protecting the organization's information technology and resources. Example: a user recognizes the presence of a key logging program during periodical inspection of the processes currently running on his PC.
- *Basic hygiene* - low technical expertise, beneficial intentions. The behaviour requires no technical expertise, but there is a clear intention to preserve and protect the organization's IT and resources. Example: an employee fences off a social

engineering attempt by not disclosing his authorization codes to a caller claiming to be a member of the help desk.

- *Dangerous tinkering* - high technical expertise, neutral intentions. This behaviour calls for technical expertise, but there is no clear intention to harm the organization's IT and resources. Example: an employee sets up a wireless gateway that he uses for his laptop and inadvertently allows wireless access to the company's network for everyone within the range of the gateway.
- *Naïve mistakes* - low technical expertise, neutral intentions. This behaviour requires negligible technical expertise and no clear intent to do harm to the organization's information technology and resources. Example: a user forgets to log himself out of his workstation at the end of the day, letting a door open for e.g. the cleaners.
- *Intentional destruction* - high technical expertise, malicious intentions. The behaviour requires technical expertise together with a strong intention to do harm to the organization's IT and resources. Example: an employee codes a malicious program that corrupts thousands of data files.
- *Detrimental misuse* - low technical expertise, malicious intentions. Behaviour calls for minimal technical expertise but nonetheless includes intention to do harm through e.g. annoyance, harassment and rule breaking. Example: an employee uses company email for spamming thousands of messages marketing his sideline business of cheap mortgaging.

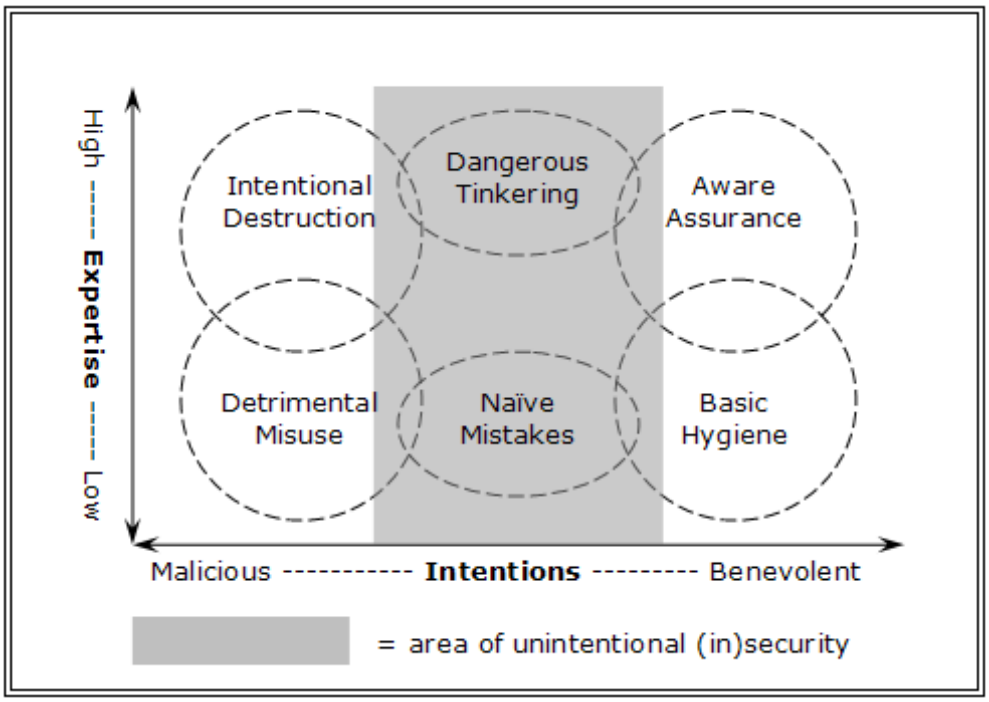


Figure 2.4 Two-factor taxonomy of end user security behaviour (Stanton et al., 2005)

The dark grey area depicted in Figure 2.4 is the area of so-called unintentional (in)security, which suggests that people sometimes act without explicit intentions. They might want to help or harm information security behaviour, even though the outcome of their behaviour may suggest otherwise.
Stanton *et al*. (2005) suggest that one practical strategy for improving security performance in organizations might lie in shifting the enactment of behaviours in the naive mistakes category toward the enactment of basic security hygiene behaviours. Only a relatively small increase in security expertise or awareness would be needed, resulting in a substantial boost in benevolent intentions or motivations. An example would be when employees no longer open emails from unknown recipients, but instead directly report them.

> *Hypothesis 2c: Companies make sure that their employees have some basic expertise concerning computer and information security, meaning e.g. they don't open potentially malicious e-mails but instead report them.*

2.8 Summary

In this chapter some theories and models concerning (security) behaviour have been discussed. After reviewing these theories and models, it becomes very clear that there are countless factors that directly, or indirectly, influence the way people behave in general and with regard to security. As described in this chapter, people's behaviour depends on such factors as (among others) making implicit, intuitive trade-offs for a decision, imitating someone you've come to associate with, and the presence, or absence, of certain social bonds.

3. Modelling the insider threat

3.1 Introduction

In this chapter three different models will be analyzed. Generally, they all have the purpose of modelling the threat posed by insiders. Applying these models in practice is supposed to help prevent insider attacks by detecting them early on. First, Parker's SKRAM-model, and a variation on it, will be analyzed. Next, Wood's model for insider threat prediction is discussed. Finally, Schultz's insider detection framework, which is a twist on previous research (such as Parker, 1998; and Wood, 2000), will be reviewed.

3.2 Parker's SKRAM-model

3.2.1 The basic SKRAM model

Parker (1998) developed the S.K.R.A.M. model to assess potential threats posed by computer criminals. "Overall, the greatest potential threats to our information systems comes from those individuals or groups… that posses the skills, knowledge, resources, authority, and motivation to abuse or misuse information" (Parker, 1998, p. 16).

Parker says that the SKRAM model is a summation of a suspect's alleged skill, knowledge, resources, authority, and motivation (Parker, 1998, p. 136-138). The individual components of Parker's model are (as stated in Frank, 2003):

- *Skills*. The first component of the SKRAM model, skills relates to a suspect's proficiency with computers and technology. To determine the level of a suspect's proficiency and skills, an investigator can start by examining that suspect's work experience. Typically, those who are proficient with computers commit computer crimes. Technical training in networking, hardware, software packages, operating systems, security systems, software development, data basing, and systems administration are all key areas that should be examined by an investigator.
- *Knowledge*. At first glance knowledge seems to closely resemble skills. Unlike skills, however, knowledge is a more general measure of specific data acquired by a suspect that is critical for accomplishing the computer crime attack in question. Knowledge includes a suspect's ability to plan and predict the actions his or her victims, his or her target's computing infrastructure, and a firm knowledge of what they are after. Investigators should try to identify who has the infrastructure specific knowledge to carry out the computer crime being investigated.
- *Resources*. A skilled and knowledgeable suspect might not be able to commit a crime if they do not posses the required resources. Resources include both the physical components as well as the contacts a suspect has at their disposal. When examining a suspect's resources, investigators should not overlook a suspect's business partners, club members, and network of friends if they can be identified.

- *Authority*. Authority is a measure of a suspect's access and control over information required to commit a crime. A suspect might be the primary administrator over vital information such as password files and therefore have an easy time committing a crime using that information. Investigators must determine a suspect's relationship to the data needed to accomplish a computer crime.
- *Motive*. All the technical skills in the world might not be enough to indicate that a particular suspect committed a computer crime. Independent of technical skill and knowledge, motivation is perhaps the most important overall criteria to evaluate. Possible motives could include emotional, social, political, or economic gains. Highly motivated criminals might be able to convince other more technically adept criminals to help them carry out a crime. It has been suggested that investigators look for abnormalities including: "Excessive absenteeism or unwarranted overtime, persistent late arrival for work, sudden low-quality and low-production output, complaints, [and] putting off vacation" (Duyn, p. 102).

By understanding the skills, knowledge, resources, authority, and motivation of a suspect, we are provided with a framework for profiling his or her ability to commit a computer or computer-related crime. Parker's research provides a baseline for understanding what type of person is potentially dangerous based on identifying their motive, opportunity, and means. In Parker's view, there only is an insider threat if the potential perpetrator has enough content of each of the five characteristics.

3.2.2 Frank's SKRAM risk assessment model

Frank (2003) has made a practical risk assessment model based on SKRAM. The SKRAM based risk assessment model has a base of 16 separate point categories. A suspect can acquire more than 16 points by having multiple motivations or being technically skilled in more than one relevant area. A low overall SKRAM assessment would fall between within the range of 0 to 5 points. A medium-risk suspect would have a risk assessment value somewhere between the ranges of 6 to 11 points. A high-risk individual would have a risk assessment value somewhere between the ranges of 12 or more points.

The basic SKRAM criteria are expanded into 16 specific risk assessment criteria.

- Criteria 1 through 3. The first three criteria directly measure a suspect's demonstrated skill set of the technologies used to accomplish the computer crime being investigated.
- Criteria 4 through 6. These criteria deal with the suspect's knowledge of the infrastructure compromised or used during the attack.

Nr.	SKRAM-Based Risk Assessment Criteria	Points Awarded
1	Suspect uses the skill(s) needed for the attack	1 point per skill used
2	Suspect demonstrates advanced knowledge of the skill(s) needed for the attack	1 point per expertise
3	Suspect has formal education in the technologies or methods used in the attack	1 point per technology
4	Suspect has knowledge of the affected system infrastructure(s)	1 point if yes
5	Suspect works with the affected system(s) regularly	1 point if yes
6	Suspect is familiar with the operating system/environment of affected system(s)	1 point if yes
7	Suspect has direct access to the affected system(s)	1 point if yes
8	Suspect has direct access to programs needed for the attack	1 point per program match
9	Suspect has managerial role over those who could perform attack	1 point if yes
10	Suspect knows/has the permissions/security access needed to perform attack	1 point if yes
11	Suspect has knowledge of the affected system(s) networking environment	1 point if yes
12	Suspect has identifiable monetary benefit(s) from attack	1 point per match
13	Suspect has identifiable grievance(s) with the owner(s) of the targeted system(s)	1 point per match
14	Suspect shows no concern/grievance with loss incurred from attack	1 point if yes
15	Suspect has plans for leaving the company/institution of the targeted system(s)	1 point if yes
16	Suspect has had previous behavioural problems/policy violations	1 point if yes
	Total Points	

Table 3.1 The SKRAM based risk assessment model (Frank, 2003)

- Criteria 7 through 11. The following four criteria assess the suspect's authority and access to the systems and information involved in the crime.
- Criteria 12 through 16. The final five criteria identify the suspect's potential motives to commit the computer crime.

To avoid a dilemma of randomly assigning values that could skew the results of a suspect's SKRAM level, points were assigned on a 1 or 0 basis according to behavioural evidence deduced from the analysis of the case study records. Only the criteria that match both the method of the crime and the suspect's skill set were evaluated. Collectively, these criteria form an investigative baseline for evaluating a suspect's potential for committing a given computer crime (Frank, 2003).

3.3 Wood's insider threat model for adversary simulation

Wood's model (2000) is an extension of previous work (Schudel & Wood, 2000). Like many others (e.g. Parker, 1998; Schultz, 2002), Wood proposes that an insider can be described from a variety of characteristics. His characteristics, which partly overlap those in Parker's model (as noted by Spee, 2004), include: access, knowledge, privileges, skills, risk, tactics, motivation, and process, and their respective details are summarized

below. For the purpose of his model, Wood (2000) defines a system as "the overall network within the scope of some relevant management domain". He defines a target as "the portion of a system that is subject to attack by the malicious insider".

- *Access*. The insider has unrestricted access to some part of the system. Some assertions can be made that are assumed to be true. For instance, the insider attacks the target from behind or inside a system's perimeter defences. Or, the insider can breach a system's perimeter defences without arousing the suspicion of network security managers.
- *Knowledge*. The insider has extensive knowledge of both the system and the target. Specifically, the insider has unfettered access to all documentation on the target and the system, among other things. Also, he or she can collect intelligence and perform discovery without arousing suspicion. Sometimes the insider is the only one entrusted with accurate, detailed information on the target.
- *Privileges*. The insider should have no problem getting the privileges needed to set up an attack. In particular, the adversary may not need root or administrator access to mount an attack, or he or she may already have privileged access to the target. It can also happen that an insider simply recruits someone who has the privileges needed to mount an attack. The adversary may in fact be the one responsible for monitoring or enforcing the security policy on the target or system.
- *Skills*. The informed insider has the skills to mount a credible attack, which is subject to some limitations. For example, the insider may in fact be the local domain expert on certain parts of the system. Also, a given malicious insider is not likely to attack an unfamiliar target. This hypothesis is based on the principle that the adversary will prefer to attack a target familiar to him or her, rather than gain expertise with an unfamiliar target.
- *Risk*. The insider is generally very risk-averse. Their ultimate defeat is to be discovered before they have set up a successful attack. This leads to some assumptions, such as that the insider generally works alone, that the adversary may recruit (trusted) colleagues on an operation (but only to the extent necessary) and that the insider may be able to co-op a colleague into enabling an attack without that person's knowledge.
- *Tactics*. The tactics used by an adversary are completely dependent on the goal(s) of the attack. Two possible tactics are:
  - *Plant, run, & hit*. In this scenario the adversary e.g. attempts to plant some malicious code, leave the premises, and be out of reach of any authority when the attack itself is launched.

- *Espionage*. In this case, the value of the adversary is measured in their ability to exfiltrate information from an enterprise. The only reason for an insider to cease espionage would be if they were discovered.

- *Motivation*. Wood (2000) expects that the typical insider is trying to force some sort of detrimental effect within an enterprise. The goals he or she aims to achieve with this can be profit (being paid to e.g. disrupt systems), to provoke change (e.g. policy change or blackmail), subversion (undermine target organization's mission) and personal motive (e.g. showing off expertise, or taking revenge).
- *Process*. An insider attack follows a basic, predictable process. The process generally goes as follows. Somebody becomes somehow motivated to mount an inside attack. Then the insider identifies the target. Following the identification, the insider plans the operation of the attack. Finally, the insider launches his or her attack. After the actual attack has taken place, an insider has various options, which include: damage assessment, flee in a hurry, flee when convenient, or repeat the operation until either successful or caught.

Several observations can be made based on the abovementioned insider characteristics, which lead to some questions.

First, who would mount an insider attack? According to Wood (2000), it is either someone with a character defect, an operative from a competitive organization, or a combination of both. A well-informed insider probably knows how to set up an attack within a particular system without getting caught, or he or she might believe this is true. Actually, the malicious insider may in fact control the mechanisms that are supposed to thwart his attack.

Secondly, are cyber means the best way to prevent insider attacks? Wood (2000) proposes that vulnerability analysis should identify potential targets in a given system. Furthermore, people with access to targets should be monitored. Also, it may be feasible to counter this threat using traditional counterintelligence methods. Finally, personnel reliability methods might identify malicious insiders.

Last but not least, what are the manifestations of an insider attack? It is not clear that a typical cyber defender could identify insider activity even it was known to exist (Wood, 2000). The insider detection framework by Schultz (2002) could prove helpful in successfully identifying (malicious) insider activity.

3.4 Schultz's insider detection framework

Einwechter (2002) has proposed that a combination of IDS systems (network intrusion detection systems (NIDS), network node intrusion detection systems (NNIDS), host-based intrusion detection systems (HIDS), anomaly-based intrusion detection systems, and a distributed intrusion detection system (DIDS)) should be used to detect insider attacks. His proposition is a great step forward, since collecting and analyzing data that are likely to yield multiple indicators are in fact the only feasible direction given the subtlety of insider attack patterns and their difference from conventional (external) attacks.

But, according to Schultz (2002), Einwechter has overlooked several important concerns. First, since insiders have legitimate access to certain computer systems, they're able to interfere with IDSs much easier than outsiders. Secondly, many insider attacks are substantially different from externally initiated attacks and IDSs are mostly geared towards detecting externally initiated attacks. So relying on IDSs to detect insider attacks is unwise.

Previous studies and models propose an approach for predicting and detecting insider attacks. They point out that to conclusively indicate an insider attack, many different potential indicators should be taken into account, for no single indicator can generally provide such a conclusive indication (e.g. Tuglular & Spafford, 1997; Suler, 1998; Shaw *et al.*, 1998; Gudaitis, 1999).

These potential indicators include (as stated by Schultz, 2002; see Figure 3.1):

- *Deliberate markers*. Previous studies (e.g. Suler, 1998) indicate that attackers sometimes leave deliberate markers to make a "statement." Markers can vary in size and obviousness. Finding the smaller, less obvious markers earlier—before the "big attack" occurs—should be a major goal of those faced with the task of detecting insider attacks.
- *Meaningful errors*. This category of indicators comes from actual investigations of insider incidents. Attackers usually make mistakes in the preparation leading to, and while carrying out, an attack. They might, for example, forget to erase the error logs they have generated due to badly typed commands.
- *Preparatory behaviour*. Wood (2000) mentions behaviours that occur in preparation of an attack. For instance, the attacker may attempt to gain as much information about the potential victim system as possible. In so doing, an attacker can expose intentions. Use of commands such as ping, nslookup, finger, whois, rwho, and others is just one example of preparatory behaviour.
- *Correlated usage patterns*. Correlated usage patterns are patterns of computer usage that are consistent from one system to another. These patterns might not be noticeable on any one system, but the fact that they occur on multiple systems can

reveal intention on the part of a potential perpetrator. A perpetrator may, for example, search for files with particular words in them on dozens of systems.

- *Verbal behaviour*. Several studies (e.g. Morahan-Martin, 1998; Collins, 1992) showed how in the technical arena verbal behaviour is linked to aggression, dominance and other factors. So it's obvious that verbal behaviour (either spoken or written) can also provide an indication of an impending attack. A well-known example is email messages in which a possible perpetrator displays hatred and/or hostility towards someone else, usually an employer. Particularly recording and analyzing requests for e.g. higher privileges seems really promising.
- *Personality traits*. A study by Shaw *et al.* (1998) suggests that personality factors (particularly introversion) can be used in predicting insider attacks. Although potentially very valuable, the measurement and use of personality traits in predicting insider attacks is overwhelmed with many problems, e.g. ethical problems. Nevertheless, personality traits promise to be a useful indicator for insider attacks.

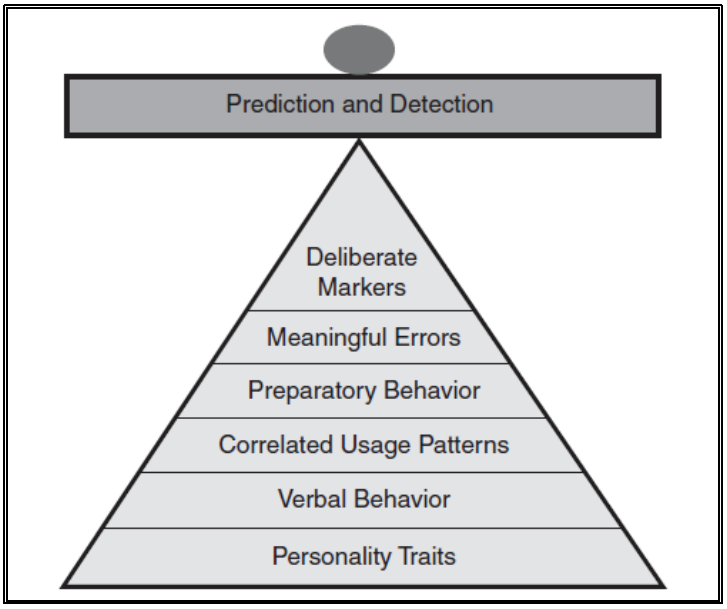


Figure 3.1 Potential indicators of insider attacks, a heterogeneous model (Schultz, 2002)

Schultz (2002) puts these potential indicators of an insider attack in a mathematical equation. He assumes that it is very likely that each of the potential indicators can be quantified. The mathematical equation is similar to a multiple regression equation that consists of a number of variables, with weights for each variable. An example equation would be along the lines of:

$$Y = a_0 + a_1x_1 + a_2x_2 + \ldots + a_nx_n = \sum_{i=0}^{n} a_ix_i$$

In this equation, Y is the predictive value. The larger its absolute value, the greater the chances of an attack. x_1, x_2, etc. are the indicators and a_1, a_2, etc. are their weighting in the regression equation, with a_0 being the constant. Real values can be determined by carefully scrutinizing a large number of insider attacks that have taken place for the presence of potential indicators (deliberate markers, meaningful errors, preparatory behaviour and so on). Other feasible (mathematical) techniques are e.g. least squares calculation.

> *Hypothesis 3a: Organisations do not use special models to model/map the threat posed by insiders, like Wood's insider threat model.*

3.5 Summary

In this chapter three different models were analyzed, which all have the purpose of modelling the insider threat. Applying these models, or some techniques similar to them, in practice can help to deter insider attacks by detecting a threat early on. In this context, the models by Parker and Wood show various similarities, and their approach is more or less the same. We have seen that Schultz's model tries to incorporate several theories and models, among which are Parker's and Wood's models, into a practice-based insider detection framework. His framework puts potential indicators of an insider attack in a weighted mathematical (regression) equation, where the weights can be based on real values by examining the characteristics of large quantities of past insider security incidents.

4. Preventing insider attacks

4.1 Introduction

In this chapter two different methods that can be used in deterring insider threats will be discussed. First, we will look at the effect of a code of ethics, consisting of personal, formal and informal codes, on the (ethical) decision making process. Secondly, a very interesting method for deterring insider attacks is examined. This technique tries to enhance security awareness by changing one of the foundations of an organization: it's culture. Since this method 'fights' the problems at the root, i.e. organizational culture, it seems crucial in the struggle against improper security behaviour.

4.2 Computer ethics

Computer ethics refers to a set of rules or principles used for moral decision making regarding computer technology and computer use (Pierce and Henry, 1996). There are more than a few reasons computer ethics is an important topic. First, it is general knowledge that technology users face ethical problems in the workplace on a daily basis. Secondly, computer abuse is continuing to be a widespread phenomenon (FBI/CSI, 2004). Additionally, although some corporate codes of ethics mention computer technology, most do not provide a structured framework needed to guide employees.

Corporate codes of ethics are "any written corporate statement of ethics, law, or policy that define standards, either by direct articulation or by articulating values or norms, for the work group's behaviour" (Stevens, 1994). They typically consist of a combination of directive statements for certain kinds of conduct, as well as general statements of corporate commitments to constituencies or a management philosophy (Berenbeim, 1992). Many managers believe corporate codes can help deter improper actions of employees. Moreover, codes specific to the use of information systems are able to provide even more explicit guidance to information systems employees (Forcht, 1994). This guidance is important for information systems employees, who can commit larger scale crimes than non- information systems employees, because of their extensive computer knowledge.

Therefore, the issues of developing codes, communicating the codes to employees, and selecting employees who demonstrate appropriate ethical behaviour are crucial issues for organizational success. Ethical decisions related to computer technology and computer use are subject to three primary influences (Pierce & Henry, 1996):

- the individual's own personal code
- any informal code of ethical behaviour that exists in the work place
- exposure to formal codes of ethics

In their study, Pierce and Henry (1996) found that there is a difference in the code (personal, informal, formal) that people say is important and the code they say they will really use in ethical decision making related to computers or computer technology. In this study, personal code was chosen as both "most important" and "used" by the majority of those surveyed, informal codes were indicated next most frequently in both cases, and the formal code was chosen least frequently. However, the percentages in the categories differed dramatically with 80% indicating personal code as the one they used while 49% indicated that the personal code was the most important ethical code. This may be due to the fact that self-report responses are sometimes biased by what a person feels is an acceptable answer. This bias is less a problem when an impersonal question (which code is most important) is asked rather than a more personal one (what code do you use). For this reason, the percentage responses regarding the importance of the personal, informal, and formal codes in guiding behaviour in making ethical decisions are used in the relationships proposed in Figure 4.1.

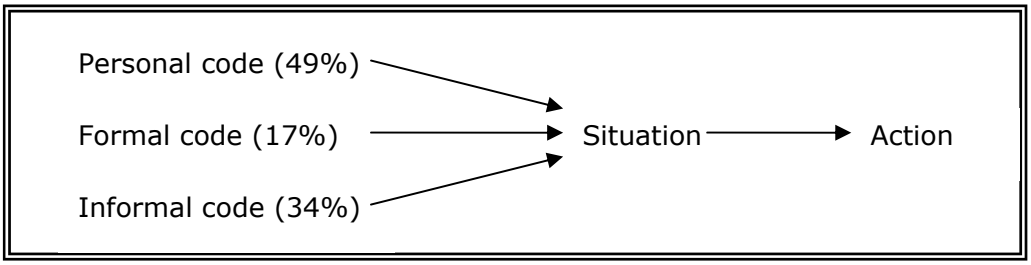


Figure 4.1 - The influence of personal, informal, and formal codes of ethics on decision making

The results of the study show that a formal company code of computer ethics has an impact on decision making. Therefore, it is vital to have and to communicate to all members of the organization a formal code of computer ethics. The involvement of computer experts in the construction of a formal computer ethics code is particularly important since this is a technological and continuously changing field. Additionally, computer ethics codes should contain a distinguishable philosophic direction, be substantial enough in detail to be used as a framework to guide ethical conduct, and contain specific topics of concern.

The informal code is also important since it is subject to change and guides many employees' daily activities. Two important considerations related to this code are communication and content. The informal code of computer ethics should be unambiguous communicated to all employees in the organization (e.g. by using a combination of mentoring by peers and explicit direction by supervisors). The content of the informal code must be constantly monitored to make sure it is directed by the formal code and does not fall victim to improper changing social norms. The individual's

perception of acceptable behaviour must constantly be evaluated and re-evaluated to insure appropriate computer related behaviour.
The personal code of ethics of employees is not easily influenced. In the model by Pierce and Henry (1996), ethics study, professional codes, and law are shown as impacting the personal code. Although its is hard to address the personal codes of ethics of employees, an organization may be able to indirectly influence personal codes through e.g. training on new computer law provisions impacting employees' jobs. Furthermore, high personal ethical standards may become an explicit condition in the recruiting process.
Finally, decisions related to proper behaviour should be made based upon clearly established guidelines which are embedded in the personal, informal, and formal codes of ethics, all supporting the same action decision.

Codes of computer ethics, be it formal, informal or personal, are seemingly beneficial to the security behaviour within an organization. Employees abiding by these codes of ethics will undoubtedly display a reduced tendency towards criminal behaviour, and thus also towards committing an insider attack. However, people who have a perseverant criminal attitude will probably not abide by the codes of ethics, as their personal codes of ethics are most likely distorted. So codes of ethics will fall short on substantially deterring abusive behaviour concerning computers and computer systems. It nonetheless plays it's part in making employees more aware of what they're doing, on the level of e.g. security policies and security awareness training, and is therefore a vital part of an organization's complete set of security mechanisms.

> *Hypothesis 4a: Most companies have some form of formal code of computer ethics in place.*

4.3 From policies to culture

This paragraph is based on two papers, which focus on an uncommon approach to combating the issue of unacceptable security behaviour. The first is by Vroom and Von Solms (2004), the second is by Von Solms and Von Solms (2004). They propose that organizations should not just enforce security policies, but should undergo a cultural change, turning the organizational culture into one with a strong focus on security awareness. This solution to the problem of improper security behaviour is thus not a mechanism as for example codes of ethics, instead it entails a company-wide (security focussed) cultural shift. Doing this, it becomes possible to audit employees behaviour, not just the results of it, which is important for deterring a (possible) insider threat.

4.3.1 Limitations of security auditing

An organization's information security policies deal with processes and procedures that the employee should adhere to in order to protect the CIA[2] of information and other valuable assets (BS 7799, British Standards Institution, 1999). They are one of the most important security controls for an organization (Höne & Eloff, 2002; Karyda *et al*., 2005): they contain the security goals of the organization and are basically the guidelines that state the rules and regulations of the organization, which in turn govern the security of information and its related information systems (Halliday & Von Solms, 1997). IS security auditors use these security policies to perform their audit. The security policies need to be assessed to ensure that they are in line with the objectives, goals and vision of the organization, and with best practice standards (Vroom & Von Solms, 2004).

One major problem with security auditing is that only the results of employee behaviour is taken into consideration, not the behaviour itself (Vroom & Von Solms, 2004). So, the results of an employee's behaviour and actions can be detected and audited, but not the behaviour itself. This shows that auditing confirms only the consequences of behaviour, not actual behaviour. Employees (and thus their behaviour) have an enormous influence on the business with regard to information security and it is important to know the role that they play in securing information.

Employees are vital to the success of any organization, but unfortunately they're also the weakest link when it concerns information security. Security incidents regarding insiders of the organization rival the amount of security breaches with outsiders, which demonstrates the fact that employees are a big threat to the company (Information Security Industry Survey, 2001; FBI/CSI, 2004). According to the 2001 Information Security Industry Survey, of all the insider security breaches, 48% of them were accidental, 17% was intentionally committed, and of the other 35%, it was unsure whether it was malevolent or not. This demonstrates that a lot of security breaches may be the result of negligence or ignorance of the organization's security policies.

It is very important that employees behave and act responsibly in order to adhere to the security policies of the organization. To achieve this, some form of evaluation is required to examine the performance of security behaviour at an individual level. However, auditing of employees' behaviour with regard to information security doesn't seem to occur in practice. Therefore a method needs to be found to ensure that employees' behaviour is conform company policies. Through the auditing of individuals, attempts could be made to stop the occurrences of security incidents from within the organization. The major problems associated with auditing individuals can be summarized in two words, reliability and validity (Szilagyi and Wallace, 1990). Together they describe both

[2] The commonly used abbreviation CIA stands for Confidentiality, Integrity and Availability. This term is widely used in all kinds of literature on security of information (systems).

the adequacy of the information gathered as well as the quality of the whole evaluation process. If the assessment and the ensuing information is not reliable and valid, then the resulting basis for decision-making would prove to be useless. The problem is that there are many factors that can negatively influence the reliability and validity of the assessment and its results. Furthermore, a number of practical obstacles come into play when attempting to investigate employee behaviour, e.g. large amounts of resources and manpower would be needed for a thorough assessment (Vroom & Von Solms, 2004).

4.3.2 Organizational culture and behaviour

Organizational culture is defined here as:

> *''the pattern of basic assumptions that a given group has invented, discovered, or developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and, therefore to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.'' (Schein, 1999)*

Organizational culture is the single most important factor accounting for success or failure in an organization (Deal & Kennedy, 1982). Schein (1999) has developed a model dividing culture into three main layers (see Figure 4.2). The first level contains the artifacts in the organization, which are clearly visible and easily noticed by outsiders. In the context of information security, a locked door is an example of an artifact. The second level is the espoused values, norms and knowledge of the organization, which are visible to a lesser extent. An information security related example of these espoused values is the information security strategy stated, resulting in artifacts in the form of information security policies. The third, and deepest, level are the basic assumptions and beliefs, which are unseen and mostly unconscious and occur at the individual level. These assumptions and beliefs are the underlying values and beliefs of the people in the organization. Schein (1999) describes them as follows: "they were normally the original thoughts and beliefs of the founders that have unconsciously been communicated to the employees and form the core of the organization."

> *Hypothesis 4b: Organisations recognize the importance of organizational culture as a key factor in their computer and information security.*

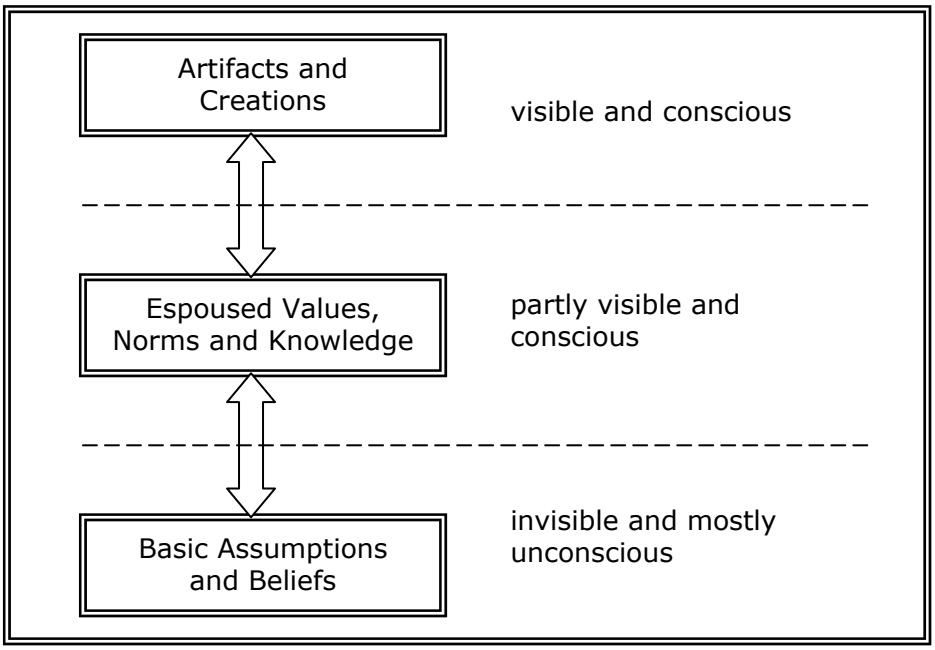


Figure 4.2 – Schein's model of organizational culture (Schein, 1999)

Each of the three levels influences the levels surrounding them, so that changes cascade through all three levels. Applying this to information security, it follows that shared knowledge of the information security policies and an underlying belief in the importance of information security would result in a change in behaviour of individuals and eventually in the organization as a whole (Vroom & Von Solms, 2004).
Organizational culture can have a huge impact on the information security, both negative and positive. It is of utmost importance that the culture reflects a positive attitude towards information security throughout the entire organization. A utopian information security culture is attained when employees voluntarily follow the organization's guidelines as second nature.

Once an organization clearly understands it's culture, it can start to see how that culture can be transformed into a more secure one. By transforming the organization into one that is more aligned with information security, individual (i.e. employee) behaviour will adjust to integrate security awareness.
In order to attain this security awareness among employees (and throughout the organization), the organization has to be changed at the three levels where organizational behaviour occurs, namely the individual, the group and the formal organization (Szilagyi and Wallace, 1990; see Figure 4.3). The behaviour of the individual plays an important role in the development and progress of the organizational culture and factors that have an effect on this behaviour need to be beneficial to information se-

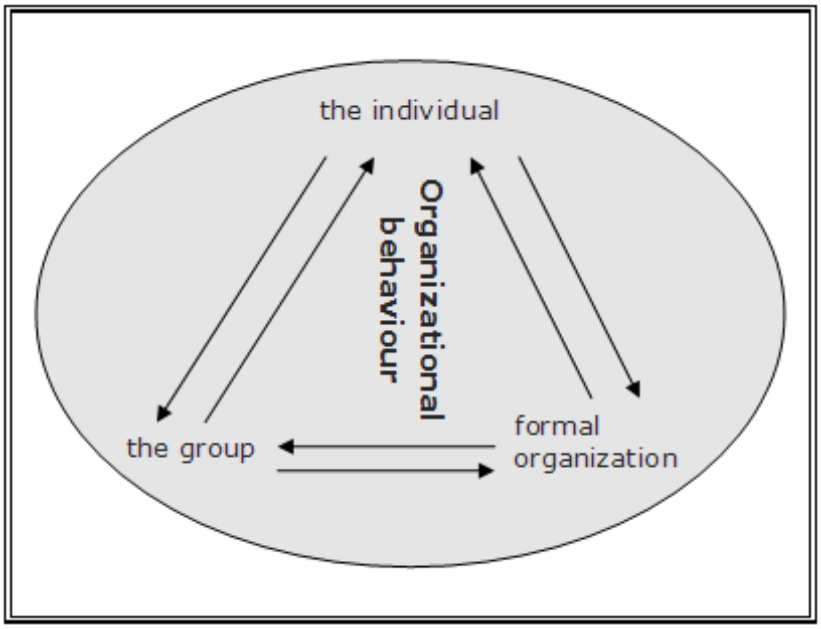


Figure 4.3 - The three levels of organizational behaviour

curity. The group (consisting of different individuals) values and norms play a vital role in the way groups of employees act and behave while performing their work. The formal organization can be compared according to characteristics common to both the individual and the group, for example the type of business they're in. The formal organization is influenced by it's environment and therefore influences its employees and internal operations (Szilagyi and Wallace, 1990). Each of these levels in organizational behaviour influences each other to shape the culture of the organization. A change in the culture of an organization requires change at all three levels. An example: the group becomes more security aware, which can benefit the organization as a whole, thus leading to a changed culture which incorporates information security in daily routine.

4.3.3 Changing the culture

Top management should clearly spell out their attitude regarding the importance of information (and information security) in an executive information security policy. In the end, top management would like all employees to share this attitude with them and ensure that appropriate information security controls are set up and adhered to. Therefore, supporting policies need to be defined, implemented and educated throughout the organization. It would be beneficial to an organization if it is able to integrate proper security behaviour into daily employee routine to such an extent that an information security culture is cultivated (Von Solms & Von Solms, 2004). In order to do so, the organization's current information security culture needs to be transformed into one that is more aligned with the organizational security policies and the vision of the management (Von Solms & Von Solms, 2004). The first thing that needs to be done

when changing culture, is to identify the areas that require change. To achieve this, it is necessary to analyze the different levels of both Schein's model and those of organizational behaviour, where Schein's model can be used to see how each level influences each other in the organization (see Figure 4.4). Categorizing the organization into different categories simplifies the process of changing the information security related problems.

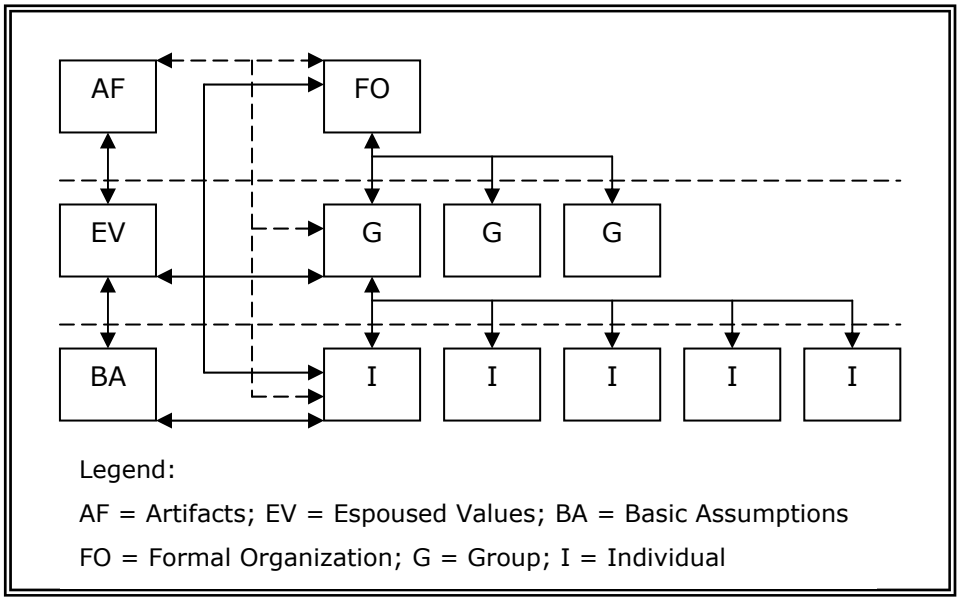


Figure 4.5 - Interaction between the organizational culture and behaviour

The following example (taken from Vroom & Von Solms, 2004) demonstrates how organizational (security) culture can be changed. To begin with, organizational behaviour is used to change the knowledge and shared values of the group. As soon as group behaviour starts to change, it influences both the individuals and, eventually, the formal organization. These changes are reflected by the artifacts of the organization (i.e. several visible aspects, like new security systems). By changing one aspect, it will gradually, but steadily, filter through the organization at the individual and formal levels, eventually resulting in a more secure culture.

Finally, auditing or monitoring employee behaviour seems virtually impossible, because of the sheer number of possible outcome-distorting factors, as well the logistical problems (i.e. the necessary manpower). As it turns out, auditing is not a favourable method to influence the employee's compliance with the organization's information security policies. The culture of the organization seems a good starting point for finding an alternative auditing method. Changing the culture of the organization into a more security aware one begins with the understanding of organizational behaviour and how employees are influenced, clearly spelling out the importance of the human factor. The

security policies need to be successfully communicated and educated to employees (see for example a study by Finch *et al*, 2003; Furnell *et al*. (2002) have developed a tool specifically for the purpose of security training and education), so they will affect organizational culture. Employees will learn how to respond to things like social engineering, i.e. unknown people requesting information, and they need to be aware of how easily they can be manipulated (Erlanger, 2004). Once the organizational culture has become (highly) security aware, individual behaviour auditing will not be necessary, as (almost all of) the behaviour will emanate from the security aware organizational culture. That is not to say that a cultural shift will prevent all security incidents (e.g. malicious actions stemming from such things as revenge will always exist), but it is likely that the majority of insider incidents, i.e. the unintentional security breaches, will be eradicated. Almost, for people will always be the weakest link.

> *Hypothesis 4c: Organisations are not willing (or able) to change their organizational culture to achieve a higher security awareness among their employees, but will opt for "regular" security awareness training instead.*

4.4 Summary

In this chapter we have seen two different methods that can be used in preventing insider attacks. A code of ethics, although having a positive effect on security enhancement, is just another security mechanism like, for example, security policies. The second method for deterring insider attacks that has been discussed, changing an organization's culture, turned out to be very promising. Since this technique is based on the human factor and attacking improper behaviour at its roots, it is something that all organizations coping with improper security behaviour by employees should apply. If, eventually, culture is aligned with company (security) policies, security awareness is enhanced and the odds of any insider security incidents will be greatly reduced. However, there are more factors that come into play when it comes to intentional malicious behaviour, e.g. personality traits and upbringing of the individual.

5. A small security survey

5.1 Introduction

In this chapter the results of a small survey on security are discussed. The survey was done in the financial services sector, which is comprised of banks, insurance companies, investment firms, etc. The questions of this survey are based on some hypotheses that were formulated based on the reviewed theories and models (see previous chapters and appendix A.3). These hypotheses were mapped to a framework, the insider security Capability Maturity Model (IS-CMM), which is loosely based on the People Capability Maturity Model (P-CMM 2.0; Curtis *et al*., 2001), to find out the current maturity level of organisations (that participated in the survey) concerning insider security.

5.2 A custom-tailored CMM

5.2.1 The People CMM

As noted in the preface of the P-CMM, "The People Capability Maturity Model (…) is a tool that helps you successfully address the critical people issues in your organization". Insider security is just such a critical people issue. The level of security awareness and knowledge among employees of an organization is a way to measure the level of insider security. The P-CMM is divided into five maturity levels, which are briefly explained further on. Moreover, the P-CMM states: "Each maturity level is a well-defined evolutionary plateau that institutionalizes new capabilities for developing the organization's workforce". So, as the employees develop their security competence and thus their security practices, they will reach a higher security maturity level, which is a good foundation for evolving their competence even further and reaching the next maturity level.

The five maturity levels of the P-CMM are:

- Level 1: Initial

  Characteristics of the initial level are:

  1. Inconsistency in performing practices;
  2. Displacement of responsibility;
  3. Ritualistic practices;
  4. An emotionally detached workforce.

  Constant agitation among employees reduces its capability. High turnover limits the level of skill available in the workforce, limiting an organization's ability to improve its performance.

∇ Level 2: Managed

The second level is characterized by the capability of units to meet commitments. This capability is achieved by ensuring that people have the skills needed to perform their assigned work and that performance is regularly discussed to identify actions that can improve it.

∇ Level 3: Defined

All employees begin sharing responsibility for developing increasing levels of capability in the organization's workforce competencies. The employees' practices implemented at maturity level 2 are now standardized and adapted to encourage and reward growth in the organization's workforce competencies.

∇ Level 4: Predictable

The combined availability of workforce competences baselines and process capability baselines for competency-based processes enables both unit and organizational performance to become more predictable. These data allow management to make more accurate predictions about future performance and better decisions about tradeoffs involving workforce capability or process performance issues.

∇ Level 5: Optimizing

The workforce capability of maturity level 5 organizations is continually improving. This improvement occurs through both incremental advances in existing employee practices and implementation of new and innovative practices that may have a great impact. The culture in an organization routinely working at the optimizing level is one in which everyone strives to improve their own capability and performance as well as that of the people around them and the organization as a whole. Employees' practices are perfected to support a culture of performance excellence.

(Adapted from Curtis *et al.*, 2001)

5.2.2 The Insider Security CMM

The People CMM provides a good basis to derive a custom capability maturity model. Here, a CMM for insider security will be described. It is not meant to be as comprehensive and richly detailed model like the standard CMM's (e.g. CMMI and P-CMM) which are covered in documents consisting of hundreds of pages. Instead, it will only be used to categorise the organisations that respond to the survey/questionnaire into different levels of insider security awareness. Security awareness and knowledge among employees is a capability (or competency) and thus the P-CMM is used for the custom insider security CMM's maturity levels, but merely as a guideline. The insider security CMM (IS-CMM) also consists of five maturity levels, which are linked to the hypotheses formulated in this thesis (see previous chapters and appendix A.3).

The five maturity levels of the IS-CMM are:

- Level 1: Unaware

  The organisation is oblivious of the potential threat that insiders pose to computer and information security, or just ignores the threat, and consequently no insider-specific measures are taken at all. Employees do not consider security an issue at all.

- Level 2: Aware but insecure

  Organisations that are at level 2 are aware of the potential threat of insider attacks, but still there are no special measures for insider security breaches compared to externally initiated breaches and usability is chosen over security in 9 out of 10 cases. Employees have little or no security knowledge and awareness.

- Level 3: Basic security

  When on level 3, employees have some basic security knowledge and awareness. Furthermore, employees don't just prioritise usability over security, but instead look at the costs and benefits of both options. Prior inside security offenders are regularly checked for their security awareness. Although organisations at level 3 use security measures, they are usually not specifically constructed for insider security issues or the company's specific infrastructure. Examples are general security policies and off-the-shelf security systems, but also hard to learn awareness programs.

- Level 4: Good security

  Organisations on level 4 use special models, or other techniques, to map the threat posed by insiders. Security has become a prime concern among employees. Organizational culture is seen as a key factor in the companies computer and information security. Security awareness programs are understandable and tie into employees' daily work. Other security measures are also tailored to the company's specific situation, instead of off-the-shelf products and general measures. The number of insider security breaches will be declining.

- Level 5: Optimally secure

  When insider security has reached this level, a high level of security awareness and knowledge will be part of the organisational culture. Organisations on this level will continually adapt the organisational culture to incorporate the highest level of security awareness. Employees choose security over usability (when the expected "pay-off" of both options is equal).

5.3 Hypotheses and survey questions

The hypotheses are used to formulate the survey questions, both of which are stated below, showing their linkage (the hypotheses and questions are also described in Appendices A.3 and A.4 respectively). The actual survey will be in Dutch and can be found in Appendix A.5. The answers to the questions are used to categorise the participating organisations in the IS-CMM. Since the survey questions are directly related to the hypotheses and thus the IS-CMM, the answers to these questions can be easily used to see what the current insider security maturity levels are by how the participants score. Additionally, it will become clear which hypotheses are falsified and which are not.

∇ - *Hypothesis 1a*: Companies, in practice, do not use different methods and/or measures to repel inside attacks when compared to external attacks.

- Does the organisation use different methods for detecting and preventing inside attacks compared to external attacks?

Yes No

∇ - *Hypothesis 1b*: Companies tend to ignore the overall threat of insider attacks to computer and information security.

- Is the organisation aware of the potential threat that employees pose to computer and information security?

Unaware 1 2 3 4 5 Highly aware

∇ - *Hypothesis 1c*: The occurrence of insider attacks is declining, but it remains an issue in computer and information security.

- On a yearly basis, does the number of internally initiated security breaches related to computer and information security in your organisation show a declining or rising tendency?

Declining Rising Unknown

∇ - *Hypothesis 2a*: In most cases, legitimate users (and companies themselves) will prioritise usability over security (i.e. with regard to systems, software, etc.).

- What has a higher priority when it comes to systems and software: usability or security?

Usability Security Evenly distributed Unknown

- Do employees (everyone from the secretary to the CEO) generally prioritise usability over security concerning their daily work? (An example is not locking a PC because of laziness)

Yes No Unknown

∇ - *Hypothesis 2b*: GDT-mechanisms such as off-the-shelf security systems and general security policies still prevail in most organisations, thus unnecessarily limiting the level of computer and information security.

- Are the security systems in the organisation (such as IDS) off-the-shelf or tailored to the organisation's specific needs?

Off-the-shelf Custom tailored

∇ - *Hypothesis 2c*: Companies make sure that their employees have some basic expertise concerning computer and information security, meaning e.g. they don't open potentially malicious e-mails but instead report them.

- What is generally the level of security expertise the employees that work with computer and information systems (such as PCs) have?

None

Basic – e.g. not opening potentially dangerous emails, frequently changing passwords

Moderate – e.g. reporting suspicious CPU activity on computer

High – highly security aware, think security first

∇ - *Hypothesis 3a*: Organisations do not use special models to model/map the threat posed by insiders, like Wood's insider threat model.

- Does the organisation use special models or methods to map the threat posed by specific employees, like for example prior offenders?

Yes No

- If yes, what kind of methods/models are used? ……

∇ - *Hypothesis 4a*: Most companies have some form of formal code of computer ethics in place.

- Does the organisation have guidelines for computer ethics and security behaviour of employees, stated in e.g. a security policy or formal code of (computer) ethics?

Yes No

- If yes, are all employees aware of these guidelines?

Yes No

∇ - *Hypothesis 4b*: Organisations recognize the importance of organizational culture as a key factor in their computer and information security.

- To what extent is the organisational culture seen as an important factor in companywide computer and information security?

Not important 1 2 3 4 5 Very important

∇ - *Hypothesis 4c*: Most organisations are not willing (or able) to change their organisational culture to achieve a higher security awareness among their employees, but will opt for "regular" security awareness training instead.

- Would your organisation consider changing the organisational culture to one that revolves around high security awareness among employees?

Yes No

- If no, explain your objections/problems: ……..

5.4 Survey results

5.4.1 General survey results for the financial services sector

The survey was conducted among organizations that are active in the financial services sector. Organizations in this sector include banks, insurance companies and investment firms, which consider (computer and information) security a top priority. Due to the sensitive nature of the information that was asked for in the survey, the number of participants to the survey was low, with a total of 4 surveys returned. Additionally, some people sent me some general information on how they think about certain security issues and how their security was implemented. However, this low response rate was already expected and the results that did come back were very useful and helped to create some insight in how the financial services sector copes with computer and information security, especially when it comes to the insider threat.

First, the organizations were all large in size, with many thousands of employees. All of the participating organizations were aware of the possible threat of insiders. Most of their employees (about 90 to 95%) have only basic computer skills, like working with (a) specific MS Office application(s). Furthermore, these employees seem to generally prioritise usability over security, but they do have some basic security knowledge.

As for the security systems, all organizations report that they do not have straight off-the-shelf systems in place, but rather highly customized standard packages and custom-tailored systems. These systems are designed and implemented with both usability and security in mind. When it comes to a differentiation between systems for detecting and preventing insider attacks and those for outside attacks, banks generally do make that distinction, while for the other types of organizations there was not enough data to make such a statement.

It also became clear that, especially in banks, special models and/or methods are used to map the threat that employees pose to computer and information systems. These include such methods as screening new employees before hiring them and anti-money laundering techniques.

Concerning the methods and mechanisms used to guarantee a certain level of security, the participating organizations indicated they use a great selection of possible measures. Among these are technical and physical measures, security policies, codes of ethics, security training and security awareness. The codes of ethics and security policies are internally mostly communicated through the internet and/or intranet, and externally through such things as brochures (e.g. for new employees).
In contrast, the participating organizations were generally reluctant to change their organizational culture, for various reasons. First, security is not seen as a goal in itself, but more as a means to secure a goal being reached. Additionally, one participant commented that "end-users can't do anything on their workplace that isn't requested beforehand, assessed on all possible risks, approved and finally installed by others." Last but not least, as a bank, all of the services it provides and the security thereof are accountable to De Nederlandsche Bank (DNB). This means security is already tightly woven into risk management, the development process, daily operations and end-user security awareness. Finally, the participating organizations noticed an increase in the occurrence of internally initiated attacks, which conflicts with the results of the 2004 Annual FBI and Computer Security Institute.

The answers that were given in the surveys by most participating organisations (the banks in this case) show a high (insider) security awareness in those organisations. They are highly aware of possible insider threats, have different security systems for inside and outside attacks and they have all kinds of security measures like security policies, security training and security awareness programs as well as physical security measures in place. Furthermore, usability is not prioritised over security, there are special models and techniques used to prevent insider abuse and the organisations recognize the importance of organisational culture for their security. This means the banks can be categorized in level 4 of the IS-CMM, due to their high security awareness and multitude of implemented security measures, systems and methods. The only thing that they feel needs continuous further improvement is actual employee security awareness. One participant falls into category 3 of the IS-CMM, due to the lack of specialised methods for detecting and preventing insider attacks and the fact they do not map the insider threat. It would be advisable for this company to move up one level by starting to treat insider attacks as different from outsider attacks. Furthermore, it would be wise to shed some more light on the current insider threat level in the organization (mapping the threat using e.g. Parker's model).
Concluding, it can be said that the financial services sector is already a secure sector, due to the high priority that is given to security and the rules and regulations that govern the sector.

5.4.2 Hypotheses falsification

Due to the low number of respondents to the survey, there are few hypotheses that were falsified. Several hypotheses however, can be falsified, due to the survey results contradicting the hypotheses. Below I have categorised the hypotheses into 2 categories, namely the ones that were falsified and those that were not falsified by the survey results. Further, more extensive research would probably lead to the falsification of more hypotheses.

Falsified

Hypothesis 1b: Companies tend to ignore the overall threat of insider attacks to computer and information security.

Hypothesis 1c: The occurrence of insider attacks is declining, but it remains an issue in computer and information security.

Hypothesis 2b: GDT-mechanisms such as off-the-shelf security systems and general security policies still prevail in most organisations, thus unnecessarily limiting the level of computer and information security.

Hypothesis 3a: Organisations do not use special models to model/map the threat posed by insiders, like Wood's insider threat model.

Not falsified

Hypothesis 1a: Companies, in practice, do not use different methods and/or measures to repel inside attacks when compared to external attacks.

Hypothesis 2a: In most cases, legitimate users (and companies themselves) will prioritise usability over security (i.e. with regard to systems, software, etc.).

Hypothesis 2c: Companies make sure that their employees have some basic expertise concerning computer and information security, meaning e.g. they don't open potentially malicious e-mails but instead report them.

Hypothesis 4a: Most companies have some form of formal code of computer ethics in place.

Hypothesis 4b: Organisations recognize the importance of organizational culture as a key factor in their computer and information security.

Hypothesis 4c: Most organisations are not willing (or able) to change their organisational culture to achieve a higher security awareness among their employees, but will opt for "regular" security awareness training instead.

5.5 Summary

In this chapter a short survey on insider security has been discussed. The survey was based upon hypotheses which were based on the reviewed literature. These hypotheses were also used to construct an insider security capability maturity model (loosely based on the People CMM). The survey results were then linked to the IS-CMM. The results showed that the financial services sector (banks, insurance companies, etc.) are quite secure and can be categorised in the IS-CMM somewhere around level 4, which is quite high. Due to a low response rate, with only 4 completed surveys, many hypotheses weren't falsified. A larger scale study would most likely falsify more hypotheses.

6. Summary and conclusion

6.1 Introduction

In this chapter a summary of the thesis is given, followed by some recommendations for future research. Finally, the problem statement, as it was stated in the introduction, is answered in the conclusion.

6.2 Summary

In chapter one some basics on the phenomenon of insider attacks in information and computer security were discussed. A few different definitions were stated, most of which amount to more or less the same. Several myths concerning security, specifically on insider attacks, were defaced. It seems that a lot of people have marginalized the insider threat over the years, but some have come to see that the threat poses one of the greatest risks to information and computer security. Finally, several recent statistics on computer security were discussed, from which it was apparent that inside abuse was on the decline, but far from eradicated. Still nearly 60% of respondents to the 2004 FBI/CSI survey reported insider abuse over the preceding twelve months.

In chapter two some theories and models concerning security behaviour have been analyzed. After reviewing these theories and models, it becomes very clear that there are countless factors that directly, or indirectly, influence the way people behave in general and with regard to security. As described in this chapter, people's behaviour depends on such factors as (among others) making implicit, intuitive trade-offs for a decision, imitating someone you've come to associate with, and the presence, or absence, of certain social bonds.

In chapter three, different models were analyzed, which all have the purpose of modelling the insider threat. Applying these models, or some techniques similar to them, in practice can help to deter insider attacks by detecting a threat early on. In this context, the models by Parker and Wood show various similarities, and their approach is more or less the same. We have seen that Schultz's model tries to incorporate several theories and models, among which are Parker's and Wood's models, into a practice-based insider detection framework. The framework puts potential indicators of an insider attack in a weighted mathematical (regression) equation, where the weights can be based on real values by examining the characteristics of large quantities of past insider security incidents.

In chapter four we have seen two different methods that can be used in preventing insider attacks. The first was implementing a code of (computer) ethics. Although having some positive effect on security, codes of (computer) ethics are, in my opinion, nothing more than just another security mechanism like, for example, security policies. That is

not to say they are worthless, but they're just another piece of the puzzle. The second method for deterring insider attacks, changing an organization's culture, turned out to be very promising. Since this technique is based on the human factor and attacking improper behaviour at its roots, it is something that all organizations coping with improper security behaviour by employees should apply. If, eventually, culture is aligned with company (security) policies, security awareness is enhanced and the odds of any insider security incidents will be greatly reduced. However, there are more factors that come into play when it comes to intentional malicious behaviour, e.g. personality traits and upbringing of the individual.

In chapter five the results of a security survey were discussed. The survey was done among companies in the financial services sector, which is comprised of banks, insurance companies, investment firms, etc. to find out the current state of 'insider security' in that sector. These results were then linked to an insider security capability maturity model (IS-CMM). The computer and information security, especially related to insider security, in that sector turned out to be quite high. The companies were aware of the threat that insiders pose, employees had basic security knowledge, good security awareness en security was a top priority. Furthermore, in several cases special techniques and methods were in place to detect and prevent insider attacks. The only somewhat surprising result that this survey revealed was that the occurrence of insider attacks in this sector is rising.

6.3 Future research

Although more and more research is being done on the insider threat, there are still some subjects that need further, more extensive, covering. One can think of testing Schultz's insider detection framework in various practice situations, as to gain empirical data on it's value and applicability. Another topic that deserves further, more in-depth, research is that of deterring the insider threat by changing organizational culture, as described by Vroom and Von Solms (2004). This seems to be so promising, since it attacks the problems at their roots, that it justifies extensive further research. Additionally, it would be interesting to see the results of a large scale investigation of the insider security levels in different sectors, such as banking, telecom, industry, etc.

6.4 Conclusion

I will now try to answer the problem statement, as defined in the introduction (see § i.3). The problem statement runs as follows:

What are the reasons for/motivations behind insider attacks, what has already been tried to deter these insider attacks and what can organizations do further to efficiently reduce/prevent the occurrence of insider attacks?

It is crucial to have an understanding of the reasons/motivations behind insider attacks. These reasons are nearly countless, since human behaviour and decision making is affected by so many different factors. For example, there is the fact that people make implicit, intuitive trade-offs for their decisions, they sometimes imitate someone they've come to associate with, and there's the influence of certain social bonds. These are just a tiny fraction of the complex web of factors that influence human behaviour and the human decision making process.

Furthermore, organizations implement various mechanisms to enforce behavioural compliance by their employees. Some of the more familiar security mechanisms are security policies, codes of computer ethics, and of course physical mechanisms such as doors equipped with cardkey readers. Additionally, organizations try to deter improper behaviour by imposing penalties on such behaviour, or by rewarding good behaviour.

Organizations can further prevent insider security incidents by modelling the insider threat, by using the models developed by Parker, Wood and Schultz, where Schultz's framework tries to quantify the insider threat based on several models and real-world data. The single most promising solution to insider attacks, is described in two papers, by Vroom and Von Solms (2004) and Von Solms and Von Solms (2004). They propose a shift from simply enforcing security policies to a change in organizational culture. As soon as the culture becomes aligned with company security policies, security awareness among employees is enhanced and the likelihood of an insider security breach is greatly reduced.

Appendices

A.1 Facts and figures on security incidents

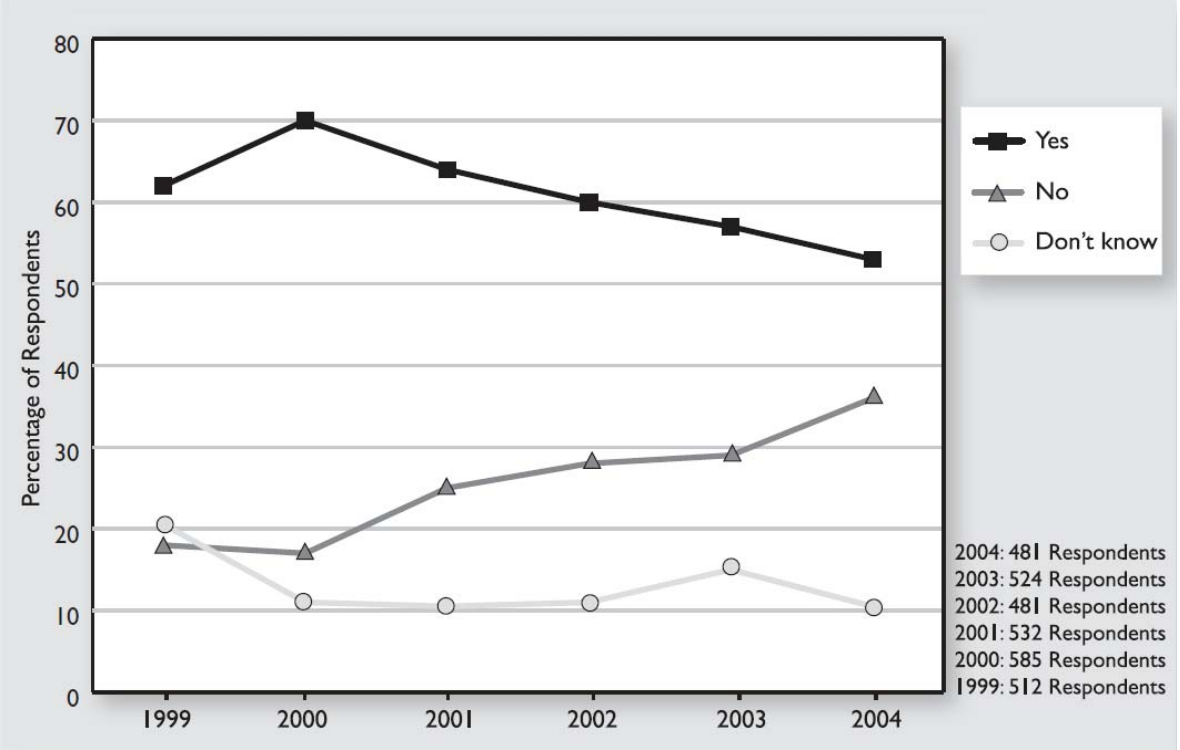


Figure A1.1 – Unauthorized Use of Computer Systems (up to 2nd half of 2004)
Source: Annual FBI and Computer Security Institute survey on computer crime 2004

How Many Incidents? by percentage	1 – 5	6 – 10	>10	Don't Know
2004	47%	20%	12%	22%
2003	38%	20%	16%	26%
2002	42%	20%	15%	23%
2001	33%	24%	11%	31%
2000	33%	23%	13%	31%
1999	34%	22%	14%	29%
How Many Incidents From the Inside?	**1 – 5**	**6 – 10**	**>10**	**Don't Know**
2004	52%	6%	8%	34%
2003	45%	11%	12%	33%
2002	42%	13%	9%	35%
2001	40%	12%	7%	41%
2000	38%	16%	9%	37%
1999	37%	16%	12%	35%

Figure A1.2 – Number of incidents total, from the outside and from the inside
Source: Annual FBI and Computer Security Institute survey on computer crime 2004

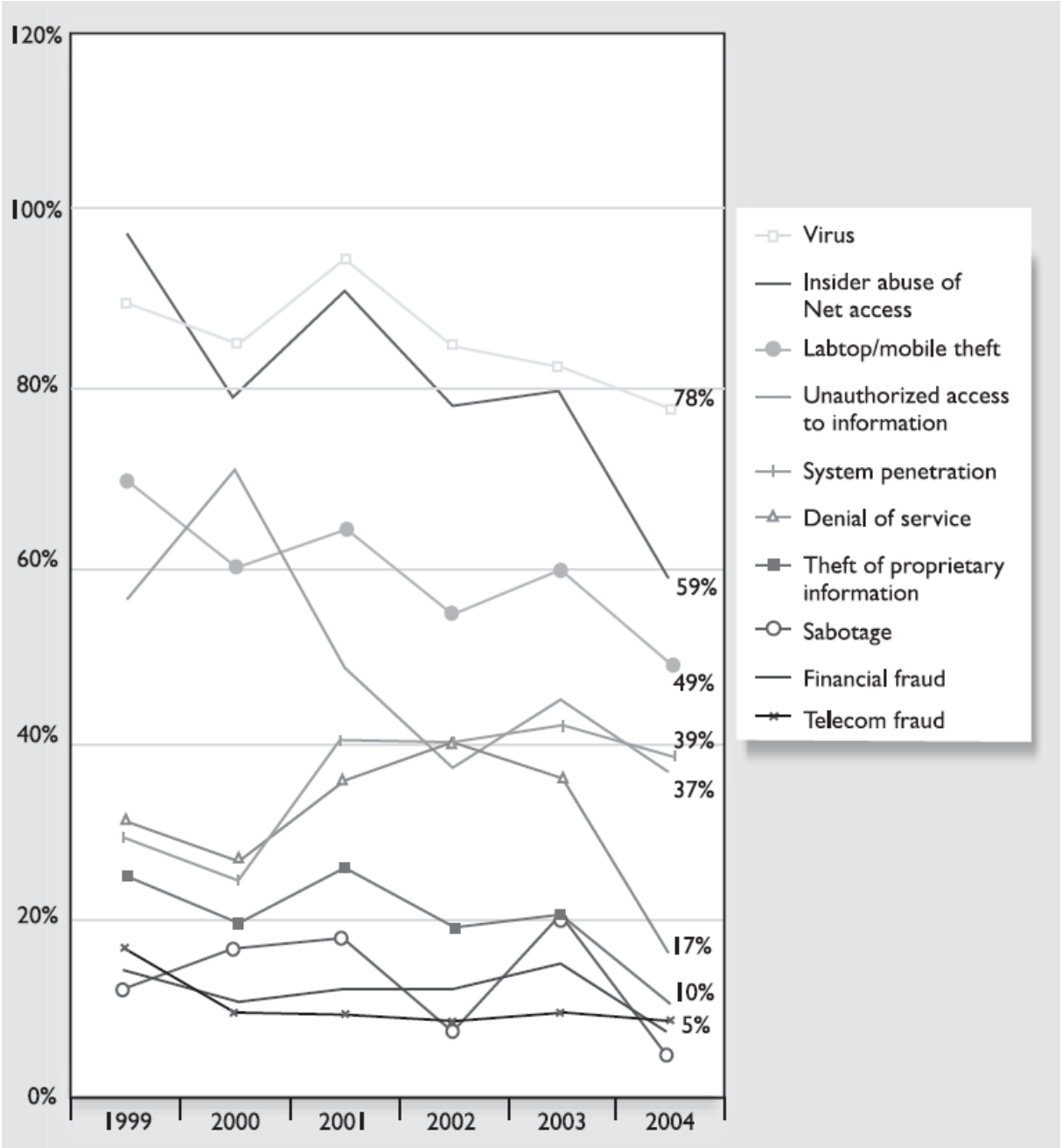
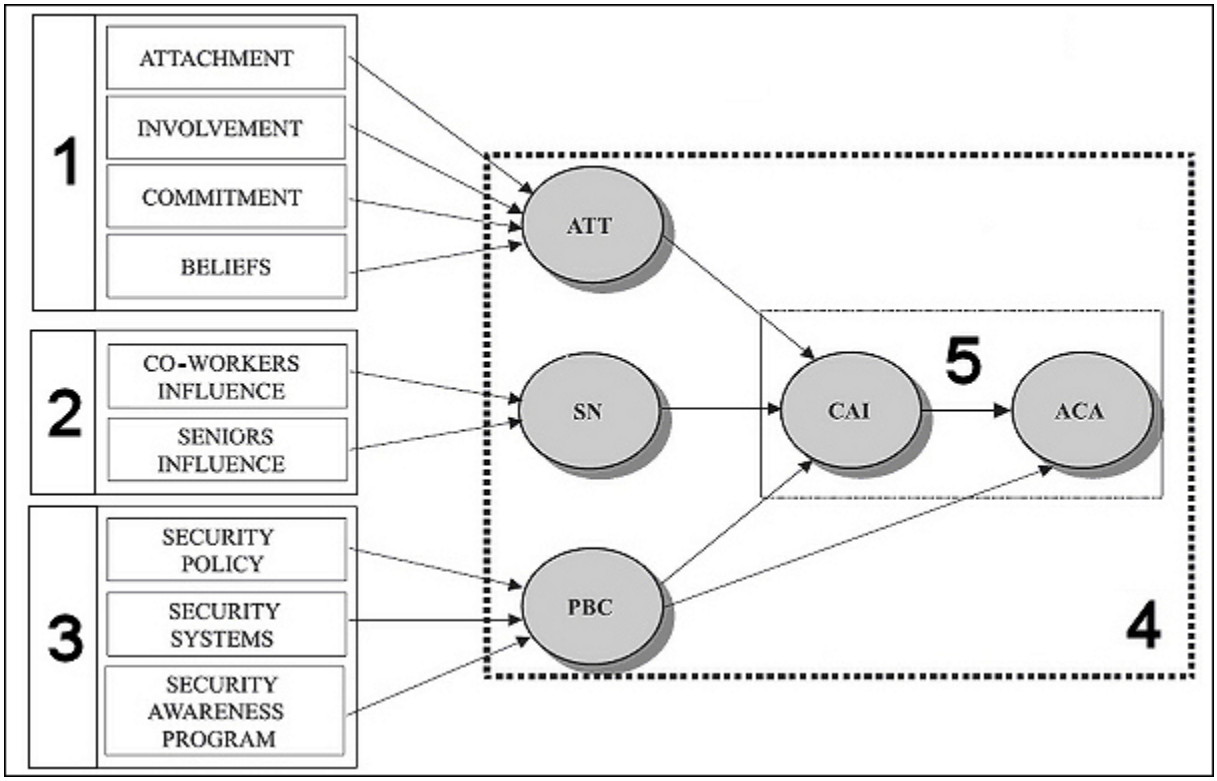


Figure A1.3 - Types of attacks or misuse detected (up to 2nd half of 2004)
Source: Annual FBI and Computer Security Institute survey on computer crime 2004

A.2 A holistic model of computer abuse



- 1 = Social Bond Theory, 2 = Social Learning Theory, 3 = General Deterrence Theory, 4 = Theory of Planned Behaviour, 5 = Computer Abuse Factors
- ATT = attitude, SN = subjective norm, PBC = perceived behavioural control, CAI = computer abuse intention, ACA = actual computer abuse

Figure A.2 – A holistic model of computer abuse (adapted from Lee and Lee, 2002)

The attitude toward the behaviour is the degree to which the person has a favourable or unfavourable evaluation of the behaviour in question. The subjective norm is the social pressure to perform or not to perform the behaviour. The perceived behavioural control (PBC) is the perceived ease or difficulty of performing the behaviour (Beck and Ajzen, 1991; in Lee and Lee, 2002).

A.3 Hypotheses

Hypothesis 1a: Companies, in practice, do not use different methods and/or measures to repel inside attacks when compared to external attacks.

Hypothesis 1b: Companies tend to ignore the overall threat of insider attacks to computer and information security.

Hypothesis 1c: The occurrence of insider attacks is declining, but it remains an issue in computer and information security.

Hypothesis 2a: In most cases, legitimate users (and companies themselves) will prioritise usability over security (i.e. with regard to systems, software, etc.).

Hypothesis 2b: GDT-mechanisms such as off-the-shelf security systems and general security policies still prevail in most organisations, thus unnecessarily limiting the level of computer and information security.

Hypothesis 2c: Companies make sure that their employees have some basic expertise concerning computer and information security, meaning e.g. they don't open potentially malicious e-mails but instead report them.

Hypothesis 3a: Organisations do not use special models to model/map the threat posed by insiders, like Wood's insider threat model.

Hypothesis 4a: Most companies have some form of formal code of computer ethics in place.

Hypothesis 4b: Organisations recognize the importance of organizational culture as a key factor in their computer and information security.

Hypothesis 4c: Most organisations are not willing (or able) to change their organisational culture to achieve a higher security awareness among their employees, but will opt for "regular" security awareness training instead.

A.4 Security survey questions

Is the organisation aware of the potential threat that employees pose to computer and information security?
Unaware 1 2 3 4 5 Highly aware

On a yearly basis, does the number of internally initiated security breaches related to computer and information security in your organisation show a declining or rising tendency?
∇ Declining
∇ Rising
∇ Unknown

Does the organisation use different methods for detecting and preventing inside attacks compared to external attacks (like viruses, DoS-attack)?
∇ Yes
∇ No

What has a higher priority when it comes to systems and software: usability or security?
∇ Usability
∇ Security
∇ Evenly distributed
∇ Unknown

Do employees (everyone from the secretary to the CEO) generally prioritise usability over security concerning their daily work? (An example is not locking a PC because of laziness)
∇ Yes
∇ No
∇ Unknown

Are the security systems in the organisation (such as IDS) off-the-shelf or tailored to the organisation's specific needs?
∇ Off-the-shelf
∇ Custom tailored

What is generally the level of security expertise the employees that work with computer and information systems (such as PCs) have?
∇ None
∇ Basic – e.g. not opening potentially dangerous emails, frequently changing passwords
∇ Moderate – e.g. reporting suspicious CPU activity on computer
∇ High – highly security aware, think security first

Does the organisation use special models or methods to map the threat posed by specific employees, like for example prior offenders?
∇ Yes
∇ No
If yes, what kind of methods/models are used? ……

Does the organisation have guidelines for computer ethics and security behaviour of employees, stated in e.g. a security policy or formal code of (computer) ethics?
∇ Yes
∇ No
If yes, are all employees aware of these guidelines?
∇ Yes
∇ No

To what extent is the organisational culture seen as an important factor in companywide computer and information security?
Not important 1 2 3 4 5 Very important

Would your organisation consider changing the organisational culture to one that revolves around high security awareness among employees?
Yes No
If no, explain your objections/problems:
- ∇ Too complex
- ∇ Not feasible
- ∇ ……

A.5 Survey - Aanvallen van binnenuit: insider threat in IT

1. Hoeveel medewerkers telt uw organisatie?

2. Wat is het algemene niveau van de computerkennis van de medewerkers in uw organisatie?
[ ] Laag (enkel gebruikersvaardigheden met specifieke applicaties, zoals bijv. tekstverwerken)
[ ] Gemiddeld (kunnen zelf eenvoudige problemen oplossen)
[ ] Hoog (kennis van computerbeheer, inclusief bijv. installatie van nieuwe software)

3. Spelen computer- en informatiebeveiliging een grote rol in uw organisatie?
Geen issue [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 Hot topic

4. Is de organisatie zich bewust van het potentiële gevaar dat de eigen medewerkers vormen voor de computer- en informatiebeveiliging van het bedrijf?
Onbewust [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 Zeer bewust

5. Wat is algemeen gezien het niveau van beveiligingsexpertise van de medewerkers die werken met computer- en informatiesystemen (zoals Pc's en servers)?
[ ] Nihil
[ ] Basaal – bijv. het regelmatig veranderen van wachtwoorden
[ ] Gemiddeld – bijv. het melden van verdachte CPU activiteit op computers
[ ] Hoog – beveiliging voor alles, zeer beveiligingsbewust, hoge expertise

6. Geven medewerkers een hogere prioriteit aan "gebruiksgemak" dan aan "beveiliging"? (bijv. het uit gemakzucht niet 'locken' van een werkstation tijdens afwezigheid)
[ ] Ja
[ ] Nee
[ ] Onbekend

7. Wat heeft een hogere prioriteit wat betreft (computer)systemen en software: gebruiksgemak of beveiliging?
[ ] gebruiksgemak
[ ] beveiliging
[ ] gelijk verdeeld
[ ] onbekend
8. Gebruikt de organisatie verschillende methoden voor het detecteren en voorkomen van aanvallen van binnenuit in vergelijking met aanvallen van buitenaf (voorbeelden van aanvallen van buitenaf zijn virussen en DoS-aanvallen)
[ ] Ja
[ ] Nee

9. Zijn de beveiligingssystemen/-software in de organisatie (zoals Intrusion Detection Systems) standaardsoftware of op maat gemaakt naar de wensen en eisen van de organisatie?
[ ] Standaardsoftware
[ ] Aangepaste standaardsoftware (standaardpakket met veel custom parameters)
[ ] Op maat gemaakt ('custom tailored')

10. Gebruikt de organisatie speciale modellen en/of methoden om de bedreiging die bepaalde medewerkers voor de computer- en informatiebeveiliging vormen in kaart te brengen?
[ ] Nee
[ ] Ja
Zo ja, wat voor methoden/modellen worden er gebruikt?

11. Welke methoden/mechanismen gebruikt uw organisatie om de computer- en informatiebeveiliging vorm te geven cq. te waarborgen? (meerdere antwoorden mogelijk)
[ ] Technische (o.a. fysieke) maatregelen
[ ] Gedragslijnen (security policies)
[ ] Code van computer ethiek
[ ] Security training
[ ] Security awareness programma's (verhogen beveiligingsbewustzijn)
[ ] Het veranderen van de organisatiecultuur in een beveiligingsbewuste cultuur
[ ] Anders, namelijk:

12. Heeft de organisatie richtlijnen m.b.t. computerethiek en beveiligingsgedrag van medewerkers?
[ ] Nee
[ ] Ja
Zo ja, hoe worden deze richtlijnen naar de medewerkers gecommuniceerd?

13. In hoeverre wordt de organisatiecultuur gezien als een belangrijke factor in de bedrijfsbrede computer- en informatiebeveiliging?
Niet belangrijk [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5 Heel belangrijk

14. Zou uw organisatie bereid zijn om de organisatiecultuur te veranderen in een cultuur die draait om een hoog beveiligingsbewustzijn onder de medewerkers?
[ ] Ja
[ ] Nee
Zo nee, wat zijn mogelijke obstakels?
[ ] Te complex
[ ] Niet rendabel
[ ] Anders, namelijk:

14. Vertoont het aantal intern geïnitieerde beveiligingsincidenten, gerelateerd aan computer- en informatiebeveiliging, in uw organisatie een stijgende of dalende tendens?
[ ] Stijgend
[ ] Dalend
[ ] Gelijkblijvend
[ ] Onbekend

A.6 Reference list

- Agnew, R. (1995), Testing the leading crime theories: an alternative strategy focusing on motivational process, *Journal of Research in Crime and Delinquency*, Vol. 32 (4), p. 363-398 *in Lee and Lee, 2002*
- Ajzen, I. (1985), From intentions to actions: a theory of planned behavior, in Kuhl, J. and Beckman, J. (Eds), Action-control: From Cognition to Behavior, pp. 11-39, Springer, Heidelberg *in Lee and Lee, 2002*
- Ajzen, I. (1991), The theory of planned behavior, *Organizational Behavior and Human Decision Processes*, Vol. 50, p. 179-211 *in Lee and Lee, 2002*
- Akers, R. (1985), Deviant Behavior: A Social Learning Approach, Wadsworth, Belmont, CA, USA *in Lee and Lee, 2002*
- Akers, R. (1997), Criminological Theories: Introduction and Evaluation, 2nd edition, Roxbury Publishing, Los Angeles, CA, USA *in Lee and Lee, 2002*
- Akers, R., Krohn, M., Lanza-Kaduce, L. and Radosevich, M. (1979), Social learning and deviant behavior: a specific test of a general theory, *American Sociological Review*, Vol. 44, p. 636-655 *in Lee and Lee, 2002*
- Annual FBI and Computer Security Institute survey on computer crime 2004, On-line document, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf
- Bainbridge, L., (1998), Difficulties in complex dynamic tasks, http://www.bainbrdg.demon.co.uk/Papers/CogDiffErr.html, *in Besnard and Arief, 2004*
- Banerjee, D., Cronan, T. and Jones, T. (1998), Modeling IT ethics: a study of situational ethics, *MIS Quarterly*, Vol. 22 (1), p. 31-60 *in Lee and Lee, 2002*
- Barrett, N., (2003), Penetration and social engineering: hacking the weakest link, *Information Security Technical Report*, Vol. 8 (4), p. 56-64
- Baskerville, R. (1993), Information systems security design methods: implications for information systems development, *ACM Computing Surveys*, Vol. 25 (4), p. 375-414 *in Lee and Lee, 2002*
- Beck, L. and Ajzen, I. (1991), Predicting dishonest actions using the theory of planned behavior, *Journal of Research in Personality*, Vol. 25, p. 285-301 *in Lee and Lee, 2002*
- Berenbeim, R., (1992), Corporate Ethics Practices, The Conference Board, New York NY, USA, *in Harrington, S., (1996), The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions, MIS Quarterly, Vol.20 (3), p. 257-278*
- Besnard, D. and Arief, B., (2004), Computer security impaired by legitimate users, *Computers & Security*, Vol. 23, p. 253-264
- Briney, A., (2001), 2001 Information security industry survey (online), available from www.infosecuritymag.com, cited September 30, 2002; *in Vroom and Von Solms, 2004*
- BS 7799, (1999), Code of practice for information security management, *British Standards Institute*, UK, *in Von Solms and Von Solms, 2004*
- Carr, J., (2002), Strategies and issues: thwarting insider attacks, *Network Magazine*, 4 September 2002, www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=8703398
- Curtis, B., Hefley, W. and Miller, S., (2001), *People Capability Maturity Model 2.0*, CarnegieMellon S.E.I., http://www.sei.cmu.edu/pub/documents/01.reports/pdf/01mm001.pdf
- Deal, T. and Kennedy, A., (1982), Corporate culture - the rites and rituals of corporate life, Addison-Wesley, New York NY, USA, *in Vroom and Von Solms, 2004*

- Dhillon, G., (2001), Violation of safeguards by trusted personnel and understanding related information security concerns, *Computers & Security*, Vol. 20, p. 165-172
- Duyn, J. Van, (1985), The Human Factor in Computer Crime, Petrocelli Books, Princeton, New Jersey, USA *in Frank, 2003*
- Einwechter, N., (2002), The enemy inside the gates: preventing and detecting insider attacks, *SecurityFocus*, http://www.securityfocus.com/printable/infocus/1546
- Erlanger, L., (2004), The weakest link, *PCMag.com*, 16 March 2004, http://www.pcmag.com/article2/0,1759,1537426,00.asp
- Evans, S., Harries, C., Dennis, I. and Dean, I., (1995), General practitioners' tacit and stated policies in the prescription of lipid lowering agents, *British Journal of General Practitioners*, 1995 (45), p. 15-18, *in Besnard and Arief, 2004*
- Finch, J., Furnell, S., and Dowland, P., (2003), Assessing IT security culture: system administrator and end-user, *Proceedings of ISOneWorld Conference 2003*, Las Vegas, USA, April 23-25, 2003
- Flechais, I. and Sasse, M., (2003), Developing secure and usable software, *Summary of Workshop WS9 held at OT 2003*, Cambridge, UK, March 2003, http://www.cs.ucl.ac.uk/staff/I.Flechais/downloads/oct2003.pdf, *in Besnard and Arief, 2004*
- Forcht, K., (1994), Computer Security Management, Boyd & Fraser Publishing Company, Danvers MA, USA, *in Harrington, S., (1996), The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions, MIS Quarterly, Vol.20 (3), p. 257-278*
- Frank, S., (2003), Can S.K.R.A.M. Support Quantified Risk Analysis of Computer Related Crime?, In Partial Fulfillment of the Requirements in the Honors Research Class at the Rochester Institute of Technology, www.sparsa.org/research/QTAssess.pdf
- Furnell, S. and Phyo, A., (2003), Considering the problem of insider IT misuse, *Australian Journal of Information Systems*, Vol. 10 (2), p. 134-138
- Furnell, S., (2004), Enemies within: the problem of insider attacks, *Computer Fraud & Security*, Vol. 2004 (7), p. 6-11
- Furnell, S., Gennatou, M., and Dowland, P., (2002), A prototype tool for information security awareness and training, *International Journal of Logisitics Information Management*, Vol. 15 (5), p. 352-357
- Halliday J. and Solms, R. von, (1997), Effective information security policies, in: Information technology on the move, Port Elizabeth Technikon, Port Elizabeth, South Africa, p. 12-20, *in Vroom and Von Solms, 2004*
- Hirschi, T. (1969), Causes of Delinquency, University of California Press, Berkeley, CA, USA *in Lee and Lee, 2002*
- Hoc, J. and Amalberti, R., (1994), Diagnostic et prise de de´cision dans les situations dynamiques, *Psychologie Française*, 1994 (39), p. 177-192, *in Besnard and Arief, 2004*
- Hoffer, J. and Straub, D. (1989), The 9 to 5 underground: are you policing computer abuses?, *Sloan Management Review*, Vol. 30 (4), p. 35-44 *in Lee and Lee, 2002*
- Höne, K. and Eloff, J., (2002), Information security policy – what do international information security standards say?, *Computers & Security*, Vol. 21 (5), p. 402-409
- Karyda, M., Kiountouzis, E., and Kokolakis, S., (2005), Information systems security policies: a contextual perspective, *Computers & Security*, In Press
- Krohn, M., Skinner, W., Massey, J. and Akers, R. (1985), Social learning theory and adolescent cigarette smoking: a longitudinal study, *Social Problems*, Vol. 32 (5), p. 455-71 *in Lee and Lee, 2002*

- Le Blanc, M. and Kaspy, N. (1998), Trajectories of delinquency and problem behavior: comparison of social and personal control characteristics of adjudicated boys on synchronous and non-synchronous paths, *Journal of Quantitative Criminology*, Vol. 14 (2), p. 181-214 *in Lee and Lee, 2002*
- Leach, J., (2003), Improving user security behaviour, *Computers & Security*, Vol. 22, p. 685-692
- Lee, J. and Lee, Y., (2002), A holistic model of computer abuse within organizations, *Information Management & Computer Security*, Vol. 10 (2), p. 57-63
- Loch, K., Carr, H., and Warkentin, M., (1992), Threats to information systems: today's reality, yesterday's understanding, *MIS Quarterly*, June 1992, p. 173-186
- Magklaras, G. and Furnell, S., (2005), A preliminary model of end user sophistication for insider threat prediction in IT systems, *Computers & Security*, In Press
- Mancini, G., (1987), Commentary: models of the decision maker in unforeseen accidents, *International Journal of Man-Machine Studies*, 1987 (27), p. 631-639, *in Besnard and Arief, 2004*
- Parker, D., (1998), Fighting computer abuse – a new framework for protecting information, Wiley & Sons, New York, USA, *in Lee, Y. and Lee, J., (2002)*
- Parker, D.B. (1998), Fighting Computer Abuse - A New Framework for Protecting Information, John Wiley & Sons, New York, NY, USA *in Lee and Lee, 2002*
- Pierce, M. and Henry, J., (1996), Computer ethics: The role of personal, informal, and formal codes, *Journal of Business Ethics*, Vol.15 (4), p. 425-437
- Randazzo, M., Keeney, M., Kowalski, E., Capelli, D., and Moore, A., (2004), Insider threat study: illicit cyber activity in the banking and finance sector, *N.T.A.C. U.S. Secret Service and CERT Coordination Center, S.E.I., Carnegie Mellon University*, August 2004
- Redmill, F., (2002), Some dimensions of risk not often considered by engineers, *Journal of System Safety*, Q4 2002, p.22-40, *in Besnard and Arief, 2004*
- Schein, E., (1999), The corporate culture survival guide, Jossey-Bass Publishers, San Francisco CA, USA, *in Vroom and Von Solms, 2004 & in Von Solms and Von Solms, 2004*
- Schudel, G. and Wood, B., (2000), Modeling behaviour of the cyber-terrorist, *2000 National Information Systems Security Conference*, Baltimore MD, October 2000, published in *Research on Mitigating the Insider Threat to Information Systems – #2 - - Proceedings of a Workshop Held August 2000, National Defense Research Institute*, p. 49-59, www.rand.org/publications/CF/CF163/CF163.pdf
- Schultz, E. and Shumway, R., (2001), Incident response: a strategic guide for system and network security breaches, New Riders, Indianapolis, USA *in Schultz, 2002*
- Schultz, E., (2002), A framework for understanding and predicting insider attacks. *Computers & Security*, Vol. 21, p. 526-531
- Shaw, E., Post, J., and Ruby, K., (1999), Inside the mind of the insider, *Security Management*, Vol. 43 (12), p. 34-41
- Skinner, W.F. and Fream, A.M. (1997), A social learning theory analysis of computer abuse among college students, *Journal of Research in Crime and Delinquency*, Vol. 34 (4), p. 495-518 *in Lee and Lee, 2002*
- Solms, R. von, and Solms, B. von, (2004), From policies to culture, *Computers & Security*, Vol. 23, p. 275-279
- Spee, A., (2004), Insider threat in IT (de factor mens beschouwd), gebaseerd op referaat postdoctorale opleiding IT auditing, EURAC, versie 1.2, 14 juni 2004
- Stanton, J., Stam, K., Mastrangelo, P. and Jolton, J., (2005), Analysis of end user security behaviour, *Computers & Security*, Vol. 24, p. 124-133

- Stevens, B., (1994), An analysis of corporate ethical code studies: where do we go from here?, *Journal of Business Ethics*, Vol. 13, p. 63–69, *in Pierce, M. and Henry, J., (2000), Judgements about computer ethics: do individual, co-worker, and company judgements differ? Do company codes make a difference?, Journal of Business Ethics, Vol. 28, p. 307-322*
- Szilagyi, A. and Wallace, M., (1990), Organizational behavior and performance, 5th ed., Scott, Foresman and Company, Illinois, USA, *in Vroom and Von Solms, 2004*
- Tesser, A. (1988), Toward a self-evaluation maintenance model of social behavior, in Berkowitz, L. (Ed.), Advances in Experimental Social Psychology, Vol. 21, p. 181-227, Academic Press, New York, NY, USA *in Lee and Lee, 2002*
- Thomson, M. and Solms, R. von, (1998), Information security awareness: educating your users effectively, *Information Management & Computer Security*, Vol. 6 (4), p. 167-173
- Tittle, C.R., Burke, M.J. and Jackson, E.F. (1986), Modeling Sutherland's theory of differential association: toward an empirical clarification, *Social Forces*, Vol. 65, p. 405-32 *in Lee and Lee, 2002*
- Vroom, C. and Von Solms, R., (2004), Towards information security behavioural compliance, *Computers & Security*, Vol. 23, p. 191-198
- Wood, B., (2000), An insider threat model for adversary simulation, *SRI International*, published in *Research on Mitigating the Insider Threat to Information Systems – #2 -- Proceedings of a Workshop Held August 2000, National Defense Research Institute*, p. 41-48, www.rand.org/publications/CF/CF163/CF163.pdf
- Zajac, B.P. Jr (1988), Personnel: the other half of data security, *Computer & Security*, Vol. 7 (2), p. 131-2 *in Lee and Lee, 2002*