1997

Security decay: The erosion of effective security

Shawn A. McClure
Edith Cowan University

Edith Cowan University

Copyright Warning

Security Decay : The erosion of effective security

By

Shawn A. McClure

A Thesis
Submitted to the Faculty of Science, Technology and Engineering
Edith Cowan University

Principal Supervisor : Associate Professor Cliff Smith

Submission Date : 14th of November 1997

In Partial Fulfilment of the Requirements for the Degree of
Bachelor of Science (Security) Honours

USE OF THESIS

The Use of Thesis statement is not included in this version of the thesis.

Abstract

The discipline of security lacks formal conceptual tools which can be used by security managers, advisers and consultants when attempting to provide effective security. This is because of security's relative age as a discipline, it is very new.

The aim of the thesis was to contribute to the security discipline by taking Underwood's (1989) idea of security decay and to a certain extent exploring and formalising it. The security decay theory is primarily concerned with the influence apathy has on security and how management react to risk materialisation when decay is evident. The thesis focused on the first of these two components only.

In focusing on the influence apathy has on security, a number of Likert tests were administered to a stratified sample of both security specialists and non - security people. The security specialist sample provided good indications that effective security will be provided when a synergy of functions and elements are implemented. This sample also believed that apathetic attitudes towards security would cause the effectiveness of security to decrease.

The results derived from the non - security sample were inconclusive, with no determinations to be made. This sample were unsure as to whether or not effective security was achievable, whether effective security would cause a lack of security incidence and whether a lack of security incidence would result in apathy towards security.

The results achieved are only representative of the attitudes of the respondents from within the sample. The two tests that derived conclusive results can not be generalised across the whole security specialist population. This was the major limitation of the thesis.

The recommendations resulting from the study include the need to further research the security decay theory in a longitudinal study, as well as researching the section of the theory which was excluded in this thesis. The implications for security specialists are that they need to have an awareness of the ramifications of having effective security. Also, the fact that the non - security sample were generally unsure about all sub - concepts put to them highlights the need for efficient and effective awareness and education programs.

Declaration

I certify that this thesis does not, to the best of my knowledge and belief;

(i) incorporate without acknowledgment any material previously submitted for a degree or diploma in any institution of higher education;

(ii) contain any material previously published or written by another person except where due reference is made in the text; or

(iii) contain any defamatory material

Signature

Date 22.1.97

Acknowledgments

I would like to acknowledge and express my sincere thanks to Associate Professor Clif Smith who provided invaluable guidance and assistance in completing this thesis.

I would like to express the same degree of thanks to Andrew Blades who provided great advice and support throughout the year.

To those who took the time to participate in the study, your co- operation made the thesis possible and I thank you for this.

Finally, thanks to my family for providing fantastic support not only this year, but all my years to date.

Definition of Terms

Security Decay :	a concept and phenomena where effective security indirectly causes an attitude of apathy towards the provision of security, resulting in ineffectiveness
Risk :	" The chance of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelihood" (AS/NZS: 4360, 1995)
Security :	"... implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of destruction or injury" (Fischer and Green, 199?, p. 3)
Residual Risk:	The degree of risk an organisation is exposed to after the implementation of countermeasures.
Risk Exposure:	The level of risk the organisation is exposed to prior to countermeasure implementation.
Threat :	A threat may be defined as a situation, event or action which will affect, or has the potential to effect, the security of an asset

Countermeasure :	A security measure, used to 'counter' a designated threat or threats
Criticality :	Also known as consequence. A factor of harm or damage which is to be considered when conducting a risk assessment
Intelligence :	" The product resulting from the processing of information concerning actual and potential situations, events, risks and threats to an organisation and its activities" (Blades, 1997, p. 2).
Defence in Depth :	A security theory concerned with the layering of countermeasures to provide deterrence, a degree of detection and delay, as well as aiding response actions
CPTED :	Crime Prevention Through Environmental Design. A security theory outlining the benefits to be derived from natural access, natural surveillance and territoriality

Table of Contents

List of Figures

List of Tables

When we have a free path, we go forward

If we meet an obstacle, we go around it

If the object can not be overcome, we retreat

When the enemy is unprepared, we surprise him

If he is alert, we leave him alone

(Bader Meinhof, www.tscm.com)

CHAPTER 1

INTRODUCTION

Background of Security Theory

Security as an academic discipline is in its infancy and has only relatively recently begun taking its first steps towards being fully recognised in its own right. As a result of this, the body of literature and conceptual tools available for analysis are small when compared to other, more well established disciplines.

However there are a number of related theories, as well as specific security theories, that have been either adapted, evolved or developed over the years. Security theories cover broad areas which are reflective of the nature of security itself. One will find technological security theory, sociological security theory and psychological security theory. The reason for such an integration of various fields into the security discipline is because of security's wide ranging scope, within both an organisation and society. There is a complex interrelationship between technology, people and management processes within a security function and because of this, a variety of differing fields have been utilised to aid in the provision of effective security. Each of these areas will influence the practicing of security and it is for this reason that these areas are of considerable importance.

As an example, the theory surrounding risk management did not originate from the field of security, but from fields such as environmental science (Fiskel and Covello,

1986), engineering (Crossland, Bennett, Ellis, Farmer, Gittus, Godfrey, Hambly, Kletz, and Lees 1992), medicine (Cooper, 1985), political science (Glen, 1993) and finance and insurance (Vaughan, 1982). However the application of this theory is well suited to the provision of security and has therefore been integrated into the security discipline by a substantial number of authors (Toft, 1997; Broder, 1984; Fites & Kratz, 1993; Schultheiss, 1994; DePasquale, 1989; Fay, 1993; Oliver & Wilson, 1988; Elbra, 1992; Strutt & Patrick, 1995; Custance, 1996; Healy & Walsh, 1996; and Kinsman & Tarr, 1996).

This study sets out, as one of its primary aims, to increase the body of security knowledge by developing and enhancing the term "security decay" which was first used by Underwood (1989, p. 249) in his book entitled "The Security of Buildings."

The Security Decay Theory

The security decay theory can be viewed as consisting of a seven step process as seen in Figure 1. The security decay theory as a whole will include two primary components; apathy, which is postulated to be caused by effective security, which in turns creates decay, and an incorrect reaction to risk materialisation caused by decay.

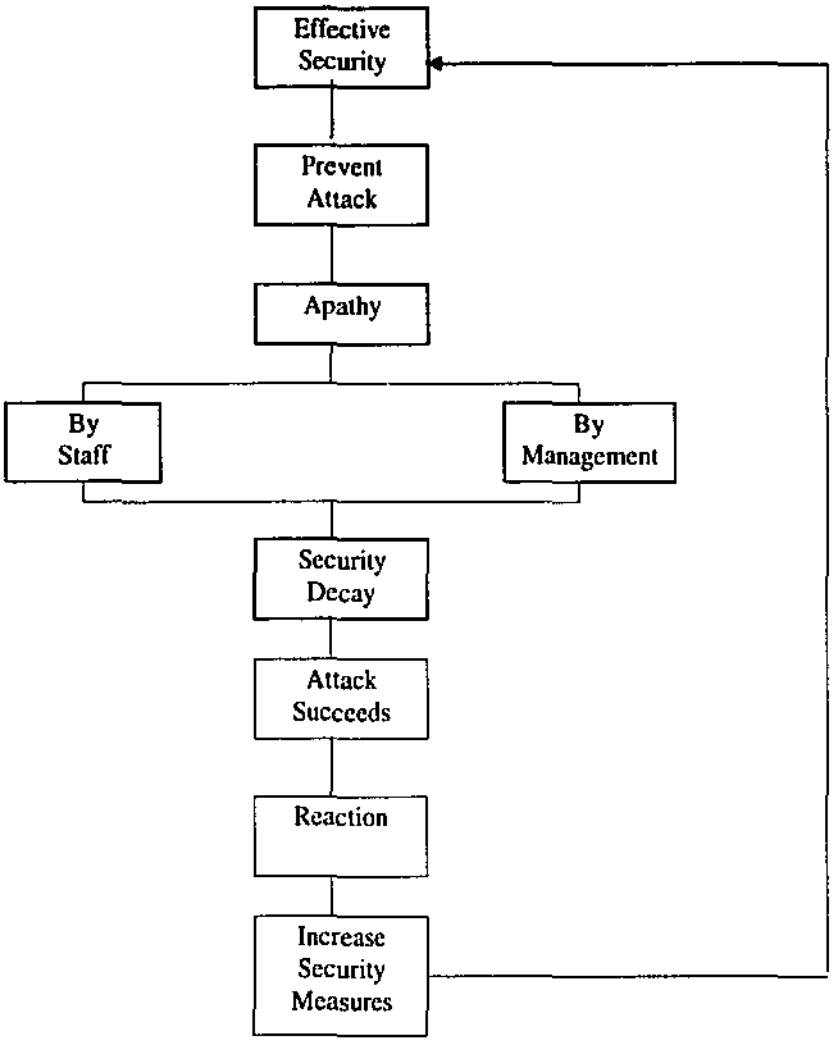

Figure 1: The Security Decay Theory

However the theory as a whole was not examined within the study, as this would have presented too large a task. The section of the security decay theory, which was examined, can be seen in Figure 2.

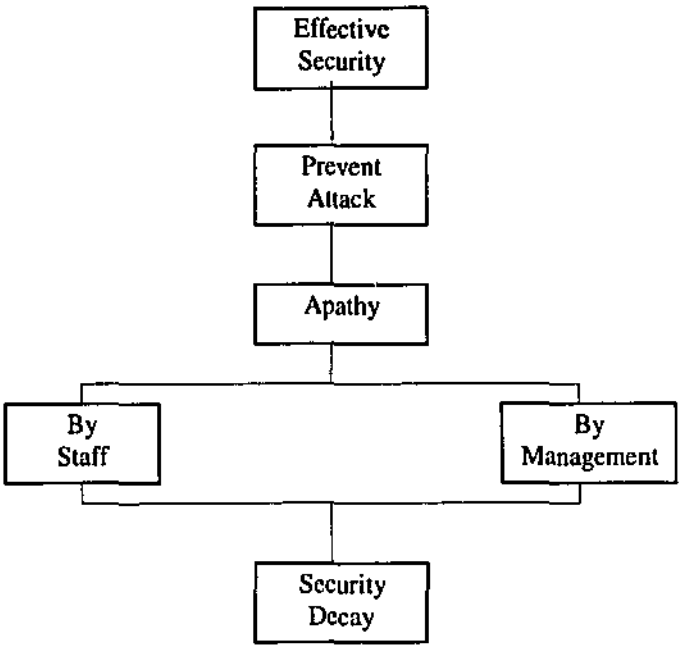

Figure 2: Security Decay Theory; section under examination

The dependant variable within the section of the theory under examination in the study is security decay, with the independent variables being effective security, the prevention of threat occurrence and apathy.

Effective security refers to a state where security's role has been defined, the need for security established and the level of protection required having been achieved. Effective security is postulated to exist when the level of risk exposure is reduced, through various means, to a level that is acceptable to the organisation.

It is postulated that the result of having effective security will be the possible prevention of threat occurrences. A lack of security threat occurrences may result in an attitude of apathy towards security by those influenced by it. When those people

become apathetic, they may cease to comply with security policy and procedure, which is postulated to cause a decaying of security effectiveness.

For people to become apathetic towards security, according to the security decay theory, they must first believe that security can reach a state of effectiveness, and that this will cause threat occurrences to be prevented. Also, they must believe that a lack of security incidents will result in an attitude of apathy. If any of these variables are missing within any given scenario, then the security decay theory will not be applicable.

The theory is robust as it extends beyond giving reason to an erosion of security effectiveness, by providing a possible explanation as to why management often react with an over - kill of security countermeasures. That is, when decay is attributable, a higher level of security may not be needed, but the required action may be to re - establish the original level of protection. However this section of the theory is not under examination within the thesis.

Background of the Security Decay Theory

The premise behind the concept of security decay is that the more effective is security, the greater the probability that at some time in the near future, the need for security will diminish. Thus security is postulated to be working towards its own demise (Underwood, 1989, p. 249). This outcome results because of apathy on behalf of staff, management and contractors towards security. Indeed Underwood (1989, p. 249) can

be quoted as saying; "It [decay] is almost exclusively a function of the human component of a security system."

If security is reducing security risk, then the perception generated by the stakeholders towards security may be one of unnecessariness. When people do not perceive the need for security, apathy towards it is the logical resultant effect.

In his book, Underwood (1989, p. 249-250) states that, "The provision of effective security is paradoxically the first step towards decay." As we are aware, a paradox is a statement that seems to be self-contradictory but contains a truth. Thus security decay can be perceived as a paradox as security is ultimately working towards it's own demise, as the more effective it is in theory, the less likely it will be needed in some point in the near future.

Security within an organisation is, like other specialties, working towards a goal. All of the planning and other efforts are directed towards achieving this goal (Bartol, Martin, Tein & Matthews, 1995, p. 154). Ultimately this goal is directed towards maximising the profit of the organisation by reducing the level of risk exposure and devising means to management risk realisation. Security will be seen to be successful if it is able to achieve this goal. To accomplish this, the security function must deter, deny, detect, delay (Hayes, 1991, p. 93) and respond to attacks effectively and efficiently.

If security is effective, and it is able to repel or prevent attacks, as well as detect, delay and respond to attacks, then what can be expected as a result?

The decay theory argues that the result of effective security is security being seen as unnecessary (Underwood, 1989, p. 249-250). With effective security in place, there are no incidents of threat occurrence. A situation where the security system is unchallenged may result in the prevailing attitude by staff and management being that security is unnecessary. It may be logical to think that if we have A in place to have an effect on B, but when B is not present, then the need for A diminishes (where A is the security countermeasure and B is threat occurrence).

When a threat eventuates it will come to the attention of management. The question they will now ask is; 'As a security incident has occurred, were the measures in place suitable'?

Underwood (1989) argues that often the answer to the above question is: as a security incident has occurred, the measures could not have been suitable. Management will then devise new security measures that offer a level of protection above that which the original measures offered. The disadvantage in reacting incorrectly, such as increasing the level of protection when decay is evident, is appropriately emphasised by Hansen (1992, p. 44) when he states that;

> " All too often security risks are taken seriously only after information [asset] is lost. The reaction is a flurry of expensive and mostly ineffective countermeasures."

The security decay theory will be cyclic in nature as once management increases security above the original level, it is argued that 'effective security' is achieved and the process begins again.

Security Decay - an example

If an organisation had a policy in place that required the scanning of computer hard drives for viruses before using, and over a given period of time there were no virus attacks on the organisation's computer systems (as a result of this policy), the users of the computer systems may believe that the scanning of hard drives for viruses is unnecessary and a waste of valuable time. Underwood (1989, p. 249-250) argues that at this point in the process, and as a result of security being seen as unnecessary, the only logical result will be decay.

To continue the example, as the users feel that scanning for viruses is a waste of time, they may bypass the scanning procedure. This amounts to decay in security as management have a policy and procedure in place to counter the threat, but it is not being complied with as security is now seen as unnecessary because of the lack of threat occurrence (no virus attacks).

Decay is obviously not restricted to computer security efforts. It may also occur in access control procedures, guard patrol procedures, confidential information control procedures, cash handling procedures and all other areas of security operations which are reliant on the compliance by staff.

Decay is now evident, as the users are not scanning for viruses. Then as a result of this decay, a virus successfully penetrates the computer system and all data contained therein is lost. Security will then be seen as necessary again.

With virus penetration (threat occurrence) comes a reaction by management which is often inappropriate, as management did not contribute the cause of the threat occurrence to decay. Management may now insist that integrity checkers, behaviour blockers and disk validation systems be implemented (Ford, 1995, p. 141). This would allow for a significantly higher level of virus protection. But in this circumstance, the measures were suitable and it was the decay of these measures that resulted in the threat materialising. Therefore all that is required is to re - establish and re - emphasis the original virus scanning measures.

The Purpose of the Study

Security managers, consultants and advisors need to be able to refer to conceptual tools when providing advice on complex security issues such as the management of security risk. The greater the number of relevant analytical and management tools available, the more likely it is that the security function can positively contribute towards organisational goals.

The aim and purpose of the thesis was to contribute towards the generation of conceptual tools in the security discipline. This purpose has been accomplished by

enhancing the security decay theory through the testing of perceptions and attitudes of this model.

The Significance of the Study

The security decay theory is one which has received little attention and one must assume this to be because of its relative obscurity. To date, the security decay theory had not been formally studied. While this situation alone may highlight the need for further exploration of a theory, it is believed that the nature of security decay and the potential consequences that may arise from its occurrence warranted it being examined.

Security from an application viewpoint, is a discipline of some importance as people rely on it in all forms for physical well - being, and organisations rely on it for the protection of valuable and critical assets. The further development and refinement of the security discipline therefore will provide innovative and effective ways in ensuring the safety of the community as well as contributing towards the success of an organisation.

Also, as the security discipline continues to develop, theories relating to differing aspects must be explored. This exploration of the security decay theory will contribute towards the goal, as the security discipline will have gained another conceptual tool for analysis.

Research Questions

There are a number of pertinent questions that must be considered before the relevance of the security decay theory can be judged. Upon the completion of this study, the research questions will have been sufficiently addressed, with consideration for limitations and scope of the study.

While the testing of the entire security decay theory is beyond the scope of the study, the questions of the theory that will be addressed include:

- What constitutes effective security and is effective security achievable?

- Does effective security cause an attitude of apathy towards the provision of security?

- Does an apathetic attitude towards the provision of security cause a decaying of security?

For the security decay theory to be evident, security must be functioning so well as to cause people to think that there is no need for it. It is proposed that if security is not effective, then security decay is not the cause of threat occurrence. This outcome warrants the inclusion of the question regarding what constitutes effective security.

An intriguing question of the study is whether or not people believe that effective security will result in apathy. Will people believe that security becomes an unnecessary burden when it has proved so successful as to prevent threat occurrence? When there is no threat occurrence because of successful security, will people become apathetic?

For the decay theory to be considered a relevant theory in the security discipline, it must be shown that apathy towards security will cause security to decay, or decrease in effectiveness. Establishing this effect is beyond the scope of this study and therefore the assessment of peoples' initial perceptions will be an important first step towards making a determination.

CHAPTER 2

LITERATURE REVIEW

The literature review will outline a number of factors that must be considered in a study of security decay. As there have been no previous studies conducted on security decay, the literature review will focus on relevant topics such as risk, security decay, maintenance and decay, complacency and security decay, overconfidence and security decay, and research methodologies.

Risk

Risk is a concept of immense importance from a security viewpoint. It is not possible to implement a security program of any worth without first assessing and considering the security risk. This principle is supported by Sennewald (cited in Broder, 1984, p. 7) who argues that;

> " Before a question of security can be addressed, it is first necessary to identify those harmful events which may befall any given enterprise."

Risk is often used in reference to security issues, but it may be argued that it is never fully understood. Ansell and Wharton (1992, p. 4) state;

> " The origin of the word risk is thought to be either the Arabic word risq or the Latin word risicum... [The Arabic word] has connotations of a fortuitous and favourable outcome... [The Latin word] originally referred to the challenge that a barrier reef presents to a sailor and clearly has connotations of an equally fortuitous but unfavourable event."

Ansell et al. (1992, p 4) believe that in English usage the word has very negative connotation such as " you run the risk of..." or "... at risk." For example, the Australian Oxford Dictionary (1988, p. 401) defines risk as; " [the] possibility of meeting danger or suffering harm..."

Therefore as Ansell et al. (1992, p. 4) state;

> " Clearly over time and in common usage the meaning of the word has changed from one of simply describing any unintended or unexpected outcome, good or bad... to undesirable outcomes and the chance of their occurrence."

One could argue therefore that risk has now taken on a negative form, and this form would seem to be evident in a security context, as security professionals are dealing with risk as an unfavourable occurrence.

Westhuizen (1990, p. 36) however makes reference to both positive and negative risk, in the form of speculative and pure risk. Speculative risk is a risk which will either result in a gain or a loss if the risk is realised; for example, the trading of shares on the

stock market. Pure risk however will, if realised, result in either a loss or a no loss situation. Examples of pure risk include fire, flooding, theft, industrial espionage, sabotage and fraud.

However it is important to note the term, 'if realised'. Blades (1996, p. 1) defines risk as; " the possible occurrence of an undesirable event, or the uncertainty of financial loss." The key words in this definition are "possible occurrence" and "uncertainty".

As Foster (1995/96,72) points out;

> " If there is no uncertainty then knowledge exists. If knowledge about the future exists then we have a deterministic environment - for example: " you will die". This is deterministic - certain. This is not risk; it is a fact. Thus regardless of how you define risk, it must incorporate an element of uncertainty."

Therefore from a security viewpoint, when one refers to risk, one more commonly refers to possible, uncertain occurrences that will cause no financial gain, but some degree of harm. However, and while many security professionals do not appear to be taking advantage of this, it is becoming increasingly important to view security risk in a speculative sense. Dalton (1989) highlights this when he argues that the security function must take on a more competitive, value added role within the organisation, that the 'corporate cop' image be disbanded and security become more economically accountable. Security risk must be viewed as an opportunity to add to the financial performance of the organisation. While the security event itself (theft, fraud or fire)

will not produce an opportunity for financial gain, the implementing of security to negate these risk events will (Jones, 1994, p. 96).

Security's ability to generate profit through the practicing of risk management is appropriately outlined by Toft (1997, p. 89) in Figure 3.

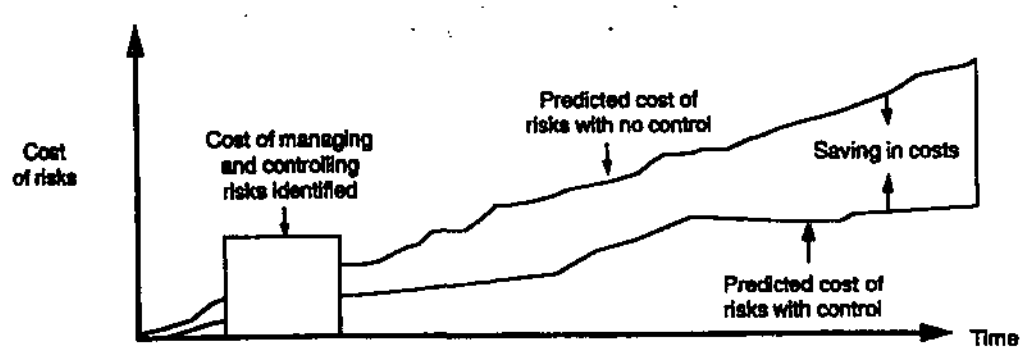

Figure 3: Risk Management's ability to generate profit

The figure 3 shows that by expending resources on the controlling of risk, so long as the cost of the resources combined with the cost of the remaining risk is less than the cost of the original risk, then the provision of security countermeasures will provide for a profit.

The reason why risk itself must be given due consideration is because of the nature and relationship between risk and security. Any security related research must include acknowledgment of the influence risk has upon security. The relationship between risk and security decay is found in the perception of security risk and the assessment and management of risk and decay.

The way in which people perceive their level of risk exposure will influence the decisions they make. Robbins, Waters - Marsh, Cacioppe and Millet (1994, p. 163) define perception as; " a process by which individuals organise and interpret their sensory impressions in order to give meaning to their environment." If the security program in place is effectively reducing the level of risk exposure the organisation faces, the staff and management may perceive their environment as having no security risk present. This perception may lead to apathy.

Pidgeon, Hood, Jones, Turner and Gibson (1992, p. 101) upon discussing risk perception argue that there are two types of risk; "dread risk" and "unknown risk". Unknown risk refers to the degree of familiarity towards the risk. If security is effectively reducing risk to such an extent that no threats are occurring, then the risk becomes unknown or unfamiliar and the perception of the risk changes accordingly. In this instance, one may be unfamiliar with the risk and therefore one could argue, perceiving that there is no present danger. This perception of the risk may again lead to apathy.

Tversky and Kahneman (1982) outline another factor influencing the perception of risk and therefore the degree of apathy that a person may have. This factor is known as the "availability heuristic" (Tversky et al. 1982, p. 18). The word heuristic simply refers to a judgmental rule (Slovic, Fischhoff and Lichtenstein, 1982, p. 464), with heuristics ultimately being used to simplify complex mental tasks. The availability heuristic refers to a situation where an event which has happened more recently, or on numerous occasions, will be more mentally available to a person. In - effect events

(including security events) that are more easily recalled by a person will be considered more often than events, which are not, even to a point where events that are not easily recalled are ignored.

In the decay context, a lack of security incidents will result in the person having a 'low level of availability'; they will not recall security incidents and therefore not consider them. This may result in the person giving little consideration to security and effectively becoming apathetic towards it.

The elements of cultural theory, as outlined by Wartofsky (1986), will be another factor influencing the way in which a person perceives risk. Wartofsky (1986) argues that peoples' cultural surroundings will influence them to see risk in a certain manner. Cultural influences are derived from the value system within which the person resides and values, one can argue, are "socially constituted, socially learned and socially enforced" (Wartofsky, 1986, p. 131). The culture within the organisation may be one in which the need to comply with security policy is non - existent. The organisation may have a very weak security culture which will influence the degree of apathy towards the provision of security.

The security professional must practice risk management in an organisation. The Australian / New Zealand Standard on Risk Management (AS 4360:1995) defines risk management as the;

> "... systematic application of management policies, procedures and practices to the tasks of identifying, analysing, assessing, treating and monitoring risk."

Without practicing risk management, it will be unknown as to whether the cause of security incidence is due to security decay, unsuitable security countermeasures, a changing threat environment and so on. This is because a reactive approach to security will see decisions made without analysis. If risk management is practiced, all variables will be assessed. If risk management is practiced and decay is attributable, then the resulting management decision will be more appropriate and less costly.

The accuracy of the risk analysis is also an issue. As Broder (1984, p. 2) states;

> " [risk analysis] ... is a method for estimating the anticipated or expected loss from the occurrence of some adverse event. The key word here is estimating, because risk analysis will never be an exact science."

As a result of risk analysis being at best an estimation of the condition, one must always be wary of the results.

The risk management process consists of completing a risk analysis and then projecting the level of protection on the risk analysis results. However if this level of protection turned out to be higher than needed, the effect between the next review may be a decay of security countermeasures. The reason for this is because an over emphasis of security will only cause security to be seen as unnecessary.

Therefore a delicate balance must be struck between the minimal and maximum security countermeasures needed. Too little security may result in high risk materialisation, while too much security may result in decay leading to risk materialisation.

Broder (1984, p. 41) correctly states that one step in the risk management process is the conducting of a security survey. One of the aims of the security survey is to determine the vulnerabilities that exist within the organisation. Fites and Kratz (1993, p. 53) describe a vulnerability as a security weakness which does not in itself cause damage but is a condition that will aid threat occurrence. Security decay is an example of a vulnerability. Security decay will provide a condition that will aid threat occurrence, as although security measures are in place, they are no longer operating to their intended level of effectiveness.

Security Decay Literature

As has been stated, the security decay term was first used by Underwood (1989) in his book "The Security of Buildings." The following reference to security decay is the most prominent. Underwood (1989, p. 249) states that;

> " The provision of effective security is paradoxically, the first step towards decay. This is because the effective system will not only repel successful attacks, but will also prevent the attacks being made; the illusion is thus created that the security is unnecessary and decay will follow until the degree

> of security falls to the point at which the attack succeeds. In such cases the immediate reaction is often to increase the original security measures established, but in fact this is not usually necessary and all that may be required is the re - establishment of the intended level of protection."

Apart from Underwood's (1989) reference to decay, although the remaining literature does not specifically discuss the concept of security decay, there is literature on decay with reference to maintenance and on other factors which may lead to an erosion of security such as complacency and overconfidence.

Maintenance and Decay

The principle of decay has been proposed by Howlett (1995) upon presenting a paper on maintenance issues with regards to security systems to the 1995 International Carnahan Conference on Security Technology. Howlett (1995, p. 223) argues that maintenance should not be left for too long a period as the system will deteriorate to an unacceptable level. Howlett (1995) illustrates this maintenance issue in Figure 4.

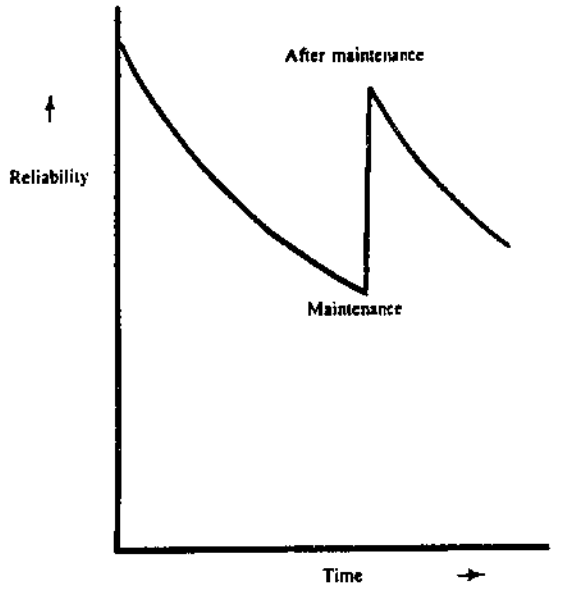

Figure 4 : Maintenance and Decay

The figure 5 below has been adapted from the previous diagram from Howlett (1995) to include security terminology which presents the security decay theory in graphical format.

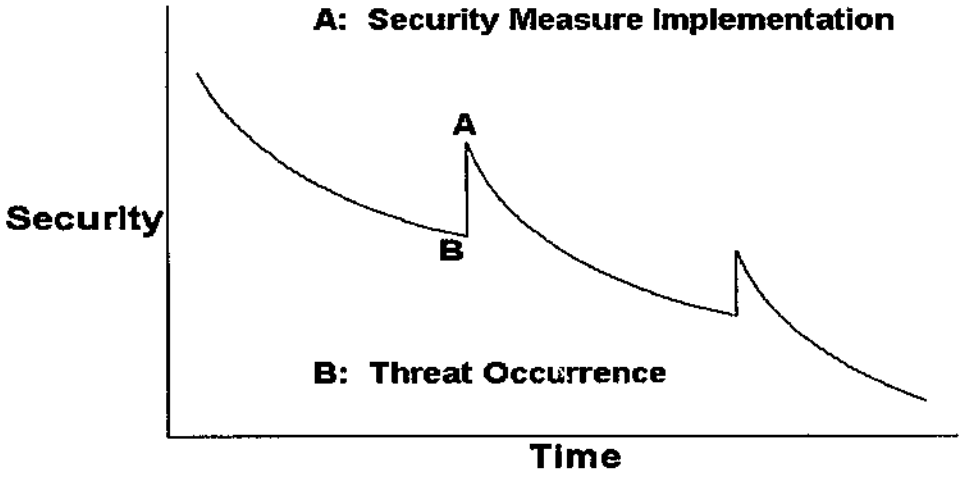

Figure 5 : Security decay in graphical format

Security Decay and Complacency

In regards to complacency, Nossiter (1993, pp. 1 - 6) stated in an interview with a prominent security consultant that; "There's danger in complacency about the possible threats from terrorists at the 2000 Olympic Games..." Adams (1996, p. 40 - 41) stated, in an article on Qantas and security, that; " Australia's official terrorist threat to airports and airliners is currently low, but there's no room for complacency..." Also Gips (1996, p. 51) upon discussing security issues within CNN stated that; "... the bureau has recently switched guard service companies because the officers were becoming too familiar with personnel and too complacent..."

While it is important for security professionals to be aware of complacency, it must be stressed that there is a difference between complacency and security decay. Complacency can result when security measures are both poor or adequate, security decay on the other hand, can only occur when security is effective as it is the effectiveness of security that is postulated to cause decay. Security decay is to be viewed in a specific, theoretical context.

Overconfidence and Security Decay

Purpura (1991, p. 123) in discussing how a person was able to penetrate White House security stated that;

> " Did the Secret Service believe its protection measures were impenetrable? Perhaps this thinking allowed security to defeat itself. Indeed a false sense of

> security can leave an organisation open to serious and unexpected vulnerabilities. Security practitioners can develop a feeling of invulnerability and overconfidence in their actions and plans."

If personnel within the organisation become over confident with the effectiveness of the implemented security countermeasures, they are indeed likely to become apathetic. While over confidence may result in an erosion or decaying of security, this effect is different from that which is postulated in the security decay theory. The security decay theory is specifically concerned with the effect an effective security program has on the behaviour of personnel towards it. It is postulated by the theory that apathy is a result of effective security preventing threat occurrence.

Methodology Literature

In the conducting of a research study, it is important to draw upon literature relating to various methodological issues one may encounter.

The study focused upon collecting and analysing peoples attitudes to selected elements of the security decay theory. Therefore, the method used must be one which is suitable for the measurement of attitudes.

Likert tests

It has been stated by Keats (1988, p. 258) that attitude measurement began with the development of scale values by Thurstone who discovered that by using scale measurements, it was possible to collect both negative and positive attitudes on a particular subject. Following Thurstones' work, Likert proposed that;

> " the methods which had been previously been developed for constructing objective tests of cognitive abilities could be applied to the construction and use of scales for measuring attitudes" (Keats, 1988, p. 258).

Dane (1990, p. 272) defines the Likert scale in the following manner;

> " The Likert scale consists of items reflecting extreme positions on a continuum, items with which people are likely to either agree or disagree."

The development and administration of Likert tests has been discussed by many authors (Keats, 1988, p. 258; Anderson, 1988, p. 427; Lin, 1976, p. 183; Best, 1981, p. 181; Payne, 1974, p. 189; Lewin, 1979, p. 159; Dane, 1990, p. 272; Thorndike and Hagen, 1969, p. 414; Bordens and Abbott, 1988, p. 174; and Hopkins, Stanley and Hopkins, 1990, p. 293). These authors argue that by using a Likert scale, one can generate quantitative data on attitudes. This is achieved by constructing a set of both positive and negative statements and then directing the respondent to endorse the statement based on a given set of response options, typically strongly agree, agree, not

sure, disagree and strongly disagree. Depending on either the favourable or unfavourable position of the statement (either positive or negative) a numerical value is given. For example, responses marked strongly agree may be scaled with a value of five and progressively scaled to a score of one for strongly disagree. These quantitative data can then be used to estimate the attitudes of the respondents.

Likert scales are not without disadvantages. Lewin (1979) highlights one problem by arguing that the response options may mean different things to different respondents. Lewin (1979, p. 163) states that " what does strongly approve as used in the Likert scale mean to Fred, as compared with what it means to Jack or Betty." For example, strongly approve to one respondent may lean more towards approve than it does for another who may indeed strongly approve of the statement.

Another disadvantage of the Likert scale, as outlined by Lin (1976, p. 185) is that it does not give the respondents the opportunity to express the degree of intensity to which they feel they either agree or disagree. The Likert scale assumes that all responses given are done so with the same intensity. There is also the possibility, as Best (1981, p. 185) outlines, that people will mark the response option they think should be marked instead of that which they really believe.

Thorndike et al. (1988, p. 415) argue that a very significant problem with attitude scales is that "they operate purely on a verbal level. The individual doesn't do anything to back up his stated attitude."

While the Likert scale method does have disadvantages, there are a number of advantages in using such a scale. Lin (1976, p. 183) states that the Likert test method is general enough to be applied to a wide range of variables, therefore being suitable for the study. Dane (1990, p. 272) indicates that using a Likert scale is significantly less labour intensive and time consuming. Payne (1974, p. 189) argues that the attraction to the Likert scale is because it is less complex than other methods, but as Lewin (1979, p. 159) points out, the results derived from a Likert scale are just as accurate. This is because Likert himself completed the same study using both the Thurstone and Likert methods and produced identical results.

In developing a Likert test, Anderson (1988, p. 427) and Lin (1976, p. 184-185) believe that the following steps should be undertaken;

(a) Construct statements which are both favourable and unfavourable.

(b) Judges from a sample of the population going to test are used to determine whether the statements are favourable, unfavourable or neither.

(c) Those statements not classified by the majority of the judges as either favourable or unfavourable are eliminated.

(d) Remaining statements are presented in random order.

(e) This initial version of the test is administered to a sample population.

(f) The correlation between the total scores and the individual statements are computed.

(g) Each statement whose correlation with the total score is not statistically significant may be eliminated. This procedure is referred to as Likert's criterion of internal consistency.

(h) The final version of the test is prepared.

These steps are included as they are necessary for the Likert test to be constructed correctly, in order for the best possible results to be achieved.

Sampling

Best (1981, p. 8) points out that the study of an entire population is impractical, if not impossible. Lin (1976, p. 146) states that a population is "... the total group of cases which conform to certain designated set of specifications. In this case the populations involved are professional security people and people with no security expertise. As it is not possible to study the entire population, samples of the population must be used. A sample is a "... small proportion of a population selected for observation and analysis" (Best, 1981, p.8).

As it is not the intention of the study to generalise with regards to the security decay theory across both the expert and non - expert security population, then nonprobability sample methods were judged sufficient.

Lin (1976, p. 157) states that nonprobability sampling methods are suitable when generalisations of results across a population are not required. It is highlighted by Lin (1976, p. 157) and Best (1981, p. 13) that nonprobability sampling methods will not produce results that can be attributable across the population, but will provide results that can only be generalised across the specific sample group. Lin (1976, p. 187) states that;

> "Nonprobability samples may be useful in providing the researcher with insight or a general idea of what is happening in the population, but they are not scientific reflections of the population itself."

Lin (1976, p. 157) presents a number of nonprobability sampling methods of which "Purposive Sampling" was believed to be the most appropriate for the study.

Lin (1976, p. 158) describes the purposive sampling method as one which; " ... involves the use of judgement on the part of the researcher. He forms his sample by selecting cases he thinks are representative of the population."
Purposive sampling is believed to be a viable sampling method when the boundaries of the population under examination are impossible to define and when time and facilities available are limited (Lin, 1976, p. 158).

In regards to sample size, it is argued by Lewin, (1979, p. 188) that a smaller population can be represented by a small sample, and that even though a population size may increase, the increase in the requisite sample size is not proportional. The population for this study is small, therefore a small sample size is sufficient.

Validity

Hopkins et al. (1990), Zeller (1988), Payne (1974) and Lewin (1979) all state that validity is a concept that relates to whether or not the study conducted actually measures what it intended to measure. For example, Lewin (1979) argues that; " A measure is valid if it really measures what it is supposed to measure." Shaughnessy and Zechmeister (1985, p. 15) point out that "... validity refers to the truthfulness of a measure. A valid measure is one that measures what it claims to measure."

Lewin (1979, p. 78) argues that one way of determining validity is by "face validity." Face validity refers to the self-evident nature of the validity of the test and may be gained through expert scrutineering of the test.

Reliability

Reliability refers to the consistency of the test. Lin (1976, p. 168) states that a measure will be reliable if it generates similar responses on every subsequent usage. Lewin (1979, p. 77) describes reliability as the extent to which the method of measurement produces the same results under the same conditions.

When discussing validity and reliability, one important point must be noted, a test method can be reliable, but not necessarily valid (Hopkins et al. 1990, p. 113; and Shaughnessy & Zechmeister, 1985, p. 15). An example to illustrate this point is given by Shaughnessy et al. (1985, p. 15) when they state that;

> " ... subjects whose intelligence was being tested might be able to perform consistently (reliably) on a balancing task, but there is serious questions about the validity of this measure of intelligence."

CHAPTER 3

The Study

To thoroughly examine the concept of security decay, one would be required to conduct a longitudinal study which can be defined as the " ... examining of a population over a prolonged period of time" (Payne, 1974, p. 201). Such a longitudinal study could take the form of a researcher located within an organisation for a prolonged period of time and constantly assessing the effectiveness of security, degrees of apathy towards its provision and the effect that this has on the operational effectiveness of security. However, this investigation does not permit a longitudinal study, therefore the gathering and assessment of the attitudes to specific aspects of the security decay theory were sought.

Sample and Subject Selection

The attitudes of two distinct samples were sought which include professional security specialists and non - security persons. This stratification of sample was required as the non - security person's represent those that are instructed, influenced and operate within the security guidelines. It is the non - security persons that will, if at all, become apathetic towards security. Therefore, the test concerned with whether or not effective security causes apathy will be directed at this sample.

It must be assumed that the security specialist will have an understanding of the security decay concept, how effective security functions and whether apathy will cause security to decay. This is because it is the security specialist who construct the security programs and monitor their effectiveness.

It was believed that for the study, the nonprobability purposive sampling method would suffice. The population of what one may call a "security specialist" is ambiguous. There are people operating within the security field whose claim to expert status is not without some concern. There are people whose occupation requires them to conduct security, as well as other tasks and it is assumed that these people are not security specialists. With regards to non - security personnel, how does one define this population? As has already been stated, the security specialist population is ambiguous, so where is the line drawn discriminating the security expert from the ignorant?

For the purposes of the study, a non - security person was defined as someone who has no direct responsibility for security and who is influenced or 'controlled' by security policy and procedure during the course of their daily routine business activities.

The security specialist population consisted of those persons who have a direct responsibility for security, either in a managerial, consultative or advisory role. Formal security training and education was not a prerequisite where considerable experience was evident.

The purposive sampling method was used in the study, as it was believed that cases could be chosen from the population that would provide for an appropriate sample. As a result of this sampling method being used, it will not be argued that the attitudes evaluated will reflect those of the wider security and non - security populations.

A security specialist sample size of around fifteen was deemed achievable and a similar non - security sample was also sought.

Instrumentation

The instrument used to assess the attitudes and perceptions from which interpretation could be made was in the form of a Likert test. Three Likert tests were constructed and administered to the specified sample groups where each test, Test 1 part A and B (Appendix A and B) and Test 2 (Appendix C) related to the three research questions. A positive or negative position (relative to the decay theory) was taken with each statement, with positive and negative statements being presented in a random order. A negative statement was one, which was in contradiction with the theory, and a positive statement was one, which was aligned with the theory. The negative or positive polarities of these statements will determine the numerical ratings for each item.

The response options of strongly agree, agree, not sure, disagree and strongly disagree were utilised. The number scale ranged from 5 - 1 (on a positively framed statement) and from 1 - 5 (on a negatively framed statement). For example, if the statement was positive, then strongly agree would equal 5, agree would equal 4, not sure would equal

3 and so on. Therefore, the higher the numerical value, the more the attitude is one of agreement.

Procedure

The three Likert tests were developed so that a pilot study could be conducted. Upon completing the construction of the Likert tests (before they were distributed to the pilot sample), validity of the tests was evaluated.

Validity of the Likert test statements was examined through the face validity method. Associate Professor Cliff Smith conducted the examination and came to the conclusion that the tests would satisfactorily fulfil their functional requirements and had face validity for their proposed function and application (Appendix D).

Upon completing the validation process, the pilot study was then conducted.

Pilot Study

The Security Specialist Test (Test 1) Part A consisted of 47 statements and Part B consisted of 12 statements. These two tests were completed by three people from the security specialist sample.

The Security Effectiveness Test (Test 2) consisted of 17 statements. This test was completed by three people who matched the description of non - security people.

As a result of the low number of respondents completing the pilot study, the ability to accurately assess each statement was reduced. However those statements which did not appear to be consistent were identifiable. This was achieved by summing the total score for each statement, and those statements with a score which was extremely dissimilar to the others was eliminated.

Also, those statements eliciting a variety of responses (for example, responses of both strongly agree and strongly disagree), it will be argued in the majority of cases, could be justifiably included in the final test version. A small number of statements elicited varying responses and were eliminated as a result of this scrutiny.

A discussion of the pilot study results will be presented, with the results of the pilot study in Appendix E.

Security Specialist Test - Test 1 (Part A)

Test 1 (Part A) was developed to attempt to evaluate what may constitute an effective security program.

Below is an outline of those statements which warranted further analysis before they were either eliminated or used in the final test version. Those statements that did not warrant further analysis will not be discussed.

Statement 3 : The responses to this statement were extreme enough to warrant further analysis. However a re - wording of the statement would modify it to a point that would justify its inclusion in the final version of the test. The statement included the word *vital*; that a certain function is 'vital' to effective security. A response of disagree was brought about because of the strong nature of this word. The word 'vital' was changed to the word 'important'.

Statement 7 : Although there was a variation in response options chosen (two SD, one A), this statement was included in the final test version as it was thought that the statement was misinterpreted in the pilot study. However, the statement was re - phrased to provide clarity of intent to the test subjects.

Statement 9 : There was a variation in response options chosen for this statement due to a misinterpretation. The statement was re - phrased to provide clarity.

Statement 10 : This statement was thought to be misinterpreted. The statement was fairly long and as a result, was re - phrased.

Statement 16 : This statement was classified as a positive statement which elicited all negative responses. This resulted in an inconsistent statement score and was therefore removed from the final test version.

Statement 18 : This statement elicited responses of agree, disagree and not sure. However instead of eliminating it from the final test version, it was presented as two separate statements.

Statement 19 : This statement was misinterpreted and subsequently resulted in a modification of the statement.

Statement 26 : This statement was also misinterpreted. However this statement was necessary in ensuring that the aim of the test was achieved.

Statement 33 : Although three different response options were chosen, (with two leaning towards agreement), and because of the small number of pilot study participants, it was thought that such a circumstance should result in the statement being included in the final test version.

Statement 35 : Although one response option was Not Sure (NS), the others indicated a degree of agreement. For this reason the statement was included in the final test version.

Statement 42 : This statement was misinterpreted but the subject matter of this statement was needed to be included. This resulted in the statement being re - phrased and included in the final test version.

Statement 47 : The responses indicated that this statement was poorly constructed. Although it was included in the final test, extensive modification was undertaken to alleviate respondent's difficulties.

Security Effectiveness Test - Test 2

Test 2 was developed in order to examine whether the respondents thought that effective security was achievable, that this state of security would cause a lack of security incidence, and that an environment lacking in security breaches would cause decay.

Statement 3 : This statement was designed with positive polarity. However it elicited negative responses. This made it inconsistent and resulted in its removal for the final version of the test.

Statement 7 : Although this statement elicited varying responses, this statement is of considerable importance to the study. The statement is concise and modification will bring about no benefit. For this reason, the statement was included in the final version of the test.

Statement 12 : This statement was inconsistent as a result of its positive construction and negative response, and was therefore eliminated.

Security Specialist Test - Test 1 (Part B)

This test was developed in order to assess the security specialist respondent's perceptions towards whether or not apathetic attitudes to security would cause security to decay, or reduce in effectiveness.

Statement 2 : This statement was misinterpreted but because of its critical importance to the study, it was included in the final test version.

As a result of the pilot study, there were three omissions of statements with statement 16 in the Security Specialists Test - Test 1 part A, and statements 3 and 12 in The Security Effectiveness Test - Test 2. There were also a number of modifications of statements that were included in the final version of the test.

The pilot study was a valuable facet of the study as it allowed those statements that were unsuitable for whatever reasons, to be evaluated and either modified or eliminated.

Reliability of the Likert tests was addressed through the conducting of the pilot study. The pilot study allowed any inconsistent statements to be omitted. Statements were deemed inconsistent when their total score varied significantly from other statement scores. Upon completion of the pilot study, three statements were omitted as their scores varied significantly.

After the pilot study, the final version tests were developed, with the appropriate modifications made. As the final test versions were being developed, the researcher identified those people who would be suitable and likely to be willing to participate in the study. These people were identified through professional security management societies.

The respondent's chosen were contacted by telephone to determine if they were willing to participate. The majority of participants contacted agreed to participate, and arrangements were made to either visit them at their place of work to complete the tests, or to mail or facsimile the test to them. This procedure required them to return the test through similar means.

The targeted participants were those representing the security specialist sample. In order to collect completed tests from the non - security sample, certain members of the security specialist sample were requested to pass on the Security Effectiveness Test - Test 2, to people within their organisation who had no direct security responsibility, but were influenced by security initiatives. This allowed for easier access to both subjects and ensured that those completing the test were in fact influenced by security initiatives.

With the final version tests completed and returned, the data analysis phase of the study commenced.

Data Analysis

The data were analysed in a four part process, with each of the three individual test results being outlined and interpreted, and then being discussed in relation to the theory as a whole. This four step process resulted from each test addressing one of the variables of the section of the security decay theory under examination. Each variable had to be assessed individually, before being assessed in relation to the theory.
The Security Specialist Test - Test 1 examined the concept of effective security and as such, was divided into specific categories (called sub - concepts) for analysis. This was done as an effective security program will consist of many elements. Effective security may include some aspects and not others, therefore each was highlighted individually.

The Security Effectiveness Test - Test 2 focused on the relationship between effective security and apathy and it too required categorical analysis. The reason why this test was divided into sub - concepts was because each sub - concept had to be present before the other could be attributed. That is, if the respondents did not believe effective security was achievable, then they could not have thought effective security would cause a lack of security incidents.

The third test, the Security Specialist Test - Test 1 Part B was concerned solely on whether or not apathy will cause a reduction in effectiveness and therefore no further categorisation was required.

For each test, and those tests requiring categorical analysis, the summated sub - concept mean score was given, as well as total concept mean scores. This process allowed the prevailing attitude from within the sample population to be considered.

Following the outlining of the study results, analysis and outcome determinations were undertaken which addressed each of the test results and how they related to the security decay theory.

Limitations

A limitation of the study is the inability to generalise outcomes, which is a result of the sampling method utilised. The attitudes assessed in the study will not necessarily reflect those of the broader security and non - security population. This limitation can be overcome by conducting representative random sampling, as well as collecting a larger sample size, which was not feasible for this study. It was deemed sufficient to collect a representative sample, which would provide an indication of the prevailing attitude within both populations.

Another limitation of the study is that it provides no proof that effective security is achievable or that effective security will cause apathy and that apathy will cause decay. That is, there will be no conclusive evidence supporting the hypothesis. To be able to demonstrate evidence of the existence or lack of existence of security decay, a longitudinal study must be undertaken.

Also the Security Specialist Test - Test 1, will not provide a theoretical basis for an evaluation of whether security is effective or not; that is, one could not argue that effective security specifically consists of the concepts under examination in the test. The concepts are present in the test solely because they were included by the researcher, and would not constitute all factors necessary for security to be effective. Add to this the notion that security is a very flexible phenomenon and what may indeed be effective at one facility may not at another. This results from a multitude of factors including facility location, industry type, crime demographics, business operations of neighbouring facilities and so on. Ultimately, each facility will have differing levels of risk exposure, requiring differing levels of security. Therefore, the Security Specialist Test - Test 1 will only provide an indication as to what may be included in an effective security program.

CHAPTER 4

Study Results

The measurement process consisted of three Likert tests. A Likert test (Security Specialist Test - Test 1 part A) was administered to the security specialist sample, addressing the research question, What constitutes effective security? Thus the total concept score for this test relates to what constitutes effective security.

This test was also divided into a number of categories that represent aspects within a security function that may enable security to become, if implemented and implemented correctly, effective. The sub - concepts included;

(a) Management of the Security Function

(b) Awareness / Education

(c) Application of Security Theory

(d) Investigation / Intelligence

(e) Measuring Effectiveness

(f) Legal Aspects

(g) Professionalism of the Security Manager

Each of these sub - concepts were tested, enabling a sub concept score to be determined. This sub - concept score enabled the sub - concept to be analysed, and then assessed in relation to the total concept.

The second Likert test (Security Effectiveness Test - Test 2) was administered to the non - security sample addressing the research question; Does effective security cause an attitude of apathy towards the provision of security? This test was also divided into sub - concepts and included;

(a) Effective security is an achievable state

(b) Effective security causes a lack of security incidence

(c) A lack of security incidence causes apathy

This categorisation was necessary as to gauge the respondents' attitude to this concept, the respondents attitude towards whether effective security is achievable had to be determined, as well as whether or not this causes a lack of security incidents, resulting in apathy.

The third Likert test (Security Specialist Test - Test 1 part B) was also administered to the security specialist sample addressing the research question; Does an apathetic attitude towards the provision of security cause a decaying of security? This research question consisted of the only concept under examination within this test.

Security Specialist Test - Test 1 Part A

The sub - concept and total concept mean scores for the Security Specialist Test - Test 1 Part A are as follows;

Management of the security function	4.23
Awareness / Education	4.53
Application of Security Theory	4.33
Investigation / Intelligence	3.76
Measuring Effectiveness	4.53
Legal Aspects	4.58
Professionalism of the Security Manager	4.18
Total Concept Score	**4.30**

Table 1: Sub - concept and Total concept scores for Security Specialist Test - Test 1 Part A

The 'management of the security function' sub - concept consisted of numerous management issues such as risk management, financial aspects, the management of people, technology and information and the management of the integration of security into the organisation. The mean score (N = 15) for this sub - concept (4.23) resided between agree (numerical value of 4) and strongly agree (numerical value of 5), indicating that the respondents believed that management considerations such as those included are of significant importance.

The 'awareness and education' sub - concept highlighted the importance of educating and communicating the security message. The mean score for this sub - concept (4.53) resided between agree and strongly agree which indicates that awareness and education programs should be included for security to be effective.

The mean score for the 'application of security theory' sub - concept (4.33) resided between agree and strongly agree, indicating that when ensuring security is effective, one should consider applying relevant security theory.

The sub - concept mean score for 'investigation / intelligence' (3.76) resided between not sure (numerical value of 3) and agree (numerical value of 4). This would indicate that the respondents were indecisive as to the importance of these to a security function. This may have resulted from the combining of the two into one concept, as some of the respondents may have thought one was important and the other not so. This may also have resulted from the respondent's personal use of investigations and intelligence, or lack thereof.

The 'measuring effectiveness' sub - concept was concerned with the need to set a measure of effectiveness for security, that security must have a criterion on which to judge its performance. The mean score for this sub - concept (4.53) resided between agree and strongly agree indicating that the respondents agreed with the need to set an effectiveness standard.

The sub - concept mean score for 'legal aspects' (4.58) resided between agree and strongly agree. This would suggest that the respondents agreed with the need to take into consideration legal aspects when providing an effective security function.

The sub - concept 'professionalism of the security manager' was concerned with the levels of integrity a security manager must uphold, including their personal history. The mean score for this sub - concept (4.18) resided between agree and strongly agree, indicating the respondent's agreement with such levels of professionalism

Each sub - concept is to be equally weighted, with no sub - concept being more important than the other. A summated combination of these sub - concepts resulted in the total concept score. The total concept score (4.30) resided between agree and strongly agree indicating that the respondents believe the sub - concepts will be necessary elements of an effective security program.

Security Effectiveness Test - Test 2

The sub - concept and total concept mean scores for the Security Effectiveness Test - Test 2 are as follows;

Effective security is an achievable state	3.92
Effective security causes a lack of security incidence	3.69
A lack of security incidence causes apathy	3.26

Total Concept Score	**3.62**

Table 2: Sub - concept and Total concept scores for Security Effectiveness Test - Test 2

The first sub - concept under examination within this test posed the question; is effective security an achievable state? The mean score (N = 12) for this sub - concept (3.92) resided between not sure and agree, leaning towards agree however. This result would suggest the respondents were indecisive with this sub - concept, however one may argue that they believe, albeit tentatively, that security can reach an effective state.

The sub - concept concerned with whether effective security causes a lack of security incidence resulted in a mean score between not sure and agree (3.69). This would suggest that the respondents were not sure as to whether this would be the case or not.

The third sub - concept within this test focused upon whether the respondents thought that a lack of security incidence causes an attitude of apathy. The mean score for the sub - concept (3.26) resided between not sure and agree. The indication therefore is that the respondents were unsure as to whether an environment where there was little or no threat occurrence would result in one becoming apathetic.

The total concept score (3.62) resided between not sure and agree. The overriding indication is that the respondents were indecisive to this concept. It could be argued that the respondents were either unsure as to whether effective security causes a lack

of security incidence and that a lack of security incidence causes an attitude of apathy. Therefore the respondents did not disagree with these possibilities, nor did they agree, which in effect, provides inconclusive data.

Security Specialist Test - Test 1 Part B

The total concept score for the Security Specialist Test - Test 1 Part B is as follows;

Apathy causes decay	4.31
Total Concept Score	4.31

Table 3 : Total concept scores for Security Specialist Test - Test 1 Part A

There was only one concept under examination within this test. The mean score for the concept (4.31) resided between agree and strongly agree indicating that the respondents believe that an attitude of apathy towards the provision of security will cause security to decay.

CHAPTER 5

Analysis and Interpretations

From the test results presented in the previous chapter, the analysis and interpretations phase will now follow. Each of the three tests and their sub – concepts (where applicable) will be analysed and interpreted, with the aim of providing an indication as to relevance and likelihood of the existence of the security decay theory.

Security Specialist Test - Test 1 Part A

All of the sub - concepts within the Security Specialist Test - Test 1 Part A would appear to be important to a security function striving for effectiveness. Although no weighting was given to the sub - concepts during development and testing, each derived reasonably similar mean scores (except for the investigation / intelligence sub - concept). This result would suggest that the implementing and managing of an effective security function requires the inclusion of many varied elements, providing a synergistic effect.

While this may indeed be true, is one sub - concept more significant than another when providing an effective security function? An assessment of the mean scores shows that the 'legal aspects' sub - concept derived the highest score (4.58) from within the sample, but is this deserving of the highest score? Ensuring compliance with legislation, documenting policy and procedures and reducing the likelihood of

negligence suits are all legal issues which must certainly be addressed, but if one was to state security's core business, would legal compliance be it?

Within the 'management of the security function' sub - concept were issues such as; integrating security's influence into all organisational departments, financial management of the security function, managing the relevance of people, technology and information, and risk management.

The researcher would argue that it is risk management that will 'represent' a security function's core business and therefore, will be of the greatest significance. Although the 'management of the security function' sub - concept derived a lower mean score than others, this could be attributed to the merging of the integration, financial, technology, people and information issues into the sub - concept. In order for the sub - concept to receive a high mean score, all respondents would needed to have strongly agreed with all issues, and one could argue that the greater the number of issues within a sub - concept, the less likely it is that one would agree significantly with it.

The statements within the 'management of the security function' sub - concept concerned directly with risk management produced results, which can be seen in Table 4.

Statement	Mean Score
1.	4.73
2.	4.80
3.	4.67
4.	4.20
5.	4.47
6.	4.47
7.	4.00
9.	4.53
10.	4.00
16.	4.27
17.	3.80
18.	3.67

Table 4: Mean statement scores for statements relating to risk management within the 'management of the security function' sub - concept.

The summated mean score for risk management relevant statements was 4.30. This score resides between agree and strongly agree indicating that the respondents believe that risk management is an important component of effective security. However compared with other sub - concepts, it ranks relatively low. The reason for this would appear to have resulted from the low mean scores for statements 17 and 18.

Statement 17 reads as " a security function which reduces identified threat consequence will be deemed effective" and statement 18 reads as " a security function which reduces identified threat frequency will be deemed effective." There would appear to be indecision as to the importance of reducing threat frequency and consequence from within the sample. The researcher would argue that for security to be effective, threat frequency must be reduced, as well as the consequences of any threat occurrence. It is possible that some of the respondents did not take the

statement at face value; that is, they read more into the statement than was expected. Yes a security program which only reduces threat frequency will not be effective, but the statements were not referring to frequency or consequence in isolation.

The reason why risk management should be the over riding factor in ensuring a security function is effective is because of the role a security function is tasked to perform. Security's role is to reduce the level of risk an organisation is exposed to, via numerous methods, to a level which the organisation is willing to accept. The risk management process, which can be argued to include the following components; asset identification, threat identification, vulnerability assessment, risk analysis (threat consequence multiplied by probability), risk treatment options and treatment option implementation and review, will allow the security function to specifically identify those risks which are not acceptable, and effectively and efficiently reduce their probability of occurrence and consequence.

Indeed Elbra (1992) highlights the importance of risk management when outlining the options in which a security function could operate. Elbra (1992, p. 27) argues that there are four basic approaches to security which are;

- to invest all the security devices that are available

- habitually react to the latest scare

- to patch up holes as they appear or;

- to carry out a risk management exercise.

It is obvious that the first three methods alone do not provide for an efficient and effective security program, as Elbra (1992, p. 27) states " ... the result [would] be islands of security in a sea of risk." Only through the practicing of risk management can security expenditure be consumed effectively and efficiently.

Risk management however is not often utilised, or when utilised, is done so incorrectly. Keller (1994, p. 104) in discussing how much security is sufficient within a museum environment, stated that; "... all that security professionals can do is make an educated guess based on experience." However, the practicing of risk management involves more than merely making guesses based on experience. While experience will significantly aid in the accuracy of any assessment and decision making, the results of a risk assessment are derived from statistics, qualitative data such as emerging crime trends and historical reports and the understanding of such issues as cultural influences and heuristical biases.

The practice of risk management however is not without criticism. Toft (1997, p. 85) states that;

> " .... risk management [to some] can be envisaged as being similar to soothsaying and prophecy; in so far as the general idea is to forecast what potential misfortunes the future might hold for the organisation and then try to prevent them from occurring."

The foundation for this criticism lies in the idea that risk management does not deal in the absolute, but in possibilities and likelihoods. Being able to predict the future is indeed a difficult task, and while this criticism does exist, the relevance of risk management to the provision of an effective security function must be argued to reside in the efficiencies it allows.

Risk management will be the management tool on which the security program is planned and developed. While its practice is of ultimate importance, it can only be effective when combined with other factors.

The implementation of the risk management process will result in the security manager being able to report to senior management the level of risk exposure, but how is this level of exposure to be reduced to an acceptable level? The level of risk exposure is reduced by outlining recommended treatment options to senior management, who will proceed to evaluate each and determine which are to be implemented. But what do the treatment options consist of?

The treatment options are exhaustive and consist of any countermeasure or any process modification that will reduce risk consequence and / or probability. Indeed, treatment options can consist of the sub - concepts within the Security Specialist Test - Test 1 Part A.

In recommending treatment options and developing security countermeasure plans, it would appear necessary to apply security theory. This is supported by the 'application

of security theory' sub - concept which derived a high score (4.33). A security theory may provide the manager with a greater insight into the problem, or may allow them to address the problem in a way that has been proven to work in the past. For example, the implementing of various countermeasures giving consideration to the defence in depth principle.

With a risk assessment completed and countermeasures implemented, the security function will not automatically become effective. There will be an ongoing need to 'sell' the security function to the organisation because of personnel turnover and emerging threats (Sennewald, 1985, p. 241). Also, and as Sennewald (1985, p. 241) states;

> " Employees at all levels of the organisation must first be made aware of, then understand, and then come to appreciate the fact that the security function is a viable and integral part of the business..."

This can only be achieved through constant awareness programs and education initiatives. The sub - concept relating to this within the Security Specialist Test - Test 1 Part A derived a very high score (4.53), indicating that the respondents agree with the importance of such programs in an effective security function.

Does a security function need to undergo a process of self evaluation to become and / or remain effective? The 'measuring effectiveness' sub - concept derived a very high

score (4.53) indicating that the respondents did indeed believe so. But how does the security function measure effectiveness?

One possible way to measure effectiveness is through benchmarking. O'Leary (1995, p. 25) defines benchmarking as "... the process of continuously measuring and assessing products, services and practices against recognised standards." However the problem faced in benchmarking a security function, is recognising a standard on which to compare. One may be tempted to compare the results of one year with years past, but will this provide a legitimate comparison? The operating environment is so dynamic that the level of risk faced one year may be significantly greater or less from previous years.

The researcher would argue, that in order to measure effectiveness, the security function must first set objectives which are attainable based on the current environment and then, after some determinable period of time, evaluate whether the objectives have been achieved. These objectives may be categorised into financial objectives, levels of satisfaction of security by staff and management and so forth.

Those who are tasked with ensuring the security of the organisation are placed in positions of great trust. Therefore the integrity of the security manager must be of the highest order. Not only that, but the security manager must have a high degree of knowledge and some relevant experience for security to be effective. The security manager must understand the philosophy of security and all its intricacies. Therefore, one could argue that the professionalism of the security manager is of some

importance. For security to be effective, it must be respected by the organisation, and this is likely to be more forth coming if the security manager him / her self is respected. The 'professionalism of the security manager' sub - concept derived a reasonably high score (4.18), suggesting that the respondents agree with this need.

The 'investigation / intelligence' sub - concept provided the most surprising sub - concept mean score (3.76), residing between not sure and agree. There was in effect, two concepts under examination in relation to investigations and intelligence. Firstly, whether they were necessary in effective security programs, and secondly how they related to pro - activeness and reactiveness.

Statements 26 and 42 were concerned with the importance of investigations to an effective security program, deriving mean scores of 3.80 and 3.93. This would suggest that the sample were unsure, although leaning towards agreement.

Statements 43 and 45 were concerned with the importance of security intelligence, deriving mean scores of 4.40 and 4.20, indicating that the respondents do consider intelligence to be of some significance when attempting to achieve a state of effective security.

When combining investigations and intelligence to issues of pro - activeness and reactiveness, the sample were again indecisive. Statement 27 argued that intelligence will provide the necessary proactive element of an effective security program and derived a mean score of 3.60. Statement 35 argued that investigations will provide the

necessary reactive element in an effective security program, deriving a mean score of just 2.60, which resides between disagree (2) and not sure (3).

The researcher believes that it is the wording of statement 35 which resulted in the low sub - concept mean score. It would be argued that investigations provide 'a' reactive element in a security program, not 'the' reactive element. It is believed that the respondents read the statement correctly, but that is was poorly worded and not discovered in the pilot study.

The researcher would argue that for security to be effective, it must provide both proactive and reactive capabilities. An inherent concept of the defence in depth principle is redundancy. In order to provide sufficient redundancy, the security function must be able to both prevent risk materialisation as well as reacting to it. As the elimination of security risk is unattainable, we provide infrastructures that will manage the crisis. Also, often upon risk materialisation, an investigation is commissioned to determine the how and the why, and recommend ways to prevent the event from occurring in the future. These capabilities are examples of reactionary elements of a security function.

The most effective way of being proactive is to forward plan, to recognise events that may occur and develop ways in which to either prevent their frequency and / or consequence. In order to forward plan, information must be collected and evaluated. Information which has been evaluated is known as intelligence and intelligence is an important security tool because of the influence it has over planning and decision

making. Indeed "intelligence deals with all things which should be known in advance of initiating a course of action" (Eells and Nehemkis, 1984, p. 48). Intelligence will provide the security manager with the information needed to make the most timely and relevant recommendations to senior management, before an event occurs.

Therefore, should the security function strive for both reactive and proactive elements, the researcher would argue that investigation and intelligence capabilities would fulfil these roles. However, the data fails to support this argument conclusively.

Security Effectiveness Test - Test 2

The results of the Security Effectiveness Test - Test 2 were generally inconclusive, with the three sub - concepts all deriving mean scores between not sure and agree, resulting in a similar total concept mean score (See Table 2).

The first concept put to the non - security sample was whether or not they believed that effective security was an achievable state. To this they responded with a mean score of 3.92 suggesting they were unsure, however leaning towards believing that security could be effective.

So is effective security achievable? The researcher would argue in the affirmative because of the plan that a correctly conducted risk management process will allow one to develop. Such a process allows one to accurately assess threat types, frequencies and consequences and therefore implement countermeasures to negate these. The risk

management process combined with new technologies and traditional management practices all allow security to achieve a state of effectiveness.

The second concept put to the non - security sample was whether they believed that effective security would cause a lack of security incidents. The mean score for this sub - concept was 3.69, again demonstrating some indecision and ignorance from this sample. It was argued previously that effective security will result when numerous factors are integrated with the practicing of risk management in order for threat occurrences to be reduced in both frequency and consequence. Therefore, if security is effective, a reduction in incidents (frequency) will result.

The final sub - concept put to the non - security sample was whether a lack of security incidents causes an attitude of apathy towards the provision of security. This sub - concept derived a mean score of 3.26, suggesting that the respondents were not sure if this situation would arise or not.

There were a number of ways in which the statements were put to the respondents within this sub - concept. Some of the statements were directed at the respondents themselves, and were then combined with concepts of perceptions of unnecessariness towards security and experiences of security incidents.

Statements 4 and 8 were directed at the respondents themselves and stated (with different polarities) that when the respondents perceive security as unnecessary, they do not follow security policy and procedure. Both of these statements resulted in mean

scores of 2.42, indicating that they disagree with this. Therefore, the respondents believe that even though they may perceive security as unnecessary, they still comply will all procedures. Whether or not this would be reflective of the wider population is indeterminable.

The statements directed at the respondents themselves which dealt with the influence a lack of security breaches experienced, had over their degree of apathy (statements 12 and 15) resulted in mean scores of 3.58 and 3.67. These mean scores suggest that the respondents were indecisive as to whether or not their experiences of security breaches influenced their degree of apathy. That is, the respondents could not decide whether or not circumstances where they do not experience security breaches resulted in them feeling apathetic towards security. The data from within the sample is therefore inconclusive.

The researcher would argue however that if one does not experience a security incident and is surrounded with security procedures, one would be likely to consider the security irrelevant, thereby becoming apathetic. The theory and the researcher's opinion are by no means arguing that this is the proper way to view security. The fact that no incidents are occurring is because of the existence of security and it therefore should be maintained. However the non - security people do not comprehend this (in theory), making it the task of the security function to highlight and re - enforce the need for security.

Security Specialist Test - Test 1 Part B

There was only one concept under examination within this test. This concept was concerned with whether or not apathy would cause a decaying or an erosion of security effectiveness. The summated mean score for this concept was 4.31, indicating that the respondents did indeed believe that apathetic attitudes towards security, by people within an organisation, would cause security to decay.

This concept is primarily concerned with the issues of compliance and the reliance of security initiatives on organisational personnel. Staff compliance with security procedure is of paramount importance to a security function and one could argue that without it, security will decay. This process is because of the nature of security itself.

A security function can only identify risks, develop plans to counter the risk, implement the plan and review effectiveness. The security function can only provide a guide, recommending ways to achieve a secure state. The security function may indeed be able to force its message in other environments such as prisons and the military, but generally not within the private sector.

It is the staff who require access to company spaces, it is the staff who handle monies or valuable product and it is the staff who are trusted with confidential information. In effect, all staff are empowered with the responsibility of being company security officers. For security to be effective, it must be a collaborative effort between those

who are responsible for guiding the security function, the security manager and subordinates, and those who must provide the actual security, the staff.

If the staff perceive security as irrelevant, the collaborative effort is broken, the security function will in effect be rendered inoperable, and security may decay.

Analysis Summary

To summarize the results, one could argue that effective security will be created through a synergistic combination of many elements including, but not limited to, those contained in the Security Specialist Test - Test 1 Part A. The elements to an effective security function will be application specific, with the over riding element of an effective security program being the risk management process as this will represent a security functions core business. With elements identified and implemented, one can argue that effective security is achievable.

The data from the non - security sample regarding whether they believe effective security will cause apathy was inconclusive. Therefore, one can not rule out such an effect, nor attribute apathy to effective security. The study can make no generalisable determination regarding this concept.

The security specialist respondents believed that apathetic attitudes towards security would cause security to decay. This would provide a fairly strong indication with

regards to this concept, however and again, no generalisable determination can be made.

The likelihood and relevance of the security decay theory can be viewed in an assessment of the component variables.

Is an organisation likely to be able to achieve a state of effective security? Through the practicing of risk management and with the implementation of various countermeasure strategies an organsiation will indeed be able to achieve a state of effective security.

Does a state of effective security cause apathy through the prevention of security breaches? The results of this study do not allow for a conclusive determination, however one may argue that this is indeed likely because effective security will reduce risk materialisation. With no risk materialisation and combined with factors such as risk perception, heuristical biases and cultural influences, people may believe that there is no need for such a level of security, which in turn, influences their degree of compliance with security policy and procedure.

Does an attitude of apathy towards the provision of security cause a decaying of security? The indication to be derived from the study was that apathy would indeed cause security effectiveness to decay.

Therefore the researcher would argue that security decay within an organisation is likely and therefore relevant.

CHAPTER 6

Recommendations and Implications

Recommendations

There are a number of recommendations to be made resulting from the study. They are primarily concerned with the further exploration of the security decay theory.

The results of this investigation were reasonably restricted, providing in a number of cases conclusive results which are however un - generalisable, and in other cases, providing generally inconclusive results.

The first recommendation is for the theory as a whole to be scrutinised under a longitudinal study. It is envisaged that such a study would be inherently complex, involving accurate assessments of attitudes towards security and how they may vary over time. Also and in doing this, examining the factors which are influencing these attitudes. If such a study were to be successful, it would provide the security manager with invaluable information which would allow him / her to address the problem at the cause.

The study did not address the security decay theory in its entirety. In further exploration of the theory, the way in which management reacts to threat materialisation needs to be examined. It is postulated that when decay is evident,

management often react with an over emphasis of security. This results because either they are not heeding the advice of the risk assessor, or they are interpreting the risk data incorrectly.

When security decay's, the amount of residual risk may increase, however the original level of risk exposure may or may not change. This is because the implemented countermeasures have reduced the risk exposure to a level that the organisation is willing to accept. That risk which remains is residual risk and when a vulnerability such as decay arises, the countermeasures reduce in effectiveness, therefore causing the amount of residual risk to increase. The level of risk exposure will only change when a factor within the external environment changes, or when the internal vulnerability is so severe as to cause an increase in the level of risk exposure. It is recommended that the reaction to risk materialisation be studied, taking into account the various reasons resulting in a need to react and how that reaction influences both residual risk and risk exposure.

Another recommendation is concerned with the need to develop security theory which is applicable. Gale (1994) in discussing the value added role of security stated that;

> " For while it may be interesting and even thought - provoking to construct an abstract model, managers must be able to use the model in pragmatic contexts and be assured that the results will indeed be beneficial."

The security decay theory is a long way from extending beyond being an abstract model, however this must be the primary goal in conducting further research. The results from this study suggest that at least certain elements of the security decay theory appear to be valid, which will provide a starting block towards the generation of an applicable model.

Implications for Security Specialists

Security managers, consultants and advisers must be aware of the ramifications of having effective security. While effective security is to be the objective, ensuring it remains effective requires constant review. Although there is no firm data to support the hypothesis (the respondents in this study were unsure), it is postulated by the security decay theory that effective security may result in attitudes of apathy towards security. This should be taken into consideration when reacting to threat occurrence. If not, a level of protection could be implemented which is both unnecessary and expensive.

An unexpected implication of the study arises from the inconclusive results derived from the non - security sample. The fact that the respondents from within this sample were unsure as to all sub - concepts highlights the ignorance of security by those people who are not tasked with providing it. The need for continual awareness and education programs becomes apparent as a result of these findings. Awareness and education programs will not only aid in heightening the awareness of security's role, but it should, if carried out correctly, reduce apathy towards security.

CHAPTER 7

Conclusion

The discipline of security lacks formal conceptual tools which can be used by security managers, advisers and consultants when attempting to provide effective security. This is because of security's relative age as a discipline, it is still being developed. Many technological, sociological and psychological theories can be applied to a security function, while other theories such as Defence in Depth and CPTED have been developed with security as a frame of reference.

The aim of the study was to contribute to the security discipline by taking Underwood's (1989) idea of security decay and formalising and exploring it. This was achieved by outlining the security decay theory and in part, testing people's attitude towards it.

The security decay theory is primarily concerned with the influence apathy has on security and how management react to risk materialisation when decay is evident. The study focused on the first of these two components. There are a number of variables within the section of the theory that was under examination which include; effective security, the prevention of threat occurrence, apathy and decay. The variables represent a linear process as presented and each variable must be present before the other can be attributed.

Each of these variables were addressed in one of three Likert tests. The Likert test instrument allows the respondents to indicate their level of agreement with the statement presented to them, and when combining response options chosen with recognised numerical values, one is able to determine their attitude relative to the concept under examination.

A Likert test (Security Specialist Test - Test 1 Part A) was administered to a security specialist sample and addressed the question; What constitutes effective security? A second Likert test (Security Effectiveness Test - Test 2) was administered to non - security people addressing the question; Does effective security cause an attitude of apathy towards the provision of security? A third Likert test (Security Specialist Test - Test 1 Part B) was again administered to the security specialist sample addressing the research question; Does an apathetic attitude towards security result in security decaying?

The two tests administered to the security specialist sample provided results from which some determinations could be made. The Security Specialist Test - Test 1 Part A consisted of a number of sub - concepts which may be included in an effective security function, allowing one to argue that effective security consists of many varied elements, with the over riding factor being the ability to reduce risk exposure to an acceptable level. The Security Specialist Test - Test 1 Part B provided conclusive results, suggesting, but without proving, that apathetic attitudes towards security will result in security decaying

The Security Effectiveness Test - Test 2 which was administered to the non - security sample, produced inconclusive results. This sample proved to be indecisive, neither agreeing nor disagreeing with whether or not effective security will lead to a lack of security incidence and in turn apathy. Therefore no conclusions could be drawn.

The results achieved are only representative of the attitudes of the respondents from within the sample. The two tests that derived conclusive results can not be generalised across the whole security specialist population. This was the major limitation of the investigation.

The recommendations resulting from the study include the need to further research the security decay theory in a longitudinal study, as well as researching the section of the theory which was excluded in this study. A longitudinal study may produce generalisable results which may in fact, lead to the security decay theory being one of theoretical value.

The implications for security specialists are that they need to have an awareness of the ramifications of having effective security. Although some results were inconclusive, it is postulated by the security decay theory that when effective security is achieved, attitudes of apathy towards security are most likely. Also, the fact that the non - security sample were generally unsure about all sub - concepts put to them highlights the need for efficient and effective awareness and education programs.

References

Adams, R. (1996). Airline security: Carrier risk low. Security Australia 17 (6), 40-41.

Anderson, L. W. (1988). Likert Scales. In Keeves, J. P. (Ed). Educational Research, Methodology, and Measurement: An international handbook. Oxford: Pergamon Press

Ansell, J. and Wharton, F. (Eds). (1992). Risk: analysis, assessment and management: Chichester: John Wiley & Sons

Bartol, K. Martin, D. Tein, M. and Matthews, G. (1995). Management; a pacific rim focus: Sydney: McGraw Hill Book Company

Best, J. W. (1981). Research in education. New Jersey: Prentice - Hall

Bintliff, R. (1992). Corporate and industrial security. London: Prentice Hall

Blades, A. J. (1996). Conducting and documenting a security survey. Course notes, Unpublished

Blades, A. J. (1997). The development and application of a security intelligence system to support the security manager as a decision maker. Unpublished Masters Dissertation

Bordens, S. K. and Abbott, B. B. (1988). Research design and methods : a process approach. California: Mayfield Publishing

Broder, J. (1984). Risk analysis and the security survey. Boston: Butterworths

Caelli, W. Longley, D. and Shain, M. (1989). Information security for managers. New York: Stockton Press

Cooper, M. G. (1985). (Ed). Risk: man-made hazards to man. Oxford: Clarendon Press

Crossland, B. Bennett, P. A. Ellis, A. F. Farmer, F. R. Gittus, J. Godfrey, P. S. Hambly, E. C. Kletz, T. A. and Lees, F. P. (1992). Estimating Engineering Risk. In Risk analysis, perception and management. London: The Royal Society

Custance, N. D. E (1996). The use of baseline measures in risk assessment. Proceedings of the 30th Annual 1996 International Carnahan Conference on Security Technology (pp 163 - 166) Lexington: IEEE Inc

Dane, F. C. (1990). Research Method. California: Brooks / Coleman Publishing Company

DePasquale, S. (1989). Use this security masterplan to better minimise risks. Security: the magazine for security decision makers. May, p 42-43

Eells, R. and Nehemkis, P. (1984). Corporate intelligence and espionage; a blue print for executive decision making. New York: MacMillion

Elbra, R. (1992). Computer security handbook. Oxford: NCC Blackwell Ltd

Fay, J. (1993). Encyclopedia of Security Management. Boston: Butterworths - Hienmann

Fischer, J. and Green., G. (1992). Introduction to security. Boston: Butterworths - Heinemann

Fiksel, J and Covello, V. (1986). (Eds). Biotechnology risk assessment; issues and methods for environmental introductions. New York: Pergamon Press

Fites, P. and Kratz, M. (1993). Information system security; a practitioners reference. New York: Van Nostrand Reinhold

Ford, R. (1995). Fending off a virus attack. Security Management. July, p 136-141

Foster, K. (1995/96). Cybernetic Risk Analysis. Interdata Risk Handbook. p 7 2-78

Gips, M. A. (1996). Security anchors CNN. Security Management. September, p 46 - 55

Glen, J. D. (1993). How firms in developing countries manage risk. Washington D. C: International Finance Corporation

Hansen, M. (1992). Counterespionage techniques that work. Security Management. September, p 44 - 52

Hayes, R. (1991). Retail security and loss prevention. Boston: Butterworths - Heinemann

Healy, J. R. and Walsh, T. J. (1996). Protection of Assets Manual. California: Merrit

Hopkins, K. D. Stanley, J. C. and Hopkins, B. R. (1990). Educational and psychological measurement and evaluation. New Jersey: Prentice Hall

Howlett, J. F. (1995). Maintenance: The specifiers influence. Proceedings of the 29th Annual 1995 International Carnahan Conference on Security Technology (pp. 219 - 224). Surrey: IEEE Inc

Jones, R. F. (1994). Security as a profit centre: contributing to the bottom line. Security 5 (2), 89 - 97

Keats, J. A. (1988) Measurement in Educational Research. In Keeves, J. P. (Ed). Educational Research, Methodology, and Measurement: An international handbook. Oxford: Pergamon Press

Keller, S. R. (1994). How much security is enough? Security Management. February, pp. 104 - 103

Kinsman, P. and Tarr, C. J. (1996). The validity of security risk assessment. Proceedings of the 30th Annual 1996 International Carnahan Conference on Security Technology (pp 167-170) Lexington: IEEE Inc

Lewin, M. (1979). Understanding psychological research; the student researcher's handbook. New York: John Wiley and Sons

Lin, N. (1976). Foundations of social research. New York: McGraw Hill Book Company

Nossiter, P. (1993). No room for complacency over games security, says UK expert. Security Australia 13 (5), 1-6.

O'Leary, J. (1995). Benchmarking your security program. Computer Security Journal XI (2), 25 - 34

Oliver, E. and Wilson, J. (1988). Practical security in commerce and industry. Vermont: Gower

Payne, D. A. (1974). The assessment of cognitive learning; cognitive and affective. Lexington: D. C Heath and Company

Pidgeon, N. Hood, C. Jones, D. Turner, B. & Gibson, R. (1992). Risk perception. In Risk analysis, perception and management (pp. 89 - 135). London: The Royal Society

Purpura, P. P. (1991). Too secure to be true? Security management. July, p. 124 - 123

Robbins, S. P. Waters - Marsh, T. Cacioppe, R. and Millet, B. (1994). Organisational behaviour. New York: Prentice Hall

Schultheiss, R. A. (1994). Evaluating Corporate Exposures. Security Management. January, 69-70

Sennewald, C. A. (1985). Effective security management. Boston: Butterworths - Heinemann

Shaughnessy, J. J. and Zechmeister, E. B. (1985). Research methods in psychology. New York: Alfred A. Knopf

Slovic, P. Fischhoff, B. and Lichtenstein, S. (1982). Facts versus fears: understanding perceived risk. Judgement under uncertainty: Heuristics and biases. Cambridge: Cambridge University Press

Standards Australia. AS/NZS 4360 : 1995 Risk Management. Sydney: Standards Australia

Strutt, J. E. and Patrick, J. D. (1995). A risk assessment methodology for security advisers. Proceedings of the 29th Annual 1995 International Carnahan Conference on Security Technology (pp. 225-229). Surrey: IEEE Inc

The Australian Oxford Dictionary. (1988). Melbourne: Herron Publications

Thorndike, R. L. and Hagen, E. (1969). Measurement and evaluation in psychology and education. New York: John Wiley and Sons

Toft, B. (1997). Protecting the Organisation. International Journal of Risk, Security and Crime Prevention 2 (2), 85 - 94

Tversky, A. and Kahneman, D. (1982). Judgement under uncertainty: heuristic's and biases. London: Cambridge University Press

Underwood, G. (1989). The security of buildings. London: Butterworths

Vaughan, E. J. (1982). Fundamentals of risk and insurance. New York: John Wiley and Sons

Vietch, S. Dexter, J. Ross, G. Driscoll, J. and Wats, M. (1995). The 3DIS system. Proceedings of the 29th Annual 1995 International Carnahan Conference on Security Technology (pp. 53 - 58). Surrey: IEEE Inc

Wartofsky, M. (1986). Risk, relativism and rationality. In Covello, V. Menkes, J & Mompower, J (Eds.), Risk evaluation and management (pp. 131 - 139). New York: Plenum Press

Westhuizen van der, J. (1990). Security management. Durban: Butterworths

Zeller, R. A. (1988). Validity. In Keeves, J. P. (Ed). Educational Research, Methodology, and Measurement: An international handbook. Oxford: Pergamon Press

Appendix A

Security Specialist Test - Test 1

Part A

1.	The assessing of threat must be conducted for security to be effective	SA	A	NS	D	SD
2.	The assessing of criticality must be carried out if security is to be effective	SA	A	NS	D	SD
3.	Determining probability of threat occurrence is an important component of a security program	SA	A	NS	D	SD
4.	effective security is achieved when security managers habitually react to incidence without prior analysis	SA	A	NS	D	SD
5.	effective security is achieved with the practicing of risk management which allows the analyst to pre - empt security incidence in both frequency and consequences	SA	A	NS	D	SD
6.	rather than the ability to reduce security risk, security should only be deemed effective when all risk is eliminated	SA	A	NS	D	SD
7.	unless the risk is known in the absolute, money should not be spent on security initiatives	SA	A	NS	D	SD
8.	effective security will be a profit generating operation for the organisation	SA	A	NS	D	SD
9.	for security to be effective, one does not need to consider threat	SA	A	NS	D	SD
10.	The frequency of security threat occurrence need not be assessed for security to be deemed effective	SA	A	NS	D	SD
11.	security will only be effective when it focuses upon the security relevance of people, technology and information	SA	A	NS	D	SD
12.	Generic management processes are irrelevant to the management of a security function	SA	A	NS	D	SD

13.	security can only be effective with company wide support, thereby warranting integration	SA	A	NS	D	SD
14.	in order for security to become effective, it needs to continually communicate its message via awareness and education programs	SA	A	NS	D	SD
15.	effective security will be a financial burden on the organisation	SA	A	NS	D	SD
16.	The assessment of criticality / consequence is not required for a security program to be effective	SA	A	NS	D	SD
17.	a security function which reduces identified threat consequence will be deemed effective	SA	A	NS	D	SD
18.	a security function which reduces identified threat frequency will be deemed effective	SA	A	NS	D	SD
19.	in determining whether or not security is effective, an analysis of its ability to generate profit is not considered	SA	A	NS	D	SD
20.	security is more likely to be effective when it incorporates generic managerial processes	SA	A	NS	D	SD
21.	for security to be effective, the security manager must work towards integrating the security function into all organisational areas	SA	A	NS	D	SD
22.	security can fulfil its aims without the co - operation of company personnel	SA	A	NS	D	SD
23.	security is a distinctly separate function and should exist outside the realm of all other organisational departments	SA	A	NS	D	SD
24.	awareness programs are only one factor that must be established so that security can be effective	SA	A	NS	D	SD
25.	the application of security theory will not influence security effectiveness as security theories are, in the main, irrelevant	SA	A	NS	D	SD

26.	investigations are unimportant when attempting to achieve a state of effective security	SA	A	NS	D	SD
27.	intelligence will provide the necessary proactive element in a security program	SA	A	NS	D	SD
28.	a security function need only be reactive in order to be effective	SA	A	NS	D	SD
29.	the process of self evaluation is unnecessary and is a burden on security	SA	A	NS	D	SD
30.	security programs that implement security theory such as defence in depth and CPTED are more likely to be effective	SA	A	NS	D	SD
31.	no standard of effectiveness need be set for the security function	SA	A	NS	D	SD
32.	security need not be concerned with legal issues	SA	A	NS	D	SD
33.	security can be effective regardless of the security managers knowledge of security	SA	A	NS	D	SD
34.	a security function need only be proactive in order to be effective	SA	A	NS	D	SD
35.	investigations will provide the reactive element in a security program	SA	A	NS	D	SD
36.	the security function must establish a means of determining effectiveness in order to justify expenditure	SA	A	NS	D	SD
37.	the security function must have an understanding of how the relevant laws will influence the way in which operations are conducted	SA	A	NS	D	SD
38.	to ensure security is effective, the security manager and officers must uphold extremely high integrity	SA	A	NS	D	SD
39.	to ensure the organisation is not liable to litigation, the security function should ensure all policies and procedures are formally documented	SA	A	NS	D	SD

40.	security can only be effective if it undergoes a process of self evaluation to determine whether the defined objectives have been met	SA	A	NS	D	SD
41.	continual security awareness and education programs are unnecessary as security can be effective without these programs	SA	A	NS	D	SD
42.	for security to be effective, an investigation capability is necessary	SA	A	NS	D	SD
43.	intelligence is an irrelevant practice in effective security programs	SA	A	NS	D	SD
44.	both reactive and proactive elements are required for security to be effective	SA	A	NS	D	SD
45.	the use of intelligence is a vital component in ensuring security is effective	SA	A	NS	D	SD
46.	security managers must have sufficient knowledge of security in order for security to be effective	SA	A	NS	D	SD
47.	a security manager's integrity has no influence on the effectiveness of security	SA	A	NS	D	SD

Appendix B

Security Specialist Test - Test 1

Part B

1.	the effectiveness of security is dependant on the compliance by staff in following procedures	SA	A	NS	D	SD
2.	security will remain unchanged when procedures and polices are not complied with	SA	A	NS	D	SD
3.	when people become apathetic towards security, security's ability to counter threats diminish	SA	A	NS	D	SD
4.	situations whereby staff perceive security to be unnecessary will cause the level of security effectiveness to decrease	SA	A	NS	D	SD
5.	to ensure effective security, security managers must have staff support for all implemented security policies and procedures	SA	A	NS	D	SD
6.	compliance by staff of the security procedures has no bearing on the effectiveness of security	SA	A	NS	D	SD
7.	security will remain effective when staff become apathetic	SA	A	NS	D	SD
8.	security has decayed when procedures and polices are not complied with	SA	A	NS	D	SD
9.	when staff become apathetic towards security, security will decay	SA	A	NS	D	SD
10.	security managers can reasonably suspect that security will be effective, whether or not the staff support the initiatives implemented	SA	A	NS	D	SD
11.	security's level of effectiveness is in no way effected by the negative perception staff have of security	SA	A	NS	D	SD
12.	security's ability to counter threats will not diminish when people become apathetic towards security	SA	A	NS	D	SD

Appendix C

Security Effectiveness Test - Test 2

1.	effective security is an achievable state	SA	A	NS	D	SD
2.	when security is effective, security risk will be reduced	SA	A	NS	D	SD
3.	threat occurrence is unlikely when security is ineffective	SA	A	NS	D	SD
4.	you do not follow security procedures when you feel they are unnecessary	SA	A	NS	D	SD
5.	effective security is not an achievable state	SA	A	NS	D	SD
6.	effective security will not reduce breaches of security	SA	A	NS	D	SD
7.	a lack of security knowledge results in apathy towards security	SA	A	NS	D	SD
8.	even though security procedures in place seem unnecessary, you still comply with them	SA	A	NS	D	SD
9.	a lack of security knowledge has no bearing on the degree of apathy towards security	SA	A	NS	D	SD
10.	when security is effective, threat occurrence is unlikely	SA	A	NS	D	SD
11.	when one is not aware of the importance of security, one is likely to be apathetic	SA	A	NS	D	SD
12.	when you do not experience security incidents, you become apathetic towards security	SA	A	NS	D	SD
13.	a lack of security incidence will result in one perceiving security to be unnecessary	SA	A	NS	D	SD

14.	when you do not experience security incidents, you remain compliant with all security procedures and policies	SA	A	NS	D	SD
15.	when you do not experience breaches of security, you become complacent towards security	SA	A	NS	D	SD

Appendix D

Face Validity - Security Specialist Evaluation and Effectiveness Tests

The security specialist evaluation test and the security effectiveness test were examined by Clif Smith with the purpose of examining the effectiveness of the instruments to perform the functions outlined by their objectives. The tests are setting out to gain insight into the perceptions of effective security and security decay by experienced security personnel at security management and consultant levels, as well as non security people alike.

The tests are composed of strong statements in several categories to be responded to by a Likert scale. An examination of the tests shows them to be substantial in content and application, and that the tests will most satisfactorily fulfil their functional requirements.

The tests have face validity for the proposed function and applications of the instruments.

Associate Professor Clifton Smith

Appendix E

Pilot Study Raw Data - Security Specialist Test - Test 1 (Part A)

	Statements		SA	A	NS	D	SD
1.	The assessing of threat must be conducted for security to be effective		2	1			
2.	The assessing of criticality must be carried out if security is to be effective		2	1			
3.	Determining probability of threat occurrence is a vital component of a security program		2			1	
4.	effective security is achieved when security managers habitually react to incidence without prior analysis					1	2
5.	effective security is achieved with the practicing of risk management which allows the analyst to pre - empt security incidence in both frequency and consequences		1	2			
6.	rather than the ability to reduce security risk, security should only be deemed effective when all risk is eliminated						3
7.	money should not be spent on security unless the risk is known in the absolute			1			2
8.	effective security will be a profit generating operation for the organisation		2	1			
9.	One need not review threat for security to be effective			1			2
10.	The frequency of security threat occurrence is a factor which need not be assessed for security to be deemed effective		1				2

11.	security will only be effective when it focuses upon the security relevance of people, technology and information		1	2			
12.	Generic management processes are irrelevant to the management of a security function					1	2
13.	security can only be effective with company wide support, thereby warranting integration		3				
14.	in order for security to become effective, it needs to continually communicate its message via awareness and education programs		2	1			
15.	effective security will be a financial burden on the organisation					1	2
16.	effective security is determined by its ability to generate profit					2	1
17.	The assessment of criticality / consequence is not required for a security program to be effective					1	2
18.	a security function which reduces identified threats in both consequence and frequency will be deemed effective		1	1	1		
19.	security's ability to generate profit does not factor into an analysis of whether security is effective		1			2	
20.	security is more likely to be effective when it incorporates generic managerial processes		1	2			

	Statements		SA	A	NS	D	SD
21.	for security to be effective, the security manager must work towards integrating the security function into all organisational areas		3				
22.	security can fulfil its aims without the co - operation of company personnel					1	2
23.	security is a distinctly separate function and should exist outside the realm of all other organisational departments					3	
24.	awareness programs are only one factor that must be established so that security can be effective		1	2			
25.	the application of security theory will not influence security effectiveness as security theories are, in the main, irrelevant						3
26.	investigations are unimportant when attempting to achieve a state of effective security			1			2
27.	intelligence will provide the necessary proactive element in a security program		2	1			
28.	a security function need only be reactive in order to be effective						3
29.	the process of self evaluation is unnecessary and is a burden on security					1	2
30.	security programs that implement security theory such as defence in depth and CPTED are more likely to be effective		2	1			
31.	no standard of effectiveness need be set for the security function						3

	Statements		SA	A	NS	D	SD
32.	security need not be concerned with legal issues					1	2
33.	security can be effective regardless of the security managers knowledge of security				1	1	1
34.	a security function need only be proactive in order to be effective					2	1
35.	investigations will provide the reactive element in a security program		1	1	1		
36.	the security function must establish a means of determining effectiveness in order to justify expenditure		2	1			
37.	the security function must have an understanding of how the relevant laws will influence the way in which operations are conducted		2	1			
38.	to ensure security is effective, the security manager and officers must uphold extremely high integrity		3				
39.	to ensure the organisation is not liable to litigation, the security function should ensure all policies and procedures are formally documented		3				
40.	security can only be effective if it undergoes a process of self evaluation to determine whether the defined objectives have been met		3				
41.	continual security awareness and education programs are unnecessary as security can be effective without these programs					1	2

	Statements		SA	A	NS	D	SD
42.	the use of investigations play an important role in ensuring security is effective		1	1		1	
43.	intelligence is an irrelevant practice in effective security programs						3
44.	both reactive and proactive elements are required for security to be effective		2	1			
45.	the use of intelligence is a vital component in ensuring security is effective		3				
46.	security managers must have sufficient knowledge of security in order for security to be effective		2		1		
47.	the integrity and previous history of the security manager will have no influence on the effectiveness of security			1		1	1

Pilot Study Raw Data - Security Effectiveness Test - Test 2

	Statements		SA	A	NS	D	SD
1.	effective security is an achievable state			3			
2.	when security is effective, security risk will be reduced		1	1	1		
3.	when security is eliminating security risk, the need for security decreases					2	1
4.	threat occurrence is unlikely when security is ineffective					2	1
5.	you do not follow security procedures when you feel they are unnecessary					2	1
6.	effective security is not an achievable state					3	
7.	effective security will not reduce breaches of security			1	1	1	
8.	a lack of security knowledge results in apathy towards security			3			
9.	even though security procedures in place seem unnecessary, you still comply with them			3			
10.	a lack of security knowledge has no bearing on the degree of apathy towards security			1		2	
11.	when security is effective, threat occurrence is unlikely			2	1		
12.	when security is eliminating security risk, security procedures are maintained		2				
13.	when one is not aware of the importance of security, one is likely to be apathetic			3			

	Statements		SA	A	NS	D	SD
14.	when you do not experience security incidents, you become apathetic towards security		1	2			
15.	a lack of security incidence will result in one perceiving security to be unnecessary			3			
16.	when you do not experience security incidents, you remain compliant with all security procedures and policies			2		1	
17.	when you do not experience breaches of security, you become complacent towards security			3			

Pilot Study - Security Specialist Test - Test 1 (Part B)

	Statements		SA	A	NS	D	SD
1.	the effectiveness of security is dependant on the compliance by staff in following procedures			2	1		
2.	security will remain unchanged when procedures and polices are not complied with			1		1	1
3.	when people become apathetic towards security, security's ability to counter threats diminish		3				
4.	situations whereby staff perceive security to be unnecessary will cause the level of security effectiveness to decrease		2	1			
5.	to ensure effective security, security managers must have staff support for all implemented security policies and procedures		2	1			
6.	compliance by staff of the security procedures has no bearing on the effectiveness of security						3
7.	security will remain effective when staff become apathetic					1	2
8.	security has decayed when procedures and polices are not complied with		1	2			
9.	when staff become apathetic towards security, security will decay		3				
10.	security managers can reasonably suspect that security will be effective, whether or not the staff support the initiatives implemented					2	1
11.	security's level of effectiveness is in no way effected by the negative perception staff have of security						3

12.	security's ability to counter threats will not diminish when people become apathetic towards security						3

Appendix F

Security Decay - the erosion of effective security

This study is being conducted in order to fulfil the research component of the Bachelor Of Science (Security) Honours degree at Edith Cowan University. This research is being conducted independently, with the researcher having no affiliations with any organisation or institution.

The study is focusing on a new theory in security called "security decay" and it is hoped that with your participation, an insight will be achieved into the perceived relevance and merit of the theory.

Below you will find some statements about effective security and the relationship between apathetic attitudes towards security and security decay. I would like to know what your feeling is regarding each statement. There are no right or wrong answers so chose the response option you feel is the most appropriate.

Opposite each statement is a response option. Please circle the response option you feel is most appropriate and be sure to answer every statement.

You will remain anonymous, unless you wish to be personally acknowledged for your participation.

Thank you for your assistance

Shawn McClure

Code

SA	Strongly Agree
A	Agree
NS	Not Sure
D	Disagree
SD	Strongly Disagree

Appendix G

Mean Statement Scores

Security Specialist Test - Test 1 (Part A)

Management of the Security Function

Statements	Mean Score
1.	4.73
2.	4.80
3.	4.67
4.	4.20
5.	4.47
6.	4.47
7.	4.00
8.	3.67
9.	4.53
10.	4.00
11.	3.93
12.	4.53
13.	4.67
15.	4.33
16.	4.27
17.	3.80
18.	3.67
19.	3.67
20.	4.27
21.	4.53
22.	4.60
23.	4.40
28.	4.67
34.	4.13
44.	4.40

Awareness / Education

Statements	Mean Score
14.	4.60
24.	4.47
41.	4.53

Application of Security Theory

Statements	Mean Score
25.	4.40
30.	4.27

Investigation / Intelligence

Statements	Mean Score
26.	3.80
27.	3.60
35.	2.60
42.	3.93
43.	4.40
45.	4.20

Determining / Measuring Effectiveness

Statements	Mean Score
29.	4.60
31.	4.73
36.	4.33
40.	4.47

Legal Aspects

Statements	Mean Score
32.	4.67
37.	4.47
39.	4.60

Professionalism of the Security Manager

Statements	Mean Score
33.	3.80
38.	4.53
46.	3.87
47.	4.53

Security Effectiveness Test - Test 2

Effective security is an achievable state

Statements	Mean Score
1.	3.92
5.	3.92

Effective security causes a lack of security incidence

Statements	Mean Score
2.	4.25
3.	3.67
6.	3.67
10.	3.17

A lack of security incidence causes apathy towards security

Statements	Mean Score
4.	2.42
7.	3.92
8.	2.42
9.	3.50
11.	3.83
12.	3.58
13.	3.58
14.	2.50
15.	3.67

Security Specialist Test - Test 1 (Part B)

An attitude of apathy causes decay

Statements	Mean Score
1.	4.33
2.	3.20
3.	4.60
4.	4.53
5.	4.27
6.	4.60
7.	4.47
8.	4.27
9.	4.33
10.	4.27
11.	4.47
12.	4.33