

Maximising the Effectiveness of Information Security Awareness Using Marketing and Psychology Principles

Geordie Stewart

Technical Report
RHUL-MA-2009-02
16th February 2009



Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England

<http://www.rhul.ac.uk/mathematics/techreports>

Maximising the Effectiveness of Information Security Awareness Using Marketing and Psychology Principles

Name: Stewart, Geordie Buchanan

Student Number: 01552745

Supervisor: John Austen



Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

Declaration

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature:

Date:

Acknowledgements

I would like to thank John Austen, Lizzie Coles-Kemp and Angela Sasse. They knew my questions would never be “just two minutes” but gave me the time anyway.

The NR Information Security Team has been invaluable to test ideas especially Richard Paul and Peter Gibbons who read and critiqued far too many drafts.

Thanks also to Paul Lewis for convincing me to try a maths degree.

Finally, thanks to Virginia and William for their patience and understanding.

Abstract

Over the last twenty years, technical controls for information security have advanced and matured considerably. Despite these technical advances, information security breaches still occur on a regular basis. It appears that technical security controls have evolved faster than management controls. Despite efforts at promoting information security awareness there is evidence that human behaviour remains a potential vulnerability in any information security system.

This thesis presents an alternate perspective of the “human problem” and assesses information security awareness as a management control by applying principles of Psychology and Marketing. Psychology and Marketing principles show significant opportunities for a more holistic approach to information security awareness. The methodology identified for Mental Models shows significant promise in mapping existing audience beliefs and attitudes. The use of punishment sanctions is reviewed and reveals an unintended consequence that people have an incentive not to report an information security breach. A case study is presented for an organisation that has used rewards to motivate compliance behaviour instead of relying on fear sanctions.

An analysis of relevant Marketing principles identifies Direct Marketing as a methodology closely aligned with the goals of information security awareness. The importance of audience research, measuring existing attitudes and beliefs and finding quantifiable metrics all have important implications for information security awareness.

Two models were created as part of this thesis. The first one in Chapter Two illustrates the steps involved in achieving a behavioural change and demonstrates the number of potential barriers that need to be considered. The second model in Chapter Five is a scorecard that information security professionals can use to evaluate the extent to which an information security awareness campaign takes into account Psychology and Marketing principles. While both models offer significant opportunities to help refine approaches to information security awareness it will be difficult to quantify the benefit until improvements are made to the way that organisations measure the success of information security awareness.

"I'm watching a DVD the other day. A Horror DVD. Hostel Part One. It's about men being tortured to death in an underground bunker for the pleasure of others...I'm about to watch this film and before I watch it I have to sit through the DVD piracy warning...It's the patronising nature of it. They go: You wouldn't steal a handbag. You wouldn't steal a car. So why would you steal a movie?"

And I'm sitting there going, don't tell me what I would or wouldn't do. You don't know me. I'm drunk at 4 o'clock in the afternoon. In my pants. I'm about to watch women be tortured to death in an underground bunker in eastern Europe and you're telling me I wouldn't nick a poxy handbag? I think you don't know me very well at all sir."

Ed Byrne, Mock the Week

BBC 9th Aug 2008

1. Introduction - The Human Problem	7
1.1. Background.....	7
1.2. Rationale.....	8
1.3. Scope.....	9
1.4. A Question of Effectiveness	9
1.5. Those Unpredictable Humans.....	16
1.6. Motivation.....	18
1.7. Chapter Summary	19
2. Defining the Problem	20
2.1. Definitions	20
2.2. Information Security Policy.....	20
2.3. Information Security Awareness	23
2.4. Effectiveness.....	26
2.5. Chapter Summary	31
3. Psychology and Information Security	32
3.1. Motivation.....	35
3.2. Reward Schedules	41
3.3. Reward / Punishment Asymmetry	42
3.4. Heuristics	43
3.5. Fear.....	45
3.6. Learned Helplessness.....	48
3.7. Risk Perception.....	49
3.8. Risk Communication	52
3.9. Attitudes	58
3.10. Organisational Culture	60
3.11. Risk Compensation.....	62
3.12. Groupthink	64
3.13. Internalisation.....	65
3.14. Chapter Summary	66
4. Marketing and Information Security	67
4.1. Mass Marketing.....	70
4.2. Direct Marketing	71
4.3. Market Research.....	74
4.4. Social Media	76
4.5. Chapter Summary	79
5. Proposed Qualitative Model for Measuring Security Awareness Effectiveness	81
6. Conclusions: Psychology and Marketing Implications for Information Security Awareness	83
7. Appendix A: Sample Information Security Mental Models Questionnaire ...	89
8. Appendix B: Euston Road Warning Signs	93
9. References.....	100

1. Introduction - The Human Problem

1.1. Background

“Human error rather than flawed technology is the root cause of most security breaches” Deloitte Global Security Survey 2005 [DEL-05]

“... the greatest root cause of external breaches continues to be the human factor”
Deloitte Global Security Survey 2007 [DEL-07]

Human behaviour contributing to information security breaches is a serious problem. It appears that the design and implementation of technical security controls has evolved faster than management controls. Despite efforts at promoting information security awareness there is evidence that human behaviour remains a potential vulnerability in any information security system.

Over the last twenty years, technical controls for information security systems have matured considerably. Compared to twenty or even ten years ago there is now an amazing variety of technical security controls:

- Firewalls running on desktops and laptops
- Real time antivirus scanning on networks and computing devices
- Advanced techniques to inspect and control internet traffic
- Local disk encryption

However, given all these technical advances we have not witnessed the extinction of the information security breach. Passwords are written down by humans and put at risk of disclosure. Confidential information is copied to removable media by humans and lost. Sensitive personal data is sent over the internet by humans without using encryption.

1.2. Rationale

One of the ways that organisations attempt to manage information security risk caused by human behaviour is by implementing information security awareness programmes [RC-06], [HR-05]. Information security awareness is a form of management control which is intended to achieve prevention and mitigation. Prevention, in that information security awareness seeks to avoid situations where a security incident is allowed to happen and mitigation, in that information security awareness seeks to limit the impact of an incident when it occurs.

All organisations appear to be at some degree of risk from human interactions with their information systems. Unfortunately, it is hard to consider an information system that does not have a human component. Design, implementation and operation are all part of an information processing lifecycle that is exposed to the “human problem”.

Human vulnerabilities are defined by the Human Vulnerabilities Special Interest Group as:

“Human behaviour that creates a vulnerability in the system, or allows an attacker into the system, or allows an attacker to exploit a vulnerability” [KTN-07].

Opinions [MA-06], [BBJ-04], [PS-07] have been expressed that information security awareness is often ineffective at managing human information security risks. This thesis examines the effectiveness of information security awareness using the disciplines of Psychology and Marketing.

Psychology is a discipline covering cognition and motivation [GR-05] and seeks to improve our understanding of human behaviour.

Marketing is a discipline covering communications and the creation of customer demand [BP-08]. Marketing has the ability to improve communication methods in an information security context.

How humans process and respond to security messages and the methods used to communicate are key ingredients when implementing information security awareness [MA-06]. This thesis will review the implications of Psychology and Marketing in an information security context and make recommendations for improvements.

1.3. Scope

For the purposes of this thesis an “information security policy” is defined as a documented record of an organisation’s intention to control and communicate information security risk [PT-04].

“Awareness” is defined as the process by which an organisation communicates the information security policy to individuals or groups that need to be cognisant of some or all of its contents [LT-05].

These definitions will be expanded further in Chapter Two. The concept of an organisation is deliberately left open to include any situation where owners of an information system need to influence human behaviour. An organisation could be a listed company, a government body or even an internet banking site that needs to educate its users.

1.4. A Question of Effectiveness

If human error remains the primary cause of security breaches, does this mean the current approach to information security awareness campaigns is ineffective or sub-optimal in some way? “Effectiveness” in this context is interpreted as the degree to which a method achieves its objectives. Angus McIlwraith criticised the effectiveness of information security awareness in his publication “Information Security and Employee Behaviour”:

“Information security ‘awareness’ has been promoted for many years as being fundamental to information security practice. In reality, it is something that is often done poorly – so much so that I have seen very limited progress since I started in information security over 20 years ago.” [MA-06]

In light of McIlwraith's comments and the Deloitte survey it appears a problem persists with managing human behaviour, despite the effort organisations may have put into their information security awareness. There could be many possible reasons for this including one or more combinations of the following:

1. **A Lack of Investment:** The first possibility is that organisations have not invested sufficient resources creating and developing information security awareness. This implies that security awareness is effective but has not been funded to an efficient level. "Efficient" in this context is being interpreted as the optimal allocation of resources for maximum benefit – in this case it is an implied under-funding. The lack of investment in information security awareness appears to be a view common to information security professionals [HR-05], [HM-08]. Monique Hogervorst offers an explanation for this apparent lack of funding:

"Information security training and awareness is not recognised as a contributor to security." [HM-08]

There is an apparent contradiction in however in Hogervorst's position. She also states that:

"Security awareness is probably the most significant single defence measure that any company can institute." [HM-08]

If information security and awareness is as beneficial as Hogervorst says it is, then why isn't it more in demand? Presumably when Hogervorst laments the lack of recognition she is referring to the budget holders who are expected to fund information security awareness. Does it make sense to state that information security awareness is so valuable and yet at the same time so under-recognised? This appears to represent an asymmetric perspective of value between security professionals and the budget holders. Why would information security professionals apparently value information security awareness more than those who are asked to fund it? There could be two possible reasons for this:

Does the perception that information security awareness is not a contributor to security stem from a lack of actual value from the activity? This might be the logical conclusion from McIlwraith's observation that information security policy and awareness is "...often done poorly." [MA-06]

Or, is it the case that the benefit of information security awareness is difficult to quantify which contributes to a lack of perceived value? Information security awareness can be performed at a fixed point in time (such as for inductions for new staff [RC-06]) or it can be included as part of an ongoing campaign (such as monthly newsletters [RC-06]), or a combination of the two. If a security event can go unrecognized (either as a success or as a failure), then how practical is it to link the results to a concept as abstract as awareness?

It is also difficult to recognise the value of prevention. Here, McIlwraith notes the problem with justifying spending on a non-event:

"Asking people to invest in security is extremely difficult because the returns are rarely the same as those you would get from a standard cost-benefit analysis of a business opportunity. This is because the returns are uncertain, and the benefits are measured in events that have not happened rather than positive benefits that can be obtained." [MA-06]

McIlwraith is correct that there are significant difficulties in measuring benefits from information security expenditure. However, if budget holders show a reluctance to fund information security awareness it is up to information security professionals to make the value of information security awareness more obvious.

- 2. Lack of Effective Methods:** The second possible explanation for a lack of greater success for information security awareness is that the current approach to managing human behaviour in information systems been ineffective. Not being "effective" in this context means that the method employed has not been optimised to the task being attempted. This is the key point that this thesis attempts to evaluate. If the goal of security awareness is to influence human behaviour then disciplines specialising in the study of

influencing human behaviour such as Psychology and Marketing offer an opportunity to review the effectiveness of information security awareness.

The effectiveness of information security awareness is a topic of significant discussion, very little of it empirical as acknowledged by Jeff Bock-Brown:

“...few studies have attempted to measure the effectiveness of information security awareness training. There is, I suspect, frequently an intuitive assumption made, that raising awareness leads to inevitably to a security-enhancing change in behaviour. The association may not be that simple.”
[BBJ-04]

It seems that there has been limited research into the effectiveness and efficiency of information security awareness. Instead, much of the debate is heavily subjective and based on the assumption that awareness will equal security:

“Raising awareness is the single most effective thing that an information security practitioner can do to make a positive difference to their organization.”
[MA-06]

“The more personnel know about information security and privacy issues, requirements and impacts, the more you will be assured of success with implementing security policy and awareness measures, complying with applicable regulations, and having business success with information security and privacy goals.” [HR-05]

However, in the midst of this enthusiasm for information security awareness, Bock-Brown sounds a note of caution:

“Many authors and organisations emphasise the necessity and importance of good security awareness throughout an organisation. None of these papers encouraging awareness-raising offer empirical evidence that the techniques discussed (largely conventional training) are effective in changing behaviour.”
[BBJ-04]

Bock-Brown raises an important point about the lack of metrics to demonstrate effectiveness. However, the lack of metrics does not stop other authors from making bold claims about information security awareness. Hogervorst states that:

“...information security training and awareness is a very cost effective counter measure to put in place as a protective control against the threats modern organizations face.” [HM-08]

However, Hogervorst does not offer any empirical evidence for this statement beyond her own perspective as an information security trainer.

Another information security practitioner perspective is available from Rebecca Herold:

“For the past 25 or so years that I have been closely involved in information security, security awareness training has been the most valuable yet the most overlooked and under funded mechanism for improving the implementation of information security.” [HR-05]

Herold does not offer any empirical evidence to support her view that information security awareness is the most “valuable” type of security control or what measure this claim could be evaluated by.

Measuring security incidents as a baseline is difficult. Security failures are not always obvious [SB-06]. Arguably, there are more “silent failures” than visible failures and it is not necessarily in the interest of all organisations to report security incidents. For example, organisations with a listed share price have an incentive not to report security incidents because revealing a security breach could damage investor confidence.

Ideally, the decision to implement any security control, technical or managerial, should be on a cost benefits basis [SB-06]. The basic premise being that an expenditure on a security control is justified by a reduction in risk. Layton criticises the lack of metrics as a risk in itself:

“Management is expecting people to act and behave in a manner that supports organizational policies, standards guidelines and procedures. How can management in good faith assume their users will support their policies, if there are no tools in place to measure their user’s acceptance and internalization of their policy messages?” [LT-05]

The problem is that the benefit of information security awareness is difficult to measure. Traditionally, benefits have been inferred by measuring the awareness component through surveys, questionnaires and interviews. The difficulty with this is that it is the change in human behaviour that delivers a benefit to the organisation [MA-06]. The change of awareness is only a prerequisite to behaviour change. The problem with awareness not always corresponding with a change in behaviour is explored in Chapter Three.

Surveys are a traditional method of measuring awareness [RC-06]. However, measuring attitudes and awareness have a poor correlation with behaviour:

“...the relationship between people’s attitudes and their behaviour is less than perfect. An example is our reaction to the invasion of privacy of the rich and famous by the media. When public attitudes about such invasions are surveyed the outcome is very clear – between 70 per cent and 80 per cent say they are against such acts. Yet every newspaper editor knows that sales will rise considerably if they print such material.” [MP-04]

A number of reasons could be behind this apparent inconsistency. Bias can interfere with survey results. Responder bias occurs when the responder answers questions according to their expectations of what the survey taker is looking for. Confirmation bias is where the reviewer looks for evidence to support their expectations. Unfortunately, a number of information security authors [HR-05], [MA-06] still recommend surveys as a primary measure of information security awareness effectiveness.

3. **Limited Cost Benefits:** The third possible explanation for a lack of greater success for information security awareness is that excessive demands are being placed on the users of information systems. An implication of the two

options above is that the expectations for humans are unrealistic. It may be that the level of security awareness that is expected to result from information security awareness activities is not cost efficient given the means that we have to obtain it.

Is the complexity of systems increasing the awareness requirements demanded of information system users? If systems were more intuitive for their users then would they make fewer mistakes? Fewer mistakes leading to information security breaches would mean that less training and awareness was required. This is the view of researchers such as Sasse et al [SA-01b] who have concluded that information security demands on users are excessively complex and helps drive an increasing demand for awareness and training.

It does appear that improving the efficiency of information security awareness offers the opportunity to save costs or reach greater levels of risk reduction. Jeff Bock-Brown notes a relationship between system design and training costs in his review of information security and human factors:

“Understanding how people interact with information security systems can facilitate the reduction of anthropogenic information security costs...” [BBJ-04]

So system design is relevant to the level of information security awareness that is required to operate a system securely. However, the focus of this thesis will be on awareness methods, not calculating the level of awareness required for a given information system.

There appears to be support for all three options having an impact on the success of information security awareness. In theory, these questions could be solved with the analysis of relevant metrics. Unfortunately, there appears to be a lack of methodology to evaluate the effectiveness of information security awareness which will be explored further in Chapter Two.

1.5. Those Unpredictable Humans

“...Mathematics is logical; people are erratic, capricious and barely comprehensible.”

[SB-04]

At the heart of Bruce Schneier’s observation in his book “Secrets and Lies” is the notion of predictability. Mathematical logic is subject to a high degree of prediction, therefore computers operating on mathematical logic are subject to a high degree of prediction. People, characterised as “erratic” and “capricious” are not subject to the same degree of prediction. Yet don’t humans also follow some kind of logic? Logic is an instruction operating within a set of parameters and variables. Do humans also have a similar set of parameters that influence the outcome of an instruction? What would those parameters be for a human with a phobia of spiders? We could call such a phobia “illogical”, but would our perspective as external observers not be entirely subjective?

“Many of the behaviours we don’t want to see happen are in fact predictable, but only if you take the time to understand how people come to make decisions.” [MA-06]

If the parameters of the human system were better understood might some apparently illogical actions start to make sense? What logic does a human follow when deciding to write down a password? What experiences and learning created the process which culminated in the action? As security professionals we can be swift to blame the users. To what extent is this an external perspective which exists because of a failure to understand the variables that created the action? Rather than blaming the user, should the system designer be criticised? Perhaps the focus needs to be on improving our understanding of human behaviour in an information security context?

There are a range of reasons why information security incidents occur. This thesis focuses on awareness and the factors that impact the likelihood or severity of incidents with a significant human element as a cause. Information security incidents include:

1. **Deliberate breaches of security policy.** This situation occurs when the information security “rules” are known. It is a problem of optimum motivation - deliberate breaches occur because an individual or group has been motivated to breach policy more than they have been motivated to comply.

2. **Accidental breaches of security policy caused by a lack of awareness.** This category of breach happens when a lack of knowledge about technology or risk causes individuals or groups to take actions which expose the organisation to risk of an incident.

3. **Accidental errors that occur despite the presence of awareness and adequate motivation.** These include slips (when an action is performed incorrectly) and lapses (when a required action is missed) [BBJ-04]. This is a significant issue with researchers such as Sasse et al [SA-01b] examining the extent to which usability problems contribute to information security breaches. This third category is acknowledged as important when examining the causes of information security breaches but will not be covered in this thesis. Instead, this thesis will be concentrating on perception, communication and motivation of users, not the degree to which systems have been optimised for human use.

As directly measuring the effectiveness of security awareness is a significant challenge and beyond the scope of this thesis an alternate approach will be used. Principles of Psychology and Marketing relevant to the effectiveness of information security awareness will be identified. The implications of these principles will be explored in an information security context and used to create a qualitative scorecard for an information security awareness review. Although the findings will not constitute an empirical measurement of information security awareness, the findings should present an alternative to the current methods of measuring awareness.

1.6. Motivation

The motivation for this thesis was a personal interest in the possibility that disciplines outside of information security such as Psychology and Marketing might hold some of the answers to the human security problem.

Firstly, could Psychology help explain the mystery of apparently irrational human decisions when faced with information security choices? Why does the human decision making process appear prone to failure when faced with decisions that require an evaluation of risk? Individuals are more aware than ever about the range of security threats that could impact information systems such as identity thieves, viruses and hackers. Yet has this growing awareness translated into safer behaviour? What is the link between awareness and behaviour? Would information security awareness be more effective if human behaviour was better understood by the designers and implementers of information security awareness programmes?

Secondly, what could the Marketing profession teach information security professionals about influencing an audience? If information security awareness was implemented as a Marketing campaign what would it look like? Drink driving and stop smoking campaigns have many parallels to information security awareness – they both seek to influence human behaviour to reduce risk. What could public Marketing campaigns such as “Think! Road Safety” teach information security professionals?

Human computer interaction (HCI) is another field of research which helps to explain why humans fail to perform information security tasks correctly. This is highly relevant but due to space and time constraints will not be covered in detail in this thesis which is focusing on Psychology and Marketing principles. Where relevant, HCI concepts and impacts are acknowledged.

1.7. Chapter Summary

Information security awareness is one of the main ways that organisations attempt to manage the human risk to information systems. A number of potential problems have been identified with this approach:

1. Opinions have been expressed that the value of information security awareness has not been adequately recognised
2. There is very little research available to measure the impact of information security awareness
3. Partly as a consequence from the lack of metrics, it is difficult to judge if the current methods of implementing information security awareness are effective (using a method likely to achieve maximum impact)

This thesis aims to help answer to these questions by:

1. Identifying principles of Psychology and Marketing relevant to the effectiveness of information security awareness
2. Analysing the impact of these principles on information security awareness
3. Creating a qualitative scoring system for reviewing approaches to information security awareness using principles of Psychology and Marketing
4. Reporting on the results of a survey to measure information security attitudes and beliefs
5. Identifying any patterns which can be presented as findings relevant for information security professionals

Chapter Two examines the concept of information security awareness in more detail and examines key concepts such as effectiveness.

2. Defining the Problem

2.1. Definitions

Before a discussion about the effectiveness of information security awareness can take place it is necessary to expand on the definitions of three key concepts:

- Information Security Policy
- Information Security Awareness
- Effectiveness

2.2. Information Security Policy

An information security policy is normally a written document that provides centralised control for information security risk management efforts [PT-04]. ISO 27001, the international standard on Information Security Management Systems (ISMS) defines the objective of an information security policy as:

“To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.” [PT-04]

Some organisations implement a security policy as part of an ISMS although it is important to acknowledge that not all organisations implement all components of an ISMS. The definition above appears to be a common one which is shared by security practitioners such as Thomas R Peltier:

“Management establishes its goals and objectives for protecting the assets of the enterprise by implementing policies. Policies are used to introduce the concepts of what is expected of all employees when using enterprise assets and what non-compliance can lead to.” [PT-04]

All organisations have information security risks to their existence or operations which information security awareness helps mitigate such as:

- The risk of losing money
- The risk of regulatory sanction

- The risk of negative publicity
- The risk of extinction
- The risk of injury or death

Security policies are becoming more common for organisations. According to the 2008 BERR study, 55% of organisations polled reported having a documented security policy. This is up from 27% in 2002. Large businesses (defined as having over 500 staff) were far more likely to have a documented security policy.

There are many reasons why an organisation might have an information security policy and publicise it through an awareness programme. Therefore, there are many definitions of what a successful implementation of policy and awareness would be. These reasons and benefits are explored in this chapter. A common theme, important to the rationale of this thesis, is that the expected consequence of an organisation's investment in security awareness is a net reduction in risk caused by the human element. In real terms this means that there will be a tangible result such as a change in behaviour for users of an information system of which the outcome is an improvement of security [RC-06], [LT-05], [HR-05].

The reasons for publishing an information security policy include:

- An expectation that users modify their behaviour in a way that benefits the organisation's information security risk profile
- Demonstrating to external entities such as an industry regulator that information security is being managed appropriately
- Providing a degree of control over employment contracts. Employees that violate the policy can be subject to disciplinary action

Influencing the behaviour of information system users is not the only reason why an organisation might decide to implement an information security awareness programme. It could be required to meet regulatory compliance requirements [HR-05] such as the Sarbanes-Oxley Act. Or, it could be that external stakeholders such as customers and business partners need evidence that the organisation is serious about information security [MA-06].

The focus of this thesis will be on introducing information security awareness to influence the human element in an attempt to achieve a risk reduction. Tolerances to risk will be unique to each organisation and its activities and therefore the degree of human risk reduction required will also be unique for each organisation.

The implementation of an information security policy normally means finding a balance between controlling threats to information systems and not unduly restricting the organisation's information processing activities.

The concept of perfect security is not the same as risk removal. An attempt to remove all risks would likely mean permanently locking buildings and barring all staff, including guards [SB-04]. Computers would be unplugged from networks and isolated. Under these circumstances it would become impossible for an organisation to achieve its objectives. Information technology is a tool to aid achievement of objectives and information security must not remove information technology's value as a tool. Schneier supports this view:

"Every security system has costs and requires trade-offs...We don't have limitless resources or infinite patience. As individuals and a society, we need to do the things that make the most sense, that are most effective for use of our security dollar."

[SB-06]

Typically, an information security policy is:

- A centralised way of communicating information security knowledge throughout an organisation. A particular organisation's policy is communicated so that users can adapt their behaviour appropriate to the organisation
- Demonstration of commitment by management to manage risks inherent in information processing
- A definition of responsibilities for information security within the organisation. Responsibilities are communicated so that roles such as managers or system administrators can understand specifically what they need to *do* to support information security
- A communication of the overall tolerance to information security risk within the organisation. Overall risk tolerance is communicated to influence how users react when confronted with high risk situations

- A set of high level controls and procedures designed to achieve appropriate risk management within the organisation. Risk management processes are communicated to influence what users *do* to manage risks

It is important to note however that some organisations publish information security policies partly because of a requirement for legal or regulatory compliance [HR-05]. In some cases it is a value in itself being able to demonstrate that information has been communicated. The change in behaviour was not required or essential to the process.

2.3. Information Security Awareness

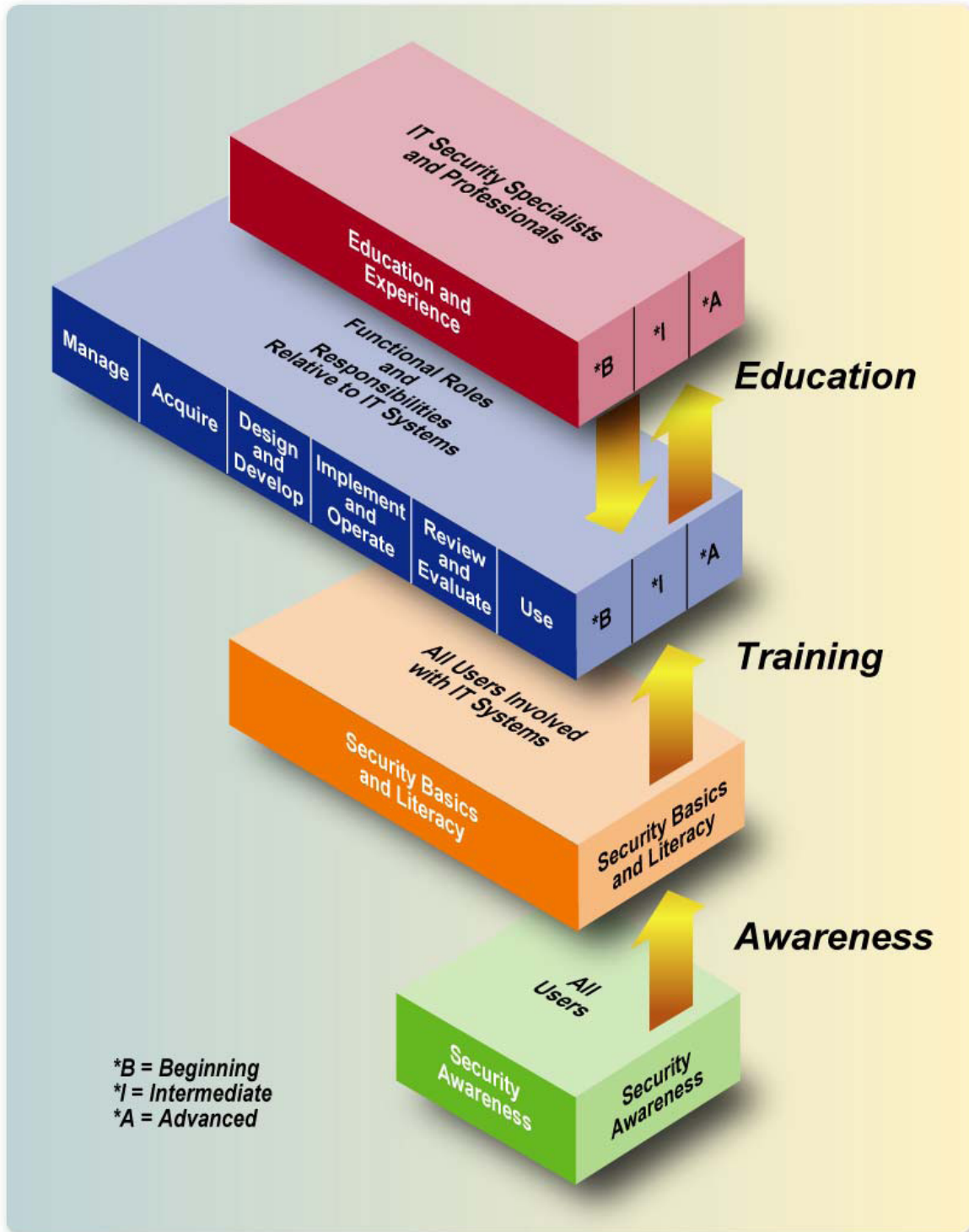
Information security awareness is the publication and presentation of elements of an organisation's security policy to an audience.

A review of information security awareness publications [NIST-A], [HR-05], [LT-05] has found a broad consensus for three layers of information security publication to an audience:

1. Information security ***awareness***
2. Information security ***training***
3. Information security ***education***

All users receive some form of *awareness*, some users receive *training* for specific tasks and those involved in administering information security receive *education*.

The National Institute for Standards and Training (NIST) defines the following relationships [NIST-A] between training components:



NIST Awareness, Training and Education diagram [NIST-A]

The information security awareness business case appears to rest on the expectation that improving awareness will improve security [HM-08]. This assumption has come into criticism with authors such as Angus McIlwraith [MA-06] and Timothy Layton [LT-05].

NIST's original information security awareness document "SP 500-172" did not specifically reference behaviour. The original description was:

"(Creating) the employee's sensitivity to the threats and vulnerabilities of computer systems..." [DS-08]

NIST's updated 2003 publication "Building an Information Technology Security Awareness and Training Program" has a new emphasis on the behavioural component by introducing a verb into the description:

"Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly." [NIST-B]

NIST now recognise that the success of information security awareness rests on an action or inaction. This is the "*respond*" component in their definition. The original reference to "*sensitivity*" was an internal property that potentially existed independent of the individual's actual behaviour.

As well as achieving a behaviour component, information security awareness is also about creating a consistent approach. As organisations increase in size it becomes more challenging to retain a consistent cohesive information security strategy. Individuals within an organisation separated by geography and function would likely adopt different attitudes to information security. The Department for Business Enterprise and Regulatory Reform (formerly the Department of Trade and Industry) takes the following view:

"As companies grow, previous methods of communication can become less effective. For example, informal understandings and chats in the corridor can prove insufficient. Legal and regulatory pressures increase as companies expand. Providing the entire company with clear, concise, internal governance can bring real benefits in terms of efficiency as well as a means of reducing information risk." [DTI-06]

Clearly, the rationale for awareness is that it changes the variables in a human logic process. For example, if users are aware of the potential for fines to result from installing unlicensed software the expectation would be that they are less likely to

install software on their own initiative. If users were aware of the potential impact that could result from the loss of personal data on a USB key they might be more careful.

2.4. Effectiveness

This thesis has found widespread support for the effectiveness of information security awareness to be judged by the extent to which it results in optimal behaviour by information system users [LT-05], [RC-06], [HR-05]:

“...it's not what people know, or feel, or are aware of that is the final determinant of the quality of security – its what they do. If the purpose of security education is to establish, enhance and maintain quality security, we should keep our eyes firmly fixed on performance.” [RC-06]

Traditionally, the way of measuring security policy effectiveness has been by using surveys which measure reported awareness [HR-05]. Unfortunately, it appears that using people's *intentions* to comply with a policy as a predictor of behaviour is fraught with problems:

“Security managers and senior management assumes that the majority of their users will verbally agree with their policies. They also know this is the standard response they will receive no matter how their users really feel.” [LT-05]

Layton's position is that individuals might respond to a survey and deliberately misstate their intention to comply. Other critics are concerned that there is an unconscious discrepancy between attitudes and behaviour. Authors such as McIlwraith [MA-06] in the information security field, and Makin and Cox [MP-04] from an organisational behaviour viewpoint have stated that the link between awareness and behaviour is weak. Looking outside the information security discipline there are numerous examples of widespread awareness that has not resulted in optimal behaviour.

- **Smoking:** it is likely that most smokers are aware of the health impact from smoking, yet their behaviour continues. Not only is their behaviour not consistent with their awareness (or knowledge) but their cognitive process to

rationalise the risk is apparently selective. The concept of risk rationalisation will be explored further in Chapter Three.

- **Drink Driving:** the risks and consequences have been extensively communicated for a generation of television viewers yet drink driving is still a social problem. In 1979, the first year that drink driving statistics were recorded there were 1640 fatalities [DFT-A]. In 2003, the latest reported year there were 560. While this is a significant drop in fatalities, drink driving remains a problem even after millions of pounds have been spent on awareness for radio, television and print. Does this result suggest that 100% compliance in eliminating drink driving is impossible?

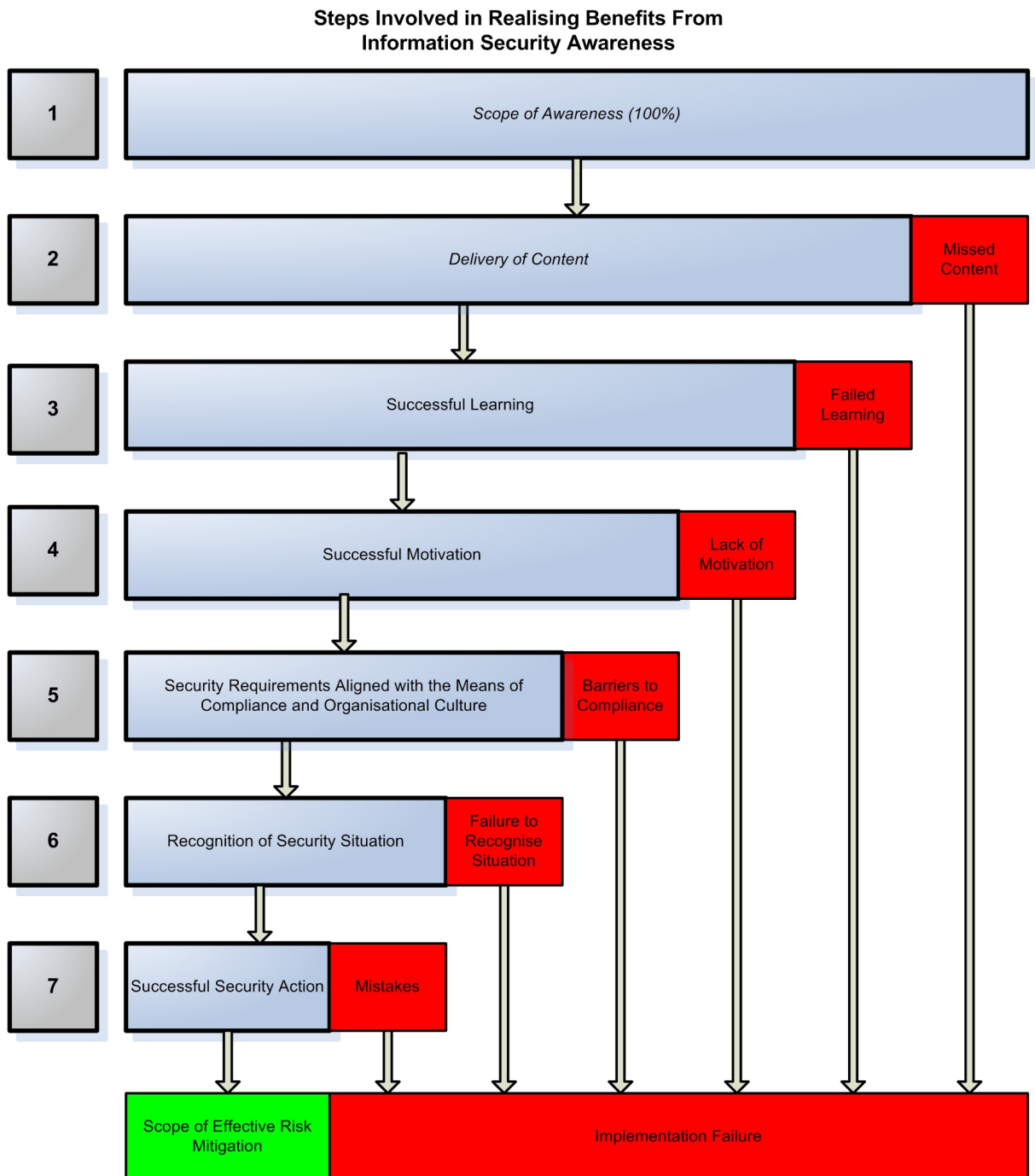
At the heart of the debate about information security awareness effectiveness is the lack of reliable metrics to prove the assertions of either side. Authors such as McIlwraith [MA-06] have criticised poor choices of metrics to measure effectiveness. Other authors such as Roper et al [RC-06] complain that the measurement component is often “...*neglected or given little thought*” [RC-06]. There is little doubt that this lack of metrics will contribute to ongoing difficulties justifying spending on information security awareness.

In the absence of reliable metrics it is difficult to estimate the degree to which different approaches impact the success of information security awareness. The problem is that information security awareness can come from multiple sources. Failures could be attributed to the organisation’s lack of action while successes could be the result of awareness communicated from other sources such as previous organisations, personal experiences at home or mass media sources such as the BBC [BBC-B]. The organisation’s actions in promoting information security awareness may have actually been inconsequential.

In evaluating effectiveness, there are a number of reasons why information security awareness might not impact behaviour, even if the target audience has been exposed to an opportunity for learning. Achieving a change in behaviour is more complex than just the communication of “facts”.

Defining the Problem

Publications [MM-02], [HR-05], [LT-05], [MA-06], [RC-06], [SP-02] on information security awareness programmes have been reviewed to create a model to show the steps contingent to a successful behavioural outcome. It helps illustrate reasons why information security awareness may have a declining effectiveness. Each stage represents a possibility for diminishing returns:



Model to show steps contingent to a behavioural outcome © Geordie Stewart

Step One is the selection of information security content. A review of publications shows two distinct approaches to this. It can be done as a product of a risk assessment where specific behaviours have been identified as a source of risk for the organisation [MA-06], or, content can be selected by aligning with best practice or regulatory requirements [HR-05]. Although there may be some merit in a best practices approach this risks losing audience focus. The importance of developing content specifically relevant to the audience is discussed in step three.

Step Two is the presentation of communication to an audience for the opportunity for learning to take place. It is likely that in any information security awareness programme a percentage of the audience will not be exposed to awareness material. At any point in time it is likely that some staff will be absent or otherwise unavailable. An example is geography whereby head office staff might receive more training than other locations [MA-06].

Step Three involves the audience drawing the right conclusions after being presented with the awareness material. The role of existing perceptions interfering with risk communications is reviewed in Chapter Three which examines the Mental Model approach recommended by Morgan et al [MM-02].

Information security is a relatively new discipline even though some of the concepts are not. Information security awareness is sometimes created and delivered by information technology staff who may not be the best communicators.

It is acknowledged that individuals have different learning styles [OJ-02], [EM-05] and each training method will suit some users and not others. Some users may benefit from classroom sessions and other users may prefer a hands on approach. However, all users need to be presented with content they can perceive as relevant. The Deloitte Global Security Survey 2007 makes a specific reference to the needs of the audience:

“Organizations that are in the process of developing training and awareness programs need to take into account the audience. They need to provide case studies that the audience can relate to, not a one size fits all training program.” [DEL-07]

Step Four aims to motivate the audience to act on the knowledge that was conveyed in step three. In any communication process it is unlikely that all of the audience will be successfully convinced to act on a particular request or instruction. Motivation will be explored further in Chapter Three where it is covered as part of a review of Psychology principles.

Step Five could result in a further decrease in training effectiveness because of barriers to compliance. This is when the user understands what is required of them and has been successfully motivated but lacks the ability to actually perform the behaviour. Barriers to compliance could include:

- **Lack of facilities:** for example a lack of shredders enabling staff to act in accordance with a secure disposal policy [HR-05]
- **Excessively complex technology:** researchers such as Sasse [SA-01b] have noted the impact of complexity on human computer interaction as a barrier to secure computing
- **Social barriers:** some organisations have a culture where lax security is considered a demonstration of trust [MA-06]

Step Six requires the individual to recognise a situation that the training or awareness applied to. Several authors [LT-05], [HR-05] have noted that security issues presented in training sessions may not resemble actual examples encountered by users. This means a very real chance that the user will fail to recognise the situation for which the awareness was intended.

Step Seven requires the individual to perform the task correctly. In this situation the user is aware of the security issue, has the means and motivation to perform the correct action but makes a mistake. This includes slips and lapses as previously mentioned.

This thesis focuses on steps three and four to examine factors that influence human awareness of risk using Psychology and Marketing doctrines. The previous steps were presented to acknowledge the other stages involved in reaching optimal behaviour.

2.5. Chapter Summary

Chapter Two has expanded on the form and expected purpose of information security awareness. Other key concepts such as policy, compliance and effectiveness are identified as relevant to managing human security risk.

Organisations implement information security awareness for a variety of reasons but a common theme is to influence the behaviour of their information system users. A key point is raised that in order to achieve a risk reduction, awareness must translate into a behavioural change in order to be effective.

A review of information security publications dealing with information security awareness has revealed a concern that current methods of information security awareness are not effective. If methods are not effective, there is a case that information security awareness is inefficient, in that the results obtained are not worth the cost.

A model was presented in Section 2.4 to demonstrate how many factors influence the eventual outcome and success of delivering information security awareness.

Chapter Three will review Psychology issues that impact the effectiveness of information security awareness methods.

3. Psychology and Information Security

Psychology is an established discipline of academic research dealing with human behaviour and thought processes. It offers the opportunity for increased understanding and prediction of human actions through appreciating the cognitive functions underlying human actions. Increased understanding could be invaluable to information security professionals when attempting to predict the outcome of efforts directed at information security awareness.

The goal of this chapter is to identify the key principles of Psychology which are directly relevant to influencing human behaviour in an information security context. Psychology is a large field and it is not possible to cover all areas of relevance so a summary is presented here. Numerous branches of Psychology exist but this thesis will focus on the subgroups most closely aligned with predicting behaviour including:

1. **Cognitive Psychology:** uses information processing models to explain the thinking underlying behaviour. This includes perception, memory and problem solving
2. **Personality Psychology:** the study of patterns of behaviour within an individual
3. **Industrial and Organisational Psychology:** the study of humans in an occupational and work context

Central to a review of Psychology's relevance to information security is the debate about the extent to which humans can be considered rational, logical entities. Human behaviour has been criticised by some Psychologists as fundamentally irrational. When a human reaches an irrational result (usually defined as failing to maximise self interest through selection of available options), some Psychologists such as Reisberg and Watson [EM-05] argue that human reasoning is fundamentally flawed and cannot be regarded as rational. In contrast, other Psychologists such as Evans [EM-05] argue that the way we measure logic in a laboratory setting distorts the results and humans are actually mostly rational. Eysenck et al [EM-05] offer several convincing arguments of why innate human irrationality might be overestimated. Firstly, errors in judgment where the subject fails to select the "best" choice could be a product of complexity.

Concepts involving large numbers such as “One in a million” are new in an evolutionary context. Schneier makes a strong case [SB-08] that humans are not well cognitively equipped to deal with such abstracts. Eysenck et al [EM-05] argue that if the problem is reframed the cognition process is significantly improved:

“...findings suggest that people can think rationally when problems are presented in a readily understandable form not requiring extensive calculations.” [EM-05]

Secondly, language interpretation differences between the subject and the experimenter could contribute to a difference of what a perceived logical outcome would be:

“...the participants’ understanding of the problem may differ from that of the experimenter. Indeed, some participants who produce the “wrong” answer may actually be reasoning logically based on their interpretation of the problem.” [EM-05]

In this example, the individual interpretation of language frames the perceived problem. Unless the experimenter and subject have exactly the same understanding of words used this means that the subject will not perceive exactly the same problem as the experimenter.

The case of Eysenck et al [EM-05] for limited rationality appears to make sense. For the purposes of this thesis the important factor is that generally individuals *attempt* to be logical. The fact that this process is not always apparently successful does not mean that the notion of rational humans is invalid. Indeed, the factors causing this gap between illogical and logical behaviour in an information security context is part of the focus for this thesis.

Part of the problem in the debate about humans being rational is the difficulty defining what it means to be rational. Eysenck et al make a strong case for “Bounded Rationality”:

“The notion that people are as rational as their processing limitations permit.” [EM-05]

This is supported by the view from Evans and Over [EM-05] that humans have two forms of rationality – Rationality₁ and Rationality₂.

Rationality₁ is demonstrated when:

“(Humans)...are generally successful in achieving their basic goals, keeping themselves alive, finding their way in the world, and communicating with each other.”
[EM-05]

Rationality₂ is when:

“(Humans)...act with good reasons sanctioned by normative theory such as formal logic or probability theory.” [EM-05]

This appears to demonstrate a distinction between “generally successful” behaviour and “best” behaviour. Rationality₁ appears to explain how humans can drive cars and fly planes fairly reliably without widespread carnage. Their behaviour may not be “optimised” in a formal mathematical sense but it is enough to be “generally successful” in their activities.

Rationality₂ by contrast may partly be a behaviour which exists largely in a hypothetical, sterile laboratory. Humans do not have the luxury of expending infinite time and resources when making a decision. Examples where humans are given an hour to solve a problem in a test do not resemble a busy work place where time is limited and distractions are likely to be present.

In this thesis, the concept of rational behaviour is interpreted in a Psychology context to mean the extent to which a decision reflects the individual’s ability to express self interest. This could be expressed in anything of value to the individual and would not necessarily be constrained to money.

In Marketing there is an associated concept called “opportunity cost” which can be defined as:

“The difference between the revenues generated from undertaking one particular activity compared with another feasible revenue generating activity.” [BP-08]

This is a definition for an organisation which is interested in maximising profits, but for an individual, an opportunity cost decision could mean choosing actions that could lead to rewards in order to achieve a perceived benefit. These benefits could be rewards such as avoiding work, leaving early or even a social gain such as being seen to be generous with colleagues. Normally in an information security context, the self interest that security directives appeals to as a management control would be job security [PT-04]. It is the threat of disciplinary action which acts as a deterrent (the negative outcome) that users attempt to avoid.

It is necessary to acknowledge that the interests of the individual are not always the same as the interests of the organisation. The “best” or “acceptable” option in a situation for an individual is unlikely to be exactly the same as for the organisation. While the “best” option for the individual might be to go home early, the organisation might prefer a quality output.

A key point is that behaviour normally achieves acceptable outcomes which are not necessarily optimised in a true quantitative sense. This chapter is focusing on the factors that might contribute to an information security incident caused by human cognition.

3.1. Motivation

“Practical experience as evidenced by current research studies indicate the passing out of security policies does little to motivate or ensure employee commitment and compliance. In fact, it can create negative feelings and make the users motivation and attitude move in a negative direction away from the intended goal of the security awareness program.” [LT-05]

Timothy Layton’s observation is that simply asking people to comply with a directive may not be effective. This section explores the reasons why individuals might be motivated to follow an information security policy and act according to awareness or training.

Operant conditioning is an important concept that applies when an outcome or result is used to impact the form and occurrence of behaviour. It is described by Makin and Cox as *"behaviour is a function of its consequences"*. [MP-04] The outcome can be positive in some way which has a chance to increase the likelihood of the behaviour. Alternately, it can be negative in some way which has a chance to decrease the likelihood of the behaviour.

Note that the process does not always have to involve the addition of stimulus. Positive outcomes can include the removal of unpleasant stimulus and negative outcomes can include the removal of pleasant stimulus. It is also important that the individual (or subject) is able to perceive the link between the behaviour and the result. Noise in the form of multiple stimuli occurring at once could prevent this perception with the result that if the subject is unable to perceive the link between behaviour and stimuli, there will not be a motivational impact on behaviour.

Positive reinforcement is when behaviour is associated with the introduction of favourable stimuli which is perceived as a form of reward and causes the behaviour to continue. It can also increase the frequency or magnitude of the behaviour. Positive punishments could take the form of praise, money, attention or a variety of other benefits that might be perceived to be of value to an individual.

Negative reinforcement is when behaviour is associated with a removal of unpleasant stimuli which is perceived as a form of reward and serves to encourage the behaviour in a similar way to positive reinforcement. Negative reinforcements could take the form of removal of unpleasant tasks which the individual does not enjoy.

Positive punishment is when behaviour is associated with the introduction of unpleasant stimuli and serves to extinguish the behaviour. It can also reduce the frequency or magnitude of the behaviour. Positive punishments could take the form of ridicule from peers or warnings from a person of authority.

Negative punishment is when behaviour is associated with the removal of pleasant stimuli and serves to extinguish behaviour in a similar way to positive punishment. Negative punishment could take the form of removing privileges such as special breaks or internet access.

Operant Conditioning

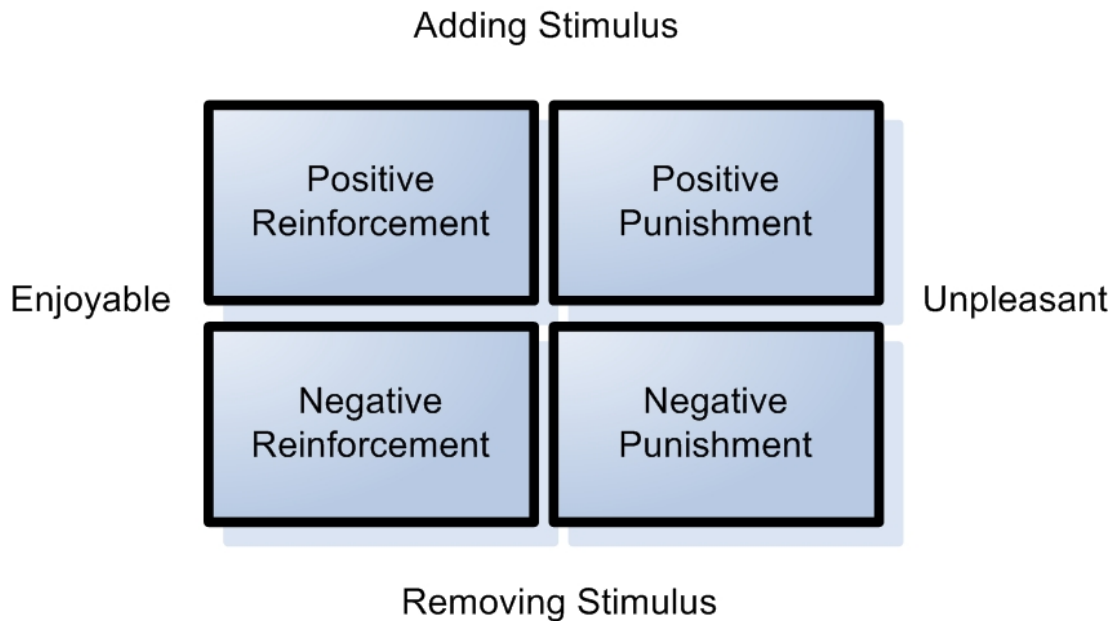


Diagram to show relationships between behavioural consequences © Geordie Stewart

While operant conditioning explains some of the causes for behaviour, problems have been identified with using operant conditions in an information security context. Edward Deci has challenged the assumption that rewards are the best way to encourage behaviour in the long term [GR-05]. Deci's research suggests that it is the sense of autonomy which correlates most closely with sustaining behaviours in the longer term. His research also found that behaviour declined more quickly when an individual was expecting a reward as a result of the behaviour.

One of his famous experiments was with children who were asked to draw pictures. One set of children were asked to draw pictures with no expectation of reward. Another set of children were offered a reward to draw. Interestingly, when the rewards were suspended, the children who had never expected a reward continued to draw the longest. In contrast, the children expecting a reward quickly lost interest. For the children drawing the pictures without expectation of an external reinforcer, the act of drawing itself was perceived as a reward. The implication is that the desired behaviour ceases quickly once the reward stops. Therefore any reward scheme must be sustainable in the long term if long term behaviours are required.

There also appears to be a relationship between the level of motivation and the practicality of attaining a particular goal:

“Research spanning the last sixty years indicates that when a person’s perception of goal achievement is beyond their reach, commitment declines significantly. Hence, it is imperative that people believe the goal is attainable.” [LT-05]

Implications for information security awareness:

When an organisation has problems with behaviour impacting information security it is important to recognise the implications of operant conditioning which suggests that all behaviour exists because it is or has been rewarded in some way:

“When organisations face problems with costs, quality, productivity and attendance, these problems often stem from ineffective patterns of behaviour that the organisation is unwittingly encouraging. To prevent and stop these problems, a behavioural approach to managing people is often the most effective.” [MP-04]

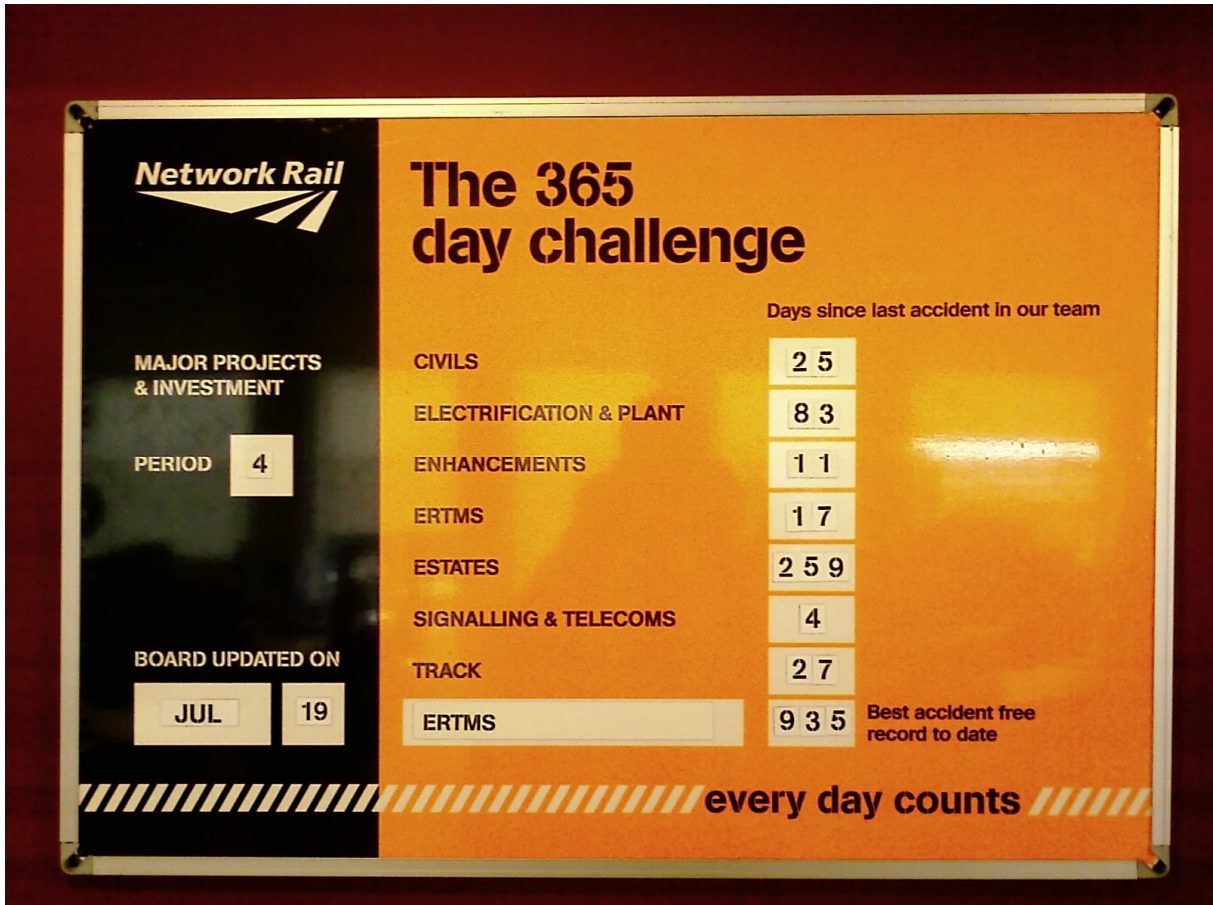
The “natural reaction” noted by Makin and Cox is to resort to the traditional stick approach – to punish behaviour which is considered noncompliant. It usually consists of pressure and cajoling from management. This approach, which is used in support of compliance with security management controls, may not always be the most effective motivator in the operant conditioning equation. Recent examples from the field of organisational management have shown that rewards can be powerful tools.

Network Rail has had a significant challenge raising awareness of safety issues for staff and contractors. To address this Network Rail embarked on a major awareness campaign:

“Safety 365 is the communications campaign that we run for all our employees across the whole organisation. The key issues that we cover are slips, trips & falls, manual handling, near misses, alcohol & drugs and occupational diseases.”

[NR-A]

Safety 365 is an interesting example from a compliance perspective because it uses positive reinforcement as a behavioural motivator. Pride is created through successfully meeting safety targets and a healthy sense of competition is fostered with prizes for the business areas that have the best safety record:



Safety 365 photo taken by the author

Results are displayed in a prominent place helping to foster the shared company value of a safety culture. Here, a poster is displayed in the head office in a prominent position near the lifts:



Safety 365 photo taken by the author

The result has been a significant decline in both accidents and predictors of accidents (NR-A):

	2005/06	2006/07	2007/08
Accident Frequency Rate	0.359	0.263	0.226
Fatalities	4	0	2
Major	98	69	79
Lost Time	301	216	189

This approach by Network Rail to use positive reinforcement instead of positive punishment is significant because of its potential impact on staff accident reporting rates. The principles of operant conditioning suggest that incidents are less likely to

be reported if the reporting results in a sanction. Incidents that are not reported cannot be measured and the lack of measurement inhibits the refinement and optimisation of processes to deal with the incidents.

Therefore, by using positive reinforcement as a motivator in this scenario Network Rail is influencing behaviour without reducing its ability to monitor compliance through reported incidents. This factor is important in any situation where policy violations are not detected automatically and rely on a human element.

Potentially, the information security approach and its frequent resort to positive punishments, means that many incidents go unreported for fear of sanctions. One of the problems identified in the rationale of this thesis was that it is difficult obtaining metrics for information security because of silent failures. It is also difficult linking preventative controls with so many intertwined causes and effects. Organisations that need to improve their metrics and increase the rate of incident reporting should look at limiting the extent to which they employ positive punishment. Using positive reinforcement is still effective at influencing behaviour but will not limit incident reporting to the same extent as positive punishment.

3.2. Reward Schedules

Early work by Skinner [GR-05] has shown that the *timing* of the response in the form of reinforcement or punishment is a significant factor in the degree of influence that the response poses. Schedules of reinforcement can be fixed or variable based. Fixed ratio schedules of reinforcement mean that an outcome is delivered for every X examples of the behaviour. This is commonly written as FR(X). A variable schedule of reinforcement means that a consequence is provided *on average* once for every X examples of the behaviour. This is written as VR(X).

Skinner helped confirm the following principles:

1. The greater the time in between the behaviour and the reinforcement or punishment, the less effect the process will have on behaviour.
2. The reinforcement or punishment does not have to occur every time the behaviour does in order to be effective. It can occur on a fixed variable (such

as one result for every ten instances of the behaviour) or on a variable basis (on average one result for every ten instances of the behaviour).

3. Variable reinforcements have a greater long term effect on individuals. Variable reinforcements can be time based or ratio based. Research shows that behaviours are maintained for a longer term in variable schedules in comparison to fixed schedules. Makin and Cox give an example of a simulated computer stock market experiment [MP-04] where subjects who experienced a variable ratio reinforcement continued their behaviour long after other subjects who were on a fixed ratio of reinforcements.

Implications for information security awareness:

Organisations do not have to commit to rewarding users every time they comply with desired behaviour. Instead, a variable ratio of rewards could be used to sustain desired behaviour with an accordingly reduced value of expended rewards or resources on behalf of the organisation.

One method of measuring the level of behaviour compliance with information security policy is by performing an audit. If time elapsed between behaviour and the response (triggered by an audit) is important then audits that occur infrequently, such as a yearly compliance audit, will have less impact on behaviour than a response that happens within a few days of the behaviour. The response could be a punishment for non-compliance or it could be a reward for successful compliance. Either way, a response to an action delivered up to a year after the behaviour is unlikely to act as a significant motivator unless the punishment is severe. The implication is that continuous auditing of security policy compliance is more effective at influencing behaviour than a yearly or quarterly approach.

3.3. Reward / Punishment Asymmetry

Experiments [MP-04] and live examples have indicated that while reinforcement can operate on a variable or infrequent basis and still be effective, variable punishment is less effective. According to Makin and Cox:

“The certainty of being punished has an important influence on behaviour...unless the behaviour can be punished every time it occurs the punishment is unlikely to change the behaviour.” [MP-04]

Makin and Cox go on to conclude that *“Punishment is not an effective way of trying to change behaviour”* [MP-04]. This view is supported by Criminologist Tim Newbury [NT-07] who points out that re-offender rates are not significantly different between white collar workers who have been imprisoned and those who had not. Therefore, the generalisation that inconsistent punishments will not be effective seems to overestimate the role of frequency without allowing for severity of punishment.

Implications for information security awareness:

For sanctions to be effective the chance of being punished must be highly likely. In most organisations severe punishments are not practical. The exception being when an employee is dismissed or demoted which acts as a warning to other employees. In this case however the behaviour of the individual is not being impacted - it is other spectators within the organisation.

Taking into account the findings above in Reward Schedules, the optimum support that can be provided for information security policy in the form of compliance is a real time monitoring scheme. Having a high likelihood of detection which delivers swift feedback to individuals will achieve maximum impact on behaviour. The “yearly audit approach” is useful to provide a snapshot of the security of an organisation but will have limited impact on behaviour unless the punishments for non-compliance are severe.

3.4. Heuristics

Heuristics are “Rules of thumb” [EM-05] that humans use in decision making processes. They are effectively a mental shortcut that allows decisions to be made without considering all input all of the time. *“...the complexity of most problems means that we rely heavily on heuristics or rules of thumb.”* [KM-05]

Heuristics can also be a source of error in the decision making process. As a mental model a heuristic represents a simplified abstract which will not exactly match reality. As such it is strongly tied to perspective. A by-product of the construction of heuristics is bias.

Biases are the result of simplified decision making processes that can interfere with an individual's ability for optimal decision making and can lead to results that can appear "illogical". Normally, these decision making aids or "rules of thumb" serve us well. Many different biases have been identified and this section presents a summary of the ones most relevant to risk decisions and information security.

The "*availability heuristic*" is a recognised source of error and inaccuracy in human decision making [SB-08]. Humans tend to assess the likelihood of an event by the ease they can imagine it. Therefore, events which have happened to the individual will be easier to imagine than hypothetical events. Recent events will be easier to recall than old ones. The degree to which an event is emotional and vivid will also be significant.

The "*affect heuristic*" is a bias interfering with the accuracy of risk perception [SP-00]. This is where feelings and emotions distort the perception of risk severity. For example, where a risk is being accepted for the purpose of gaining a benefit, the risk tends to be downplayed. Schneier notes that this applies to comparatively risky sports such as skydiving [SB-08]. The perceived risk is downplayed because of the emotional attachment to the activity.

Implications for information security awareness:

It is important to acknowledge how heuristics influence information security processes. Secure Socket Layer (SSL) encryption in internet browsers is an example of a visual cue for users that could play a role in simplified decision making. When a user notices a padlock in their internet browser they assume it is a secure session. This visual input allows an assumption that may be faulty as the padlock only means that a session is encrypted. It does not communicate anything about the identity of the party the communication is with.

Information security awareness needs to predict the impact of heuristics on human decision making processes relevant to information security. Potentially, compensating for the availability heuristic might mean extra emphasis focusing on security incidents considered a real threat that have not occurred previously to the organisation. The availability heuristic suggests that there will be a lower perception of risk for incidents which have not occurred at the organisation before.

3.5. Fear

Fear is an evolutionary survival aid which is governed by the amygdala [SB-08]. The amygdala governs the human reaction to fear – it controls the release of hormones in the bloodstream to generate the “flight or fight response”. This function may have been an evolutionary advantage in the past but in modern times it is a potential handicap against risks that we can’t outrun. An increased heart rate and the urge to flee is less useful in a modern context when dealing with risks that require a more logical, analytical approach. It is unlikely to be of benefit to flee in terror at the prospect of a job interview or being asked to give out your credit card number over the web, although some of us may be tempted to.

There are two main problems with this fear response in a modern context. Firstly, we seem to target our fears in an irrational way, more of which will be explored in the next section on the perception of risk. Stephen Pinker, a psychologist with a background in Experimental Psychology suggests that some of our current fears are the result of evolutionary threats in our recent past:

“Fears in modern city-dwellers protect us from dangers that no longer exist, and fail to protect us from dangers in the world around us. We ought to be afraid of guns, driving fast, driving without a seatbelt, lighter fluid, and hair dryers near bathtubs, not of snakes and spiders...but when Chicago schoolchildren were asked what they were most afraid of, they cited lions, tigers, and snakes, unlikely hazards in the windy city.” [SP-97]

Secondly, the problem with the inbuilt fear response is that a raised heart rate and the urge to flee interfere with cognitive functions:

“When someone is emotionally aroused, his or her cognitive functioning changes. In times of high arousal (stress), cognitive focus becomes narrow and the individual can attend to less at a time...high levels of arousal can lead to mistakes.” [BBJ-04]

Dennis Ford has noted the following stress impact on memory [FD-93] but the concept is also applicable to other cognitive functions such as decision making:

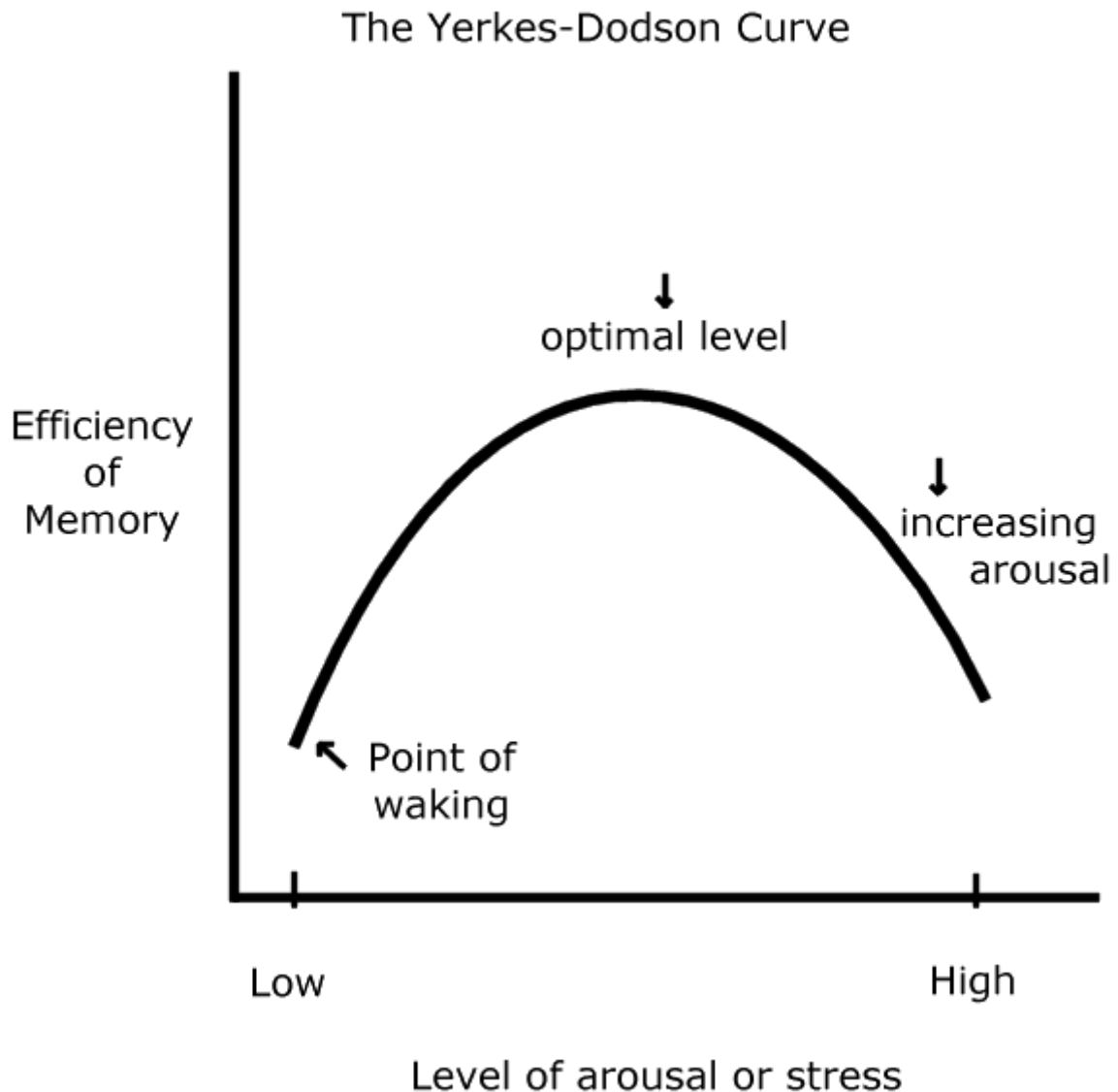


Diagram to show relationship between memory efficiency and stress [FD-93]

Bock-Brown notes that organisations often appeal to fear in pursuit of information security objectives such as *“disciplinary measures, litigation threats, retraining, naming, blaming and shaming.”* [BBJ-04]

As well as creating situations where cognitive function is impaired through excessive fear, an appeal to fear approach is also vulnerable to what Kim Witte has termed the “Boomerang effect” [BBJ-04]. When an individual is confronted with a risk, it is not just the severity of the risk which is evaluated from the perspective of the individual. The individual also considers their ability to control or eliminate the threat.

Where the individual perceives that danger and their own ability to manage the danger is high, they are likely to take steps to control the risk. However, if the danger is high but the individual perceives a low ability to manage the danger, the individual is likely to develop a “Cognitive Dissonance”. This is when a contradiction exists between two cognitions or thoughts. This could include a contradiction between cognitions such as knowledge, attitude or behaviour. Stephen Pinker states that cognitive dissonance is an uncomfortable state for the individual who will “invent a new opinion” [SP-00] to resolve it. This could include an adoption of one of the biases listed above.

Jeff Bock-Brown makes an important point that perception of fear and control efficacy is an individual property. This means that an organisation wide appeal to fear is difficult to pitch at an optimum level where significant motivation is gained for some subjects without creating effective risk apathy in others.

Implications for information security awareness:

In the absence of empirical benefits for information security, information security awareness campaigns use fear to sell a message and act as a motivator rather than depending on return on investment calculations.

The language of information security is not neutral. Even before being applied to information systems, words such as “Virus” and “Hacker” all have unpleasant, fear generating properties which by causing a heightened state of fear arousal, may decrease people’s ability to make rational decisions. The language of fear may go some way to explain impaired human cognition when dealing with information systems.

Appealing to fear without addressing the audience's perceived ability to control the risk could produce information security apathy amongst the target audience which is a form of inevitability bias [LT-05]. Also, appealing to fear is a form of negative reinforcement covered above. Using positive reinforcement may offer improved behaviour without the risk of the "Boomerang effect".

3.6. *Learned Helplessness*

The level of efficacy present in a situation is not only relevant to fear, but is significant for other stimulus such as punishments.

Seligman performed a series of experiments [GR-05] on dogs where electric shocks were applied. Some of the dogs had the opportunity to avoid the shocks and some did not.

The experiment found that the dogs which had been exposed for a period to shocks without the possibility to avoid them were significantly slower at avoiding the shocks when given the opportunity. It appears that the dogs came to accept the shocks as inevitable and were not disposed to learning coping mechanisms when given the opportunity.

This experiment was repeated with human participants for a similar conclusion [GR-05].

Implications for information security awareness:

The theory of Learned Helplessness suggests that providing motivation in the absence of efficacy can have significant negative consequences on long term behaviour. For example, organisations need to check that the *means* for compliance with information security awareness is present before communication takes place. For example, raising awareness about the need to use secure paper disposal without providing secure disposal bins will lead to a learned helplessness where information system users come to accept non-compliance and any associated sanctions as inevitable.

3.7. Risk Perception

There is a growing area of research which seeks to understand the impact that certain attributes have on the perception of risk. Paul Slovic is one of the leading academics examining the perception of risk and how it is communicated. An area of his research is the adjustment of the severity of risk based on its apparent attributes. In the publication "The Perception of Risk", Slovic has identified a number of factors [SP-00] which influence the severity of how we perceive risk:

Observable / Not Observable: people appear to have a greater fear for the invisible or intangible. A possible explanation for this is that fear is exaggerated when the threat is difficult to quantify and when subjects have no way of identifying when they are exposed to the threat. An evolutionary explanation for this is that historically, risks have been relatively obvious such as fire, rancid meat or a dangerous animal. Modern threats have become less apparent and more intangible which may add to the level of risk perceived. Modern risks now include dangers such as carcinogens and poisonous gasses such as carbon monoxide. If a risk cannot be perceived then the individual is not able to take mitigative action which may explain a heightened level of fear.

Defined / Ill Defined: when an element of uncertainty is involved people tend to exaggerate the risks involved. Christopher Booker and Richard North have charted modern scares impacting the British public in their book "Scared to Death". They note that one of the important ingredients required to cause a panic is that the danger must be "*...ill defined, maximising the opportunity for alarmist speculation as to the damage it might cause.*" [BC-07] This property may be partly dependent on the observable trait listed above and is consistent with Slovic's research [SP-00] on risk perception.

Old Risk / New Risk: people have a greater fear of novel or new risks. Technology has been a significant example in this category. Nuclear power, mobile phones and computers. In theory, the risk of giving a credit card over the phone is comparable to the risk of giving out a credit card online. However, there is a significant difference in perceptions. Surveys have revealed that people are much more reluctant to give out their credit card numbers online. This can be attributed in part to the "New" risk perception of computers and the internet verses "Old" risks such as the telephone

which has been around far longer. Speaking to a human is a tangible interaction where as a browser session is an abstract interaction, the mechanics of which are probably not well understood by most users.

Familiar / Unfamiliar: the old adage is that familiarity breeds contempt. People are more likely to perceive familiar items or concepts as less risky. Statistically, one of the most dangerous threats in a home environment are swimming pools, yet guns and home invasions are perceived as far more risky [LS-06]. The contradiction to the familiarity bias is when an individual has suffered an incident from a familiar item in the past which can create an availability bias causing them to overestimate the risk based on their prior experience.

Chronic / Acute: chronic conditions are those that build up over time while acute conditions are by comparison sudden and the outcome is less predictable. Angus McIlwraith notes the apparent contradiction on how we treat the risk from illness:

“The major medical killers are chronic. Acute deaths get the headlines.” [MA-06]

Controlled by Self / Controlled by Others: it appears that the perception of who controls a situation changes people’s perceptions of risk:

“Most people are less afraid of a risk they feel they have some control over, like driving, and more afraid of a risk they don’t control, like flying, or sitting in the passenger seat while somebody else drives.” [SB-08]

Risks which might be caused by the actions of others are somehow seen as worse than the same action performed by ourselves. This explains why some people insist on driving and refuse to be a passenger, citing concerns about trusting others to drive. They would often have no rational basis to claim that their driving was better, only that they feel more comfortable (in control) when driving. This may be related to a perception bias:

“...most people claim they are above average in any positive trait you name: leadership, sophistication, athletic prowess, managerial ability or even driving skill. They rationalise the boast by searching for an aspect of the trait that they might in

fact be good at. The slow drivers say they are above average in safety, the fast ones that they are above average in reflexes.” [PS-98]

Diffuse in Time and Space / Focused in Time and Space: it may be part of a survival mechanism that human attention is focused on catastrophic events at a fixed point in time. Angus McIlwraith gives a good medical example:

“If all of the 10,000 people who die prematurely each year in the UK from smoking-related illnesses were to do so at one o’clock in the afternoon on 10 February in Parliament Square, the reaction would be very negative, and rapid remedial action would follow.” [MA-06]

Implications for information security awareness:

When risks are communicated to people as part of information security awareness it is important to recognise that individuals will apply their own filters to their perceptions of risk. This will result in risk perceptions being adjusted internally. Severity, likelihood and overall risk will all be subject to adjustments unique to the individual.

The implications of Slovic’s work [SP-00] is that these adjustments are likely to have commonalities which will show degrees of consistency. The more diverse the members of the organisation, the more diverse the perceptions of risk will be. Organisations need to identify and take these perception biases into account when communicating the level of risk for threats.

Risks which are familiar, chronic (building over time) and self controllable will require extra effort to communicate over risks that are unfamiliar, acute (sudden) and controlled by others. Organisations need to follow up risk communications and check that the perceptions of the target audience match the severity of the risk being communicated.

3.8. Risk Communication

Risk communication is a key component of an information security awareness program. Educating the audience to the risks of non compliance is a key part of the message. However, when risk communication fails there is a tendency to blame the audience:

“Although citizens may begin their learning process with relatively little technical understanding, we believe that most can understand the basic issues needed to make informed decisions about many technically based risks – given time, effort, and careful explanation. Unfortunately, when a message is not understood, the recipients, rather than the message often get blamed for the communications failure.” [MM-02]

This section examines failings of risk communication and examines two possible causes:

Firstly, looking outside of information security, Morgan, Fischhoff, Bostrom and Atman [MM-02] suggest that all risk communication needs to be considered in context. They suggest that it is not enough to identify relevant risks, optimise the presentation and delivery and then allow time for the message to work:

“...for most risks, people have at least some relevant beliefs, which they will use in interpreting the communication. They may have heard some things about the risk in question. It may remind them of related phenomena. Its very name may evoke some associations.” [MM-02]

Slovic has a similar view that existing knowledge is an important factor in risk communication:

“Despite good intentions however, it may be quite difficult to create effective informational programs. Doing an adequate job means finding cogent ways of presenting complex, technical material that is clouded by uncertainty and subject to distortion by the listener’s preconceptions – or misconceptions – about the hazard and its consequences.” [SP-00]

According to Morgan, Fischhoff, Bostrom and Atman, an important preparatory step to risk communication is the construction of a Mental Model to conceptualise the beliefs and attitudes of the intended audience. This is done through asking open ended questions to explore the perceived relationships of words, their associations and the perceived severity and likelihood of associative risks. This provides an opportunity to recognise when audiences misunderstand the meaning of words or have incorrect associations. The Mental Models are used to create a series of relationships that can be quantified to create an accurate picture of linked concepts for the audience.

Once the audience has identified words and concepts related to risks Morgan, Fischhoff, Bostrom and Atman recommend the use of mental model questionnaires to identify patterns in understanding. These are intended to identify:

- The strength of beliefs held by the target audience
- The connection and depth of misconceptions held by the target audience
- The understanding of critical terms used to describe risk

Misconceptions occur when an audience consistently has a different understanding of a key word or term used by technical specialists. A gap in understanding displays a concept that needs to be clarified and communicated before effective risk communication can proceed.

Secondly, it is important to note that words used to communicate the message are unlikely to mean exactly the same things for all parties involved. Morgan, Fischhoff, Bostrom and Atman acknowledge that the perceived meaning of the words dictate the perception created for the receiver. McIlwraith makes an important point about the various terms used for information security jargon. Entire books have been written attempting to define such concepts as “Risk”, “Threat” and “Countermeasure”, so can we expect non-technical audiences to have the same perception of these words as information security professionals? Here, McIlwraith notes the importance of translating technical terms into concepts that can be understood accurately by the intended audience:

“There is a linguistic concept called a vocabulary domain. This is the distinct set of terms used within a specific area of expertise. Lawyers have their own, as do doctors...Consider your audience, and empathize with their needs.” [MA-06]

“False Fluency” is the term that Morgan, Fischhoff, Bostrom and Atman have given to the misunderstandings that can happen between technical specialists (such as information security) and individuals with a limited knowledge of the subject being communicated.

Outside of words which exist as a communications utility in a technical discipline, ordinary, everyday words can also contribute to misunderstandings and result in differences in perception. Neuro-Linguistic Programming (NLP) is a contentious concept which is not fully accepted by mainstream psychology [BBJ-04]. One area of value to information security communications is NLP’s focus on words as abstract concepts which are subject to individual interpretation:

“A map is not the territory it depicts; words are not the things they describe; symbols are not the things they represent.” [BA-00]

The NLP view is that all human cognition operates through a set of filters. There are no good or bad filters, only the extent to which a filter is effective in representing an abstract concept.

“Language is a filter. It is a map of our thoughts and experiences, removed a further level from the real world.” [OJ-02]

The more similar the background between two individuals communicating the closer their mental maps of what shared words relate to. Finding common meanings for words in modern organisations with a diverse set of backgrounds including job roles, nationality and culture can be a significant issue.

Another important factor in risk communication is the context in which communication takes place. According to Slovic [SP-00] and Morgan et al [MM-02], an audience will be influenced by the following factors:

Authority: Who is communicating the information and what are their credentials?

Trust: Has the communicating party been reliable in the past?

Efficacy: To what extent is the audience empowered to deal with the risk?

Slovic also notes that trust is slow to build but can be quickly destroyed:

“Favourable traits (such as trustworthiness) were judged to be hard to acquire...and easy to lose.” [SP-00]

Implications for information security awareness:

It is unlikely that the subject matter to be covered in an information security awareness program will be completely new to the audience. The audience is likely to have an existing awareness about issues such as identity theft, fraud and industrial espionage from previous organisations, news sources or incidents experienced personally. Any communications that take place will be affected in some way by their existing knowledge. The availability heuristic covered earlier is one way that individuals can make their own judgements about the likelihood of risk based on their own experiences. The perceived likelihood of a risk occurring will be modified based on personal experience.

The meaning of words used in risk communication is another area where information security communication could be problematic. Specialist areas develop specialist language and the language of information security is a complex area. The implication of the NLP approach to learning is that some of the words we use to describe security concepts are inherently misleading. The concept “Password” to an information security professional is a string of characters offered to an information system to confirm a proposed identity. Should there be any surprise when non-technical system users attempt to use a dictionary word as their password?

Taking into account the need to quantify existing perceptions and the need to cultivate a common understanding of language, a process of refinement is required in order to optimise communication for human participation in any proposed information system. Feedback needs to be gained from a pilot audience in order to gauge the impact and accuracy of the content being delivered. Depending on the level of importance of the communication, Morgan, Fischhoff, Bostrom and Atman suggest multiple iterations until the communication is reliable. It is also of note that distinct

areas within large organisations may need to be evaluated separately in order to identify differences that exist between departments or divisions.

To test and demonstrate this process a survey was carried out at a large UK transport company. A series of twenty questions were designed to test information security beliefs and attitudes. The survey covered the Information Security Team, a Human Resources Team and an Accounts Team. Answers could consist of

- True
- Probably True
- Neutral / Unsure
- Probably False
- False

The goal was to test the consistency of attitudes and beliefs within the two teams (the degree to which views were internally homogenised) and the degree to which the teams, even as part of the same organisation, had different attitudes and beliefs. The full survey results are available for review in Appendix A.

The results were startling. Even within the teams there were a diverse set of beliefs and polarised attitudes.

Firstly, the interpretation of words was shown to be problematic. Question Two tested the perception of the words “Threat” and “Risk” with the statement: “A risk is the same thing as a threat”. Even within the Information Security Team there was a significant divergence, indicating that there were different beliefs about the meaning of the concept of “Threat” and “Risk”. This is surprising given that the Information Security Team were the technical specialists in this language domain.

Within the Human Resources Team there was also a divergent range of perceptions about threats and risks. Faced with uncertainty in a subject matter outside of their expertise, most of the HR responses might have been expected to be “Neutral” or “Probably False” or “Probably True”. Instead, 37% of responses professed to be sure that the answer was either “True” or “False”. The debate about which answer was “correct” for each question is less important than the fact that many answers had

polarised responses. This result may be partially explained by the concept of “False Fluency” identified by Morgan [MM-02] discussed above.

The clear implication from this study is that defining key terms such as “Threat” or “Risk” needs to take place before any communications commence. An awareness campaign communicating ways to control or reduce risk is unlikely to be effective if the target audience fundamentally misunderstands the concept of what a risk is. Part of the initial communication might be to define exactly what the organisation defines a “threat” to be.

Question 17 of the survey tested an attitude: “Taking computer files home to work on a home computer is a security breach”. The results were split down the middle for the Information Security Team. Half the team said that it was a security breach and half the team said it wasn’t. While it could be argued that this reflects a healthy range of opinions, it also represents the possibility for mixed communications causing confusion within an audience. The Human Resources Team also showed a significant divergence in attitudes to taking work home.

Acknowledging the existing awareness and possible misconceptions appears to be a concept missing from the majority of information security publications surveyed. It is not enough for information security policy and awareness to be factually correct. It must also “...reinforce pertinent correct beliefs and discourage important incorrect ones.” [MM-02]

It is clear that the context must first be quantified for all risk communication activities.

3.9. Attitudes

A review of Psychology publications [GR-05], [EM-05] has found that there have been significant disagreements over the definition of an attitude. This seems to stem from the problem that the concept of an attitude is a construct and can't be measured directly. Allport (1935) saw attitudes as part of a social context and Festinger (1950) also perceived an important interdependence between the individual and a group. More recent research has focused on attitudes as predispositions for an internal process. Rosenberg and Hovland (1960) defined three classes of response:

- **Affective:** an emotional response to stimulus involving a favourable or unfavourable perception for example the *feeling* of fear when confronted with a snake
- **Cognitive:** the analysis of a stimulus for example *describing* a snake as slimy and dangerous
- **Behavioural:** this is the visible response to a stimulus for example the *action* of running away from a snake

While attitudes are a predictor of behaviour, the level of prediction has been criticised as weak. Makin and Cox [MP-04] note the experiment done by LaPiere in the 1930's:

“Over a two year period LaPiere, together with a young Chinese couple, stayed in 66 hotels and other forms of accommodation, and ate in 184 restaurants in the USA. At that time there was considerable prejudice against the Chinese, yet on only one occasion were they refused service. Following his experiences, LaPiere sent a questionnaire to all the places they had visited, asking if they were prepared to serve Chinese people. Of the 50 per cent who responded approximately 90 per cent said they would not. This demonstration of an apparent mismatch between attitudes and behaviour has troubled social psychologists ever since.” [MP-04]

This experiment clearly shows the difference between opinions gathered as part of a survey and the actual behaviour of the participants.

LaPiere's study led to a focus on “Situational Factors” which influence the degree to which an attitude is perceived as applicable by the individual. Gross [GR-05] notes that the Chinese couple in LaPiere's study were well dressed and may not have

accurately fulfilled the stereotype of Chinese people at the time. Therefore, if the Chinese couple did not fit the stereotype then the associated attitude may not have been evoked.

How attitudes change is a significant area of research in Social Psychology.

According to the theory of Cognitive Dissonance [GR-05] tension is produced when an individual simultaneously holds two cognitions which are inconsistent. This provides the motivation for change. Festinger (1957) noted that instead of behaviour changing to reflect a new attitude, the attitude is more likely to change to rationalise the behaviour. For example, when smokers are presented with evidence of smoking related diseases, it is more likely that attitudes will change to rationalise the behaviour. Smokers might "*Belittle the evidence about smoking and cancer*". [GR-05]

An important study by Freedman in 1965 found that the theory of cognitive dissonance only applies when the individual perceives the behaviour as voluntary. The perception of limited choice reduces the potential conflict between behaviour and attitudes. One of the famous studies demonstrating this effect was Milgram's obedience experiment where participants continued applying electric shocks to apparently unconscious participants. The apparent attitude of revulsion for hurting other people was overridden by the authority of the experiment supervisor. [GR-05]

Self Perception Theory [GR-05] was a concept from Bem which attempted to rationalise attitudes in a behavioural context. Bem thought that attitudes were inferred by the individual from observing their own behaviour and the situation in which it occurs.

Implications for information security awareness:

This section has provided powerful evidence for why information security awareness surveys will provide a weak indicator of effectiveness for information security awareness. In Chapter Two it was shown that information security awareness requires a behavioural change to be effective.

3.10. Organisational Culture

Organisational culture is an acceptance of common attitudes and beliefs at a collective level. An understanding of organisational culture is important in any attempt to understand or influence internal patterns of behaviour. There is a significant ongoing debate about what organisational culture is and how it evolves. Most attempts to quantify organisational culture measure the impact of culture, not culture itself.

Edgar Schein defines organisational culture as an ongoing process:

“A pattern of shared basic assumptions that was learned by a group as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think and feel in relation to those problems.” [SE-04]

Schein has described three examples of culture:

1. Artefacts are visible embodiments of culture expressed by a group. They can include dress codes and published values. While artefacts are the most visible examples of culture, they are also the most difficult to interpret. An observer can easily perceive the artefact as an example of culture but its meaning may not be clear.
2. Beliefs and values are solutions to group problems which have been perceived to have been successfully proven at some point in the group's history. Beliefs and values help interpret the artefacts present in organisations.
3. Underlying assumptions are the deeper shared perspectives of a group and the most resistant to change. To change an underlying assumption it must be challenged.

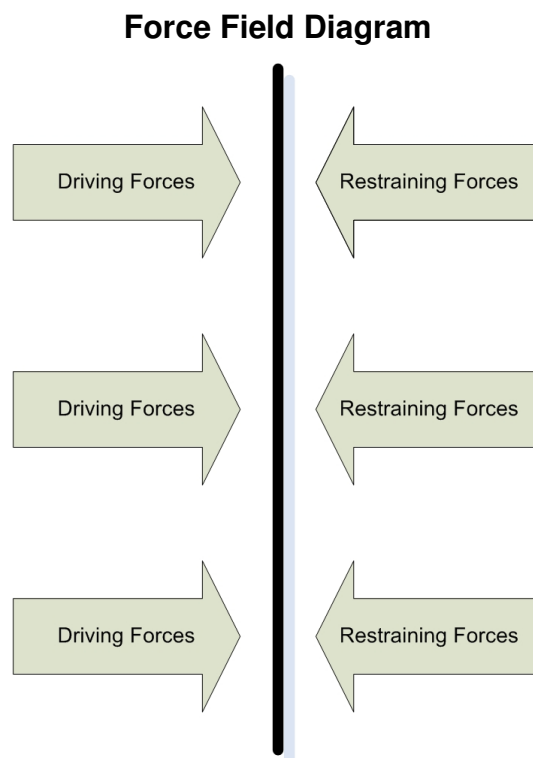
In contrast, Reason [BBJ-04] defines organisational culture in terms of an outcome:

“Shared values (what is important) and beliefs (how things work) that interact with an organisation's structures and control systems to produce behavioural norms (the way we do things round here).” [BBJ-04]

Though described from different perspectives, both views of organisational culture are consistent in that the effect is a form of behavioural control stemming from social norms.

Publications on organisational culture discuss theories on the mechanisms driving organisational culture changes. An early influence was the work of Douglas McGregor in *The Human Side of Enterprise* [CE-04]. He proposed that there were at least two management theories of workforce motivation and control. Theory X was a pessimistic view which held that people were lazy, needed to be told what to do and lacked ingenuity. Theory Y held that people were basically cooperative, capable of commitment to the organisation's objectives and would accept responsibility given the right environment. McGregor suggested that managers operating using assumptions matching theory X were less successful than theory Y.

Force Field Analysis was a concept developed by Kurt Lewin to conceptualise group dynamics [HM-08]. The idea is based on the proposition that in all organisations there are driving and restraining forces which work in opposite directions. The field in the middle represents equilibrium:



Force field diagram © Geordie Stewart

By conceptualising organisational forces it makes it possible to identify and measure the strength of the forces involved. The equilibrium can be shifted by either weakening a restraining force or strengthening a driving force.

Implications for information security awareness:

McGregor's findings indicate that audiences for information security awareness communications will respond better if given the opportunity to cooperate and accept responsibility willingly. Information security awareness could fit either a Theory X profile or a Theory Y profile depending on how it is implemented.

McIlwraith recommends that where possible, information security communications should avoid making demands, issuing deadlines and fostering a blame culture [MA-06]. Instead, organisations should encourage good information security practices with rewards and recognition.

Hogervorst has applied Lewin's Force Field concept to information security culture [HM-08] and has found an innovative way to identify and measure the forces involved when promoting information security awareness. She has also attempted to apply this concept to making a business case for information security awareness and in this effort she has been less successful. For example, when Lewin's model is used in this way it is not clear what the equilibrium represents. Hogervorst lists "Limited Budget" as a restraining force. If the equilibrium is to represent an appropriate balance between cost and control expenditure then it is not clear how changing factors such as the available budget will make an organisation "more secure". Arguably, the point at which the organisation would be considered secure should be determined by a risk assessment and costing of control options [SB-06].

3.11. Risk Compensation

Risk compensation, sometimes called Risk Homeostasis, occurs when a subject increases risk taking behaviour in response to a decrease in risk. When a risk equilibrium changes in a positive way, there is a tendency for individuals to change their behaviour in a way that nullifies some or all of the original risk reduction. Dr Ian

Walker measured the distance allowed by motorists when passing a cyclist and found a significant difference based on the cyclist wearing a helmet or not:

“Dr Walker, a traffic psychologist from the University's Department of Psychology, said: This study shows that when drivers overtake a cyclist, the margin for error they leave is affected by the cyclist's appearance.” [BBC-A]

By passing closer to cyclists, motorists were increasing the likelihood of an accident. This may have been rationalised by motorists considering a cyclist wearing a helmet is better protected in the event of an accident (a perceived reduction in the severity of impact).

The original proponent of Risk Homeostasis, Gerald J.S. Wilde, has argued that attitudes need to change in order to ascribe to a higher level of safety (or security) for the individuals involved and that most safety campaigns tend to “move risk around”. Implicitly this suggests that people come to accept the current level of risk in their particular environment and find ways to rationalise continuing at the same level of risk even when environmental factors change offering a potential overall reduction.

Implications for information security awareness:

It is important that any change in an information security risk equation in which a threat is reduced identifies the expectations of the individuals involved. This is necessary to raise the expectation of what an appropriate level of risk should be. Otherwise, with the introduction of a new information security control, individuals may increase risk taking which may impact the net benefit of the original control being applied.

3.12. Groupthink

Groupthink occurs when group decision making processes result in excessive risk taking [BBJ-04]. It can be recognised by the following characteristics:

1. Collectively, groups accept a higher tolerance for risk than an individual making the same decision. This appears to be related to a diffusion of responsibility for the decision when no individual member of the group is to be held accountable for the outcome
2. Dismissing warnings which are contrary to the group's assumptions
3. Belief that the morality of the group is absolute. This may be related to number one above
4. Stereotyping opposition to the group as dishonest or incapable in some way
5. Collective ridicule or censorship of any dissent from within the group
6. Voluntary self censorship from individuals within the group of ideas contrary to the group consensus
7. A false perception of consensus emerges because individuals self-censor and external dissent has been rationalised as unimportant

Implications for information security awareness:

To avoid the pattern of groupthink it is important that information security awareness focuses on personal accountability. Personal accountability is an essential component to motivate individuals to recognise what behaviour is required from them.

This has two important implications for information security awareness. Firstly, the design and implementation of awareness as a risk control can be developed by committee but should be approved by a responsible *individual*.

Secondly, the audience of information security awareness needs to be addressed as individuals. Organisational culture might help foster a sense of expectation for group behaviour which can provide social motivations, but the implications of groupthink accentuate the need to identify specific *actions* required by specific *individuals* in the context of information security.

3.13. Internalisation

Timothy Layton criticises the current approach which expects that the audience of information security awareness will successfully translate knowledge of the organisation's requirements into the desired behavioural outcome:

“The traditional approach to information security and information security awareness is for most organizations descriptive in nature. In practical terms, many organisations take the approach of “informing” their user community of their security practices, guidelines and procedures. This would be described as a descriptive approach, meaning users are told they must comply because management requires them to. The descriptive-based approach does nothing to help the users internalize or justify the organizations requirements, therefore their attitudes and motivations will be lacking and ultimately produce undesirable results.” [LT-05]

Layton makes a strong case for the importance of internalisation which results from prescriptive communications. Prescriptive communications are defined by Layton as internalised, rationalised decision making processes that incorporate knowledge and attitude to leverage behaviour. One of the ways to convey a prescriptive communication is to reference morals and ethics:

“The bottom line is that most people do not generally accept something just because a superior publishes a requirement, making the descriptive-based approach a poor investment. The majority of people will only internalise and support the message if they have justified it, believe in it, and think it is reasonable. It is logical to conclude the importance of measuring and understanding user's internalization of organizational policies.” [LT-05]

Layton advises an accomplishment based approach which acknowledges three developmental stages – preparation, awareness and commitment. Broadly, he suggests treating information security as an attitude rather than a technology issue. The starting point is to explain to the target audience why they should care about an issue. This is the prerequisite for developing an attitude where the consequence of compliance can be valued: *“People need to understand why and how, not just told to comply with a policy.” [LT-05]*

3.14. Chapter Summary

Areas of learning from the Psychology discipline relevant to information security awareness were identified and presented in an information security context. Motivations for compliance were analysed and evaluated in light of their application in an organisation with a view to their possible effectiveness.

It seems that compliance in an information security context usually depends on a fear motivator, and this may only apply when an individual perceives there is strong likelihood of being caught or the punishments are severe. Also, the need for real time monitoring was discussed and the possibility of increased motivation for compliance resulting from immediate feedback rather than compliance checks on a less real time basis such as monthly.

Areas of risk perception, cognition and bias were discussed. Humans appear to be broadly logical creatures but some systematic failures have been identified. Heuristics are mental shortcuts that are a consequence of the need to make decisions in a short period of time. While these mental shortcuts can lead to bias and behaviour which appears illogical, this behaviour is also predictable. Information security professionals need to anticipate the cognitive biases present in their audiences and adjust their information security awareness messages accordingly.

The concept of risk perception is exposed as a uniquely personal interpretation that organisations need to consider before embarking on a communications exercise.

In the next chapter, the concept of tuning a message for an audience is explored in a Marketing context.

4. Marketing and Information Security

At the start of this thesis it was observed that the discipline of Marketing may have a correlation with the objectives of information security awareness because of the Marketing focus on influencing the behaviour of a given audience. This chapter explains what Marketing is and identifies Marketing principles which might be valuable to information security professionals.

A review of Marketing publications [SA-01] [BP-08] [GP-07] has shown that there are numerous objectives of Marketing and a variety of ways which organisations choose to implement Marketing. Baines, Fill and Page [BP-08] identify three main definitions:

1. **A Chartered Institute of Marketing (CIM) definition:** *“The management process of anticipating, identifying and satisfying customer requirements profitably.”* [BP-08]
2. **An American Marketing Association (AMA) definition:** *“...the activity, set of instructions, and processes for creating, communicating, delivering, and exchanging offerings that have value for customers, clients, partners, and society at large.”* [BP-08]
3. **A French perspective:** *“...the endeavor of adapting organizations to their competitive markets in order to influence, in their favor, the behavior of their publics, with an offer whose perceived value is durably superior to that of the competition”* (Lendrevie, Levy and Lindon 2006). [BP-08]

There are two common themes to these definitions. The first is the communications component and the second is the notion of profit or value. A form of dialogue takes place which enables a mutually beneficial result. In the previous section on Psychology it was noted that attitudes were an important component in the process of rationalising behaviour. Could Marketing help with the problem of understanding and changing attitudes for the benefit of information security awareness?

“Since marketing is about understanding customers’ needs, we must place ourselves in the mindset of our customer if we are able to properly understand their needs.”
[BP-08]

While Psychology relies on studies where often people recognise that they are being measured in some way, marketers have the advantage that sales patterns exist with millions of participants, none of whom need be conscious of being studied.

It is important here to note the difference between “Sales” and “Marketing”. Baines, Fill and Page identify an important distinction:

“...sales emphasizes the process of product push, by creating distribution incentives for both salespeople and customers to make exchanges which may or may not benefit the customer in the long term.” [BP-08]

From this definition, the sales process is the last step in a delivery cycle of a product or service. This is in contrast to Marketing’s longer term focus:

“Marketing on the other hand is more focused on creating product pull, or demand, amongst customers and consumers, and the offering is designed and redesigned through customer and consumer input, through research to meet their longer-term needs”. [BP-08]

Some aspects of Marketing are less relevant to information security awareness. Implicit in the definition of a customer or a consumer is that normally money is exchanged and money acts as the long term motivation for the party performing the Marketing. However, profit is not always the motivation for Marketing:

“...there is a vast swathe of other organizations that operate in what is referred to as the non-profit sector. For example, local government, churches, museums, charities, universities, zoos and public hospitals all operate without profit as their central goal...Non-profit organizations have a range of goals, a multiple set of tasks they seek to achieve. These include generating awareness...” [BP-08]

The closest correlation to information security awareness would probably be government campaigns such as “Think” Road Safety”, an initiative that seeks to influence the behaviour of people for the benefit of road safety. The Department for Transport’s stated objective is:

“To reduce the number of people killed or seriously injured in road accidents by 40 per cent by 2010...” [DFT-A]

This campaign has some key similarities to information security awareness:

- Profit is not the primary objective. (Although there may be a significant shared economic benefit from reducing road accidents)
- Awareness of risk is one of the key components which the campaign seeks to communicate

Implications for information security awareness:

There are important points to note for information security professionals from the various definitions of Marketing. The CIM definition mentions “anticipating” requirements. To what extent should information security awareness be predictive? How often are information security awareness initiatives only generated as a response to a security incident?

“A frequently noticed behaviour is that companies start to think about security only after having their first incidents, and stop their actions a short time later. It is essential to develop new approaches to make sure that companies are able to handle security as a process...” [SJ-08]

The Marketing approach reinforces a focus on long term anticipation of needs rather than incident response.

The AMA definition above mentions communicating information that has “value” for the target audience. “Value” in the context of information security awareness is more difficult to define. In theory, a user of an information system within an organisation has a vested interest in protecting the information system. The problem here is that when an organisation suffers an information security breach caused by an individual, the individual is unlikely to suffer as much as the organisation, especially if the cause of the breach is never attributed. If the user is an employee and their behaviour results in damage to the information system the employee could face disciplinary action or other social sanctions within the organisation. Or, the cause of the security breach may never be identified. For companies or other profit motivated

organisations, serious damage to an information system could conceivably impact the organisation's financial viability. If the company's viability is threatened this could result in job losses or company failure. Job security should be one of the motivators for employees within profit generating organisations. Even if the cause of a security incident could not be attributed to an individual, the motivation of employment security could still apply.

Having reviewed the current theories of Marketing in an information security context, the following definition for information security Marketing is proposed:

“Anticipating the communication requirements of an audience to develop behaviour of a mutual, measured benefit which results in a reduction of an organisation's information security risk.”

Using this definition, this chapter will cover relevant Marketing topics such as:

- **Mass Marketing:** the use of one way broadcast media
- **Direct Marketing:** the use of profile based Marketing to generate a measurable response
- **Market Research:** the process of identifying needs and communication requirements of an audience
- **Diffusion Theory:** the adoption profile that results from Marketing activity
- **Social Learning:** behavioural change through the imitation of others

4.1. Mass Marketing

The Mass Marketing approach uses mass mediums [BP-08] such as television and radio to reach large audiences. Mass Marketing is frequently used to create, maintain or change brand awareness. The value of this approach has been questioned by Baines et al [BP-08] for the weak association between receipt of advertising messages and actual behaviour. Potentially, Mass Marketing is becoming more inefficient as mass markets become smaller and more fragmented.

Implications for information security awareness:

Many of the tools used for information security awareness such as posters and screen savers would likely be recognised by marketers as a Mass Marketing approach. This method anticipates low response rates and it can be difficult to quantify the results.

While marketers potentially don't care who buys their product or service, this is not the same for information security awareness. Some "sales" are worth more than others. Some members of the audience are more important than others because of the tasks they perform. Those who handle sensitive personal data are more important to communicate successfully to than those who don't. Therefore, the Mass Marketing approach is a poor method of communicating security awareness. A possible exception to this is if the Mass Marketing approach was being performed as a part of creating a security culture.

4.2. Direct Marketing

Direct Marketing is a relatively new phenomenon and is a response to the gradual inefficiency of Mass Marketing:

"In the half century leading up to 2005, the whole focus of marketing had been on optimizing mass markets...Marketers learned to analyze response rates down to a thousandth of a percentage point and to tailor campaigns that would appear to maybe 3 percent of an audience of millions...The waste was incredible, but there was no alternative in a market that had no way to efficiently speak to communities of customers." [GP-07]

Sargeant and West [SA-01] state that Direct Marketing in contrast to Mass Marketing, has an increased focus on the individual. In the later half of the twentieth century, markets became increasingly segmented with greater focus on the needs of individuals:

"It was 1970 when Alvin Toffler introduced the term demassification into marketing vocabulary, noting that mass markets were gradually eroding and with them went the

need for mass marketing approaches. By the mid 1970's consumers had started to become more discerning, thoughtful and individualist...For evidence of this new thinking it is worth remembering that it is not so very long ago that bathtubs were white, telephones were black and cheques were green." [SA-01]

When dealing with individuals instead of markets, each individual may have a preference for communication methods. The degree to which personal interests are shared can also vary. Modern databases have facilitated Direct Marketing techniques by allowing a large amount of information to be stored about an individual's preferences (previous behaviour) and attributes (characteristics which help define the person in some way). While it can take more effort to undertake a Direct Marketing approach over a Mass Marketing approach, the response rates from Direct Marketing are normally higher. Direct Marketing also supports the overall goal of building a relationship with individuals:

"In direct marketing, the goal is to use customer information to develop an ongoing, continuous relationship with each individual on the database." [SA-01]

Ideally Direct Marketing communications are personalised in a way recognisable to the audience. Rather than being a blanket communication through a broadcast medium such as radio or television, it is usually customised in some way for a particular segment of audience.

The other defining feature of Direct Marketing is the expected result – a call to action of some sort on behalf of the recipient. Rather than dealing with concepts as abstract as brand awareness, Direct Marketing has an empirical outcome expected of each set of interactions. The outcome could be to call a phone number, visit a web site or reply to a letter. Attributing the responses received allows a return on investment (ROI) to be calculated.

It is also important that medium used allows the attribution of responses to the invitation that preceded it. For example, phone numbers advertised on a letter as part of a Direct Marketing campaign could be unique to the offer. If the phone number is not advertised anywhere else the organisation will know exactly how many responses the letter generated. Exact measurement of responses is critical to

calculating further refinements to the campaign. This is in contrast to Mass Marketing:

“With mass marketing it is all but impossible to link a sale to the advertisement that initiated it.” [SA-01]

So the defining features of Direct Marketing are that communications are personal in some way, take place within the context of an ongoing expected relationship, and have a tangible outcome which is measured in order to optimise the process.

The tangible, direct outcome allows a greater degree of ongoing refinement and improvement over Mass Marketing approaches. Direct Marketing allows for variations to be made in language, content and presentation to separate audiences and the results used to optimise future communications. For example, three variations on an offer could be sent to a demographic such as 30-50 year old women who have previously purchased a book on cooking. The letters could be different in a variety of ways: design, font size, use of colour or the size and shape of the envelope. Whatever the results, the organisation will have learned how to further optimise their communications with that type of customer for that product.

The Direct Marketing approach can also be used to optimise other communication factors such as time of year and length of content [SA-01].

Implications for information security awareness:

The implication for information security awareness is that most organisations should already have the basic prerequisites to communicate information security policy based on a Direct Marketing campaign. Consider that there is usually already a relationship between the organisation and its target audience who could exist as employees or customers of its information system. Secondly most organisations would already have a significant database about their potential audience which would show many preferences and attributes useful for designing communications. For employees the company is likely to have details such as job title, how old they are, sex, where they live, what business area they work in, how long they have been working for the company and how many times they have called IT for support. For

customers of an organisation the organisation will likely know where they live, how long they have been a customer and how often they have called for support of an information system. These are all useful attributes to know when attempting to understand the perspectives and likely responses of an audience.

Another implication of a Direct Marketing approach is the importance of a quantifiable result in the form of ROI. To leverage the advantages of Direct Marketing, any information security awareness initiative must be measurable in some way. Some initiatives may be easier to measure than others.

If information security awareness really is as important as so many information security practitioners make it out to be, then is it not worth doing effectively? Taking a Direct Marketing approach to information security awareness could hold the answer to the problem of attaining and demonstrating effective communication.

4.3. Market Research

Baines, Fill and Page define Market Research as:

“The design, collection, analysis, and interpretation of data collected for the purpose of aiding marketing decision making”. [BP-08]

In this context, Market Research supports the creation of Marketing communications by defining subgroups within an audience and identifying ways in which communication with these groups might be successful.

Baines, Fill and Page [BP-08] identify two main methods of market segmentation, or defining subgroups within an audience:

1. **The Breakdown Method:** this is where a market (or audience) is assumed to be basically the same and the focus is on identifying differences.
2. **The Build-up Method:** this is where a market (or audience) is assumed to be different and the focus is on identifying similarities.

According to Baines, Fill and Page the Breakdown Method is most commonly used.

Implications for information security awareness:

Improving knowledge about individuals within the target audience offers a way to optimise communication. Direct Marketers would be unlikely to send a blanket communication to all their customers because of a poor return, so why would an organisation adopt a one size fits all approach to information security awareness? Does it make sense for all employees to be presented with the same information security policy, attend the same information security awareness training and be presented with the same motivators for compliance?

In theory, the larger the organisation, the more diverse the communication needs of the audience. The needs of office based staff will be different to field engineers. Men respond to communications differently than women. Age is another potential factor which might hold a clue to the individual's competency level with computers in general.

One of the important aspects to learn from Direct Marketing is *relevancy*. An information security policy might hold any number of chapters or sections relevant for different functions within the organisation. Does it make sense to give all policy instructions to all users of an information system? The Direct Marketing approach would suggest that at the very least, a role based approach should be taken to information security policy. For example, an information security policy laid out according to ISO 27001 headings might make sense for an information security professional, but is unfamiliar for its intended audience. Ideally, a role based approach to information security policy might look like the following:

Chapter One:	General User Security Responsibilities
Chapter Two:	Responsibilities for Managers
Chapter Three:	Responsibilities for Internet and Email Users
Chapter Four:	Responsibilities for System Administrators
Chapter Five:	Responsibilities for System Developers

For example, a manager of system administrators who has access to the internet might receive only chapters one, two, three and four.

4.4. Social Media

Traditionally, advertising is a one way transmission with little in the way of measurable response from the target audience [BP-08]. While Direct Marketing expects a response this is normally an acceptance of an offer or expression of preferences. Direct Marketing normally is not considered a full “conversation”.

In contrast to this, Gillin [GP-07] defines Social Media as including a range of two way conversations. Typical examples are web blogs and internet forums. Common features are that they are decentralised and have feedback channels. The feedback channels are the components which tend to make the interaction feel more like a one on one conversation. Gillin [GP-07] makes a strong case that the traditional one way dynamic has changed with the introduction of Social Media:

“Social media offers marketers a chance to break this gridlock and engage with their customers in a whole new way. The new discipline is coming to be known as “conversation marketing”. [GP-07]

People are exposed to a large number of advertisements every day, some of it contradictory and the expected impact on any individual member of an audience is low. Pinker [SP-97] argues that the greater the cognition focused on a communication, the more it is expected impact attitudes and beliefs. The majority of advertisements such as billboards at the bus stop and messages on mouse mats require little in the way of cognitive function, therefore little can be expected in the way of impact to audience attitudes and beliefs because specific cognitive focus is not required by the situation. Advertising in the traditional sense is limited in its cognitive engagement. Often successful advertising uses emotional engagement to increase the audience cognition level [BP-08]. This means we feel something in response to the message, be it envy, desire or revulsion.

In contrast, an interactive conversation requiring cognitive thought to construct an argument or communicate an attitude or belief has a far greater chance to contribute to attitudes or beliefs.

From a learning perspective, the two way communication of Social Media is similar to the “Socratic Method” where an audience participates in a debate about the concepts being discussed. The Socratic Method is effective partly because of the increased cognitive participation of the audience.

Implications for information security awareness:

Social Media offers two enticing potential benefits to compliance communications such as information security awareness.

Firstly, attitudes are more likely to change as a result of a personal conversation than a broadcast [SA-01]. A good example illustrating the importance of audience feedback is the controversy over security communications for the Transportation Security Administration (TSA). In this case the TSA published an account of an event that occurred at a security checkpoint [TSA-A]. This account came in to widespread criticism for its tone and logic by bloggers [SB-A], [GIZ-A]. Chapter Three of this thesis identified credibility as one of the key ingredients of influence between a subject matter expert and an audience. The security position taken by the TSA resulted in ridicule which exposed the TSA’s credibility to damage. Unusually, the TSA took the step of replying to the criticism and posted an amended article on its website:

“...We obviously had a lapse of judgement on this story and you folks in the blogosphere have done a good job of keeping us honest. The points made by Gizmodo, Boing Boing, and Bruce Schneier were compelling. First, the headline is misleading, we totally over-hyped it...” [TSA-A]

This admission by the TSA is significant. Firstly, the TSA has responded to informal, online criticism which is an unusual precedent and demonstrates the power and influence of new Social Media. Secondly, it demonstrates the value that TSA places in maintaining the perception of credibility. The three internet resources named have a significant readership which have been actively participating in criticisms of the TSA. Bruce Schneier’s blog alone has 125,000 subscribers [SB-B].

Secondly, Social Media can be a useful channel for feedback to discover potential security barriers to compliance. As discussed in Chapter Three, barriers to compliance can include issues of trust between the subject matter experts and an audience which can be very damaging. It is very important that barriers to compliance are identified and removed wherever possible.

McIlwraith cites a concern [MA-06] about the use of open media in an information security context that consistency of message could be lost and that the moderation of a Social Media forum could be resource intensive.

While it is to be expected that different opinions will be expressed in a social networking environment, these differing opinions can foster a healthy debate about the purpose and method of information security in the organisation. Rather than the audience receiving a homogenised version, it may stimulate cognitive involvement by exposure to alternate points of view. This cognitive involvement is what has been identified in Chapter Three as more likely to lead to behavioural change.

Also, if objections to information security activities are raised this gives the Information Security Team an opportunity to justify methods and build trust which was identified as an important component in Chapter Three.

McIlwraith's point about moderation of environments being resource intensive is also only partially valid. If the resources required to moderate such an environment increase this could be because the environment has become more popular and therefore more effective. Such an environment also offers the opportunity to collect reliable metrics.

4.5. Chapter Summary

Chapter Four investigated the implications for a Marketing approach to information security awareness. The importance of identifying differences in perceptions for the target market was shown to be a critical success factor in Marketing campaigns.

The Direct Marketing approach was shown to be most similar to the situation faced by organisations when dealing with known entities such as staff or customers. Direct Marketing stresses an ongoing communications relationship with feedback channels and empirical methods to measure success. This approach would be invaluable to information security practitioners designing and implementing an information security awareness programme.

Market Research showed the importance of identifying the needs of subgroups within a target audience. Communications need to be refined on an ongoing basis through content, presentation and the frequency of delivery. Consider the model proposed in Section 2.4 – the composition of every layer has the potential to either include or alienate an individual's opportunity to learn, motivate or adapt behaviour.

Social Media is discussed as a significant area of opportunity for information security professionals to engage more effectively with audiences and build trust.

The following model has been constructed to summarise the similarities between Marketing and information security:

Concept	Marketing Example	Security Example
Target Audience	 Customer	 Employee
Goal	 Sales	 Risk Reduction
Direct Marketing Method	 Letter	 Email
Mass Marketing Method	 TV	 Screen Saver
Empirical Measure	 Sales	 Compliance

Marketing and Information Security Comparison © Geordie Stewart

Chapter Five goes on to summarise the principles identified from Psychology and Marketing into a reference model that can be used by information security professionals to review the expected effectiveness of an information security awareness campaign.

5. Proposed Qualitative Model for Measuring Security Awareness Effectiveness


It is clear from the review of Psychology and Marketing that there are a complex series of factors that impact the success of an information security awareness programme.

The following reference model has been created to show designers and implementers of information security awareness programmes how to align with Psychology and Marketing principles. This includes principles such as risk perception, learning and motivation for the modification of behaviour.

Some elements are relevant to the design of an information security awareness programme and some are relevant to how it is implemented.

Proposed Model #2 - Qualitative Information Security Awareness Scorecard

Anticipating the Effectiveness of Information Security Communications

Confidence in Anticipated Effectiveness 		
Poor Antecedents For Effectiveness	Some Antecedents For Effectiveness	Strong Antecedents For Effectiveness
The Moral Case For Compliance		
<ul style="list-style-type: none"> Compliance not explained in a moral context No reference to potential impacts to the organisation or individuals Language is descriptive in nature 	<ul style="list-style-type: none"> Some moral references Impact of security breaches may be mentioned but few references made to personal or organisational impact 	<ul style="list-style-type: none"> Repeated moral references Uses prescriptive language to invoke moral cognition: "Responsibility" "Ethics" Refers to the expectations of staff, customers and other stakeholders
Rewards for Compliance		
<ul style="list-style-type: none"> Limited or no use of fear sanctions (Positive Punishment) Long delays between behaviour and a response from the organisation (if any) 	<ul style="list-style-type: none"> Appeals to fear sanctions Some use of positive encouragement Infrequent compliance checking Some delays between behaviour and a response from the organisation 	<ul style="list-style-type: none"> Use of a range of positive and negative reinforcement Rewards or punishments delivered soon after behaviour
Organisational Culture		
<ul style="list-style-type: none"> Importance of information security not mentioned by management Management often seen to break the rules Reliance on punishments to promote change 	<ul style="list-style-type: none"> Some support from management for information security Management sometimes seen to break the rules 	<ul style="list-style-type: none"> Security policy and awareness visibly supported by the organisation's top leadership Management seen to lead by example Information security successes are celebrated
Compliance Monitoring		
<ul style="list-style-type: none"> Little or no compliance monitoring Compliance checking activities generated in response to an incident No empirical metrics collected 	<ul style="list-style-type: none"> Some monitoring for compliance May be on an infrequent basis Minor breaches may be ignored Awareness metrics used to indirectly infer behaviour 	<ul style="list-style-type: none"> Real time compliance monitoring Feedback delivered to individuals in breach within a short time period Metrics directly measure behaviour
Market Research		
<ul style="list-style-type: none"> No attempt to understand the beliefs and attitudes of the target audience 	<ul style="list-style-type: none"> Some mapping of beliefs and attitudes Some attempts to understand the attitudes and knowledge of the intended audience 	<ul style="list-style-type: none"> Strengths of beliefs and attitudes have been identified and measured Demographics identified for the audience Bespoke information security policy and awareness developed specifically for the target audience
Direct Marketing		
<ul style="list-style-type: none"> Generic Information Security Policy and Awareness Communications 	<ul style="list-style-type: none"> Generic information security policy and awareness communications with some customisations Some attempt to segment audiences 	<ul style="list-style-type: none"> Audience segmentation completed to match audience needs with the organisation's information security needs Bespoke information security policy and awareness developed specifically for the target audience
Social Media		
<ul style="list-style-type: none"> No feedback channels available to generate and collect audience response 	<ul style="list-style-type: none"> Some feedback channels available such as a contact person or email address Limited or no use of social media 	<ul style="list-style-type: none"> Uses Social Networking such as forums and Blogs to energise audience involvement Feedback is encouraged to identify barriers to implementation
Presentation		
<ul style="list-style-type: none"> Frequently uses language of a technical nature Uses long sentences Not attention grabbing Visually bland and boring 	<ul style="list-style-type: none"> Some feedback channels available such as a contact person or email address Limited or no use of social media Some use of bullet points to convey messages 	<ul style="list-style-type: none"> Uses social networking such as forums and Blogs to energise audience involvement Messages are consistent Uses simple themes with specific point Uses bullet points, bolding and font variations to convey key messages

6. Conclusions: Psychology and Marketing Implications for Information Security Awareness

This thesis has focused on information security awareness and the extent to which Psychology and Marketing could help effectiveness and efficiency of information security communications. It is clear from the review of Psychology and Marketing principles that there is a wealth of knowledge outside of the information technology domain which is of benefit to information security practitioners.

Finding One: A Lack of Empirical Metrics

A reoccurring theme in the review of information security awareness effectiveness is a lack of metrics to demonstrate the impact of information security awareness. Information security practitioners need to find ways of measuring results in the form of behaviours. Measuring attitudes and beliefs through the use of surveys is found to have a poor correlation with expected behaviour.

This lack of metrics not only causes problems with obtaining business support for information awareness activities, but also has contributed to a difficulty in improving information security awareness techniques. The bedrock of the Plan, Do, Check, Act management cycle is reliable metrics. If there are no reliable ways available to an organisation to demonstrate the effectiveness of a particular technique, how can improvements be made by identifying that one technique was more effective than another? Although this thesis has found ways of improving information security awareness using Psychology and Marketing principles, the benefits will be difficult to realise because of the lack of metrics.

Information security professionals are to blame for this situation but information security professionals are also part of the solution. Information security professionals need to move beyond glib statements about the criticality of awareness and focus on making a business case for awareness activities. All behaviour has a consequence and some consequences are easier to measure than others. Information security

professionals need to find ways of measuring these consequences to infer the effectiveness of communication techniques.

The model developed in Chapter Two illustrates the steps involved in achieving a change in behaviour resulting from risk communication. Each stage in the model represents an opportunity for declining effectiveness and therefore metrics are needed for each stage in order to identify problems with effectiveness or barriers to compliance.

Finding Two: The Importance of Psychology and Marketing

In the disciplines of Psychology and Marketing there are many principles which have been identified as relevant to information security communications. These principles have been summarised in a “Qualitative Information Security Awareness Scorecard” in Chapter Five to enable information security professionals to judge the extent to which their approach to information security awareness reflects optimal use of Psychology and Marketing.

Direct Marketing is identified as a discipline which is ideal to help information security professionals identify appropriate metrics and tune communications to an optimal level for a given audience. It is noted that most organisations should already have the prerequisite information to enable this approach including the existing relationship, contact details and demographics of their audience. Even if organisations do not have sufficient demographics for their information system users, these can be gathered using existing relationships.

Finding Three: The Limited Impact of Awareness

There are significant concerns about the extent to which information security awareness successfully promotes behavioural change. The detail of a study involving risk awareness is included in Appendix B. This study found very little impact to behaviour from introducing risk awareness, even when motivational factors should have contributed to risk avoidance behaviour.

The study goes some way to validating the concerns made by Jeff Bock-Brown [BBJ-04] that awareness is not reliably translating into behavioural change. Unless there is a behavioural change there is no resulting risk reduction. Being aware of the information security risks but continuing the behaviour anyway does not result in a benefit for the organisation.

Although other authors such as Monique Hogervorst [HM-08] and Rebecca Herold [HR-05] would disagree about the impact of information security awareness, no reliable evidence has been found to support their enthusiasm for information security awareness being “the most significant single defence measure...” [HM-08]. If effective information security was actually achieved their views might be true but there is no evidence that this is obtainable given the methods currently used.

It is important to note that no training will ever be 100% effective at mitigating a human risk. People can only apply their training when they recognise a situation which calls for this training to be used. The model in Section 2.4 has demonstrated that lack of attendance, learning failures and behavioural barriers are among many reasons why awareness efforts will never be 100% effective.

Finding Four: Excessive Fear Appeals

Research in the discipline of Psychology has shown the importance of the human behaviour in response to fear. The “Boomerang Effect” is shown as significant when fear is used as a motivator. Organisations need to be aware that if the perceived ability of the individual responding to the risk is too low the result is likely to be a deliberate ignoring of the threat using cognitive coping mechanisms.

Excessive fear is also associated with a decline in cognitive effectiveness. The example given was about memory performance but this applies to other cognitive tasks. The implication is that it might be possible to scare users with information security threats and risks to the extent that they perform mistakes in a usability context.

Finding Five: Risk Distortion through Human Perception of Risk

Perception of risk has an important impact on the needs of risk communication. Chapter Three demonstrated the importance of identifying and measuring existing perceptions in the target audience. Shortcuts in thinking about risk, divergent interrelations of key words and variable attitudes can all distort an information security awareness message. There is no such thing as an “average” organisation so a best practice approach which does not sufficiently allow for its target audience may be ineffective.

Research in public risk communication has shown the importance of checking the interpretation of key words and measuring the strength of associations to optimise communications plans. While perceptions and attitudes to risks such as safety have been extensively explored in the public domain with researchers such as Slovic [SP-00] and Morgan [MM-02], this same level of research has not been applied to information security communications and is an area of significant potential research.

A study was done as part of this thesis to gauge the extent to which mistaken beliefs about the meaning of information security words and differing attitudes might be effecting information security communication. Appendix A shows the result when a questionnaire was given to a Security Team, a Human Resources Team and an Accounts Payable Team within the same organisation.

There were two interesting findings. Firstly while as to be expected the three teams showed differences, all three areas were also internally inconsistent. The meaning of key information security words (beliefs) were interpreted significantly differently within each team even before comparing to other teams.

Secondly, a significant number of responders had conflicting beliefs. Some of the questions could not both be true such as Question Eight: “*Internal threats pose a greater risk to the organisation than external threats*” and Question Twelve: “*External security threats pose a greater risk to the organisation than internal threats*”. It is not understood why this would be the case. It is possible that the question order, sentence order or the availability heuristic is having an effect but more research is needed.

The study in Appendix A has demonstrated the importance of Morgan's approach in clarifying the meaning of key words before proceeding with communication. It also illustrates the need to quantify and measure existing attitudes before communicating a set of rules. Chapter Three on Psychology noted the importance of morals and ethics for motivation. Attitudes have been defined as beliefs with a value judgement attached. Therefore, existing attitudes go a long way to explaining the moral perspectives of an audience. To change the behaviour of users taking work home (Question Seventeen) it is necessary to identify and challenge any supporting moral judgements (for example working overtime is more important than information confidentiality). It is only by addressing the underlying moral judgement that a request for compliance will become reliably effective unless the sanction is severe.

Summary

This thesis set out to help improve the effectiveness of information security awareness through an understanding of Psychology and Marketing principles.

A review of Psychology and Marketing principles shows significant opportunities for a more holistic approach to communicating information security awareness. However, the lack of reliable metrics has been identified as a common barrier for demonstrating the effectiveness of these alternate methods. The Mental Models method in particular shows significant promise in mapping existing audience beliefs and attitudes.

Two models were created as part of this thesis. The first one in Chapter Two illustrates the steps involved in achieving a behavioural change and shows how many potential barriers need to be considered when promoting a behaviour change through awareness.

The second model in Chapter Five is a scorecard that information security professionals can use to evaluate the extent to which an information security awareness campaign takes into account Psychology and Marketing principles which are likely indicators of success.

While both models offer significant opportunities to help refine approaches to information security awareness it will be difficult to quantify the benefit until improvements are made to the way that organisations measure success.

7. Appendix A: Sample Information Security Mental Models Questionnaire

Purpose:

Chapter Three discussed the importance that Morgan [MM-02] placed on measuring the strengths of existing beliefs and attitudes as a precursor to communication activities. A study was completed to examine the extent to which information security attitudes and beliefs might be divergent within a large UK organisation.

Method:

A set of twenty questions was created using the methodology recommended by Morgan. These questions included measuring the strength of beliefs such as “A risk is the same thing as a threat” and attitudes such as “I should consider someone’s motivations before reporting them for suspected breaches of information security policy”.

Three teams within the organisation were invited to respond to the survey:

- The Information Security Team
- The Human Resources Team
- The Accounts Payable Team

Answers could const of one of five responses:

- True
- Probably True
- Neutral / Unsure
- Probably False
- False

Information Security Mental Models Questionnaire:

#	Proposition	False	Probably False	Don't Know	Probably True	True
1	Information security is mainly about protecting computers from hackers on the internet					
2	A risk is the same thing as a threat					
3	A firewall prevents most information security risks					
4	Complicated passwords keep computers safe from hackers					
5	Viruses and worms normally infect a computer from infected emails					
6	I have a good understanding of information security risks					
7	Most information security breaches are caused by viruses					
8	Internal threats pose a greater risk to the organisation than external threats					
9	Most of the information security risk for the organisation comes from employees using the internet					
10	Information security is the same as information safety					
11	Hackers on the internet are the greatest threat to the organisation					
12	External security threats pose a greater risk to the organisation than internal threats					
13	It is the goal of this organisation to be reasonably secure					
14	It is the goal of this organisation to be completely secure					
15	It is the goal of this organisation to be 100% compliant with the Data Protection Act					
16	Excessive use of the internet during work time is a security problem					
17	Taking computer files home to work on a home computer is a security breach					
18	I should consider someone's motivations before reporting them for suspected breaches of information security policy					
19	Everyone is responsible for information security					
20	Most breaches of information security are caused by accident					

Results:

The results were surprising in that while differences were expected between the teams, the teams were also internally inconsistent.

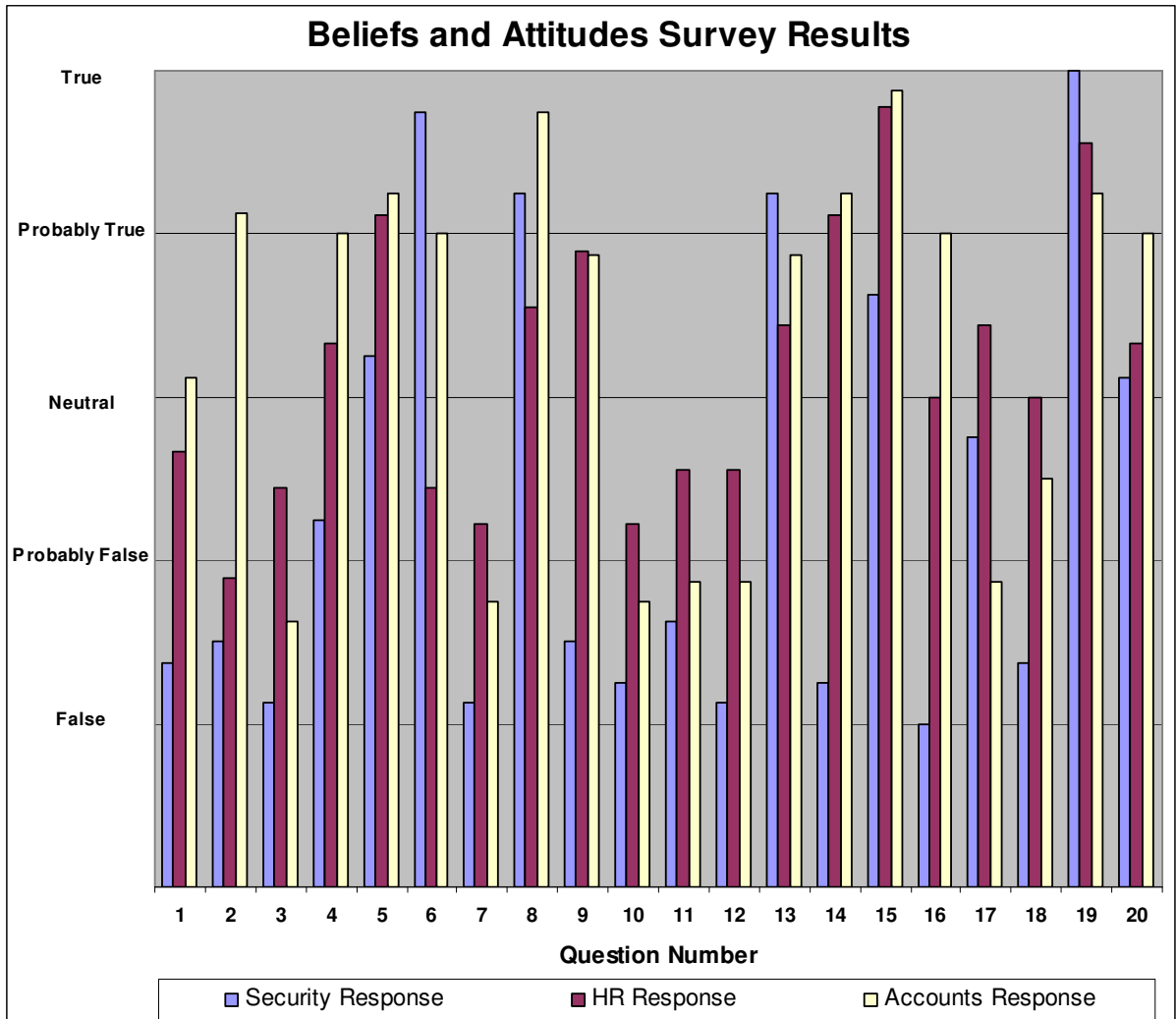
Firstly, the interpretation of words was shown to be problematic. Question Two tested the perception of the words “Threat” and “Risk” with the statement: “A risk is the same thing as a threat”. Even within the Information Security Team there was a significant divergence, indicating that there were different beliefs about the meaning of the concept of “Threat” and “Risk”. This is surprising given that information security were the technical specialists in this language domain.

Within the Human Resources Team there was also a divergent range of perceptions about “Threats” and “Risks”. Faced with uncertainty in a subject matter outside of their expertise, most of the Human Resources responses might have been expected to be neutral or “Probably False” or “Probably True”. Instead, 37% of responses professed to be sure that the answer was either “True” or “False”. The difference between “Probably True” and “True” is the degree of certainty. The individuals who answered “True” may not be aware that they are mistaken.

The clear implication from this observation is that defining key terms such as “Threats” or “Risks” needs to take place before any communications take place. An awareness campaign communicating ways to control or reduce risk is unlikely to be effective if the target audience fundamentally misunderstands the concept of what a “Risk” is. Part of the initial communication might be to define exactly what the organisation defines a “Threat” to be.

Question 17 tested an attitude: “Taking computer files home to work on a home computer is a security breach”. The results were split down the middle for the information security team. Half the team said that it was a security breach and half the team said it wasn't. Potentially, this could be contributing to mixed messages in information security communications.

The following graph shows the average results for the three teams:



Beliefs and attitudes survey © Geordie Stewart

8. Appendix B: Euston Road Warning Signs

Window cleaners operating at number 250 Euston Road in London led to an opportunity to study a human response to risk communications. Originally, this thesis was not going to include a study with a large number of subjects but this situation presented an ideal opportunity to observe how people responded to risk awareness in an everyday setting without necessarily being aware that they were being observed.

The window cleaners were operating on scaffolding above a busy footpath and six warning signs had been deployed in a row directly underneath. As laid out, the signs divided approximately 1/3rd of the footpath space directly under the cleaners.



The signs were apparently intended to communicate a safety hazard with the apparent expectation that pedestrians would avoid walking underneath. The signs were yellow, high visibility with clear black text including the word “Danger” prominently displayed:



Purpose

To measure the impact caused by the presence of the signs. Of interest would be the extent to which the signs communicated an awareness of a risk that would have an effect on how pedestrians chose to use the sidewalk.

Method

For a period of 30 minutes the following events were counted:

- The number of pedestrians walking inside the line of cones and under the hazard.
- The number of pedestrians walking outside the line of cones and away from the hazard.

Euston Road Warning Signs

- The number of pedestrians who looked up to check what the signs were referring to.

As a control comparison, the experiment was repeated at 4.30pm later that day when the signs had been removed. The distribution and number of pedestrians was counted again to evaluate the effect the signs had on how the sidewalk was used.

Results:

9.15am – 9.45am

	Number	%
Pedestrians walking inside the Cones (under the window cleaners)	36	29
Pedestrians walking outside the Cones (away from the window cleaners)	89	71
Total number of pedestrians	125	100

Only three pedestrians looked up to see what the signs were referring to. Two of the pedestrians were walking inside the cones and under the window cleaners and one of the pedestrians was walking outside the coned area. None of the three changed their direction on the footpath after observing the window cleaners above.



4.30pm – 5.00pm

	Number	%
Pedestrians walking under where the window cleaners had been	43	31
Pedestrians walking outside the area which had been marked by cones	96	69
Total number of pedestrians	139	100



Analysis:

The difference between the warning cones being present or not amounted to only a 2% influence on how pedestrians used the pavement. This difference is statistically insignificant and is unexpected given the assumed motivation for pedestrians to avoid personal safety risk.

While the 2% difference is interesting it is also significant how few people looked up to see what the danger signs were referring to. Of the two pedestrians who looked up while taking a path which took them under the window cleaners, neither changed course to manage the potential danger of falling objects.

The results are surprising because of the ingredients present to communicate risk:

- The bright yellow, highly visible danger signs
- The reference to the threat “Men Working Overhead”
- A visible threat in the form of a hanging window cleaner basket some five meters above

Measuring pavement use later that day was necessary in order to account for patterns of how people used the pavement. Potentially, preferences for walking closer or further away from the road would have been an unknown variable.

Potentially, morning pedestrians use the pavement differently than afternoon pedestrians and an improvement would have been to do the test at the same time on a consecutive day.

It's not clear from the results how many pedestrians were actually aware of the risk. The results show that there was little if any significant impact on behaviour caused by the presence of the warning signs. What the results don't show is how many pedestrians received the risk communication component successfully and how many lacked sufficient cognitive focus or motivation to act on their awareness. To find out if pedestrians walking under the window cleaners were conscious of the risk communication it would have been necessary to stop them and ask after walking under if they recalled a warning sign and what it said.

Another possible explanation for the low impact on behaviour is that pedestrians inherently felt “safe” walking down a busy street. It might be that there was a perceived safety in numbers which influenced the level of threat that pedestrians recognised.

Conclusion:

This study has demonstrated an example of how communicating awareness does not necessarily result in behavioural change. In this case the behavioural change required to manage the risk was a very minor one – pedestrians only needed to walk a few steps on a different side of the pavement and significantly reduce the risk of falling objects.

It is surprising how many pedestrians did not make an effort to walk outside of the danger area. The situation had many of the ingredients discussed in Chapter Three for promoting behavioural change – a risk posed directly to the individual, eye catching communication and a high level of personal efficacy to deal with the risk.

Potentially, the level of cognition given to the evaluation of the risk had an impact. Would it have made a difference if the signs were more specific about the threat e.g.: “Danger of Falling Objects!”? What if pedestrians were *asked* to walk under the window cleaners? How many might refuse after devoting specific attention to the threat. You as a reader are encouraged to consider if you would have chosen to walk under the window cleaners after walking past the warning cones. After a discussion of the risks and a period of cognitive focus on the issue do you think you would have behaved differently to the pedestrians in the experiment?

More research in the area of risk communication is required. It would have been ideal in this experiment to find out the extent to which pedestrians noticed and cognitively processed the signs but decided implicitly or explicitly not to change their behaviour. This would have required interviews for the pedestrians involved.

9. References

- [BA-00] Andrew Bradbury: Develop Your NLP Skills.
Kogan Page Limited 2000
- [BBC-A] BBC: Wearing Helmets 'More Dangerous'
<http://news.bbc.co.uk/1/hi/england/somerset/5334208.stm>
2006
- [BBC-B] BBC: How Personal Data Was Put at Risk
<http://news.bbc.co.uk/1/hi/uk/6287504.stm> 2008
- [BBJ-04] Jeff Bock-Brown: Human Aspects of Information Assurance.
Royal Holloway ISG MSc 2004
- [BC-07] Christopher Booker and Richard North: Scared to Death, From
BSE to Global Warming: Why Scares Are Costing Us the Earth.
Continuum UK 2007
- [BP-08] Paul Baines, Chris Fill and Kelly Page: Marketing.
Oxford University Press 2008
- [CE-04] Esther Cameron and Mike Green: Making Sense of Change
Management. Kogan Page Limited 2004
- [DEL-05] Deloitte: 2005 Global Security Survey
http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecuritySurvey_2005-07-21.pdf 2005
- [DEL-07] Deloitte: 2007 Global Security Survey
http://www.deloitte.com/dtt/press_release/0,1014,sid%253D1018%2526cid%253D171269,00.html 2007

- [DFT-A] Department For Transport: Think! Road Safety.
<http://www.dft.gov.uk/think/>
- [DS-08] Sam Dekay: Does Security Awareness Work?
<http://www.bloginfosec.com/2008/04/22/does-security-awareness-work-pt-2-it-all-depends-on-what-you-mean-by-work/>
- [DTI-06] DTI: How to Write an Information Security Policy
<http://www.berr.gov.uk/files/file34331.pdf> 2006
- [EM-05] Michael W Eysenck and Mark T Keane: Cognitive Psychology, a Student's Handbook. Psychology Press 2005
- [FD-93] Dennis Ford and Mark Zaid: Eyewitness Testimony, Memory, and Assassination Research.
<http://mcadams.posc.mu.edu/zaid.htm> 1993
- [GIZ-A] Gizmodo: TSA Confiscates Homemade Battery and Water Bottle, Declares Victory Over Terror
<http://gizmodo.com/5031144/tsa-confiscates-homemade-battery-and-water-bottle-declares-victory-over-terror>
- [GP-07] Paul Gillin: The New Influencers. Quill Driver Books 2007
- [GR-05] Richard Gross: Psychology, The Science of Mind and Behaviour. Hodder Arnold 2005
- [HR-05] Rebecca Herold: Managing an Information Security and Privacy Awareness Training Program. Auerbach Publications 2005
- [HM-08] Monique Hogervorst: Information Security Training and Awareness, The Way to Overcome Aversion Against Information Security. Royal Holloway ISG MSc 2008

- [KTN-07] Cyber Security Knowledge Transfer Network Human Vulnerabilities Special Interest Group: Human Vulnerabilities in Security Systems http://www.ktn.ginetiq-tim.net/groups.php?page=gr_humanvuln 2007
- [LS-06] Steven D Levitt and Stephen J Dubner: Freakonomics. Penguin Group 2006
- [LT-05] Timothy P. Layton Sr: Information Security Awareness, the Psychology Behind the Technology. AuthorHouse 2005
- [MA-06] Angus McIlwraith: Information Security and Employee Behaviour, How to Reduce Risk Through Employee Education, Training and Awareness. Gower Publishing 2006
- [MM-02] M. Granger Morgan, Baruch Fischhoff, Ann Bostrom and Cynthia J Atman: Risk Communication: A Mental Models Approach. Cambridge University Press 2002
- [MP-04] Peter Makin and Charles Cox: Changing Behavior at Work, A Practical Guide. Routledge 2004
- [NT-07] Tim Newbury: Criminology. Willan Publishing 2007
- [NIST-A] National Institute for Standards and Technology: Building an Information Technology Security Awareness and Training Program <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf> 2003
- [NIST-B] National Institute for Standards and Technology: Computer Security Training Guidelines <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>

- [NR-A] Network Rail: Accident Frequency Rates
<http://www.networkrail.co.uk/aspx/4815.aspx>
- [OJ-02] Joseph O'Connor and John Seymour: Introducing NLP.
HarperCollins 2002
- [PS-04] Purser, Steve: A Practical Guide to Managing Information
Security. Artech House 2004
- [PS-07] Seppo Pahnaila, Mikko Siponen and Adam Mahmood:
Employees Behaviour Towards IS Security Policy Compliance.
Proceedings of the 40th Hawaii International Conference on
System Sciences 2007
- [PT-04] Thomas R. Peltier: Information Security Policies and Procedures,
A Practitioner's Reference. Auerbach Publications 2004
- [RC-06] Carl A. Roper, Joseph A. Grau and Dr. Lynn F. Fischer: Security
Education, Awareness and Training.
Elsevier Butterworth-Heinemann 2006
- [SA-01] Adrian Sargeant and Douglas C. West: Direct and Interactive
Marketing. Oxford University Press 2001
- [SA-01b] Angela Sasse, Sacha Brostoff and Dirk Weirich: Transforming
the "Weakest Link" – a Human/Computer Interaction Approach to
Usable and Effective Security. BT Technical Journal Vol 19 No3
2001
- [SB-04] Bruce Schneier: Secrets and Lies, Digital Security in a
Networked World. Wiley Publishing 2004
- [SB-06] Bruce Schneier: Beyond Fear, Thinking Sensibly About Security
in an Uncertain World. Copernicus Books 2006

- [SB-08] Bruce Schneier: The Psychology of Security. British Telecommunications PLC 2008
- [SB-A] Bruce Schneier: August 8th 2008 Crypto-Gram
<http://www.schneier.com/crypto-gram-0808.html>
- [SB-B] Bruce Schneier: Crypto-Gram Home Page
<http://www.schneier.com/crypto-gram.html>
- [SE-04] Edgar H. Schein: Organizational Culture and Leadership. John Wiley & Sons 2004
- [SJ-08] Jan Schlueter and Stephanie Teufel: Secalyser – A System to Plan Training for Employees. Human Aspects of Information Security and Assurance 2008
- [SP-97] Stephen Pinker: How the Mind Works. Penguin Books Ltd 1997
- [SP-00] Paul Slovic: The Perception of Risk. Earthscan Publications 2000
- [SP-02] Steve Purser: A Practical Guide to Managing Information Security. Artech House Inc 2004
- [TSA-A] Transportation Security Administration: Explosive-Like Item Intercepted at Checkpoint
http://www.tsa.gov/press/happenings/scot_peekle.shtm