Information Security Training & Awareness, the way to overcome aversion against Information Security

Monique Hogervorst

Technical Report
RHUL-MA-2008-08
15 January 2008

Royal Holloway
University of London

Department of Mathematics
Roal Holloway, University of London
Egham, Surrey TW20 0EX, England
`http://www.rhul.ac.uk/mathematics/techreports`

Information Security Training & Awareness, the way to overcome aversion against Information Security.

Monique Hogervorst

Supervisor:
Keith Martin

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

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people.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:

Table of Content

Executive Summary

Information security standards, best practices and literature all identify the need for Training & Awareness, the theory is clear. The surveys studied, [PWC-06] and [D-06], show that in the real world the situation is different: the focus of businesses is still on technical information security controls aimed at the external attacker. And although threats and vulnerabilities point out that personnel security becomes more important, the attitude of managers and employees does not reflect that. Information Security Training and Awareness is not recognised as contributor to security.

This needs changing, which means changing behaviour and attitude. One way of achieving that is giving people the information security knowledge and awareness they need for their role. It seems that the solution is not to be found in technical controls but more on the non-technical side: the side of human resource security and psychology.

A psychological model is introduced in this project and applied to information security. This model can be used as a tool to visualise and quantify the forces that impact on information security. The exercise of analysing the driving and restraining forces impacting on security in general and the security of information in particular visualises how forces work together or against each other; and identifies the relationship with business processes.

The driving and restraining forces of the information security force field diagram reflect all areas of information security counter measures: technical, procedural and personnel. Visualising the forces enables the information security professional to explain to non-specialists why an organisation needs to invest, in resources and finances, to secure information. The diagram will point out where investments are most effective and efficient.

The information security force field analysis and diagram as introduced in this project, can be a useful new tool for information security professionals to:

- communicate effectively to line and senior managers about the link between business processes and information security;
- explain how investment in training and awareness can impact on information security and improve security of an organisation;
- quantify the level of security of an organisation in comparison with other organisations or in comparison with the previous moment of measuring;
- quantify the impact of information security training & awareness.

The information security force field diagram will prove that investing in training and awareness is a very cost-effective counter measure: it will increase the overall level of security of an organisation and it decreases the restraining forces and with doing so the driving forces become more effective.

Chapter 1:
Introduction and Background

1.1. Information Security Training & Awareness

More than fifteen years working in different environments has shown me that the security of an organisation is very dependent on the knowledge and awareness of employees and managers. Personal experience has convinced me that investing in Information Security Training and Awareness is a viable decision to make: it is one of the protective layers in a defence in depth approach to secure information.

From a theoretical point of view all Information Security publications identify the need for Training & Awareness, but unfortunately it is not widely recognised as a contributor to security and Senior Management is reluctant to invest time and money. Ways need to be found to change this situation.

The focus of businesses is still on technical information security controls aimed at the external attacker. Reality shows that many security incidents and breaches of security policies are traceable to people and more specifically to employees within the organisation. Not that the incidents and breaches are deliberate, in my opinion most of them are due to not knowing the security policies, not understanding the risks to information and not having the knowledge to securely using information systems and processing information.

This situation needs to change and this will not be easy, as a change in behaviour and perception is a challenging task. Communication skills and psychology will play a main part in this change.

1.2. Project Objectives

To be able to test my views and to prove the viability of investing time and money in a structured Information Security Training & Awareness program, it is necessary to investigate how it contributes to the security of an organisation. This project has three objectives; each of these is briefly described in this paragraph.

- Identify the link between Information Security Training & Awareness and overall security of an organisation.
  If professionals want to convince senior management that it is necessary to invest time and money in information security, they will have to prove to them how information security links in with the business processes. Without secure, correct and reliable information business processes will fail, therefore the first step to get senior management buy-in is to visualise the connection between securing information and their business. After this first step the link with training and awareness needs to be made clear. And again when visualising the aspects

of information security, it becomes clear that training and awareness is one of the layers of controls in the protection of information.

- Develop a method for the measurement of security in general and the impact of training & awareness in particular.
  Besides visualising the links as described above, measuring the level of security of an organisation and quantifying the impact training and awareness is essential to prove the necessity to invest finances and resources in an Information Security Program. By quantifying the impact training and awareness can have on overall security we have a tool to prove that investing in training and awareness is a viable cost-effective control that should be part of the overall Information Security Program.

- List the possible benefits of training and awareness and give a possible structure of Information Security Training Program and an Information Security Awareness & Communication plan.
  Giving real-life examples of the benefits organisations experienced after implementing training and awareness confirms firmly that it contributes to the security of an organisation. Using possible structures for training and awareness brings the actual realisation closer to the managers. It also enables the managers to for example choose parts of the training or awareness program to be implemented at first to see from their own experience what the impact can be. In a way they can opt for a phased implementation and have a "proof of concept" before the next phase is implemented.

1.3. Methods used

To test my personal views and ideas in a practical, business environment a case study has been conducted as part of this project. Two tools form the basis of the case study in this project. Interviews with a small number of Information Security professionals working in a business environment. Followed by a questionnaire for a larger group of Information Security professionals, to find additional experiences.

The interviews are based on the objectives of this project and the psychological model introduced. After analysis of the interview results a questionnaire is developed to gather more experiences on specific areas to develop the Information Security Force Field Analysis and Diagram.

1.4. Structure of report

The first part of the project report is research, studying information security standards, best practices, books and articles on the topic of training and awareness. Research is followed by the introduction of a psychological model used for change management, production improvement and decision making. This model is made applicable to information security.

The results of the case study are used in the chapters that follow in the second half of the report. Each of these chapters covers one objective of this project in turn, using the Information Security Force Field model and the results of the case study.

The final chapter summarises the project report and looks at the way ahead for using training and awareness as a cost-effective control and efficient contributor to information security.

In three chapters of this project report (2, 3 and 6) a number of publications are quoted. To reflect my opinion on these publications each titled paragraph with quotes has a sub-paragraph containing ***my view*** on these publications and may identify how they contribute to the rest of this project. Although these publications contributed to the development of the information security force field model and the use as a tool for information security professionals, the introduced model is a new way to approach the problems these professionals encounter in their day job.

Chapter 2: Problem Exploration

2.1. Introduction

More than fifteen years working in different environments has shown me that the security of an organisation is very dependent on the security knowledge and awareness of employees and managers. Personal experience in training people and making them aware of the risks that information is under, gives me the confidence that investing in Information Security Training and Awareness is a viable decision to make. To be able to test my views it is necessary to investigate how Information Security Training & Awareness contributes to the security of an organisation.

Information security standards, best practices and literature all identify the need for Training & Awareness, but it is not widely recognised as a contributor to security. As a result Senior Management seems reluctant to invest time and money in appropriate Information Security Training & Awareness.

This chapter looks at the standards, best practices, literature and surveys in support of Information Security Training & Awareness. This chapter differs from the other chapters in the way that publications will be quoted and they contribute to the developments of this project. At the end of each titled paragraph there is a section that will reflect my opinion on these publications, these sections will be marked with the sub-title ***My View***.

The last paragraph of this chapter identifies the aversion against information security and suggests that structured Information Security Training & Awareness can contribute to the overall security of an organisation.

2.2. Standards and Best Practices

The **international standard** specifying the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented **Information Security Management System (ISMS) is ISO/IEC 27001:2005 [ISO-05/1]**. One of the requirements in ISO/IEC 27001:2005 is the implementation of Information Security Training and Awareness Programmes.

Training, awareness and competence is identified as a management responsibility, paragraph 5.2.2 of standard [ISO-05/1], it states that an organisation shall ensure that:

> *"…all personnel who are assigned responsibilities defined in the ISMS are competent to perform their tasks…"*

The standard [ISO-05/1] also reads:

> *"…all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives."*

The **Code of Practice for Information Security Management, ISO/IEC 17799:2005 [ISO-05/2]** establishes general guidelines to implement selected relevant security controls to meet the requirements of ISO/IEC 27001:2005. One of the clauses in this Code of Practice is Human Resource Security (clause 8); more specifically control 8.2.2 of the Code of Practice [ISO-05/2] states:

> *"All employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function."*

The Code of Practice [ISO-05/2] continues to describe how this control could be implemented, this will be used in chapter 7 of this report.

Several Government Departments use the international standard [ISO-05/1] and code of practice [ISO-05/2] as basis for their Information Security Standards, Manuals, Policies and Procedures. The Department of Trade and Industry (DTI) have developed several Information Security Guidelines and Best Practices for businesses.

An example is the **Director's Guide: Information Security best practice measures for protecting your business [DPL-05]**. This Director's Guide is a collection of chapters each covering a specific area of Information Security, written by different authors. For this project three chapters were selected for their direct support of Information Security Training and Awareness.

Jeremy Ward, author of chapter 3 of the Director's Guide [DPL-05], states that:

> *"security awareness is probably the most significant single defence measure that any company can institute";*
>
> and
>
> *"good security policies and procedures are the foundation of security awareness."*

Angus McIlwraith identifies in chapter 7 of the Director's Guide [DPL-05] that education is vital, he links his statement to security incidents being attributable to human error and misunderstanding.

> *"Educating your staff is perhaps the most cost-effective control you can implement,…."*

Chapter 9 of the Director's Guide [DPL-05] identifies employees as the weakest link. Ted Humphreys, author of chapter 9, mentions that in many cases breaches of Information Security are traceable to an organisation's of employees.
The first paragraph of Chapter 9 of the Director's Guide [DPL-05] reads:

> *"Protecting your company requires a workforce that is:*
>
> - *aware of the risks;*
> - *aware of their responsibilities to act in a sensible and secure way;*
> - *applying the policies and best practices adopted by the business;*
> - *responsive to the reporting of security incidents;* and
> - *mindful of their legal responsibilities."*

The European Union (EU) also provides best practices and guidelines. **European Network and Information Security Agency (ENISA)** is a centre of excellence for the EU Member States and EU Institutions. In their guideline **[E-06]** for EU member states reads:

> *"The adage that* 'you are only as strong as your weakest link' *is prevalent in today's IT landscape and it is the human element that is still a critical factor when implementing any effective and robust security framework. The European Network and Information Security Agency (ENISA) and the Member States are continuing their efforts to positively influence the public's behaviour towards information security, changing the mindset of the human element in order to achieve greater self-awareness."*

My view

In my personal words [ISO-05/1] could be stronger: the employees assigned Information Security tasks must have the knowledge and skills to perform these tasks. Depending on the type of security tasks they have, the level of knowledge differs. Some knowledge can be provided by internal training, understanding and awareness can be raised by the internal information security team. Specialist knowledge on the other hand needs to be gained through Information Security education; this can only be provided by specialised Information Security training providers.

Not just *"…all relevant personnel…"* as stated in [ISO-05/1] and [ISO-05/2] but **all employees**, including senior and line management, have security responsibilities in their day jobs and **they all** contribute to the security of an organisation. Therefore an organisation should have an Information Security Awareness campaign covering all possible levels of detail, for specific groups, targeting different audiences.

The quotes from Jeremy Ward in [DPL-05] strongly support my views on how training and awareness can be used as one of the layers of defence-in-depth.

Comparing Information Security with the layers of an onion, one of the important layers of defence is information security training & awareness.
Security policies and procedures give an organisation a strong security foundation. But it is not enough to write and develop them. Information Security policies and procedures need to be established, they need to get publicity, the content needs to be transferred from the written paper to all employees in an organisation. Training and awareness is a good tool to establish Information Security policies and procedures.

No statement on cost-effectiveness of training and awareness, by Angus McIlwraith in [DPL-05] could support my views more: senior managers should invest more in Information Security Training & Awareness to on one hand increase security and on the other hand save time and money on implementation projects related to information security. Later chapters should convince readers of this report that investing in training & awareness could be beneficial to the Information Security Program.

In my opinion a workforce is only able to comply with the five bullet points given by Ted Humphreys in [DPL-05], if they receive an appropriate level of Information Security Training and Awareness; appropriate to the role and function they carry out within an organisation. People who are unaware of the risks to information, unaware of the information security policies and procedures that are in place and unaware of their security responsibilities can not be kept accountable nor liable for the consequences of a breach of security.

2.3. Literature and articles

Besides standards and best practices many writers covering Information Security topics identify training and awareness as an important factor in achieving security goals and establishing a security minded culture. A few brief examples are given in this paragraph.

Chapter 3 of **Information Security Fundamentals [PT-05]** gives the structure of an Information Security Program. An essential part of the program is Information Security Awareness, paragraph 3.3 in [PT-05] describes how awareness fits in an Information Security Program. Further on the authors identify an Information Security Awareness Program as a *"preventive control"*.

Technical books also mention the importance of Information Security Training & Awareness. An example is Dieter Gollmann's book **Computer Security [GD-06]** used during the MSc module Computer Security (Operating Systems). A few quotes from this book [GD-06].

> *"Security practitioners know that security is a people problem that can not be solved by technology alone."*
>
> Also:
>
> *"Not every member has to become a security expert, but all members should know:*
>
> - *why security is important for themselves and for the organisation;*
> - *what is expected from each member;*
> - *which good practices they should follow."*
>
> And:
>
> *"Organisations developing IT services or products have the additional task of providing security training for their developers…. Developers should also be alert to the fact that certain categories of sensitive data, e.g. personal data, have to be protected according to specific rules and regulations. Finally developers should keep up to date with known coding vulnerabilities."*

A recent article in Info-Security magazine has the title **"Put people above technology, says (ISC)^{2}" [CJ-07]**. The article reports that Information Security professionals are moving out of IT department and more often reporting to business managers.

Another article found on the Internet, more specifically on the ENISA[1] website, was a **meeting report** of the EastWest Institute ***Consortium on Security and Technology*** **[EWI-05]**. This consortium builds Public-Private partnerships for more effective protection of people, economies and infrastructure against international terrorism and organised crime. The meeting held on 1st December 2005 had the topic Information Security and Identity Management. In this report it was identified that it is not only about security in the work environment, on Awareness raising the report [EWI-05] states:

> *"Education and raising awareness of threats is one crucial to improving information security. Learning about ICT security is much needed in schools, and in organizations. This will require a significant amount of investment. This teaching is especially important because home users of ICT form the weakest link in the chain – unprotected personal computers could unwittingly house botnets. Users cannot and should not however, be expected to be aware of all information security issues. This would put an unreasonable and unrealistic burden on the user."*

[1] ENISA = European Network and Information Security Agency

Laura Taylor in her article **Security Awareness and Training [TL-04]** identifies the importance of training and awareness as part of an information security program, but also acknowledges that it is often overlooked. A quote from the article:

> *"security awareness and training is really the first line of defense your company has to protect its valuable corporate assets."*

Taylor describes in the article [TL-04] how an organisation can implement security training and awareness and indicates that implementing a training and awareness plan is worth the human and financial resources needed: it will decrease the impact of attacks and in due course will reduce the risk that an organisation's information is exposed to.

My view

Many publications identify a new group of people with very specific security responsibilities: people working in the Information Technology (IT) Department. During my career I have worked in and with IT departments of organisations. Their tasks in the smoothly running of information systems are critical. The access privileges they have to information and information systems, makes them an important target group for appropriate information security training & awareness. In my opinion it is fundamental that they have a sufficient level of knowledge and understanding in relation to information security threats and vulnerabilities.

2.4. Surveys

Modern businesses are highly dependent in information systems and therefore Information Technology (IT). Organisation more often have distributed infrastructures and have the need to connect with other organisations. This connection if often established through the Internet. Both high dependency on IT and growing global connectivity increase the complexity of IT infrastructures and threats and vulnerabilities organisations face in their day-to-day business.

The bi-annual **DTI[2] Information Security breaches survey 2006 [PWC-06]** confirms this dependency. The survey [PWC-06] also recognises that new technologies are seen as the security threat of the future, it states:

> *"Despite the high levels of confidence about today, UK businesses are more concerned about tomorrow than ever."*
>
> And also:
>
> *"Nearly two thirds of companies think there will be more security incidents in the next year than in the last."*

[2] DTI = Department for Trade and Industry

A few examples of the findings form the DTI survey [PWC-06] demonstrating the (future) security threats that new technologies pose are:

- One in five wireless networks remains completely unprotected and another one in five is not encrypting it's transmissions.
- Over half of UK businesses are taking no steps to protect themselves against the threat that removable media, such as USB data keys, digital cameras and MP3 players, pose. The most common step is to tell staff not to use these devices and rely on policies and procedures to enforce it. Actually technical disabling the facility in rare.
- Only half the companies that implemented Voice over IP evaluated the security risks associated with VoIP (Voice over Internet Protocol).

Given this future outlook organisations want more to be done to help them in this area says the survey [PWC-06], examples are public education about security risks and more information Security advice aimed at the organisations themselves.

Another conclusion from the DTI survey [PWC-06]:

> *"Many UK businesses are a long way from having a security aware culture. Their expenditure on security is either low or not targeted at the important risks."*

This conclusion is supported by a number of examples throughout the report [PWC-06]. In relation to the project in hand, the following selection from the examples is made to underline the need of structured Information Security Training & Awareness:

- Although the number of companies with a formal security policy in place has never been so high, there are still three-fifths of UK businesses that are without overall security policy.
- The higher the priority that information security is to senior management, the more likely the company is to educate their staff. Companies that have a security policy take steps to educate it's employees about their security responsibilities. But report [PWC-06] states that: *"one in six organisations does nothing to educate their staff."*
- There seems to be a strong correlation between budget spend on information security and the priority senior management gives to it. When information security has a high priority in an organisation, an average of 7% of the IT budget is spend on information security. But says [PWC-06] there are still two-fifths of businesses that spend less than 1% of their IT budget on information security.

According to the survey [PWC-06] organisations respond to incidents with a mixture of technology, people and process changes. The changes that organisations made, in response to incidents, that recognise the impact of structured Information Security Training & Awareness, the subject of the project in hand, are:

- additional staff training (23% of organisations used this in response to incidents);
- changes to policies & procedures, (26%);
- disciplinary action (8%).

Another survey is the **Deloitte's 2006 Global Security Survey [D-06] of the Financial Services Industry**. Adel Melek, one of the authors of this survey says in his Foreword:

> *"It has often been said that people are an organisation's most valuable assets. It appears that, in the world of security breaches, they are now it's most vulnerable."*

One of the key findings of [D-06] identifies that perimeter security technology is strong enough to make it more difficult for attackers to reach their goal by external brute force attacks. It now seems easier to attack the organisation's people through social engineering. Also attacks whereby authorised users abuse their privileges is on the rise.

Another quote from the survey [D-06] identifies clearly that organisations should invest more in Information Security Training & Awareness.

> *"Often the security of information is compromised by human behaviour, whereby individuals who have been entrusted with managing personal information lack adequate security qualifications, leading to an increase in release of confidential, personal identification information."*

The survey [D-06] continues with a paragraph that recognises how important information security awareness is. The survey reads:

> *"Organisations are more likely to find themselves vulnerable to threats if employees are not aware of:*
>
> 1) *relevant policies;*
>
> 2) *their role in helping to protect information of the organisation; or*
>
> 3) *how to support the organisation's security policies.*

My view

Personally I find it amazing that, although the internal threats are clearly on the rise, the survey [D-06] shows that organisations in the Financial Services Industry appear to be more concerned with threats from the outside; in their minds, external threats bring a higher degree of publicity and damage to their reputation. Would the damage to reputation not be more severe if the public is aware that misconduct or social engineering lead to breaches of security?

The figures in the survey [D-06] confirm that amazement. Of all survey respondents 96% indicate that they are concerned about employee misconduct involving their information systems. Strangely only 34% provide their employees with information security training and only 35% of respondents have orientation training to help mitigate the effects of bad habits.

Looking at the investments in security the survey [D-06] recognises that security technology deployment still receives the bulk of the information security budget; but it seems that there is a growing belief that the human aspect of an information security program is critical to the overall success.
In my opinion this is clearly not enough. Especially with the rising internal threats, Information Security Training & Awareness should become a higher priority and receive more of the information budget than currently invested.

2.5. Problem identification

This chapter shows that information security standards, best practices and literature all identify the need for Training & Awareness, the theory is clear.
The surveys studied in paragraph 2.4 show that in the real world the situation is different: the focus of businesses is still on technical information security controls aimed at the external attacker. It seems that Information Security Training and Awareness is not recognised as contributor to security.

As a result Senior Management seems reluctant to invest time and money in appropriate Information Security Training & Awareness. To change this situation it is necessary to identify the links between the overall security of an organisation and information security training and awareness. To convince senior management that investing in training and awareness is viable, you need a way to explain in business terms the impacting factors on security and how these factors can be influenced by an adequate information security training and awareness program. Chapter 5 of this report will identify the links between security and training & awareness.

One way to convince senior management is to quantify security and quantify the impact of training and awareness. Chapter 6 of this report introduces a possible way to measure security and measure the impact of information security training and awareness.

The surveys [PWC-06] and [D-06] identify that personnel security becomes more important, but the attitude of managers and employees does not follow that trend yet. This needs changing, which means changing behaviour and attitude. One way of doing just that is giving people the information security knowledge and awareness they need for their day jobs. It seems that the solution does not lay in technical controls but more on the non-technical side: the side of human resource security and psychology.

Chapter 3:
Psychology - Force Field Analysis

3.1. Introduction

As concluded in chapter 2 one of the major problems for Information Security professionals is recognition of the need for Information Security and the understanding of threats and risks to information and information systems. As identified the focus of businesses is still on technical information security controls aimed at the external attacker. It seems that Information Security Training and Awareness is not recognised as contributor to security.

Personally I am convinced that changing the attitude of employees and senior management can solve many of the problems identified in chapter 2. This chapter introduces a psychological model that is used throughout this report in support of the objectives of this project. First the model itself and it's use in general is explained; followed by the way this model is used in relation to Information Security.

3.2. Organisational behaviour

One way of changing behaviour and attitude is giving people the information security knowledge and awareness they need for their day jobs. It seems that the solution does not lay in technical controls but more on the non-technical side: the side of human resource security and psychology. Psychology identifies several theories for behavioural change. The one that appeals most to me is the model of the force fields. In this model driving and restraining forces work in opposite directions. When the two sets of forces are even in strength, there will be no movement in the current position, no change can be achieved. Increasing or decreasing the strength of forces can change that position.

Kurt Lewin is universally recognized as the founder of modern social psychology. He is renowned for his scientific approach to research and experimentation as well as his work in understanding organisational behaviour. Although Lewin did not receive much acknowledgement during his lifetime, his work remain an outstanding source to understanding group dynamics. The Force Field Analysis is probably Lewin's best-known development [LK].

3.3. Force Field Analysis, the model

According to Kurt Lewin *"An issue is held in balance by the interaction of two opposing sets of forces - those seeking to promote change (driving forces) and those attempting to maintain the status quo (restraining forces)"*, reads article [LK-06]. Lewin approached organisations as systems in a dynamic balance of forces. These forces impact on (business) process, in favour by driving towards a goals or hampering progress and restrain the process. To be able change the existing balance the driving forces must exceed the restraining forces, or as [LK-06] says *"shifting the equilibrium"*.

Another quote form [LK-06] states:

> *"The Force Field Diagram is a model built on this idea that forces - people, habits, customs, attitudes - both drive and restrain change. It can be used at any level (personal, project, organizational, network) to visualize the forces that may work in favour and against change initiatives."*

Putting the forces in a diagram visualises all forces that impact on a certain issue. Giving the forces a value indicates their strength. Doing this makes it possible to identify actions that can be taken to change the strength and therefore be able to change a specific issue or situation.

Figure 3.1 is an example of a Force Field Diagram as used in Steven Wells' Mini Tutorial Quality Management [WeS-06], the tutorial is attached as appendix A.

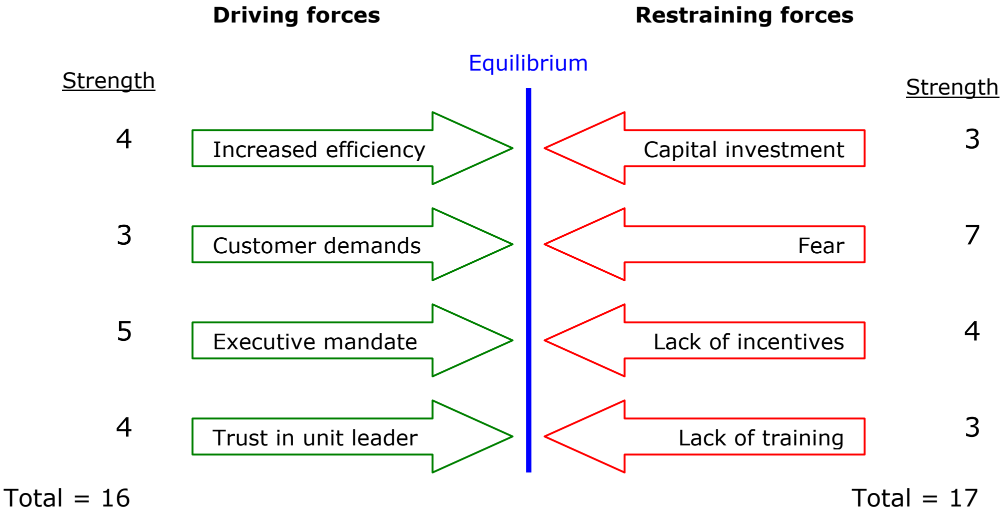


Figure 3.1: Example - Force Field Diagram [3.3]

Force field analysis can be used for different applications in all industries. According to the Mini Tutorial [WeS-06] there are three main applications of the force field analysis tool:

- Change management:
  Change is a regular occurrence in the environments that are increasingly dependent on Information Technology. People have widely varying attitudes toward computers and change in the workplace. Drawing a force field diagram helps managers to evaluate the forces that encourage and the forces that impede the change. Based on the force field analysis, strategies must be

developed to assist an organisation in moving towards aspired goals.
Change management is considered to be the *"primary application for force field analysis"* [WeS-06].

- Productivity improvement, from [WeS-06]:
  "Managers can look at forces promoting and inhibiting productivity. This analysis can shed light on methods, strategies, and systems that can promote long-term improvements in employee productivity."
- Decision making, from [WeS-06]:
  "By evaluating the forces supporting and opposing a specific decision, managers can know the likelihood of acceptance and can also manage the influencing forces to maximize the potential for acceptance and success."

The Force Field Analysis can be used to solve issues or problems that organisations have to encounter every day. The analysis helps in the investigation of powers and stakeholders involved in the issues/problems. In this way investigators can draw conclusions on the most effective and efficient solution for an identified problem. If used as a problem solving tool, Force Field Analysis is applied for decision making and implementation of change.

3.4. Force Field Analysis and Information Security

As mentioned in paragraph 3.2 the solution does not lay in technical information security controls but more on the non-technical side: the side of human resource security and psychology. Using the model of the force fields gives a visual and numerical indication of what forces impact on information security and who the possible stakeholders are. By visualising the issues information security professionals can explain in a non-technical way why information security is important; by valuing the forces it is possible to focus efforts on areas where the most effective and efficient results can be achieved.

The increasing dependence on information makes it necessary to protect information from the risks imposed on it; the need for protection identifies a number of driving forces to implement Information Security controls.
Chapter 2 identifies a number of problems in relation to acceptance and recognition of the importance of Information Security. The implementation of protective measures comes up against a number of restraining forces.

The mini-tutorial of appendix A [WeS-06] is the basis of the development of the Information Security Force Field diagram in figure 3.2, the steps leading to the diagram are:

1) issues and problems identified,
   this is done in chapter 2 of this report;

2) aim of addressing the issues and solving these problems,
   this is done in chapter 2 of this report;
3) identify the driving forces,
   from a theoretical point this can be found in paragraph 3.6, a reflection in the real world can be found in the case study of chapter 4;
4) identify the restraining forces,
   from a theoretical point this can be found in paragraph 3.5, a reflection in the real world can be found in the case study of chapter 4;
5) assign an impact level to each force, see case study in chapter 4:
   1 = very weak, 2 = weak, 3 = strong, 4 = very strong;
6) chart the forces in a diagram, figure 3.2;
7) evaluate the chart and decide on viability of a project or decide on which actions can achieve changes, this is done in chapter 6 of this report;
8) discuss how restraining forces can be decreased and driving forces increased in strength, chapters 5 and 7 covers this from a theoretical point of view;
9) discuss a strategy to eliminate restraining forces and capitalise on driving, chapters 5 and 7 covers this from a theoretical point of view.

3.5. The Restraining Forces identified in the diagram of figure 3.2 show a number of forces that are not solvable by implementing (technical) information security mechanisms and controls. The majority of the restraining forces are related to the people making up an organisation: management and employees.

- In many organisations there is a cultural aversion against Information Security and against changing business processes. “We have been doing our work like this for many years, why do we need to change it”, is an often heard reply. To change this culture, it is necessary to change people’s behaviour and their way of thinking. In my opinion the main reason for this behaviour is people not understanding the risks that modern organisations face in relation to the information held and processed by them.
- In the past couple of years there has been a turn around in this aversion against Information Security, as the DTI Information Security breaches survey 2006 [ISO-05/1] identifies. This survey shows that security awareness in UK organisations has never been better. But it also shows that only 40% of organisations have an overall Security Policy and that 40% of businesses spend less than 1% of the IT budget on Information Security. To improve these percentages Senior Management will have to be more involved in and support developments and initiatives towards better security of information.
- It seems that creating an understanding of and a more positive attitude towards Information Security, could be a good investment to achieve a decrease in the restraining forces. It is essential that all people in organisations are involved in

Information Security, managers and employees. Decreasing restraining forces will make the driving forces more effective.

3.6. The Driving Forces in figure 3.2 clearly identify the main drivers for Information Security: Confidentiality, Integrity and Availability. Implementing protective measures can improve the security of information and information systems that organisation rely upon.

- Businesses and organisations become more and more dependent on correct and reliable information. Information processed in organisations is mainly digital and business processes run on an Information Technology architecture, entwined in applications, databases and operating systems. Without (digital) information many organisations are not able to operate appropriately and availability is a major requirement for organisations.
- Depending on the sector or industry an organisation is part of, a number of regulatory requirements are laid upon the organisation. Being able to prove compliance to regulatory requirements could give customers and partners confidence in trusting that organisation. Legislation, such as the Data Protection Act, makes organisations holding and processing personal information, responsible for the protection of this information.

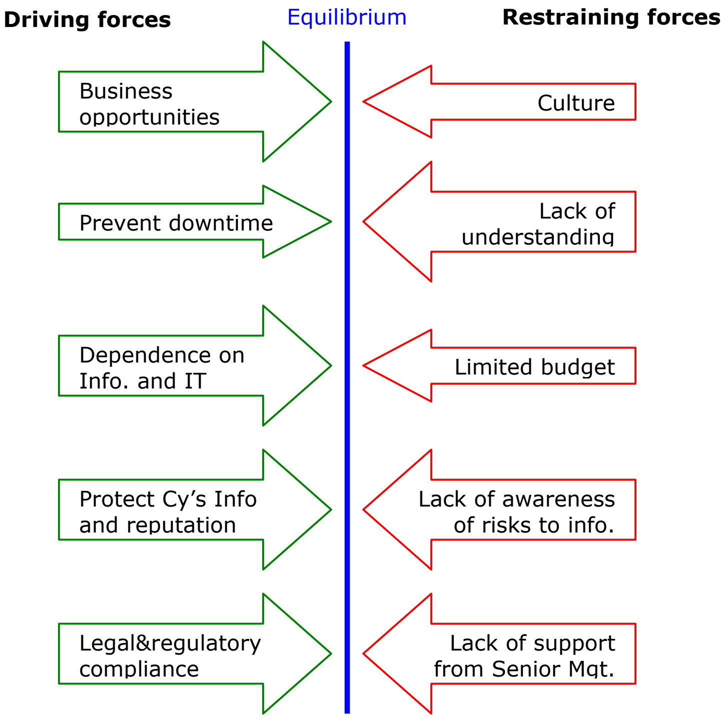

Driving forces
Equilibrium
Restraining forces
Business opportunities
Culture
Prevent downtime
Lack of understanding
Dependence on Info. and IT
Limited budget
Protect Cy's Info and reputation
Lack of awareness of risks to info.
Legal&regulatory compliance
Lack of support from Senior Mgt.

Figure 3.2: Force Field diagram for Information Security controls
© RHUL MSc Candidate 0707335 - August 2007

- Implementing an Information Security Management System can give a an organisation new business opportunities. For example being ISO27001/ ISO17799 certified will work positively towards attracting the interest of partners and customers as it proves a structured approach to securing information.

The model of the force fields as developed by Kurt Lewin is for this project applied to information security. By doing this information security professionals can visualise the forces impacting on information security. This model can be used as a tool to identify that besides technical controls, there are non-technical counter measures that can be used to secure one of the most critical assets of an organisation: information.

3.7. Summary & Conclusions

This chapter describes the tool that is used throughout this report to visualise and quantify the forces that impact on information security. The psychological model of the force fields is applied to information security. This application shows links between the security of an organisation and the potential impact that training and awareness could make when it is incorporated into the Information Security Program of an organisation.

Throughout the rest of this report this model is used to achieve the objectives of this project. The theoretical model of the force fields, figure 3.2, shows that the implementation and establishment of Information Security Training & Awareness can realise a behavioural change. Although behavioural change is one of the most difficult objectives to achieve, investing in sufficient Information Security training and awareness will decrease the restraining forces and make investments in protective measures (the majority of the driving forces) more effective.

The Information Security Force Field model will be used to:

- visualise all the forces impacting on information security, in aid of discussions with business managers and show the link between Information Security Training & Awareness and the level of security of an organisation (chapter 5);
- by valuing the forces identified, develop a model for measuring security and quantifying the impact of training and awareness (chapter 6).

Chapter 4:
Case Study – EDS Limited

4.1. Introduction

The objectives of this project as laid out in previous chapters reflect my views of the potential advantages that can be derived from structured Information Security Training & Awareness. To test my personal views and ideas in a practical, business environment a case study has been conducted as part of this project.

Two tools form the basis of the case study: interviews with a small number of Information Security professionals working in a business environment; followed by a questionnaire for a larger group of Information Security professionals, to find additional experiences. The environment chosen for this project had to have an Information Security influence in businesses.

4.2. Business environment

The Client Security Officers of Electronic Data Systems Limited, further referred to as EDS, have this Information Security influence in business environments and therefore are the ideal target group for this case study.

EDS is a leading global technology services company delivering business solutions to its clients. EDS delivers a broad portfolio of information technology and business process outsourcing services to clients in the manufacturing, financial services, healthcare, communications, energy, transportation, and consumer and retail industries and to governments around the world.

One of the units in EDS delivering services to clients is *UK Information Security*, it consists of four groups of which the Information Assurance Group is one. Information Assurance Group provides security and safety consulting services to EDS UK business units and to external clients. One of the security services provided to client organisations is the role of Client Security Officer. The **Terms of Reference of the Client Security Officer [EDS-04]** details the role in general and comprises five aspects:

- *"Security Governance*
  Information security enforcement, including: accreditation of systems (signing-off systems as being compliant with security requirements and policy); development of and enforcement of security policy; security awareness; and risk assessment."
- *"Security Operations*
  Responsibility for day-to-day aspects of the security of the client's operations (those provided by EDS), including: dealing with security incidents; reacting to alerts flagged by logs, IDS and monitoring systems; liaising with other

operations teams; liaising with Situation Management; and development of operational aspects of security such as monitoring."

- *"Security Delivery*
  Responsibility for ensuring the deployment of leveraged security resources to the client, i.e. as an interface between the account and the leveraged teams."
- *"Chief Security Architect*
  Responsibility for the architecture and design of the security of the systems delivered to the client by EDS, and for ensuring that those systems fit within an overall business-driven security architecture."
- *"Security Business Development*
  Responsibility for developing new security business with the client."

In practice each client and each account is likely to have unique requirements for the role of Client Security Officer. The document of [EDS-04] is used as template to develop client specific Terms of Reference for each customer account.

All Client Security Officers were sent a questionnaire, just over 40% replied. Paragraphs 4.5 and 4.6 give more details about the questionnaire.

In total four Client Security Officers were interviewed in two environments and one representative was a client employee with responsibilities for Security Training & Awareness. The environments had a very diverse experience with training and awareness: from almost 10 years to only a couple of months.

4.3. Interviews - structure

The interviews are divided into sections. The first section covers the structure, history, budget and encountered problems of implementing training and/or awareness. Sections 2 and 3 give details on the Training programs and Awareness activities developed and implemented by the interviewees.

The next section covers questions about the benefits that are identified from having Information Security Training & Awareness in place. The results of these first four sections are used in Chapter 7 of this report listing the benefits of and possible structure of Information Security Training & Awareness.

Section 5 of the interview tested the Force Field Analysis model of chapter 3 in the chosen business environment. The results are used in chapters 5 and 6.

The final section of the interview tried to answer the difficult question of measuring security of an organisation on one side and measuring the impact of Information Security Training & Awareness on the other. This last question turned out to be the most challenging question for the interviewees.

4.4. Interviews - results

The transcripts of the interviews are attached to this report as appendix B. As mentioned in the previous paragraph the answers given during the interviews are input to the relevant chapters of this report. This paragraph gives a summary of the results as they relate to the objectives of this project.

- *Link between overall security of an organisation and training & awareness*
  All interviewees supported the model of paragraph 3.4 and added some additional forces, restraining and driving ones. During the interview it was asked to give a strength value to each of the forces they identified. The values given identify the importance of information in their respective organisations.

  In my opinion the values given to the Driving Forces confirm the importance of the three main security services Confidentiality, Integrity and Availability. They confirm the importance of legal & regulatory compliance and the dependency of the organisations on information & information systems.

  Looking at the Restraining Forces that were identified, there is a clear connection between Training & Awareness and Security. The values given to the restraining forces, show how lack of understanding and awareness in the workforce impact on implementing information security controls. In one of the interviews the link was very clear: the value given to for example "Lack of awareness of risks to information" differs for new comers (the higher value) and employees who had information security training (lower value). This specific organisation has had Information Security Training & Awareness in place since 1998.

  My conclusion from these results is that Information Security Training & Awareness can decrease the strength of restraining forces. This decrease will make the driving forces more effective. Therefore investing in appropriate training & awareness can save time and money of implementation projects that put in place other (technical) protective controls.

- *Measuring security and measuring the impact of training & awareness*
  As mentioned before, the questions about measuring security or measuring the impact of training & awareness were the most challenging for the interviewees. After asking some additional question, exploring the experience of the interviewees there were some indicators they came up with.

  For <u>measuring the security</u> of an organisation the following indicators came up:

  - Number of security incidents. Not just numbers as that does not give enough information, it is necessary to analyse the incidents to identify the links with other events and issues.

- Number of breaches of security policies. Although this was named as a different indicator, in my opinion breaches of security policies are also security incidents and therefore should be put together with the first indicator.
- Number of non-compliances discovered during audits. Audits should be fully documented in audit reports and if audits take place on a regular basis, the changes in the number of non-compliances could be used to measure the level of security.
- Number and type of questions received by the Information Security Team.
- Number of System Security Policies (SSPs) that pass without re-work versus the number of SSPs that need to be reviewed repeatedly. In one of the accounts every IT project has to produce an SSP that needs to be reviewed and signed off by the Information Security Team before the project deliverables can be implemented into a live environment.

For measuring the impact of training and awareness on the security of an organisation the following indicators were mentioned:

- Security incidents, where the analysis of the incidents could indicate in which way training & awareness impacts on the type, seriousness and possibly on the number of incidents. Analysis of security incidents should indicate the lack of understanding and the lack of awareness of the risks to information.
- Number of security incidents classified as "misuse".
- Type of questions to Security Team and level of detail in conversations with users. Problem here is that calls to the Security Team nor the conversations Security Team members have in corridors are not recorded. So there are no numbers or descriptions available to use as indicator. It is purely an observation of the Security Team.
- Non-compliances as result of security audits.

Audits and incidents certainly can be used to develop indicators, but not just as numbers. The results need to be analysed to give sufficient information to be able to use them as measurable indicators. Another intersting way to measure security is the sign-off of project documentation such as the System Security Policy used in the client account of one the interviewees.

- *Benefits of structured Information Security Training & Awareness*

  Not all the interviewees could give benefits related to the actual implementation of an Information security Training & Awareness program as they only just started to notice the changes in people's behaviour. The following benefits were identified by the interviewees:

  - less time-wasting by users;
  - reduction of security incidents;
  - less time spent on incident investigations by the Security Team;

- improve project life-cycle time and therefore reduce project costs and less re-work on System Security Policy for projects;
- maintaining reputation of service provider and client organisations;
- better able to fulfil "duty-of-care" towards employees;
- standardisation of the security message;
- change of attitude towards information security.

The number of benefits identified by the interviewees supports my personal views of how training and awareness can impact on information security. The longer Information Security Training & Awareness has been in place the aversion against information security has reduced. These results will be used in chapter 5 and 7 of this project report.

4.5. Questionnaire – structure

After the interviews there were a few issues that I needed additional experiences about and so five questions were put in a questionnaire to other Client Security Officers, who did not took part in previous interviews.

First I needed to know of their client account has any security training or awareness programs in place. After that they were asked about their experience on the link between security incidents and training and awareness. The results are used in chapter 5 of this report.

The middle part of the questionnaire focussed on the Force Field model described in chapter 3. The Client Security Officers were asked to identify driving and restraining forces. The outcome is used in chapters 5 and 6 of this report.

The final two questions were related to measuring security and measuring the impact of training and awareness on security. The results feed into chapter 6 of my report.

4.6. Questionnaire – results

Details of the results of the questionnaire can be found in appendix C of this report. Although the total number of replies seems to be low (7), it represents just over 40% of Client Security Officers. Although 40% is not a bad response, not all answers are valuable. For example the first question may have a complete different result if all Client Security Officers would have replied. The result shows that 85% have an Information Security Training and/or Awareness program in place. I think in reality this percentage is lower and therefore the result of the first question will not be taken into consideration.

To the question which percentage of security incidents is related to users, more than 40% of respondents declared the majority of security incidents were user related, in the results table this is categorised as > 75%.

One of the respondents made clear that there is a difference in users of the client population or users of the EDS population. This is considered to be caused by the level of security training and/or awareness the user populations have received. This also came up during one of the interviews, see paragraph 4.4.

Question 3 focussed on the Force Field Analysis model. The results confirm the theoretical model developed in support of Information Security, paragraph 3.4 refers. The main driving force identified by respondents is legal and regulatory compliance. For the restraining forces it is a bit more spread over a number of forces, but 45% of the restraining forces identified are people-related.

The results of the last two questions are very useful in my challenge to find indicators to quantify the level of security and to quantify the impact of training & awareness on security.

For **measuring security** a very interesting indicator was mentioned by three respondents: the number of days exposed to known vulnerabilities, these are vulnerabilities for which security patches are published; followed by audit logs and independent reviews.

Although number (and the changes in this number) of incidents was mentioned by three respondents, I think other identified indicators **to measure impact of training and awareness** may give a more secure indication: sampling user knowledge and number of hits on security policies & procedures.

4.7. Summary and Conclusion

The interviews gave me a good idea of practical implementations of Information Security Training and Awareness in business environments. The interviews resulted in the following conclusions:

- Information Security Training & Awareness can decrease the strength of restraining forces. This decrease will make the driving forces more effective. Therefore investing in appropriate training & awareness can save time and money in implementation projects, putting in place other protective controls.
- Audits and incidents certainly can be used to develop indicators, but not just as numbers. The results need to be analysed to give sufficient information to be able to use them as measurable indicators. Another interesting way to measure security is the sign-off of project documentation such as the System Security Policy used in the client account of one the interviewees.
- The number of benefits identified by the interviewees supports my view of how training and awareness can impact on information security. The longer Information Security Training & Awareness has been in place, the more the aversion against information security reduces.

The questionnaires broadened my views and inspired me to develop my ideas, as detailed in the chapters that follow.

Chapter 5: Link between Security and Training & Awareness

5.1. Introduction

As mentioned in the surveys referenced in chapter 2, people have a very important role in keeping information assets secure. If we take a layered approach to information security, people could be one of the layers. If Human Resource Security is implemented properly, one of the protective controls in a Defence in Depth approach is Information Security Training & Awareness. Jeremy Ward states in [DPL-05]: *"security awareness is probably the most significant single defence measure that any company can institute"*.

This chapter concentrates on identifying the link between the overall security of an organisation and Information Security Training and Awareness. Using the Force Field Analysis model for Information Security, as laid out in chapter 3, my theoretical view on this link is presented. In the second half of this chapter the results of the case study are used to support the theoretical model.

5.2. Theoretical approach

As identified in chapter 2 senior management seems reluctant to invest time and money in appropriate Information Security Training & Awareness. To be able to use training & awareness as a layer in the defence in depth approach, senior management needs to be convinced that investing in training and awareness is viable. To achieve this it is necessary to identify the links between the overall security of an organisation and information security training and awareness. Professionals need a way to explain in business terms the impacting factors on security and how these factors can be influenced by an adequate information security training and awareness program.

The information security force fields diagram, as introduced in chapter 3 figure 3.2, gives a visual indication of the forces impacting on information security and possible stakeholders can be derived from the diagram. Generating a force field diagram specifically for an organisation needs the involvement of a broad group of people covering all disciplines of the organisation. Business and line managers, IT representative, risk manager, user representative, everyone has their own responsibility in securing information and will have their own view on forces that impact on the security of an organisation.

Start point in force field analysis for a specific organisation should be an valuation of the importance of information for the organisation. Followed by listing all forces that impact on information and the security of that information. By introducing the force field diagram, the information security specialist can visualise the results of this analysis, an example is given at figure 5.1.

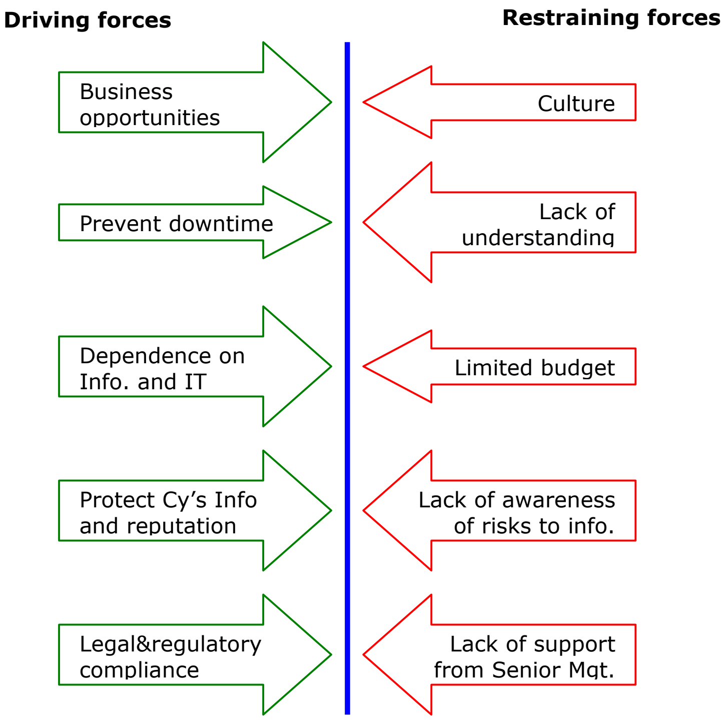

Driving forces
Restraining forces
Business opportunities
Prevent downtime
Dependence on Info. and IT
Protect Cy's Info and reputation
Legal&regulatory compliance
Culture
Lack of understanding
Limited budget
Lack of awareness of risks to info.
Lack of support from Senior Mgt.

Figure 5.1: Force Field diagram for Information Security – theoretical approach

The identified forces give an indication of the information security controls that could be used to ensure the security of an organisation's information. This will indicate technical controls, for example the force "prevent downtime" indicates that resilience and business continuity have to be ensured. Putting in place appropriate backup facilities and resilient equipment contribute to the prevention of downtime. The force field diagram will also identify the need for procedural controls. Showing "Legal & regulatory compliance" is not just a question of putting technical controls in place; it needs a Information Security Strategy and Policy to be established, including underlying procedures and instructions.

Analysis of the forces will certainly show a number of restraining forces that can be encountered by generating a higher level of understanding information security amongst managers and employees of an organisation. This can be achieved by the implementation of information security training & awareness.

The exercise of analysing the forces impacting on the security of an organisation as a whole and the security of information in particular, will generate a better understanding under employees and managers of the necessity of securing information. The result presented in the force field diagram will identify that sufficient information security training & awareness contributes to a more secure organisation. The diagram will also identify where changes can be made to increase the level of security of an organisation.

5.3. The real world

As mentioned in chapter 2 the focus of businesses is still on technical information security controls aimed at the external attacker. Although the internal threat is clearly on the rise, surveys [PWC-06] and [D-06] identify this, it seems that Information Security Training and Awareness is not recognised as contributor to security.

Surveys [PWC-06] and [D-06] show that 60-70 % of security incidents are related to people, mainly employees of the organisation. My own work experience tells me that this percentage is even a little higher: 80%. Not all security incidents and breaches of security policies are malicious or deliberate, most of them can be traced back to not knowing the security policies, not understanding the risks to information, mistakes and errors due to lack of user training. All of these incidents can be avoided by implementing structured information security training and awareness. The questionnaire used in the case study had a similar result, more than 40% of respondents identified users as main (more 75% of incidents) the cause of security incidents.

The impact that information security training and awareness can have, was illustrated by one of the interviewees: the strength of restraining forces was valued differently for newcomers versus established employees. See the next paragraph for more details.

5.4. The forces that impact on Information Security

The results from the case study of chapter 4 support the view that Information Security Training & Awareness can decrease the strength of restraining forces. This decrease will make the driving forces more effective.

Driving forces

The following driving forces were identified during interviews and in the questionnaire (in no particular order):

- Change & Project Management (cost reduction)*
  When Information Security is considered from the start (and not as an add-on at the end) this will lead to reduction of cost in changes and projects in Information Technology.
- Business opportunities
  Having established an Information Security Management System can result in potential customers and partners having confidence in your organisation.
- Prevent downtime*
- Dependence on information and Information Technology*

- Protect company's information and reputation*
- Legal & Regulatory compliance*
- Support from senior management*
  This is also identified as a restraining force. Often the direct line of managers is very supportive of the Security Team, probably because they have a better understanding of information security than senior management in other areas of the organisation.
- Duty of care
  From organisation to employees and vice versa.
- Data Protection Act
  Due to the type of organisation and the function of some of the employees the Data Protection Act is a very strong driving force; therefore this force needs to be mentioned separately (from Legal & Regulatory compliance) for some organisations.
- Security governance and organisational security structure*
  This force includes a number of forces that were mentioned separately, but they are collated together: security governance encouraging risk-based approach, distributed security organisation, respect and trust in security personnel and company policies.
- Reduction of commercial risk
- Audits
- Security minded culture

Restraining forces

The following restraining forces were identified during interviews and questionnaire (in no particular order):

- Culture*
- Lack of understanding*
  Mainly the understanding of the need to protect information
- Limited budget*
- Lack of awareness of the (current) risks to information*
- Lack of support from senior management*
  This force is also identified as a Driving force. As a Restraining force it is mainly a financial matter, managers in for example the Account Management Team see information security as costly and it hampers the business to achieve their financial goals.
- Non-availability of instructors
- Drive to adopt Commercial of the Shelve (COTS) products
- Lack of support from the IT department*
- Unreasonable business drivers

- Project pressures
  This force is related to mainly high level projects with a high visibility to senior managers and external parties. Project managers are being put under pressure to progress projects leading to the acceptance of (information security) risks that are not properly assessed. The result is that afterwards controls need to be put in place or the security team need to "clear-up" the problems. These activities are bound to be much more expensive than involving security from the start of a project.
- Lack of security governance and organisational security structure*
  This includes a number of forces mentioned by respondents such as "lack of clear security structure or security responsibilities", "no respect or trust in security personnel" and "management risk appetite".

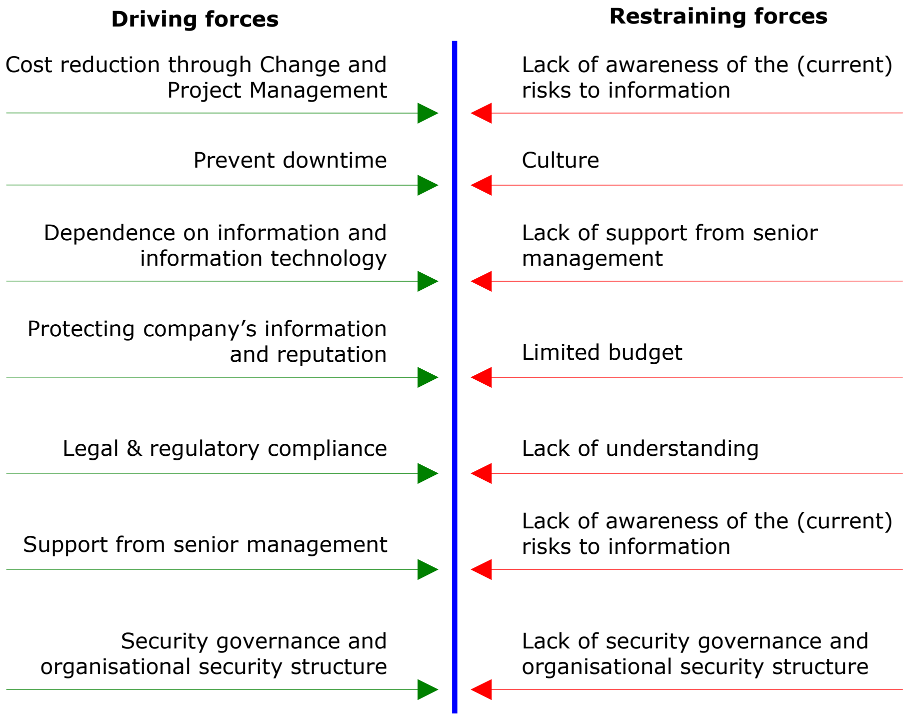

Driving forces
Restraining forces
Cost reduction through Change and Project Management
Lack of awareness of the (current) risks to information
Prevent downtime
Culture
Dependence on information and information technology
Lack of support from senior management
Protecting company's information and reputation
Limited budget
Legal & regulatory compliance
Lack of understanding
Support from senior management
Lack of awareness of the (current) risks to information
Security governance and organisational security structure
Lack of security governance and organisational security structure

Figure 5.2: Force Field diagram for Information Security – real world

The force field diagram created from the case study results, figure 5.2, are for several organisations, representing the top seven of driving and restraining forces. The selection is reflecting the number of times the force was mentioned by different participants in the case study and the values (strength) given to the forces during the interviews. The forces marked with an * in the lists and are top seven.

5.5. Using the Information Security Force Field Diagram

Depending on the organisation the force field analysis is carried out for, the list of the driving and forces is different. When a force field diagram is drawn for a specific organisation it will not often happen that the same force appears at opposing sides, as is the case in figure 5.2, because this diagram covers several organisations. An exception might be "Support of senior management" as senior management in direct line of command with the security unit has a different understanding than senior management in for example the financial department.

The diagram of figure 5.2 clearly covers all areas of information security: technical, procedural and personnel security. The diagram can be used to find out where security of an organisation can be improved. By studying each force on it's merit and visualising them in a diagram together, decisions can be made where the investments can be most effective and efficient.
A large number of the forces in figure 5.2 are closely related to people, the majority of these are restraining forces. That is where the implementation of structured Information Security Training & Awareness could make a difference: decreasing the strength of the restraining forces and therefore making the driving forces more effective and efficient. This was illustrated by one of the interviewees by giving two different values to the same restraining force. The organisation involved has information security training in place since 1998. The value given to the force "Lack of awareness of risks to information" was high for new employees, while the value for established employees who have received security training is low, more examples can be found in appendix B – part 3.

Senior management's to invest time and money in training and awareness is illustrated in one of the interviews carried out as part of the case study: different values were given to the same force in the same organisation. The restraining force "Lack of support from senior management" was given a very low strength value in the phase where initiatives of training and awareness were discussed. But as soon as the consequences became clear (time and money needed) during the implementation phase, senior management became reluctant to invest the time and money necessary. The value of the restraining force went up to high during the implementation phase.

5.6. Summary & Conclusions

Chapter 5 identifies the link between the overall security of an organisation and Information Security Training and Awareness. First the force field analysis model for Information Security, as laid out in chapter 3, is used to show a theoretical view on this link between security and training and awareness. This view is than tested against a work environment by using the results from the case study in a force field diagram with figure 5.2 as result.

The exercise of analysing the forces impacting on security in general and the security of information in particular visualises how forces work together and against each other. It generates a better understanding under employees and managers of the necessity of securing information.

The driving and restraining forces reflect all areas of information security counter measures: technical, procedural and personnel. Visualising the forces enables the information security specialist to explain to non-specialists why an organisation needs to invest, in resources and finances, to secure information.

The diagram identifies where investments are most effective and efficient and that there is a link between the security of an organisation and the level of information security training and awareness. And it will prove that investing in training and awareness is a very cost-effective counter measure: on one hand it will increase the overall level of security of an organisation, as users are more aware of the risks, on the other hand it decreases the restraining forces and with doing so the driving forces become more effective.

Chapter 6: Measuring Security and the Impact of Training & Awareness

6.1. Introduction

As identified in the previous chapters of this project report, it is necessary to have support of Senior Management to effectively implement an Information Security Strategy and Program. Several publications refer to measuring effectiveness of strategies and programs as one of the ways to get Senior Management buy-in.

Information Security professionals have to convince management that they have to invest time and money in Information Security as a whole. To take this a bit further Information Security Training & Awareness is very cost-effective counter measure to put in place as a protective control against the threats modern organisations face. In the world of distributed corporate environments, globalisation and fast developing technology, the risks to information assets are increasing. Surveys clearly identify people as the weakest link in the protection of organisation's information.

Firstly this chapter looks at the publications that cover measuring security and/or measuring the effectiveness of training programs and awareness campaigns. At the end of paragraphs 6.3 and 6.4 my personal view on these publications is given.

The middle part of this chapter takes a new approach to measuring security: using the force field analysis and diagram to measure security and the impact of training & awareness.

6.2. Publications and experiences

One way to convince senior management that they need to invest in information security in general and training and awareness in particular is to quantify both. Unfortunately for information security professionals there is no straightforward solution of techniques, parameters and indicators. A number of people have been publishing articles, books and white papers on the topic of measuring security and measuring the impact of training and awareness. Each of these authors take a specific approach. Reading these publications showed me how difficult it is to find a way to quantify security and the impact of training and awareness. The following two paragraphs give an overview of the publications I read and my opinion on them.

6.3. Measuring security

Steve Wright wrote a white paper with the title **"Measuring the effectiveness of security using ISO27001" [WrS-06]**. Wright explains why it is difficult to measure the effectiveness of the selected security controls, he states *"…forgot to* *appreciate, or map, the relationship between their organisational risks and the Information Security Management System…".* The white paper [WrS-06] provides a background of why it is necessary to measure security, objectives and benefits of doing so and what exactly we need to measure. Wright also gives a few tips on requirements to the metrics and methods used, for example the link with business goals is essential. At the end of the white paper he gives examples related to groups of controls he identified in [WrS-06]: management controls, business processes, operational controls and technical controls.

An article found on the SANS Reading Room has the title **"A Guide to Security Metrics"**, by Shirley Payne **[PS-06]**. The author of [PS-06] identifies that *"…, security managers are more than ever before being held accountable for demonstrating the effectiveness of their security program."* Security metrics could be an answer to this demand. The guide [PS-06] defines metrics and measurements, the difference between them and the requirement that metrics have to be SMART, i.e. **S**pecific, **M**easurable, **A**ttainable, **R**epeatable and **T**ime-dependent. Payne also identifies that metrics used differ depending on the audience of a presentation: metrics used amongst security professionals are different from metrics used to communicate with business managers. The guide [PS-06] continues by explaining the value of metrics, the difficulties in generating them and it suggest the method for building a security metrics program. The main benefit of using security metrics is that it gives security managers a tool to prove that an organisation is more secure than before, or more secure than competitors in the industry. Payne also mentions in [PS-06] that those who are taking up the development of security metrics should consider themselves as pioneers and they should be prepared to change tactics along the way.

My view

In addition to [PS-06], when employed by an English police force, a Statement of Applicability (SOA) was used to measure the level of compliance with the controls selected from ISO 27001. Every year the SOA was filled out and the changes in the level of compliance showed progress towards a more secure environment. The problem with that SOA was that it was useful for information security professionals but was not understandable to business managers. In my opinion this annual assessment of compliance could be used to measure the level of security in relation to business risks, but someone (the information security specialist) will need to make the information in the SOA understandable for business managers.

Although the method Payne suggests in [PS-06] is logical, the approach is too much from the perspective of the security program. In my opinion the first step to achieve a common set of security metrics is to define the link between business processes and information security. Illustrating this link to business managers generates a better understanding of information security and buy-in.

6.4. Measuring the impact of training and awareness

A comprehensive publication on the link between information security and training and awareness is Angus McIlwraith's book **"Information Security and Employee Behaviour, *How to reduce risk through employee education, training and awareness*" [MA-06]**. This book explains how corporate culture influences people's judgement of risks to information, their perception of information security and how these two affect employee's behaviour. The first part of the book [MA-06] investigates the understanding in the broader sense, by looking at risk & risk perception, culture and communication. The second part of the book creates a framework for implementation of Information Security Education, Training and Awareness. The latter part includes a chapter on measuring awareness by giving tools and techniques; and details a number of different communication materials/channels that can be used.

My view

The book [MA-06] takes a psychological approach, which is very appealing to me. McIlwraith uses the angle of Risk Management and I agree with him that Information Security Training and Awareness reduces the risks to information; his approach inspired me to look for similar approach but with a different angle to measure the impact of training and awareness on security.

To find a way to measure the impact of training and awareness on security, I decided to look at the Education and Training Industry. During research I came across a number of interesting articles and methods. One method referred to many times is Donald Kirkpatrick's four level framework for the evaluation of training. The four levels are all very much related to the person that received the training: reaction (first impression of the training), learning (what knowledge was gained), behaviour (what skills were developed, used in the job) and results or effectiveness (skills used in work and achievements). The information necessary to answer the questions at all four levels has to come from questionnaires and interviews addressed at the recipient of the training and the line manager involved. Research on practical implementation of this method shows that level 1 (reaction) and 2 (learning) is used in practice, but level 3 (behaviour) is not often found and level 4 (business impact) is not found to be implemented. My view is that it is necessary to find ways to measure the impact of training awareness that are not directly related to the actual training and the recipient, but more how the training impacts on business processes in general and security in particular.

In the Education and Training Industry measuring the effectiveness and impact is mainly focussed on the training as such and the way people's performance change.

Much more difficult to measure is the impact on business processes, the value training adds to the business by for example improving efficiency and productivity. More specifically to be able to measure the impact of information security training and awareness on the overall security of an organisation it is necessary to:
1) illustrate the connection between the business processes and security;
2) make the link between security and training and awareness; and
3) identify indicators to prove the additional value of Information Security Training and Awareness to the level of security of the organisation.

6.5. A new approach – a new method

So far in the articles and publications I have read on this topic I have not found a solution that appropriately incorporates business processes and managers in the methods to measure security. If you want buy-in from senior management in your Information Security Program in general and Training and Awareness in particular, you need to be able to measure in such a way that you can prove the additional value security brings to the business. To achieve that, business managers need to be involved in the development of a valuation method that measures the level of security and the impact of training and awareness, and can be re-used time and time again to illustrate the progress that is made over time.

In chapter 3 of this report the force field analysis model of Kurt Lewin was applied to information security. The link between security of an organisation and information security training and awareness is shown in chapter 5, using the same force field diagram of figure 3.2.

The steps described in the Mini-tutorial [WeS-06] will be re-shaped to make them usable for the development of a method to measure security and value the impact of training and awareness using the Information Security Force Field Diagram introduced in chapter 3.

From the first step it is necessary to involve a number of business managers from a wide variety of disciplines. There is no standard list of indicators that can be introduced and used in every organisation, they are specific for each organisation and should be in alliance with the business processes and objectives. Although some preparatory work must be done by information security professionals, the actual application of this method mandates the presence of "the business".

Preparatory work

The information security manager and team need to explore the objectives of the exercise and develop a force field diagram that is used as the start point of the discussion. It is easier to discuss and develop a method if there is something visible to initiate the discussion. This could for example be the force field diagram of figure 3.2 with some connections to business processes.

Another task that need to be done before starting the development is to define a scale of values to use as strengths of the forces that are defined in steps 3 and 4 of the development process. It is also important that the information security manager familiarises him/herself with the business process, how information plays a part in these business processes and what the latest business objectives are. It might be necessary to have number of versions of the information security force field diagram each relating to a specific business process or a specific information asset.

Step 1: identify the connections between business processes and security

Introduce the information security force field diagram, as mentioned before this could be more than one. Facilitate, as information security manager, the discussion identifying the connections between business processes and information security. This needs to be carefully documented as it will form the basis of rest of the development process.

Step 2: identify the objectives of developing a valuation method

The aim of the whole exercise is to develop ways to measure security and impact of training and awareness. This is work that is partially prepared in advance, but need to be addressed with the results of step 1 in mind.

Step 3: driving forces

Analyse the driving forces and add any new driving forces identified during discussions with the business managers. At this stage it is important to define the forces in such a way that they can be valued at any moment in time. In other words not just now, but when this exercise is repeated in the future that it is possible to follow the same reasoning for valuing the strength of that force and therefore be able to compare and analyse the changes in strength over time.

Step 4: restraining forces

Use the same approach as in step 3 to analyse the restraining forces.

Step 5: assign initial impact values to the forces

In preparation for this development exercise the information security team have designed a scale of values; for example 1 = very weak, 2 = weak, 3 = strong, 4 = very strong. If risk management is established in your organisation, it might be helpful to use the business impact assessment matrix as the basis for this initial assignment. Using the risk management matrix makes the values you use recognisable to business managers.

Step 6: chart the forces in a new diagram

This step will visualise the connection between security and the business based on the contributions from a multi-disciplinary group involved in this development. The diagram will give a compact overview of where and how information security training and awareness can impact on the forces identified.

Step 7: analyse forces and possible metrics contributing to the strength
The forces identified in the diagram have an initial impact value given in step 5. The next step is to identify a scale of strength values. The strength of a force is determined by one or more contributing factors, parameters and indicators. To develop a measuring method that can be used over and over again, it is necessary to identify contributing factors to the strength of each individual force. So that when the valuation method is used in practice, it can be used repeatedly without changing the baseline. This is a very important step in the development process as it forms the basis of all future measurements related to security and the impact of training and awareness. To be able to use the method over a period of time it is paramount that the reasoning behind the assignment of a strength value is repeatable. Using metrics for analysis and reasoning creates a basic tool to assess strength of forces in a reasonable objective way.

Step 8: carry out a baseline assessment
Using the strength values identified in step 7, each force is assessed and a value is assigned. The reasoning and assessment process needs to be documented, including any steps or valuations of indicators contributing to the strength of the force. This initial measurement of the forces functions as a baseline for future measurements. The difference between the total strength of driving and restraining forces can be used as an indicator for the level of security. If the balance is in favour of the driving forces the level of security is acceptable, although there is always room for improvement and new forces may appear in the future. If the balance is in favour of the restraining forces there should be concern about the level of security and major effort must be put in improving the security of the organisation. Analysis of the forces can indicate where improvement can be made and it will often also indicate where the best Return of Investment is achievable.

Step 9: repeat this assessment periodically
Periodically this assessment will have to be repeated.

Step 10: Analysis of the assessments
Changes in the strength of the forces indicate changes in the level of security. Analysis of the changes is necessary to find out exactly which improvement action has had which impact on security. Certainly this analysis will indicate the impact of training and awareness. And a repeated assessment of the strength of certain forces makes it possible to reverse engineer (using the contributing factors and indicators) put figures to the benefits, for example cost reduction or a positive Return of Investment, of structured Information Security Training and Awareness.

As the whole development process has it's roots in the business processes, the analysis of the assessments should indicate in business terms how the level of security has changed over time and how security contributes to the business objectives. This last step is crucial in the sustained support, financially and in resources, of senior management for the Information Security Program.

6.6. Summary & Conclusions

Chapter 6 investigates the published methods to measure security and to measure the effectiveness of training and awareness. Both these measuring tasks are not straightforward, especially when you want to apply the methods to information security and related training and awareness. A new method is developed by using the force field analysis and diagram introduced in chapter 3. In this chapter it is applied for measuring.

In the world of distributed corporate environments, globalisation and fast developing technology, the risks to information assets are increasing. Information Security professionals have to convince management that they have to invest time and money in Information Security to secure their information. One way to do this is to quantify both.

Unfortunately for information security professionals there is no straightforward solution of techniques, parameters and indicators. And the articles and publications do not give a solution that appropriately incorporates business processes and managers in the methods to measure security. If you want buy-in from senior management in your Information Security Program in general and Training and Awareness in particular, you need to be able to measure in such a way that you can prove the additional value security brings to the business.

The method developed in this chapter has it's roots in the business processes, the analysis of the assessments should indicate in business terms how the level of security has changed over time and how security contributes to the business objectives. The force field diagram shows how training and awareness can contribute to security of an organisation and by making the forces measurable; it gives a tool to measure the impact of information security training and awareness.

Chapter 7:
Training Program and
Awareness & Communications Plan

7.1. Introduction

Many Information Security Standards and Best Practices recognise the importance of Information Security Training & Awareness as part of the Information Security Strategy and Program. During the interviews of the case study, chapter 4 gives more details, the first three sections focussed on the Training and/or Awareness programs that are in place for the environments the interviewees work in.

This chapter builds on the identified benefits or potential benefits of a structured approach to Information Security Training & Awareness, as identified in the case study. The delivery and the content of training material is very different from delivery and content of awareness material. Therefore this project takes the approach of separate paths for Training and Awareness. The structure of both paths will differ per organisation and a good start point for development is the results of the information security force field analysis and diagram of chapters 5 and 6.

7.2. Information Security Training & Awareness

There are some publications that give an idea of topics that should be covered in information security training. The Director's Guide [DPL-05] is an example, it states that *"…, all employees should receive some sort of security awareness training that is relevant an appropriate to their job function, role and responsibilities within the organisation."* As mentioned before in this project report: the way people look towards Information Security need to change and they need sufficient knowledge of Information Security issues to be able to do their job in a secure manner, compliant with published security policies and procedures, this includes making them aware of the threats and risks to information if we do not implement Information Security Controls.

Information Security professionals have to keep in mind that users and managers do not read all the articles and publications they do; users and managers do not deal with daily security updates from for example software providers. If the professionals do not explain to users and managers why the security controls are necessary, they will not understand why professionals make their lives so difficult with all these controls and limitations.

As identified in chapter 5 a large number of the restraining forces are related to lack of understanding and unawareness of the risks to information. Implementing structured information security training and awareness will decrease these restraining forces. When using the quantification method of chapter 6 sufficient training and awareness will have a double impact:

- the decrease of restraining forces resulting in an increase in the level of security of an organisation; and
- the decrease also makes the driving forces more effective and efficient.

This makes the implementation of information security training and awareness an efficient, cost-effective protective control.

7.3. Benefits of Information Security Training & Awareness

The number of benefits identified in the case study supports my view of how training and awareness can impact on information security. It is clear that the longer Information Security Training & Awareness has been in place the aversion against information security has reduced.

Not all the interviewees could give benefits related to the actual implementation of an Information security Training & Awareness program as they only just started to notice the changes in people's behaviour. The following benefits were identified:

- less time-wasting by users;
- reduction of security incidents;
- less time spent on incident investigations by the Security Team;
- improve project life-cycle time and therefore reduce project costs and less re-work on System Security Policy for projects;
- maintaining reputation of service provider and client organisations;
- better able to fulfil "duty-of-care" towards employees;
- standardisation of the security message;
- change of attitude towards information security.

7.4. Information Security Training Program

Training as such focuses on user needs: it can be very specific for a certain role in an organisation, with specific security responsibilities, or more general to achieve the same level of understanding for larger groups of employees. The structure and content of the Information Security Training Program of an organisation should be based on the needs of the organisation. The Force Field Analysis of chapters 5 and 6 is a good basis to define the structure, the content and the priorities of the Program.

Structure

There are a number of topics that must be addressed in a training program:

- <u>Aims and objectives</u> of the program, here it is important to make the link with the Force Field Analysis as it will define what the program needs to achieve.

- Target groups, not all groups of people have the same security responsibilities in an organisation. A number of target audiences will be identified, examples are end-users, new recruited employees, line managers, senior managers and Information Technology workers. The latter group will probably be divided into a number of sub-groups such as help desk employees, database administrators, system administrators, etcetera.
- Needs, each target group will have different needs for training, depending on their security responsibilities.
- Key messages, all training provided should show consistency in the key messages that are delivered. These should be identified in advance.
- Delivery mechanisms will need to be defined for each training. Examples are presentations, computer based training, courses, modules embedded in general training sessions or on the job training.
- Training material needs to be developed for each of the sessions that is planned in the program. It is important to create a framework, or "course plan" for each piece of training material that is developed, defining the topics covered, the level of detail, the learning objectives and the way to prove that the objectives are met.

Content

Information Security is not a static environment, it changes every day. Although the key messages as defined in the structure of the program will not change often, the content of training material needs to be updated more frequently. Experiences with providing security training show it is useful to review the training material before the next session. In other words every piece of training material deserves to be reviewed shortly before using the material again for a training session. It does not mean that the whole content changes every time, but when examples are used such as real incidents it is useful to use recent incidents that people may remember or are very closely related to new vulnerabilities and changed threats. The framework of training material will often be in line with security policies and procedures and will probably change only when policies and procedures are reviewed.

The content of training material will be different for different audiences, depending on the security responsibilities of the target group. The level of detail will also vary depending on the target audience. For example an Information Security module as part of the Induction Course for new employees, will have a totally different content than training material developed for Line Managers.

The Force Field Analysis could also indicate that a specific topic needs to be covered in courses and presentation, this leads to the development of a new course/module or lead to review of existing training material.

A number of topics certainly need to be covered in training material:

- information security policies and procedures;
- the organisational structure of security, roles and responsibilities;
- document handling and information sharing;
- security incident response;
- threats, vulnerabilities and risks to information;
- social engineering;
- use of email and Internet;
- recent security incident and breaches of policy.

Priority and frequency

The priorities of information security training should not be a "one-person decision". Using the Force Field Analysis (or otherwise involving managers and risk owners) could be the basis of the priorities set in the training program. There has to be a certain flexibility as the world of information security changes every day.

What could be useful to have is a schedule of information security training. This is based on for example on how many new employees are recruited per year, how often mangers are promoted into new (higher) management levels and the review schedule of policies and procedures.

7.5. Possible courses and modules

As mentioned in the previous paragraph there are a number of different possible modules, courses and presentations that could be part of an Information Security Training Program:

- Induction training;
- Refreshment training (for example annually);
- Training for helpdesk employees;
- Training for system administrators;
- Training for receptionists (social engineering especially);
- Training for post room employees;
- Training for team leaders and line managers;
- Training in securely using email and Internet;
- Training in specific topics such as Protective Marking and Social Engineering.

7.6. Information Security Awareness & Communications Plan

Awareness is less structured than training and focuses on effective communication to target audiences on general and/or specific subjects. An Awareness and

Communications Plan in general includes short term actions and long term activities to promote and propagate a product, a subject or an issue. The communication material used are "living documents" and will need reviewing frequently.

For short term actions you have to think about making people understand the need for information security, communicate about security incident or breaches of security policies and procedures and inform employees of perceived benefits of information security.

The long term activities could include: regular moments of communication, publications on corporate Intranet and the annual acknowledgement of users to comply with information security policies and procedures.

Structure

There are a number of topics that must be addressed in an awareness and communications plan:

- Aims and objectives of the plan, awareness and communication is more about broadcasting a message. One of the objectives is to make information security understandable and recognisable as part of everybody's day job.
- Target groups and needs are more difficult to identify at the start. There will be a standard short list of different audiences, for example Line Managers and End Users, but the majority will come up as and when. Awareness is much more than training something that is developed on an ad-hoc basis.
- Key messages, all communication send out should show consistency in the key messages that are delivered. These should be identified in advance.
- Delivery mechanisms will need to be defined for each topic that needs to be communicated upon, examples are posters, leaflets, corporate intranet publications, info bulletins, screen saver and briefings.
- Communication material is different from message to message and mechanism to mechanism. What should be established is a recognisable lay-out of the material. This will give the information security unit an identity in the organisation and hopefully encourages people in the organisation to contact the unit for additional information and advice.

Content

Even more than the training material, communication and awareness material is changing all the time. The long term activities could have some sort of standard content and format, but the actual message will be different almost every time. The short term actions are totally dependent on the daily issues, events and topics that are current at the time. As mentioned before it is important that the communication material has a recognisable lay-out, users will identify the information security unit with it.

Priority and frequency

Communication and Awareness is part of the day-to-day activities of information security professionals. Decisions are made on an ad-hoc basis and in some situations it might be necessary (or advisable) to consult senior managers before sending a communication out.

The long term activities can be planned and scheduled in advance. But the short term actions will just come up and will have to be dealt with there and than.

7.7. Possible communications

A few of the communications could be planned as mentioned in the previous paragraph and although their content will be different every time, they should have a certain standard format and structure. Using a fixed lay-out gives the information security unit an identity and regular communications creates an "open door" culture towards the unit. Possible long-term communication activities:

- Information security bulletin
  For example every three months a bulletin is published informing everyone of the latest threats and vulnerabilities (explained in layman's terms) or occurred security incidents, or giving information on one specific topic that is current at that time.
- Annual acknowledgement
  Users should repeatedly confirm that they know and comply with security policies and procedures. This moment of communication can be used to point users to the Intranet page where the security policies and procedures are published and to inform the users of changes to these documents.
- Information Security Intranet Site
  The content on this site should change at least every month, but there should be a fixed list of links to security policies and procedures. Here specific topics could be explained or advice published. If for example a large number of questions are asked about viruses and email, it may be a good topic for an article on the Intranet site.
- Screen saver
  The standard screen saver on a network could be used to publish short compact but important messages; for example the message not to divulge your password to anyone.

7.8. Summary & Conclusions

The way people look at Information Security needs to change. They need sufficient knowledge of Information Security to be able to do their job in a secure manner, compliant with published security policies and procedures; this includes making them aware of the threats and risks to information if we do not implement Information Security Controls.

This chapter summarises how training and awareness can contribute to making an organisation more secure. Making users and managers more aware of threats, vulnerabilities and threats to information on one side and train them sufficiently to carry out their daily tasks in a secure manner is an efficient security control.

After listing some benefits of structured information security training and awareness, possible structures of an Training Program and an Awareness & Communications Plan are given.

Personnel security becomes more important, but the attitude of managers and employees does not follow that trend. This needs changing. One way of achieving that is giving people the information security knowledge and awareness they need for their role. It seems that the solution does not lay in technical controls but more on the non-technical side: the side of human resource security. Investing in training and awareness is a very cost-effective counter measure: on one hand it will increase the overall level of security of an organisation, as users are more aware of the risks, on the other hand it decreases the restraining forces and with doing so the driving forces become more effective.

Chapter 8: Results, Conclusions and Recommendations

8.1. Summary and Results

Information security standards, best practices and literature all identify the need for Training & Awareness, the theory is clear. The surveys studied, [PWC-06] and [D-06], show that in the real world the situation is different: the focus of businesses is still on technical information security controls aimed at the external attacker. It seems that Information Security Training and Awareness is not recognised as contributor to security. As a result Senior Management seems reluctant to invest time and money in appropriate Information Security Training & Awareness.

To change this situation it is necessary to identify the links between the overall security of an organisation and information security training and awareness. To convince senior management that investing in training and awareness is viable, you need a way to explain in business terms the impacting factors on security and how these factors can be influenced by an adequate information security training and awareness program.

One way to convince senior management is to quantify security and quantify the impact of training and awareness. This report introduces a possible way to measure security and measure the impact of information security training and awareness.

The way people look towards Information Security need to change and they need sufficient knowledge of Information Security issues to be able to do their job in a secure manner, compliant with published security policies and procedures, this includes making them aware of the threats and risks to information if we do not implement Information Security Controls.

To test my personal views and ideas in a practical, business environment a case study has been conducted as part of this project. Interviews with a small number of Information Security professionals working in a business environment. Followed by a questionnaire for a larger group of Information Security professionals, to find additional experiences.

The case study clearly supports my personal views on Information Security Training and Awareness. The interviews gave me a good idea of practical implementations in business environments. These results inspired me to develop the force field model into a tool for information security professionals to visualise the link between business processes, information security and training and awareness on one hand; and use it to measure security and quantify the impact of training and awareness on the other.

The method developed in this report has it's roots in the business processes, the analysis of the assessments should indicate in business terms how the level of security has changed over time and how security contributes to the business objectives. The force field diagram shows how training and awareness can contribute to security of an organisation. By making the forces measurable, it gives a tool to measure the impact of information security training and awareness.

This report gives a number of benefits of implementing information security training & awareness and make it part of the overall security strategy. The possible structures of a Training Program and Awareness & Communications Plan are given as a starting point for the information security specialist to create their own Program and Plan.

8.2. Conclusions

As mentioned above Information security standards [ISO-05/1] and [ISO-05/2], best practices [DPL-05], literature [PT-05] and [GD-06] and articles [CJ-07] and [TL-04] all identify the need for Training & Awareness. The surveys [PWC-06] and [D-06] look at the real world and although threats and vulnerabilities point out that personnel security becomes more important, the attitude of managers and employees does not reflect that. This needs changing, which means changing behaviour and attitude. One way of doing just that is giving people the information security knowledge and awareness they need for their day jobs. It seems that the solution does not lay in technical controls but more on the non-technical side: the side of human resource security and psychology. The Director's Guide [DPL-05] supports this view.

Changing the attitude of employees and senior management can solve many of the problems information security specialist face every day. With the aid of [LK], [LK-06] and [WeS-06] a psychological model is introduced in support of the objectives of this project. This model is applied to information security, to use it as a tool to visualise and quantify the forces that impact on information security. This application shows links between the security of an organisation and the potential impact that training and awareness could make when it is incorporated into the Information Security Program of an organisation.

In the world of distributed corporate environments, globalisation and fast developing technology, the risks to information assets are increasing. Information Security professionals have to convince management that they have to invest time and money in Information Security to secure their information. One way to do this is to quantify both.

Unfortunately for information security professionals there is no straightforward solution of techniques, parameters and indicators. And the articles [WrS-06] and

[PS-06] and publication [MA-06] do not give a solution that appropriately incorporates business processes and managers in the methods to measure security. If you want buy-in from senior management in your Information Security Program in general and Training and Awareness in particular, you need to be able to measure in such a way that you can prove the additional value security brings to the business.

The exercise of analysing the forces impacting on security in general and the security of information in particular visualises how forces work together and against each other. It generates a better understanding under employees and managers of the necessity of securing information.

8.3. The way ahead

In modern organisations information systems are intrinsically linked to their ability to perform their primary business processes. Risks to information systems have the potential to cause damage or loss, and significantly affect operational performance and reputation of an organisation.

To survive in the modern world of information technology (IT) and all the advantages this has brought, organisations have to protect themselves against the threats and vulnerabilities IT developments bring with it. Senior Management has to embrace Information Security to sufficiently protect probably one of their most critical and valuable assets: information.

The most important role of Senior Management in relation to Information Security is to take ownership and make it part of the organisation’s strategy. The risks to information will have to be weighed against other business risks such as financial, legal and operational risks. On the basis of a strategic decision Information Security responsibilities can be assigned to Information Security professionals and the necessary budget made available to achieve the required level of protection for information assets. With these two essential resources in place, professionals and budget, an Information Security Management System can be set up. This includes procedural, physical, personnel and technological controls.

The driving and restraining forces of the information security force field diagram reflect all areas of information security counter measures: technical, procedural and personnel. Visualising the forces enables the information security specialist to explain to non-specialists why an organisation needs to invest, in resources and finances, to secure information. The diagram will point out where investments are most effective and efficient.

Certainly the diagram will identify that there is a link between the security of an organisation and the level of information security training and awareness. And it will prove that investing in training and awareness is a very cost-effective counter measure: on one hand it will increase the overall level of security of an organisation, as users are more aware of the risks, on the other hand it decreases the restraining forces and with doing so the driving forces become more effective.

The information security force field analysis and diagram as introduced in this project, can be a useful new tool for professionals to:

- communicate effectively to line and senior managers about the link between business processes and information security;
- explain how investment in training and awareness can impact on information security and improve security of an organisation;
- quantify the level of security of an organisation in comparison with other organisations or in comparison with the previous moment of measuring;
- quantify the impact of information security training & awareness.

The ideas in this project report have developed from pure personal ideas, via the case study into a model that, if used appropriately, could close the gap between information security professionals and the "business-side" of an organisation. The model should be used as a tool to visualise and quantify the contributions and influences information security has on an organisation.

At this stage the model as such has not been tested in the real world. Although there is clearly a potential for this model to become a widely used tool, it needs further development, more practical influences with more guidelines for it's use.

Bibliography

[CJ-07] John Colley; Put people above technology, says (ISC)^2; Info-Security Magazine May/June 2007

[D-06] Deloitte; 2006 Global Security Survey for the Global Financial Services Industry

[DPL-05] Director Publication Ltd published for Institute of Directors and the Department of Trade and Industry; Director's Guide: Information Security best practice measures for protecting your business; May 2005

[EDS-04] EDS Limited; Terms of Reference for Client Security Officer; Issue 1.0 11-08-2004; classified document **EDS INTERNAL**

[E-06] European Network and Information Security Agency; Information Security Awareness programmes in the EU: Insight and Guidance for Member States; September 2006; from ENISA website www.enisa.europa.eu

[EWI-05] EastWest Institute *Consortium on Security and Technology*, Meeting report of 2nd meeting with the topic Information Security and Identity Management; 1st December 2005; found on the ENISA website www.enisa.europa.eu

[GD-06] Dieter Gollmann; Computer Security; second edition July 2006

[ISO-05/1]International Standards Organisation; ISO/IEC 27001:2005 Information Security Management System – Requirements; 18th October 2005

[ISO-05/2]International Standards Organisation;ISO/IEC 17799:2005 Code of Practice for Information Security Management; 16th June 2005

[KL] Kurt Lewin; The Forces are with you; www.freequality.org

[KL-06] Kurt Lewin; Force Field Analysis and Diagram; last updated September 2006; from Value Based Management .net

[MA-06] Angus McIlwraith; Information Security and Employee Behaviour, *How to reduce risk through employee education, training and awareness*; February 2006 by Gower Publishing

[PS-06] Shirley C. Payne; A guide to security metrics; 19th June 2006; SANS Reading Room

[PT-05] Thomas R. Peltier, Justin Peltier and John Brackley; Information Security Fundamentals; 2005.

[PWC-06] Price Waterhouse Coopers; DTI Information Security breaches survey 2006

[TL04] Laura Taylor; Security Awareness and Training; 10th November 2004; article found at www.intranetjournal.com

[WeS-06] Stephen Wells; Force Field Analysis – Mini Tutorial Quality Management; attached to report as appendix A; 15-03-2006

[WrS-06] Steve Wright; Measuring the effectiveness of security using ISO 27001; White Paper published in 2006

Appendix A:
Force Field Analysis – Mini Tutorial Quality Management

Force Field Analysis

Mini-Tutorial
Quality Management
Stephen Wells
March 15, 2006

Force Field Analysis

Mini-Tutorial
Quality Management

Stephen Wells
March 15, 2006

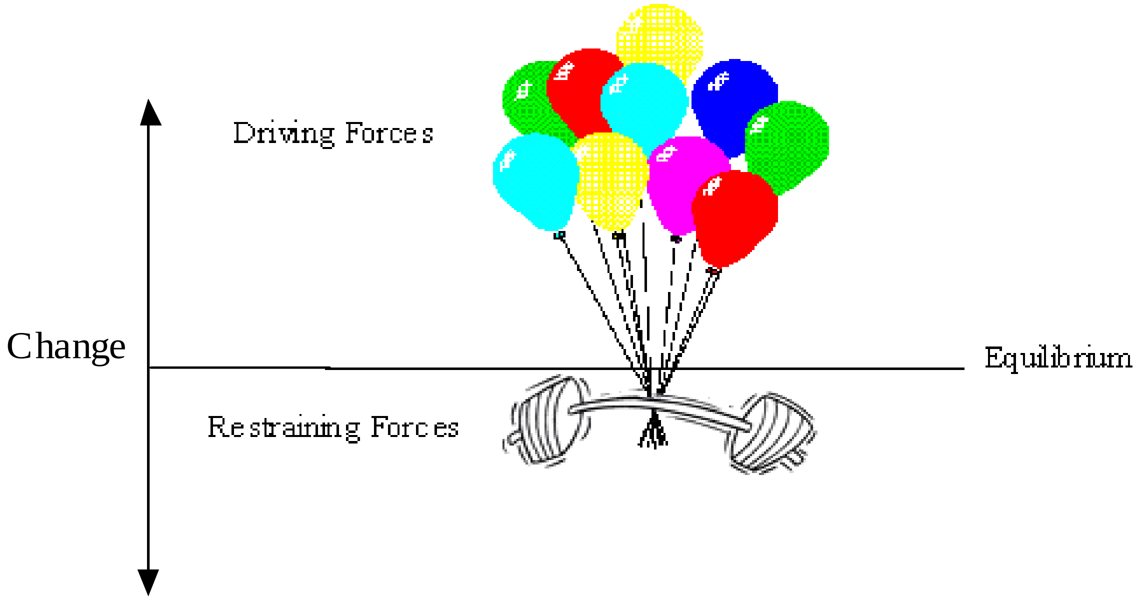
Introduction

Force field analysis is a valuable change-management tool. This management technique was developed by Kurt Lewin, an expert in experiential learning, group dynamics and action research. Although Kurt Lewin contributed greatly to the field of social science, he is best-known for his development of the Force field analysis model in 1947.

Lewin's force field analysis is evaluates the net impact of all forces that influence change. These forces can be divided into two groups: driving forces and restraining forces. Driving forces are all forces that push for and promote change. These change drivers promote and encourage the change process. Some examples of driving forces are executive mandate, customer demands, and increased efficiency. Restraining forces are forces that make change more difficult. These forces counteract driving forces and lead to the avoidance or resistance of change. Some examples of restraining forces are fear, lack of training, and the lack of incentives. When these two sets of forces are equal change is in a static state of equilibrium meaning that no movement towards or away from change is happening.

To better understand the connection between driving and restraining forces and how they impact change; a simple metaphor is of use (see illustration below). Suppose a group of helium-filled balloons are attached to a set of weights. The helium in the balloons creates an upward lift of five pounds. The weight of the attached weights is also five pounds. Because both the driving forces (balloons) and the restraining forces (weights) are equal, the balloons are unable to lift off the ground towards change. However, the addition of a single balloon or the removal of a single once of weight would change the balance and would start the system rising towards the envisioned change.

Figure 1.1



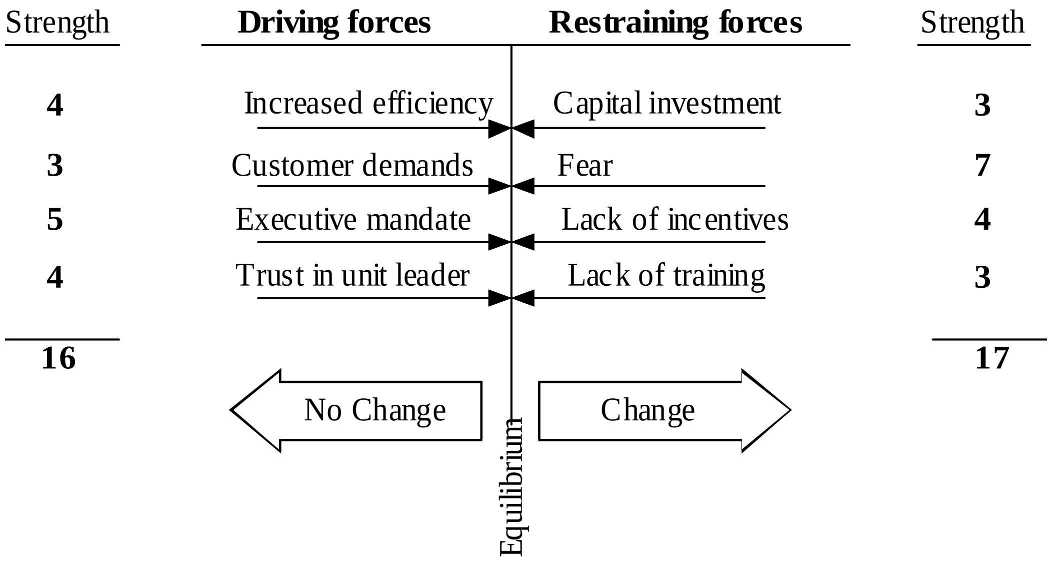
Implementation

This section discusses how to implement the force field analysis into a business setting. Although there are several different methods and variations for conducting force field analysis, there are commonalities among all of them. The steps outlined below capture many of these commonalities and represent the process needed for successful implementation of a typical force field analysis.

1. Identify and understand the current state
2. Identify and understand the desired goal state relative to the proposed change.
3. Identify and list driving forces acting to support the change. It is important to list all forces regardless of their seemingly small influence. Driving forces are forces acting to move the current state *towards* the goal state.
4. Identify and list restraining forces acting to hinder the change. Remember restraining forces are forces holding the current state *back* from the goal state.
5. For each force, designate the level of influence using a numerical scale e.g. 1=extremely weak and 7=extremely strong.
6. Chart the forces by listing the driving forces on the left and restraining forces on the right. Also chart the numbers allocated in step 5 next to their related force.
7. Evaluate the chart and determine whether change is viable.
8. Discuss how the change can be affected by decreasing the strength of the restraining forces or by increasing the strength of driving forces.
9. Discuss action strategies to eliminate the restraining forces and to capitalize on the driving forces.

Through conducting this process, a force field diagram like the one shown in figure 1.2 should be created.

Figure 1.2



As shown in the above force field diagram, the total point value for restraining forces exceeds the total value of the driving forces. This means that the proposed change would likely fail if nothing is done to change the balance. To increase the likelihood of success, management can attempt to reduce restraining forces, increase driving forces, or some combination of the two. In changing the impact of one force, the impacts of other forces often change as well. One example of this interdependency would occur if management decides to reduce the level of employee fear be providing extra training and resources. The impact of fear as a restraining force may drop from a 7 to a 4, but the capital investment restraining force may increase from a 3 to a 7 resulting in a higher restraining force than before the change. The relationships among the many forces must be understood and evaluated before strategies to eliminate the restraining forces and to capitalize on the driving forces are implemented.

Applications

Force field analysis is being used for many different applications in a wide variety of industries. There are three main applications of the force field analysis tool:

1. Change management (which has been the focus of this article)
2. productivity improvement
3. decision making

Change management is the primary application for force field analysis. One industry that has embraced the usefulness of this tool is the health care industry. Change is a regular occurrence in the healthcare environment. One area of change in which the health care industry has used force field analysis is in the computerization of nursing systems. Nurses have widely varying attitudes toward computers and change in the workplace. To help in the transition, managers are evaluating the forces that encourage and the forces that impede the change. Based on the force field analysis, strategies must be developed to assist nurses in moving forward with the transition.

Productivity improvement is the second main application of force field analysis. This universal application of how to increase employee productivity demonstrates a powerful need for the force field analysis tool. Instead of looking at factors promoting and inhibiting change, managers can look at forces promoting and inhibiting productivity. This analysis can shed light on methods, strategies, and systems that can promote long-term improvements in employee productivity.

Force field analysis is also a powerful decision-making tool. By evaluating the forces supporting and opposing a specific decision, managers can know the likelihood of acceptance and can also manage the influencing forces to maximize the potential for acceptance and success.

The force field model is a valuable tool for use in these three applications; however, it is not limited to these forms of application. By understanding the principles of force field analysis, managers can customize the technique for use in a large variety of situations.

By recognizing that every decision and every change has forces that promote the change and forces that impede the change, managers can make smarter decisions and can use force field analysis to effectively manage change in their organizations.

Sources for more Information
Although there are no books dedicated to force field analysis, there are many sources available to further learn about methods and applications of this diverse and effective tool. Here are a few that I have used in my research of force field analysis.

Force Field Analysis: A New Way to Evaluate Your Strategy *Thomas, Joe*. **Long Range Planning**. London: Dec 1985.Vol.18, Iss. 6; pg. 54, 6 pgs

Implementing great new ideas through the use of force-field analysis (Part three of a series)
Floyd Hurt. **Direct Marketing**. Garden City: May 1998.Vol.61, Iss. 1; pg. 54, 3 pgs

Force Field Analysis: New Tool for Problem Solving
Tucker, Kerry. The Public Relations Journal. New York: July 1979.Vol.35, Iss. 7; pg. 23

Using Lewin's ***Force Field Analysis*** in Implementing a Nursing Information System.Authors:MARILYNN G. BOZAKSource:CIN: Computers, Informatics, Nursing; Mar/Apr2003, Vol. 21 Issue 2, p80-85, 6p

Management of change through ***force field analysis***.Authors:Baulcomb, Jean Sandra[1]Source:Journal of Nursing Management; Jul2003, Vol. 11 Issue 4, p275-280, 6p

***Focusing leadership through force field analysis: new variations on a venerable planning tool** *Randolph E Schwering*. **Leadership & Organization Development Journal**. Bradford: 2003.Vol.24, Iss. 7/8; pg. 361, 10 pgs

***Assessing prospects for organizational change: The uses of force field analysis** *Brager, George*, *Holloway, Stephen*. **Administration in Social Work**. New York: 1992.Vol.16, Iss. 3,4; pg. 15, 14 pgs

http://www.valuebasedmanagement.net/methods_lewin_force_field_analysis.html

http://www.accel-team.com/techniques/force_field_analysis.html

http://www.mindtools.com/forcefld.html

http://www.wiley.co.uk/innovate/website/pages/atoz/ffa.htm

http://www.brainstorming.org/book/c5.shtml

http://web.mit.edu/hr/oed/learn/change/tool_forcefield.html

Appendix B – Part 1

CASE STUDY – Dennis Witham interview

16th April 2007
(pages 58 – 70)

CASE STUDY – Dennis Witham interview

16th April 2007

Section 1 – Information Security Training & Awareness in your organisation

1. How is Information Security Training and Awareness structured in your organisation?

Information Security Training & Awareness has evolved over time and there is more evolution to come. There is a pro-active approach towards Information Security Training & Awareness and there are no specifications or specific structure, it is very much open and constantly evolving.

There are a number of components of which more details are given in section 2 (Training) and 3 (Awareness):

[1] Induction for EDS employees coming onto account (see section 2)
[2] Security Presentation for groups of EDS employees (see section 2)
[3] EDS Corporate Security Promotions (see section 3)
[4] Customer specific Communication tools (see section 3)
[5] Security Briefing for specific groups (CSO request, see section 2)
[6] Mandatory EDS Security Training (see section 2)
[7] Diagonal Slice (see section 3)

For the people working in the Information Security Team, Training is part of the Personal Development Plan. Most of the Training required (maintaining knowledge, keep up to date and (new) knowledge to be gained) for the members of the Information Security Team is predominantly external training/education.

In Den's opinion Information Security Training should be part of the Personal Development Plan of all EDS employees. This would have a positive effect on Security Awareness overall, as employees and managers will be reminded of Security every year.

The CSO is responsible to provide Information Security Training & Awareness (as included in his job description and as part of the service requested (and provided) by the Customer). There is 1 other person in the Information Security Team involved: she produces all the material used for the components mentioned above.

2. When did you decide to implement information security training?

Started about two years ago and has slowly evolved

3. Was there a particular incident or event that initiated this?

No there was no specific event or incident that started this initiative. It was more a growing feeling that something needed to be done to make employees more aware of Information Security. Most of the components were Den's initiative while "doing his job".

For example during Induction Courses people would say that they didn't know how to use applications or if there were specific processes and procedures within EDS and specific for the Customer.

4. Did you receive any budget specifically for this implementation project? Was this budget

a one-off? Or annual returning?
No specific budget for work related to Information Security Training & Awareness, although Den’s time is funded as it is part of his role described in the contract with the Customer. The delivery of the security awareness training (Den’s time only) is a “standard operational element” of the budget, this does not include the venue.
5. How was the reception towards the idea/project of implementing structured Information Security Training and Awareness?
The initiative was generally well-received. Feedback received after Briefings [5] and Presentations [2] is very positive, “eye-opener”.
6. Were there obstructions, problems, aversion against the project?
Other than not having a specific budget, there were no obstructions or negative responses.

Section 2 – Infosec Training Programme

1. How does your training programme look like?
   a. Different courses or presentations?
   b. Per information security topic?
   c. Level of detail?

[1] Induction for EDS employees coming onto account

A 2-day induction course about the Customer and the EDS services and responsibilities towards the Customer. This course is Customer specific.

Information Security input (by CSO) is 30 minutes covering topics such as:

- Physical Security
- Data Classification
- Security organisation and processes
- High-level Risks and Threats (to information and IT)

[2] Security Presentation for groups of EDS employees

A 2-3 hour presentation by the CSO on request by groups/units. The presentation is built around the 10 domains of CISSP and includes a more in-depth look at specific security processes, for example the SSP-process (**S**ystem **S**ecurity **P**olicy, I will explain this in more detail in the actual report)

[5] Security Briefing for specific groups (CSO request)

These briefings are very specific per group on a very specific security topic. The briefings can be on request of groups/units or requested by the CSO.

An example is 2 times a year Den organises briefings for Service Desk employees in Peterlee; a topic that was once covered was the difference between email with malicious content and SPAM.

[6] Mandatory EDS Security Training

All EDS employees have to go through mandatory EDS Security Training. This is not in the responsibility of the CSO. It is initiated within EDS itself and line managers have to make sure their staff completes the training.

A new development/initiative is to become earlier involved in the SSP-process as Security Team (the Security Consultants of Den's team assist Project Managers and their project team to fill in the SSP-document. The plan is that the Information Security Consultant gets involved earlier and over time the Project Managers and members of the project team will become "trained" in the SSP-process and everyone involved becomes more security aware.

2. Target audience groups?

As mentioned before all groups targeted by the Training mentioned in question 1 of this section are EDS employees working for the Customer account.

All EDS employees:
[1], [2] and [6]

Specific groups:
[5]

3. Refresher training? Annual re-confirmation?

Yes, for [5], twice a year for Service Desk employees
Awareness under [3] is an annual event within EDS, but is not mandatory.
For Information Security Team as part of their Personal Development Plan, hopefully for all employees in the future.

Section 3 – Infosec Awareness

1. Do you have an awareness campaign? Regular communications to users, managers,…?

[3] EDS Corporate Security Promotions

Annually the EDS Security & Privacy Officer organises a week of security awareness activities. I will have to explain this a bit more in the report.

[4] Customer specific Communication tools

Within the account (the EDS-side not customer side) there is a monthly Account Bulletin, the CSO gives input to this bulletin in the form of an interview or an article. The input can be general on security or on a specific security topic.

[7] Diagonal Slice

Customer IT Security Director and EDS Client Security Officer make themselves available for approximately and during lunchtime to answer any security questions that employees would like to ask.

2. What type of communications do you use? (Intranet, Info bulletins, Screen Savers,…

Info bulletins are used [4]

On the Intranet (accessible for EDS employees and Customer employees) the following Information Security documents are available:

- All basic Information Security Training materials
- Processes and procedures
- Customer Security Policy

3. Do you provide different messages to different audiences? For example IT-people and non-IT people?
Yes, different messages to different target groups (see descriptions in question 1)
4. Do you use actual security incidents in communications?
Yes, real incidents are used in communications, presentations and briefings. Not as documented in "black-white" but they are given as example during the actual presentation or briefing (verbal only).

Section 4 – Benefits of Infosec Training & Awareness

1. Have you noticed a difference in overall security between BEFORE and AFTER the implemented Information Security Training & Awareness?

It is very difficult to quantify the success of training & awareness.

Especially as there is too small a number of presentations and briefings have taken place to be able to notice the difference. There is also a high turn-over of personnel which limits the success of Training & Awareness.

It also depends very much on the people who have taken part in presentations and briefings. Some people embrace the security processes (for example the SSP-process) and the result is that they become much more security aware. It takes time to notice a change.

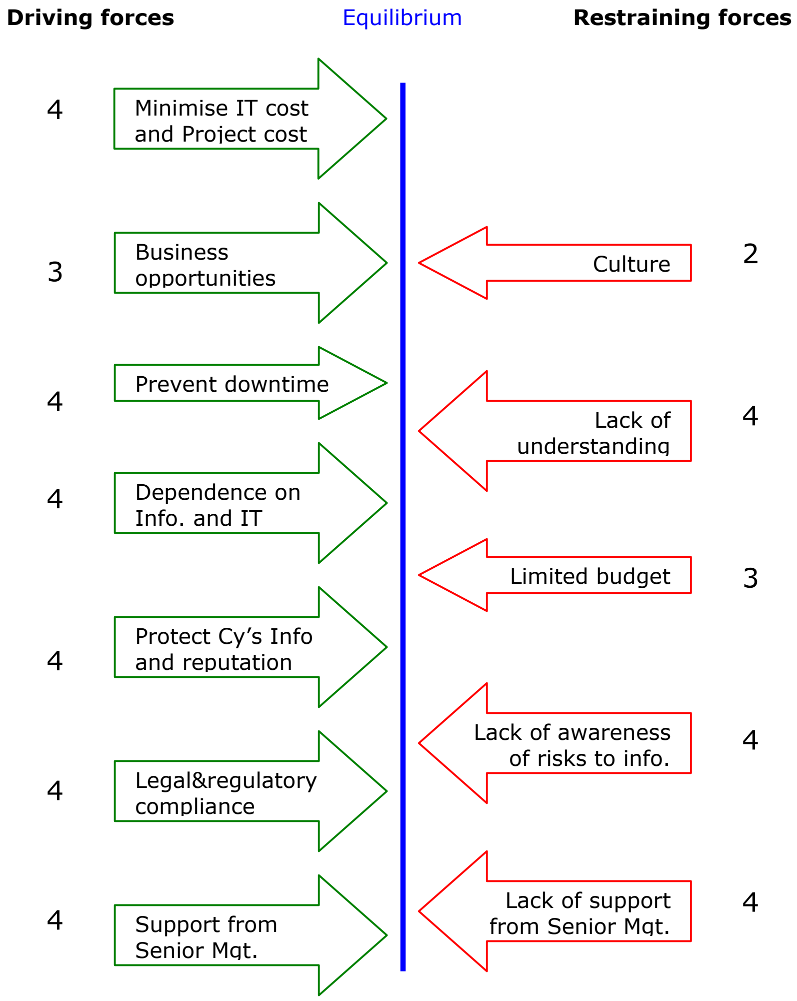
2. What are the benefits of structured Information Security Training?

Although the benefits are not noticeable yet (see question1) the CSO expects the following benefits in the near future.

- Improve project life cycle time: reduce project cost and less re-work of mandatory SSP-process
- Reduction of security incidents
- Maintaining reputation:
  - For EDS: more competent
  - For Customer: less risk of compromise

3. What are the benefits of an increased level of Information Security Awareness?
See question 2
4. Did the implementation of structured Training & Awareness change the attitude/aversion against Information Security?
There was, and there still is, aversion against Information Security, but it is changing. If you (as Security expert) spend time with EDS and Customer employees, explaining the need for Information Security, there will eventually be more understanding for the risk to information and IT and for the consequences of not complying with legal and regulatory requirements. Within the Customer organisation there is a high level of quality culture, the acceptance of security initiatives are seen as an improvement to quality.
5. Did the implementation of structured Training & Awareness impact on the role of the Information Security Unit?
CSO deliver the training as part of his role There is not other impact yet (on the Infosec Team for example) because of the level of maturity of the training.

Section 5 – Force Field Analysis


Driving forces
Equilibrium
Restraining forces
4
Minimise IT cost and Project cost
3
Business opportunities
4
Prevent downtime
4
Dependence on Info. and IT
4
Protect Cy's Info and reputation
4
Legal&regulatory compliance
4
Support from Senior Mgt.
Culture
2
Lack of understanding
4
Limited budget
3
Lack of awareness of risks to info.
4
Lack of support from Senior Mgt.
4

EXAMPLE Force Field diagram for Information Security controls

see DRAFT Chapter 3

1. What do you identify as restraining forces in relation to implementing Information Security controls?

On a scale of 1 (very weak) to 4 (very strong) give a value to each of the restraining forces.

See diagram

(Lack of) Support from Senior Management was split in 2 parts:
As Driving force (Support): the direct line managers (of CSO) recognise that for example Lack of Security awareness can lead to downtime.
As Restraining Force (Lack of support): mainly the Account Management Team, example is Bestshore (which is from a security perspective and looking at the Customer not an option)

2. What do you identify as driving forces in relation to implementing Information Security controls?

On a scale of 1 (very weak) to 4 (very strong) give a value to each of the restraining forces.

See diagram

One new force:
Minimise IT cost and Project cost

(Lack of) Support from Senior Management was split in 2 parts:
As Driving force (Support): the direct line managers (of CSO) recognise that for example Lack of Security awareness can lead to downtime.
As Restraining Force (Lack of support): mainly the Account Management Team, example is Bestshore (which is from a security perspective and looking at the Customer not an option)

3. In what way do you think investing in Information Security Training & Awareness contributes to a change in the identified restraining and driving forces?

The change in strength would mainly be in reducing the Restraining Forces. And possibly Culture could become a driving force in the future.

4. What is (or do you expect to be) the impact your Infosec Training and Awareness

programme on implementing new information security controls?
Currently there is a movement towards implementing more Standard EDS Security Controls. The combination of a higher level of security awareness and the implementation of the standard EDS Security Controls will have impact on: • Reduction in project cost and time (SSP-process involvement in earlier stages refers) • Reduction in operational cost as there are more users on fewer products

Section 6 – Indicators and parameters

1. How do you explain to senior management the importance of Information Security?

As there is high level quality culture within the Customer organisation, managers are more likely to understand and accept the need for information security.

Communication to both EDS and Customer is mainly based on the consequences of not having information security in place; consequences of non-compliance with legal and regulatory information security requirements.

2. Can you identify indicators or parameters for measuring security?

Number of SSPs processed without re-work versus the number of SSPs reviewed repeatedly before passing.

Number and type of questions received by Information Security Team

Number of Security Incidents (analysis of them leads to a number that is related to lack of security training and/or lack of security awareness).

3. Can you identify indicators or parameters for measuring or expressing the impact of infosec training and awareness on information security?
Analysis of incidents (see question 2).
4. Is it possible to have sanitised security incident reports?
Yes, not a problem to have sanitised security incident details. Den requested a reminder closer to the date I would like to have these details.

Additional information:

Dennis Witham is an EDS employee working in the role of Client Security Officer (CSO) for in an EDS customer account, this account is further referred to as the Customer.

The Information Security Unit lead by Den consists currently of 15 people and is likely to grow in the near future. This team is dedicated for the Customer.

One of the responsibilities of Den is Information Security Training & Awareness, his responsibility covers EDS employees working in this specific customer account, he has no Information Security Training & Awareness responsibilities for the employees of the Customer.

Appendix B – Part 2

CASE STUDY – Mike Watkins interview

16th April 2007
(pages 72 – 84)

CASE STUDY – Mike Watkins interview

16th April 2007

Section 1 – Information Security Training & Awareness in your organisation

1. How is Information Security Training and Awareness structured in your organisation?

It is all very early and Security Training and Awareness formally only started 3 months ago.

Currently it is solely based on Computer Based Training (CBT), but the fact that approximately 33% of Customer employees have no IT access, another form of training is also necessary.

The global CBT security module is mandatory for new employees, but not mandatory for existing employees. For this latter group the initiative is pushed through local IT directors to encourage existing employees to complete the CBT Security module.

The intention is to have a refresher CBT module as well, this will than be an annual refresher module that is less time consuming.

There was a strong buy-in from trade unions for this initiative.

2. When did you decide to implement information security training?

First ideas emerged about 2 years ago and 15 months ago the development of the CBT security module started (the chosen product needed to be customised). Formal implemented 3 months ago.

3. Was there a particular incident or event that initiated this?

There was not a specific event that triggered the first ideas, but there was a security incident that gave the final push to get the plan approved. The lessons learned from this security incident (approximately 18 months ago) made it 100% clear there was a need for security training and awareness.

4. Did you receive any budget specifically for this implementation project? Was this budget

a one-off? Or annual returning?

There is a budget for the Security Training and Awareness activities. There was a one-off investment to purchase the CBT package, and now there is an annual budget for support of the tool and maintaining the content of the security module.

5. How was the reception towards the idea/project of implementing structured Information Security Training and Awareness?

The initiative was well-received, although there were a few countries that resisted the idea because of additional time-loss due to training.

Trade unions welcomed the initiative

6. Were there obstructions, problems, aversion against the project?

The content had to satisfy trade unions and legal team (in different countries) which made the development/customisation period longer than initially planned.

Section 2 – Infosec Training Programme

1. How does your training programme look like?
   a. Different courses or presentations?
   b. Per information security topic?
   c. Level of detail?

Computer Based Training Security module, currently an Induction course only. This Security Induction is mandatory for new employees, but not mandatory for existing employees.

There is a slightly different version for 2 groups: one group is Managers and IT personnel (as they have certain responsibilities that employees don't have) and the other group are the Customer employees.

Future developments:
Based on for example outcome of a Security audit, specific topics will be content of modules on the CBT.

2. Target audience groups?
Managers + IT staff (1 group) Customer employees
3. Refresher training? Annual re-confirmation?
Intention to have an annual refresher module.

Section 3 – Infosec Awareness

1. Do you have an awareness campaign? Regular communications to users, managers,…?

Security Awareness is under development, it is very early days.

Currently information is pushed out through the (local) Heads of IT to communicate about IT security.

2. What type of communications do you use? (Intranet, Info bulletins, Screen Savers,…

Again this is very early days, under development.

No screen saver is used.

Intranet is used and pushed through Heads of IT.

3. Do you provide different messages to different audiences? For example IT-people and non-IT people?

Managers + IT staff (1 group)
Customer employees

4. Do you use actual security incidents in communications?

Yes, security incidents are used in a sanitised form.

Section 4 – Benefits of Infosec Training & Awareness

1. Have you noticed a difference in overall security between BEFORE and AFTER the implemented Information Security Training & Awareness?

Too early to say.

2. What are the benefits of structured Information Security Training?

As it is early days I asked Mike if he could give me benefits he expects from Security Training and Awareness.

Standardisation of the message

Workforce do the work they are supposed to be doing (and not misusing IT facilities as they are aware of monitoring, aware of the risks,…)

The Customer will be able to fulfil it “duty-of-care” for their employees

Beneficial for the reputation of the company.

3. What are the benefits of an increased level of Information Security Awareness?

See question 2

4. Did the implementation of structured Training & Awareness change the attitude/aversion against Information Security?

Too early to say.

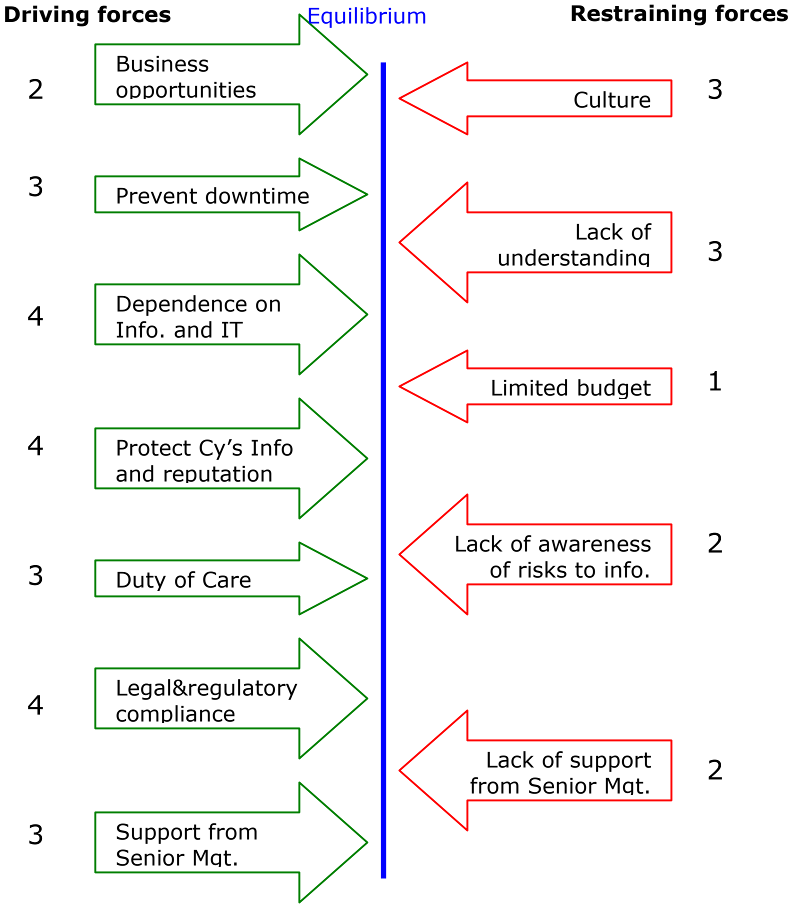
What is already noticeable is that employees are more careful in opening attachments to emails, they quicker report “dodgy” looking emails. This is a positive impact.

5. Did the implementation of structured Training & Awareness impact on the role of the Information Security Unit?

It is very time consuming

Hopefully Mike will see the impact in the audit and monitoring work which is part of is role (see additional information at the bottom of this document).

Section 5 – Force Field Analysis



EXAMPLE Force Field diagram for Information Security controls

1. What do you identify as restraining forces in relation to implementing Information Security controls?

On a scale of 1 (very weak) to 4 (very strong) give a value to each of the restraining forces.

See diagram

(lack of) Support of Senior Management was split into Restraining force "Lack of": from a business perspective Information Security is seen as a limitation to what they can achieve (financially). But there is also support from senior management, so this is also a Driving force.

2. What do you identify as driving forces in relation to implementing Information Security

controls?

On a scale of 1 (very weak) to 4 (very strong) give a value to each of the restraining forces.

See diagram

(lack of) Support of Senior Management was split into Restraining force "Lack of":
from a business perspective Information Security is seen as a limitation to what they can achieve (financially). But there is also support from senior management, so this is also a Driving force.

New Driving Force:
Duty-of-care (from the Business side as from the individual employee)

3. In what way do you think investing in Information Security Training & Awareness contributes to a change in the identified restraining and driving forces?

The way the Security Training & Awareness contributes to these force is the reduction of the Restraining forces.

There is one Driving force that could increase with a more security aware organisation is Prevent Downtime.

4. What is (or do you expect to be) the impact your Infosec Training and Awareness programme on implementing new information security controls?

If Security Training & Awareness is effective it will:

- have a positive impact on project implementation.
- workforce will become more productive

Section 6 – Indicators and parameters

1. How do you explain to senior management the importance of Information Security?

The main drive for communication to senior management is security incidents of high magnitude. The reason behind this is that these incidents focus the Senior manager on the "clean-up" afterwards and the consequences in financial terms (cost of the clean-up) and impact on reputation.

2. Can you identify indicators or parameters for measuring security?

Possibly the results of security audits and how the evolve over time. For example % of compliance or % of non-compliant legal and regulatory (security) requirements.

3. Can you identify indicators or parameters for measuring or expressing the impact of infosec training and awareness on information security?

Number of security incidents classified as "Misuse"

Non-compliances as result of security audit.

4. Is it possible to have sanitised security incident reports?

Yes, not a problem.

Mike requested to be reminded of this closer to the date I need this information.

Additional information

Mike Witham is an employee of the Customer, where the Customer is the organisation that outsourced their IT to EDS. In the Customer's organisation Mike is positioned in the team of the IT Security Director.

Mike's role comprises of:

- performing Security Audits (internally at Customer locations and externally at location of third parties contracted by the Customer)
- Information Security Investigations and Monitoring
- Security Education (of Customer employees)

Appendix B – Part 3

CASE STUDY – Geoff Stone & Stuart Martin interview

26th April 2007

(pages 86 – 98)

CASE STUDY – Geoff Stone & Stuart Martin interview

26th April 2007

Section 1 – Information Security Training & Awareness in your organisation

1. How is Information Security Training and Awareness structured in your organisation?

The Infosec training provided is for EDS employees in this specific Customer account. Currently negotiations are taking place to also provide Infosec training to the Customer's employees.

The Customer has training directives that prescribes security training for all employees. EDS is contractually obliged to comply with this requirement and provides Information Security Training to all EDS employees and all (EDS) contractors working within this account.

The Infosec training comprises of an Induction on the first day of joining the account followed by an annual returning presentation of an hour. This presentation has a different content with the passing years of employment. The sequence repeats after 5 years. See for content section 2 question 1.

The Infosec Training is organised per EDS site for this Customer. And the local Site Security Coordinator provides the presentations. Some presentations require 2 instructors (role play) and Geoff and/or Stuart will provide these.

Groups are between 15 and 20 people, or less.

Problem with this Infosec Training structure is that it gets "disturbed" by EDS Central Training, who also organise Security training. For EDS employees working in this Customer account this is a burden, as the topics are covered in the Customer specific Infosec Training.
As EDS (for this specific Customer) is contractually obliged to provide infosec training for their EDS employees, these employees are doing 2 sets of security training which is a waste of resource.

Also all EDS employees and EDS contractors have to confirm every year that they have read and understood the Information Security Policy and Procedures (see section 2).

2. When did you decide to implement information security training?

1998 at the start of the contract with this Customer.

3. Was there a particular incident or event that initiated this?

No, contractual obligation.

4. Did you receive any budget specifically for this implementation project? Was this budget

a one-off? Or annual returning?
Providing Information Security Training is incorporated in the Security function for the Customer account. If the Customer employees are also being training by the EDS Security Team, this will be a change to the contract and the budget will reflect this change.
5. How was the reception towards the idea/project of implementing structured Information Security Training and Awareness?
The requirement was there (Customer Training Directives).
6. Were there obstructions, problems, aversion against the project?
Some managers are more reluctant than other to release their personnel for training. Some EDS employees try not to come to Security training with the excuse that they have been working in "security minded" environments, such as military or public services, or have been working (as employee) for the Customer.

Section 2 – Infosec Training Programme

1. How does your training programme look like?
    a. Different courses or presentations?
    b. Per information security topic?
    c. Level of detail?

There are 2 training sessions that every EDS employee (and EDS contractor) receive only once, these are:

- General Induction:
  On day 1 of employment for this specific EDS – Customer account every employees undergoes an induction. Part of this induction is a 10 minute briefing about Security. This briefing includes only information that new employees need to know before they can start working within this Customer account. During this session everyone receives a leaflet with the information they have to know.
- Information Security Induction:
  The first specific Information Security Training session. This presentation is for new comers only, has a duration of 1 hour and cover the topics:
    - Organisation of Information Security
    - Threats to the organisation (what and who)
    - Countermeasures (Personnel, Physical, Procedural and Technical (IT))
    - Responsibilities

As mentioned in the previous section a number of presentations are given in sequence, every EDS employee (or EDS contractor) attends 1 presentation per year. After the Year 4 session the cycle repeats from Year 2. All the presentations in this cycle build on the Information Security Induction presentations and evolve with time (changing threats, new topics). Key point of all the sessions is interaction.
The following presentations currently exist:

- Year 2:
  A role-play session (2 instructors) based on the topics of the Infosec Induction. The group attending the presentation is split in 2 and each group has to list the events that are "wrong". In other words the groups have to recognise the security incidents that occur in the role-play.
- Year 3:
  A roulette game "don't gamble security". The groups attending the presentation is spilt in 2 (Black and Red) and are given play-money. The wheel is turned and the team with the colour that comes up has to answer a question. Wrong answer means the Team looses he money of the bet. The questions cover all areas of security.
- Year 4:
  This session mainly involves the threat posed by mail, especially chemical attacks and explosives (mail bombs). During the session it is explained how to recognise this kind of mail, what are the symptoms. After a short presentation, the mail bag appears on scene and every attendee is given a "package" to assess. The last package in the mail bag contains powder, this package is followed through the whole procedure to demonstrate activities to counter the Chemical/Biological threat. The group is actually taken to the isolation room (especially for this type of incidents) and shown what to do and how to use available equipment.

2. Target audience groups?

EDS employees working in this Customer account and contractors (hired by EDS for this account).

3. Refresher training? Annual re-confirmation?

Yes, the cycle starts again after Year 4.

The recording of who has done which training has to be done better. Of the 4 sites, only 1 administers all the Infosec training appropriately.

There is an annual re-confirmation of compliance to Information Security Policy and Procedures. These Policy and Procedures are published at the Intranet and reviewed annually. After this review all users (in the form of their user account) are pointed/redirected to the Intranet where they have to open all the relevant documents. If they don’t open the documents they can’t continue their work as they will be logged out of the network.

Section 3 – Infosec Awareness

1. Do you have an awareness campaign? Regular communications to users, managers,…?

There is some form of awareness activity, but not structured in a Plan or formal structure.
On an ad-hoc basis the following awareness activities take place:

- posters are used to make people aware of specific threats
- security articles are published on the Customer Info Centre (a Customer specific Intranet site)
- in the situation of increased spam activity or phishing attacks, emails are send to all email accounts to warn users and give advice on actions to take

2. What type of communications do you use? (Intranet, Info bulletins, Screen Savers,…

- Notices, posters (not frequently nor regularly)
- Intranet, Customer Info Centre (mail form of communication for awareness)

3. Do you provide different messages to different audiences? For example IT-people and non-IT people?
Messages are the same for everyone, in broadcast form.
4. Do you use actual security incidents in communications?
Yes, real incidents are used in a sanitised (de-personalised) form.

Section 4 – Benefits of Infosec Training & Awareness

1. Have you noticed a difference in overall security between BEFORE and AFTER the implemented Information Security Training & Awareness?

Although the Customer organisation is a security aware environment there is a significant difference between EDS employees and Customer employees in for example breaches of security policy/procedure on email. Content inspections reveal that only 10 breaches out of 250 involve EDS employees. Infosec Training & Awareness given to EDS employees (and NOT to Customer employees) was given as a possible reason behind this difference.

Another change in EDS employees is that people are much more interested in Information Security, there is a much more positive attitude towards security. The fact that the training sessions are interactive, gets people much more involved and the stigma of "security is boring" disappears.

2. What are the benefits of structured Information Security Training?

- The Security Team spends less time on incident investigations.
- Less time wasting (by EDS employees) on "things they should not do".
- Number of incidents involving EDS employees is going down

Geoff and Stuart feel that the EDS reputation can only be enhanced by statistically lower incident rate amongst EDS trained staff.

The lower rate of security incidents means the Security team does not divert effort from chargeable time to investigative work.

A major incident is a real threat to Service Level Agreements.

3. What are the benefits of an increased level of Information Security Awareness?

See Q2

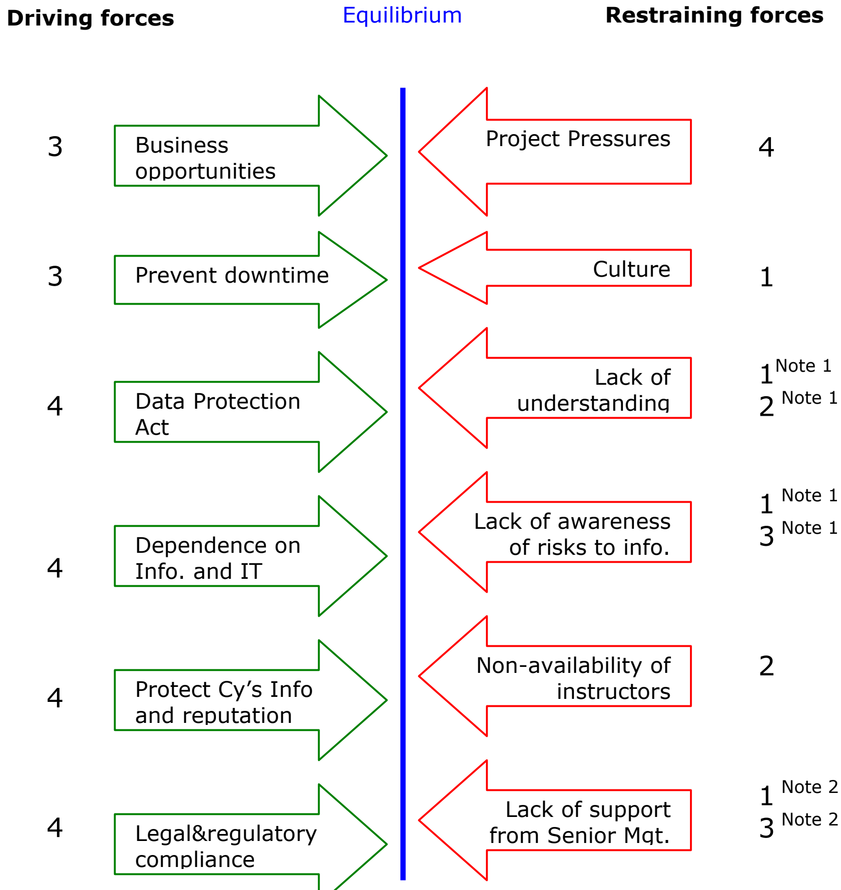
4. Did the implementation of structured Training & Awareness change the attitude/aversion against Information Security?

Yes, especially from the moment that the training sessions became interactive, the attitude towards Information Security is more positive. People realise that thy can contribute towards a more secure work environment.

5. Did the implementation of structured Training & Awareness impact on the role of the Information Security Unit?

- Less investigations of security incidents
- Some members of the security team suddenly had to become "instructors"
- More often contacted as the EDS employees now know who the Security team is and what they do
- When members of the security team are walking over corridors they are being asked questions about security and possible security incidents

Section 5 – Force Field Analysis



Force Field diagram for Information Security controls

1. What do you identify as restraining forces in relation to implementing Information Security controls?

On a scale of 1 (very weak) to 4 (very strong) give a value to each of the restraining forces.
Values given as in diagram.
Two restraining forces added:

- Project Pressures
  It happens, mainly in "top-level" projects, that the pressure on project managers to progress and deliver the project objectives is increased. This means that the Security Team is often overruled and project mangers accept project security risks they should not.
  The consequences of these decisions are not immediately clear and may cost a lot of (security) resources and additional budget to "clear-up" after implementation.
  This pressure also leads to people making mistakes that could have security consequences.
- Non-availability of instructors
  When there is a lot of Project Pressure this often leads to members of the Security Team, who act as instructor for Information Security Training, are not available for scheduled training sessions.

Note 1: The low value of the restraining force is related to those EDS employees who have received a number of the sessions described in Section 2 (Q1). The higher value is for new-comers.

Note 2: When discussed in concept senior managers do support Infosec initiatives (value = 1), but when they realise what the consequences are (in reality) the value of this force becomes 3.

2. What do you identify as driving forces in relation to implementing Information Security

controls?

On a scale of 1 (very weak) to 4 (very strong) give a value to each of the restraining forces.

One new Driving force added:
Due to the type of organisation and the function of some of the Customer's employees, the Data Protection Act is a very strong Driving force (value 4). Therefore this force is mentioned separately from the Driving force "Legal and Regulatory Requirements".

3. In what way do you think investing in Information Security Training & Awareness contributes to a change in the identified restraining and driving forces?

Looking at the diagram it is apparent that the Driving forces are stronger than the Restraining forces. This could be explained by the Information Security Training that has been taking place since 1998.

For the Restraining forces "Lack of understanding" and "Lack of awareness of risks to Information" the values given are different for new-comers and employees who have received Security training sessions.

The investment of time and effort in Information Security Training has already paid off.

4. What is (or do you expect to be) the impact your Infosec Training and Awareness programme on implementing new information security controls?

It is more likely that people accept that information security controls are put in place when they have had the Security Training.

There is more understanding of the role, the need and activities of the Security Team.
For example in relation to Content monitoring activities, Customer employees (not being security trained by the Security Team) complain about this activity, while EDS employees (who have received this security training) don’t complain about this.

Section 6 – Indicators and parameters

1. How do you explain to senior management the importance of Information Security?

- The Security Team explain to senior managers that they personally can be hold-up in court and go to prison if not compliant with Legal and Regulatory requirements.
- Senior management are informed of incidents and identified weaknesses (which have not been exploited yet).

2. Can you identify indicators or parameters for measuring security?

Number of incidents would be a good indicator. Not in isolation but in combination with "known attempts" to hack into network and the incoming mail in quarantine.
Currently the security incidents are not analysed.

Number of breaches of security policy and procedures that are picked up during monitoring activities and content inspections.

In the near future the Security Team will start security audits and the outcome will be documented in reports. The number of non-compliances could be an indicator to measure security.

3. Can you identify indicators or parameters for measuring or expressing the impact of infosec training and awareness on information security?

The type of questions EDS employees ask and the level of detail in conversations with the Security Team clearly indicates of people have had security training or not. The problem is that only calls that come through the Helpdesk are logged. All other calls, conversations in corridors or meetings are not logged. This means that there is no record of this discrepancy, it is purely an observation of the Security Team.

4. Is it possible to have sanitised security incident reports?

None available, due to the lack of security incidents for which the Security Team are responsible.

Appendix C – Questionnaire

CASE STUDY
Questionnaire EDS Client Security Officers – Results
Excel Spreadsheet - July 2007
(pages 100 – 102)

Question **Answers** **Comments**

Is there an Information Security Training and/or Awareness program?			
	Yes	***No***	
number	6	1	# 1 of yes answers is awareness only # no answer is for EDS employees of the account, client employees have a minimal awareness program

What percentage of the Security Incidents are related to users?			
>75%	3		# "majority" and "most" are considered as more than 75%
40-75%	2		# one of these is for incidents related to client-users
20-49%	-		
<20%	2		# one of these is EDS-users
no data	1		
Would Information Security Training & Awareness reduce this percentage?			
	Yes	***No data***	
number	2	5	# one Client Security Officer mentioned that the security policies are not in a "user-digestable" form (this was a Yes answer)

Question 3: Force Field Model	Number
Driving forces	
Prevention of embarrassment to Client	1
Legal & regulatory compliance	7
Company policies	2
Senior Management commitment	1
Distributed (all parts of the business) security organisation	2
Respect and trust in security personnel	1
Security governance encouraging risk-based approach	1
Reducing commercial risk to EDS	1
Change and Project Management (involved from start)	3
Service interruptions (down-time)	1
Audits	2
Security minded culture (in Client organisation)	1

Restraining forces	
Drive to adopt COTS-products	1
Lack of understanding (users and management)	2
Lack of support from IT, not seeing security as part of design and implementation	2
Lack of clear security organisation structure or security responsibilities	2
Lack of Senior Management commitment	2
No respect or trust in security personnel	1
Management risk appetite	2
Finance/budget	1
Unreasonable business drivers	1
Culture	1
What was (1960s) good enough, is still good enough	1

Question 4	Number
Indicators to measure Security of an organisation	
Days of exposure to vulnerabilities for which a patch is published	3
Compliance management using a scanning tool	1
Signed off and tested (build) standards and baselines	1
Audit trails of information systems	2
Incidents	1
Independent review	2
Number of interaction initiated by workforce with the security unit	1
Number of instances of malicious code detection	1
Number of external access attempts	1
System evaluation	1
Production of information bulletin publishing information about (actual and/or potential) security incidents	1
Assessment by Client Security Officer	1

Question 5	Number
Indicators to measure impact of Information Security Training & Awareness	
Statistics of Helpdesk calls related to security	1
Number of incidents (and possinble changes in them)	3
Audit findings	1
Number/frequency of wareness updates (Intranet, FAQs,…)	1
Sampling (and mesuring) business user knowledge	2
Sign Compliance to Security policy as part of terms of employment	1
Number of "hits" on security policies & procedures (intranet and verbal)	2
Number of security improvement suggestions	1
Number of (devlopment) projects with a risk analysis	1
Number of non-compliancies (secure nature) between documented business requirements and actual implemented projects	1