A new tool for Information Security Professionals: the Information Security Force Field Model

This thesis offers a detailed plan for how to get users onboard with information security.

BY MONIQUE HOGERVORST

Royal Holloway
University of London

A NEW TOOL FOR INFORMATION SECURITY PROFESSIONALS: THE INFORMATION SECURITY FORCE FIELD MODEL.

Changing the attitude of employees and senior management towards information security can solve many of the problems information security professionals face every day. If you want buy-in from senior management in your Information Security Programme in general, and Information Security 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 Information Security Force Field model is a useful new tool for Information Security professionals that helps to:

- visualise the link between business processes on one hand and information security and information security training and awareness on the other; and
- measure security and quantify the impact of information security training and awareness.

Monique Hogervorst

Senior Information Security Consultant
APACS (Administration) Limited
monique.hogervorst@apacs.org.uk

Keith M. Martin

Information Security Group
Royal Holloway, University of London
keith.martin@rhul.ac.uk

This article was prepared by students and staff involved with the award-winning M.Sc. in Information Security offered by the Information Security Group at Royal Holloway, University of London. The student was judged to have produced an outstanding M.Sc. thesis on a business-related topic. The full thesis is available as a technical report on the Royal Holloway website http://www.ma.rhul.ac.uk/tech.

For more information about the Information Security Group at Royal Holloway or on the M.Sc. in Information Security, please visit http://www.isg.rhul.ac.uk.

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

OVERVIEW

We all know that information security is likely to be better in organisations where both the employees and the management are:

- aware of information security issues;
- appreciate the potential impacts of information security incidents; and
- understand the need for information security controls.

We all know that the best (perhaps the only) way of providing such organisational education is via a programme that provides some level of Information Security Training and Awareness (ISTA). Anyone who has worked on the "security side" of an organisation will know very well that this is far from the case: ISTA programmes often suffer from several problems! First and foremost, it is often hard for senior management to see a direct return of investment. To a lesser extent, this attitude can also prevail amongst the employees who will be receiving the training. Secondly, it is often far from clear precisely what an ISTA programme should prioritise and where it should most effectively be deployed.

To this end, we propose a new tool for helping organisations to identify both the benefits of an ISTA programme and where best to target its energies. The approach does not employ radically new ideas. Its strength is its simplicity and its ability to help senior management visualise the problem, and clearly see the merits of the pursuit of relevant ISTA. The tool has only partially been road tested, but its ease of use is compelling. It is a very flexible model and adaptable to local conditions.

Perhaps this is just the tool you have been waiting for to help you to obtain buy-in from senior management in your Information Security Programme in general, and ISTA in particular.

THE NEED FOR ISTA

Information security standards, best practices and literature all identify the need for ISTA. The theory is clear. Surveys[1] carried out in 2006 show that in the real world the situation is different: the focus of businesses is still on technical information security controls aimed at an external attacker, while the insider attacker remains a serious threat that is often relatively poorly defended against. A natural defence against insider (and external) attackers is ISTA and yet it seems that ISTA is not always recognised as a major contributor to security of an organisation. As a result, senior management is often reluctant to invest time and money in appropriate ISTA. This situation needs changing, which means changing both the behaviour and attitude of the decision makers in organisations.

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 reputa-

A natural defence against insider (and external) attackers is ISTA and yet it seems that ISTA is not always recognised as a major contributor to security of an organisation.

[1] Surveys studied during the research phase of this project were carried out in 2006 by Deloitte (Global Security Survey for the Global Financial Services Industry) and Price Waterhouse Coopers (DTI Information Security Breaches Survey).

tion 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 that IT developments bring with them. Senior management needs to embrace information security in order to sufficiently protect one of their most critical and valuable assets: information.

Changing the attitude of employees and senior management can help to solve many of the problems information security professionals face every day. 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 in order to secure their information. If you want buy-in from senior management in your Information Security Programme in general, and ISTA in particular, you need to be able to prove the additional value information security brings to the business.

JUSTIFYING THE NEED FOR ISTA

Unfortunately for information security professionals there is no straightforward solution to the problem of providing a strong measurable case for an Information Security Program. Most published methodologies for measuring information security do not appropriately incorporate business processes and business managers into the techniques used for measuring information security.

ISTA is all about giving people the information security knowledge and awareness that they need for their day-to-day jobs. This has little to do with technical controls and everything to do with human resource security and psychology. It is this observation that provides a vital clue as to where to look for help in addressing this significant problem.

Changing behaviour and attitude is probably the most challenging task in organisations. The field of psychology has identified a number of models to achieve behavioural change. Having reviewed these extensively, one model of significant appeal is Kurt Lewin's model of the Force Fields. In this model two sets of forces work against one another: restraining forces and driving forces. Changing the strength of one of the contributing forces can result in changes to the situation being modelled. This simple

Senior management needs to embrace information security in order to sufficiently protect one of their most critical and valuable assets: information.

concept is very appealing and so the Force Field model (as presented by Steve Wells in a Mini-Tutorial[2]) was chosen in this project for adaptation to an information security setting in order to create a tool to assist information security professionals in their communication with business managers and the development of effective ISTA programmes. The result is the Information Security Force Field Model (ISFFM), which we explain in this article[3].

THE INFORMATION SECURITY FORCE FIELD MODEL (ISFFM)

Conceptually, the idea of ISFFM is to identify the important driving (enabling) forces and restraining (disabling) forces behind information security in an organisation. These forces then require some degree of quantification.

The results of the process can then be used to show in which way information security is linked with business processes and identify where ISTA can be deployed in order to achieve a more favourable balance in the ISFFM between driving forces and restraining forces. The beauty is that each resulting ISFFM can be depicted by means of a diagram. This diagram visualises the business case for information security and ISTA.

The ISFFM is a useful tool for providing evidence that ISTA is a cost-effective countermeasure because it can be used to graphically indicate that:

- on the one hand it increases the overall level of security of an organisation, as users become more aware of the risks;
- on the other hand it decreases the restraining forces, thus making the driving forces more effective.

The ISFFM can also be used by information security professionals to:

- communicate effectively to line and senior managers about the link between business processes and information security;
- explain how ISTA 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 previously used metrics;

Changing the strength of one of the contributing forces can result in changes to the situation being modelled.

[2] Stephen Wells; Force Field Analysis – Mini Tutorial Quality Management (attached to project report as appendix A; 15-03-2006).

[3] The full MSc Project report provides more details on how the Information Security Force Field model was developed.

- quantify the impact of ISTA.

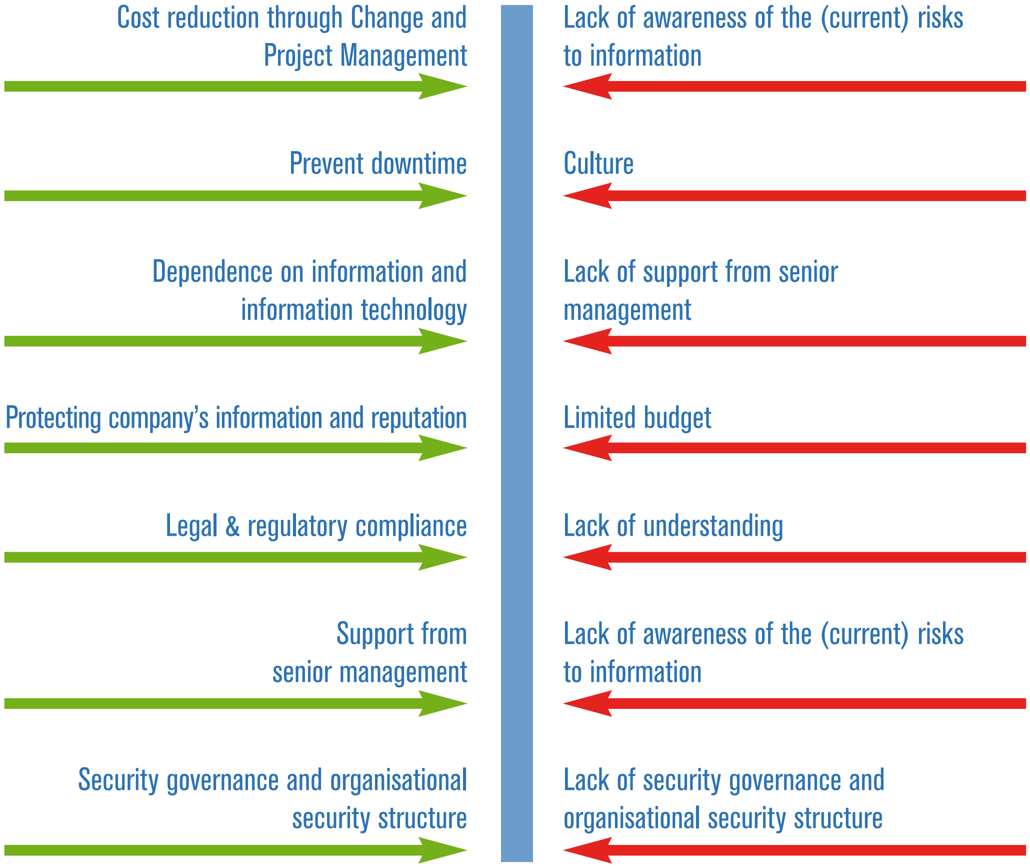
The devil is of course in the detail, which in this case is in the development of the model itself. We must identify the right forces and the right metrics by which to assess them. When using the ISFFM in an organisation, the information security professional must ensure that the model has its roots in the business processes. The analysis of the forces and the assessments of these forces should indicate in business terms how the level of security has changed over time and how security contributes to the business objectives.

The list of forces employed in the model should be configured by a particular organisation and selected forces will clearly differ between organisations.

The sample ISFFM depicted in Figure 1 (which shows only a list of forces and not the measures used to assess them) covers all areas of information security: technical, physical, procedural and personnel security. A large number of the forces in Figure 1 are closely related to people, the majority of which are restraining forces. This is where the implementation of structured ISTA could make a difference: decreasing the strength of the restraining forces and therefore making the driving forces more effective and efficient.

The following list contains examples of

Figure 1: Information Security Force Field diagram


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

potential driving forces that could be included in an ISFFM:

- *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 an established Information Security Management System can result in potential customers and partners having confidence in your organisation.

- *Prevention of downtime.*

- *Dependence on information and Information Technology.*

- *Protection of an organisation's information and reputation.*

- *Legal & Regulatory compliance.*
- *Support from senior management.*

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. (This is also, however, identified as a potential restraining force).

- *Duty of care.*

Both from organisation to employees and vice versa.

- *Data Protection.*

Depending on the type of organisation and the function of some of the employees, the Data Protection Act can be a very strong driving force; therefore this force needs to be treated separately (from Legal & Regulatory compliance) for some organisations.

- *Security governance and organisational security structure.*

This force includes a number of drivers that may need to be defined 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.*

Some organisations are part of an industry that embraces information security naturally; an example is the defence industry.

The following examples of restraining forces could be included in an ISFFM:

- *Culture*

In contrast to a security minded culture (identified as a driving force) culture can also be against information security. Often heard remarks include “I have been doing this job for 20 years in this way, why do I now need to do it differently?” or “why are limitations (by introducing information security controls) being enforced on me?” What some people do not realise is that the introduction of IT and the Internet have changed the risks to information.

- *Lack of understanding.*

Mainly the understanding of the need to protect information.

- *Budget limitations.*
- *Lack of awareness of the (current) risks to information.*

- *Lack of support from senior management.*

As a restraining force, this is mainly a financial matter. Managers in, for example, the Account Management Team may see information security as costly and a constraint on the business achieving its financial goals.

- *Non-availability of instructors.*

- *Drive to adopt Commercial off the Shelf (COTS) products.*

COTS products can save an IT department a lot of money. However their use can also result in an insecure IT solution because the COTS product does not have the precise security features that an organisation needs. This often leads to the need for additional investment in order to establish the right information security controls.

- *Lack of support from the IT department.*

- *Project pressures.*

This mainly relates to high-level projects with a high visibility to senior managers and external parties. Project managers are often put under pressure to progress projects leading to the acceptance of (information security) risks that are not properly assessed. Later, controls need to be put in place or the security team is required to "clean 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 that could otherwise be described by phrases such as "lack of clear security structure or security responsibilities", "no respect or trust in security personnel" or "management risk appetite".

DEVELOPMENT OF AN ISFFM

An ISFFM shows how ISTA can contribute to the security of an organisation. By making the forces measurable, it provides a tool to measure the impact of ISTA. So how do we go about building an ISFFM?

From the first step it is necessary to involve business managers from a wide variety of disciplines within the organisation. There is no standard list of indicators that can be introduced and used in every organisation. These are specific to each organisation and should be allied to 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".

The development of an ISFFM involves a number of steps, which we now outline.

Step 0: Preparatory work

The information security manager and team need to explore the objectives of the exercise and develop an initial ISFFM that is used as the starting point for discussions. It is easier to discuss and develop an organisation specific ISFFM diagram if there is something visible to initiate the discussion. This Initial ISFFM diagram could, for example, be a localised version of Figure 1 with some connections to business processes.

The next task to be performed before starting the development is to define a scale of values to use to measure the strengths of the forces that are defined in steps 3 and 4 of the development process. Initial values of strength will be given at step 5. 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

From the first step it is necessary to involve business managers from a wide variety of disciplines within the organisation.

necessary to have a number of versions of the ISFFM, each relating to a specific business process or a specific information asset.

Step 1: Identify the connections between business processes and security Introduce the (different versions of the) initial ISFFM.

The information security manager facilitates discussions 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 needs to be addressed with the results of step 1 in mind.

Step 3: Determine the driving forces

The list of driving forces are now determined, including any new driving forces that were identified during discussions with the business managers. At this stage it is important to try to define the forces in such a way that they can be valued both now and in the future. (to allow long term comparison and analysis of changes over time).

Step 4: Determine the restraining forces

Use the same approach as in step 3 to determine the list of restraining forces.

Step 5: Assign initial impact values to the forces

During Step 0 the information security team should have designed a scale of values (for example 1 = very weak, 2 = weak, 3 = strong, 4 = very strong). If risk management is established in the 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 recognisable to business managers. In Step 5 the strength of the identified forces will be given an initial value. This is a “first impression” of the impact of each force on the business processes it is linked to. Later, in steps 7 and 8, the values will undergo a more detailed analysis.

Step 6: Chart the forces in a new diagram

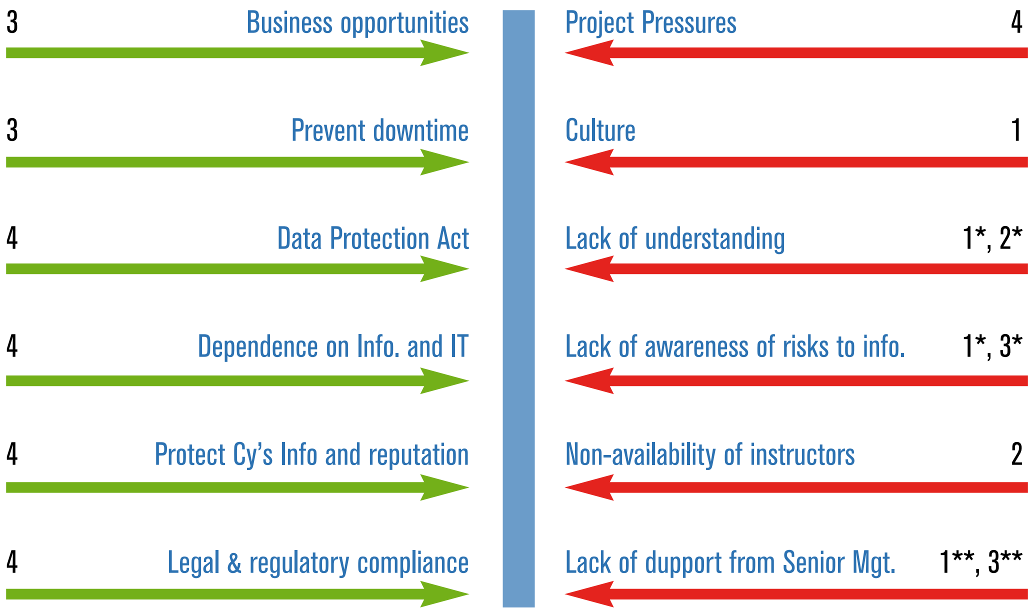
The connection between security and the business, based on the contributions from a multi-disciplinary group involved in this development, are now visualised. The resulting diagram of the ISFFM will provide a compact overview of where and how ISTA can impact on the forces identified. The result is the organisation specific ISFFM diagram that was mentioned in Step 0. Figure 2 provides an example that resulted from a case study.

Step 7: Analyse forces and possible metrics contributing to the strength

The forces identified in the ISFFM have an initial impact value given in Step 5. The next step is to identify the contributing factors that determine the strength of a force. Each force thus needs to be analysed, and the indicators and parameters that contribute to the strength of the force need to be documented. This is necessary for the development of a measuring method that can be used repeatedly without changing the baseline.

Step 7 is very important as it forms the basis of all future measurements related to ISTA. In order 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 reasonably objective way. The output of this step is a set of values that may well differ from those used in Step 5 to assign an initial impact value (but they could also be the same). The result is a set of impact values that are based on indica-

Figure 2: Organisation specific ISFFM diagram


3
Business opportunities
Project Pressures
4
3
Prevent downtime
Culture
1
4
Data Protection Act
Lack of understanding
1*, 2*
4
Dependence on Info. and IT
Lack of awareness of risks to info.
1*, 3*
4
Protect Cy's Info and reputation
Non-availability of instructors
2
4
Legal & regulatory compliance
Lack of dupport from Senior Mgt.
1**, 3**

* **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.

tors and parameters that can be measured in practice.

Step 8: Carry out a baseline assessment

Using the strength values identified in Step 7, each force is re-assessed and a new value is assigned. This new value will be underpinned by measurable indicators and parameters, as a result of Step 7. The reasoning and assessment process needs to be documented and the first version of this assessment functions as a baseline for future measurements.

The difference between the total strength of driving and restraining forces can be used as an indicator of 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 effort should be directed to improving the security of the organisation.

Analysis of the forces can indicate precisely where improvements can be made and 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. This analysis will indicate the impact of training and awareness. Further, a repeated assessment of the strength of certain forces makes it possible to put precise figures to the benefits (for example cost reduction or a positive return of investment) of structured ISTA.

PARTIAL TESTING OF THE ISFFM

At this stage the ISFFM has not been fully tested in the real world. Although there is clearly a potential for this model to become a widely used tool, it needs further development and more guidelines for its use.

Part of this project included a case study, full details of which appear in the full report. During this case study the ISFFM was tested within an organisation. Figure 2 shows an example of an organisation specific ISFFM diagram that resulted from this exercise. All the interviewees involved in the case study commented that the ISFFM, and the process required to establish it, has the potential to become a helpful tool for information security professionals like themselves[4]. More specifically, the fact that the ISFFM diagram visualises where ISTA can be effective was mentioned as one of the main benefits of the model.

The interviews that were carried out as part of the case study included questions about the impact ISTA has made (or could make) on organisations. The outcome strongly indicated that ISTA has a positive impact on the overall security of an organisation. This impact can take the form of a reduction in information security incidents (and the time information security professionals invest in investigating these), savings in project turnaround times and project costs, and increasing (timely) involvement in business projects. More examples of identified benefits of ISTA are listed in Chapter 7 of the full report.✷

Ron Condon

UK bureau chief
searchsecurity.co.UK

Ron Condon has been writing about developments in the IT industry for more than 30 years. In that time, he has charted the evolution from big mainframes, to minicomputers and PCs in the 1980s, and the rise of the Internet over the last decade or so. In recent years he has specialized in information security. He has edited daily, weekly and monthly publications, and has written for national and regional newspapers, in Europe and the U.S.

[4] All interviewees were Information Security Professionals or managers with a strong security responsibility as part of their jobs.