# Corporate Information Security

## No half measures

*Edo Roos Lindgreen, Frank Rizzo, Allen Zuk and Francis Beaudoin*

**Information security has developed from a specialist issue into a fixed item on the management agenda. Due to the growing integration of information technology in operating processes, security is now increasingly embedded in the tasks and responsibilities of existing organisations. This article explains how organisations can adopt a structural approach to information security, from assessment and policy formulation to planning and implementation. Three case studies highlight specific aspects of information security.**

### Introduction

Information security is no longer just a specialist domain. Information systems have become a prerequisite for the marketing of products and services. Outside the information industry, numerous employees use information technology. This affects the way in which the security issue must be addressed. Once a specialist area, information security has grown into an everyday responsibility for managers and employees. This responsibility can in general be summarised in two words: caution and concern.

These two do not suffice, however. Rapid changes in ICT and its application require a proactive approach and a continual reassessment of measures and potential threats. Additionally, information systems are increasingly interconnected. A situation is thus created in which the security of one system is dependent on the security of many others. Finally, most organisations are a constant subject to change. These changes can range from normal staff turnover (very common in the current ICT labour market) to drastic processes including reorganisations, mergers and acquisitions. Organisational changes often have a considerable impact on the way in which information security is set up within an organisation. This means that information security is an ongoing process that involves the management of change itself. This article describes how this process can be structurally set up. The content of the article is organised as follows.

First of all, the relationship between information security and integral risk management is addressed. Attention is also paid to the process aspect of security measures. This is followed by a discussion of the relationship between customised and standard information security systems.

Secondly, attention is given to one of the most important instruments in the security process: the *information security policy*. In drawing up such a policy, the senior management of an organisation sets out the course that security measures will follow in the coming years. Establishing and complying with a security policy is a must for every organisation that takes the security issue seriously. This article pays attention to the objectives, form, content and realisation of the information security policy. This includes an examination of the differences between small and large organisations and between the business community and government. Special attention is paid to potential pitfalls that may be encountered during the formulation and implementation of the information security policy.

The formulation of an information security policy is an important first step in establishing a durable system of security measures. However, for an information security policy to be effective, it must not just exist on paper. Paper may be a willing ally, but, as a Dutch proverb indicates, paper tigers don't bite. Unfortunately, many policy documents are destined to spend their days in the proverbial desk drawer or end up filed in the rubbish bin.

The next step therefore concerns the conversion of policy into an active *security organisation*. We address this subject and discuss the tasks, responsibilities and the authority of managers and staff; the role of security managers; the control of the organisation by management and the accountability of the organisation to management; and the formulation of security measures concerning contacts with third parties.

Finally, we will deal with ways to establish a permanent system of security measures. Attention is also given to a structural approach that combines both these angles: KPMG Information Risk Management's Corporate Information Security programme.

The article includes three case studies addressing various aspects of information security, such as an information security assessment, penetration testing and enterprise security architectures.

### Information security is ...

#### Don't break, bend

Every organisation has its own unique strategic objectives. However, what virtually all organisations have in common is the desire to deal responsibly with the risks involved in achieving these objectives. The objective of risk management is to reduce these risks to an acceptable level, at least so that the survival of the organisation is not unnecessarily compromised. The continuity of an organisation's operations is of prime importance for every organisation. In most cases, the complete elimination of risks is not possible, nor is it desirable. After all, taking risks is an inherent part of doing business.

| Resources | Total Enterprise Risk Management | | | |
|---|---|---|---|---|
| | Personnel | Assets | Finance | Information |
| Risk/risk area | * Illness<br>* Turnover<br>* Decreased motivation<br>* Knowledge drain<br>... | * Fire<br>* Burglary<br>* Theft<br>* Disasters<br>... | * Currency risks<br>* Interest risks<br>* Payments due<br>* Cash flow risks<br>... | * Eavesdropping<br>* Illegal modification<br>* Interruptions<br>* Masquerading<br>... |
| Measures | * Human resource management<br>... | * Security<br>* Alarms<br>* Insurance<br>... | * Treasury<br>* Insurance<br>... | * Information security<br>* ICT audit<br>... |

*Table 1. Information security as part of integral risk management.*

Risk management is carried out in many different areas within an organisation. Measures to manage risk can be classified in widely varying ways, for instance on the basis of the production resources used by an organisation to achieve its strategic objectives: People, Matter, Money and ... Information. The adoption of satisfactory measures for each of these production resources is an absolute necessity. In this context, information security constitutes a regular part of risk management in a general sense (see table 1).

### No half measures

Information security comprises a broad area of specialisation that contains a wide range of measures. Some of these measures are as old as time; for example, having personnel sign a statement of confidentiality. Other measures are more directly linked to technological developments, such as the installation of a firewall to regulate Internet access. A person could spend years classifying security measures. As research into the available literature shows, there are countless ways of doing this.

It is more important, however, that each security measure be drawn up according to the well-known management cycle. Control and corrective adjustments are necessary to prevent measures from losing their effectiveness. It is also true for information security that stagnation means decline: advancement is imperative. The term 'security measure' can be somewhat misleading. It suggests that the security issue can be solved by a single intervention, while, in fact, continual attention and concern are required. A better term for this would therefore be 'security process'.

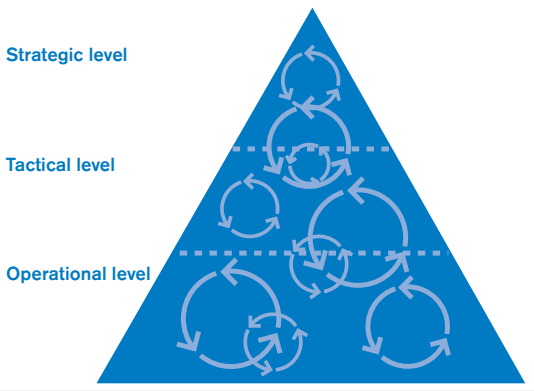



*Figure 1. Information security as a system of processes at a strategic, tactical and operational level.*

Information security is thus to be regarded as a system of measures, or rather, processes, at all levels in an organisation (see figure 1). All of these processes come together at the highest levels of the organisation. Senior management must supervise objectives and the execution of security processes. Furthermore, management must have an accurate conception of the quality of the security processes, preferably of how this relates to the importance of each process for operations and the continuity of the organisation.

### Made to order

How do senior managers know which security measures should be adopted by their organisation? Countless experts have racked their brains over this question in recent decades. Two sides can be distinguished: those who favour a customised approach to the problem and those who prefer a standard approach.

The first group likes to conduct an extensive quantitative risk analysis, on the basis of which a careful assessment can be made of which measures should or should not be adopted. A major advantage of a risk analysis is that the organisation gains valuable insight into the dependencies and weaknesses of information technology. But risk analyses are not without their drawbacks. They are costly and can lead to a profusion of information, which makes it much harder to take decisions.

The second group's approach is less labour-intensive. It relies on standard measures included in extensive checklists. Many valuable examples of such checklists have emerged as a result. Take, for example, the Code of Practice for Information Security Management (BS 7799) or the countless checklists published by professional organisations such as the Information Security Forum (ISF) or the International Information Integrity Institute (I4).

Some experts believe that the intelligent use of checklists such as BS 7799 will make the use of risk analyses completely redundant [Solm97]. It remains to be seen, of course, whether this will actually be the case. The use of checklists is not without its drawbacks. After all, 'one size does not fit all'. The security needs of different organisations actually vary to a greater extent than can be expected on the basis of other similarities. Operating processes can be poles apart, even within the same sector. The same is true of

the risks that go with the computerisation of these processes. Finally, the application of specific measures partly depends on the size, external environment and corporate culture of the organisation. It goes without saying that measures based on an extensive distribution of auditing tasks cannot be successfully implemented in small or understaffed organisations.

Even when checklists are used intelligently, measures must be weighed against each other in view of the importance of the information system of the organisation and the threats to which this system is exposed. This kind of consideration implies the need for a risk analysis. The use of checklists is therefore necessary, but insufficient in itself. Information security will always be customised work. Checklists can be a very useful aid.

## Security policy

The ultimate goal is to establish a permanent system of security measures in the organisation and in information technology, geared to satisfactorily managing the risks involved. A security policy is an essential instrument for the management and coordination of different security processes within an organisation. It offers a uniform basis and acts primarily as an instrument of communication.

Another goal of security policy is to demonstrate that the organisation satisfies the requirements set by parties in the socio-economic arena. In this context, security requirements are set, implicitly or explicitly, by shareholders, business partners, merger partners, trade associations, professional bodies and supervisory authorities. The building and implementation of an information security system ties in with certain responsibilities: to guarantee shareholder and stakeholder value; to create clear administrative and legal constructions so that unambiguous corporate governance methods can be established. Furthermore, explicit legal requirements for the security of data and information systems need to be met.

### Content and form

When drafting a security policy, the first question is what measures to include. First of all, the policy sets out the organisation's course with respect to information security and defines the organisational and managerial framework. The policy must therefore create a link between processes and organisational units, but not remain too fixed on the existing organisation. It goes without saying that all organisations are subject to change.

Another question is: should the policy also contain concrete security measures? If so, the organisational units can immediately start with the implementation. A disadvantage concerns the fact that the policy will quickly become obsolete. It is therefore recommended that no concrete measures be included in the policy if they are very detailed in terms of technology. It would be preferable to refer to existing standards and best practices.

A good information security policy should be fairly complete in its description of relevant processes, tasks and responsibilities. In spite of these requirements, a policy document should not be too lengthy and should be clearly formulated. A policy document must always be directed at the target group: the managers and staff involved in its implementation.

**The oil spill effect**
At the request of the information policy steering group of a large organisation, a project group accepted the task of creating an information security policy. While writing the policy document, the group kept coming across new measures that had to be taken into consideration. Some of the measures led to heated discussions. It became clear that exceptions had to be made for some security measures. These exceptions had to be embedded in the policy. The policy document consequently kept growing larger. An extra correction round was required to trim the policy but only revealed more elements and exceptions that warranted inclusion. The final document ran to 86 pages and provided a fairly exhaustive summary of the necessary measures. These measures were further explained in an appendix. The project group proudly presented the policy to the steering group, which endorsed the gist of the document but questioned its length. The document was distributed nevertheless. Needless to say, it ended up in filing cabinets and desk drawers ...

### Product and process

Security is not an objective in itself, but a means to an end. The costs must be weighed against the benefits. Benefits are hard to assess. A continuous consideration of these elements is therefore required, something that the policy should reflect. The drafting of a security policy provides an excellent opportunity to involve business managers in this assessment. Given the urgency of the initial thought process and related discussions, it is recommendable to address the issue at an early stage. This can be achieved by having a team of line managers from the existing organisation draft the security policy. The major advantage of this approach is that the resulting policy (if endorsed by all members of the team) is immediately supported by representatives of the different organisational units involved in its implementation. These sponsors will not only know the policy, they will also be able to defend it and provide additional explanations. Another advantage is that the policy will link up neatly with operating processes, the organisation, corporate culture and terminology used by the organisation. This will strongly increase the organisation's acceptance of the policy. Creating an information security policy concerns not just the *product*, it also concerns the *process*.

**Penny wise, pound foolish**
A large company with branches in several countries made the news due to a small, yet annoying security incident. The management of the group decided to actively address the security issue and engaged the Corporate Information Management department to draft a security policy for all divisions. The department decided against writing its own information security policy, and instead used an existing policy document from another company in the sector, adapting and expanding on the text where necessary. Why reinvent the wheel? The first draft of the policy was circulated, but met with ill reactions. Managers were highly critical of the document. 'This is one of those typical orders from the head office, these people in their ivory tower', one of them complained. 'This has appeared out of nowhere – I can't do anything with this!' The security project was delayed in its first phase and the Corporate Information Management department lost credibility. The words 'information security' were tainted for many years to come.

In short: support for and the acceptance of a policy can be increased by engaging a temporary project group to draw up the policy. This project group should consist of key players in the organisation – influential and enthusiastic people – who are aware of the risks that go with information technology and look favourably on security.

The size of a project group should obviously not exceed a certain maximum. Experience has shown that a group of seven people can successfully generate a security policy. A larger group only reduces the level of effectiveness and efficiency. The law of diminishing returns also applies to security. Don't be misguided by the enthusiasm with which managers discuss the length of a password!

The project group's working method will depend on the particular situation, but it must always be in line with the organisation's regular working method. For example, the project group may decide to meet four times. A space of two to three weeks is reserved between each meeting to draft and complete a component of the information security policy. The level of efficiency and effectiveness can be boosted considerably by thorough preparation (before each meeting, a draft of the policy component is sent to participants) and with the help of a competent final editor who is able to mould and refine both the content and form of the policy.

*Table 2. Allocation of tasks, responsibilities and authorities.*

| Management | Final responsibility |
|---|---|
| **Security manager** | Supervises the functioning of security policy as a whole and facilitates its implementation |
| **ICT Audit department** | Evaluates and reports to management |
| **Line managers** | Responsible for the implementation and execution of security policy within the organisational unit concerned |
| **Project leaders** | Responsible for drafting and implementing security requirements for the project concerned |
| **Supervisors** | Responsible for the provision of adequate security within the organisational unit concerned |
| **Staff** | Responsible for all aspects of security relating to their tasks |

The resulting policy document will then have to be submitted for approval to senior management or to a body authorised by senior management. Next, the policy can be implemented by the organisation, a process that includes its own set of problems.

## The security organisation

In order to prevent a lack of transparency regarding the various tasks, responsibilities and authorities, a security organisation must be established before implementation of the policy is begun with. If no one is held accountable, measures will never be carried out in a concrete way. Because information security is often considered a 'hot potato', this is a genuine risk. The allocation of tasks, responsibilities and authorities is therefore a crucial requirement.

### Setting up the security organisation

It has already been determined that every manager and each member of staff is responsible for information security. In practice, the allocation of tasks, responsibilities and authorities can be quite simple, as is illustrated in table 2.

There will be additional tasks for the:
* *computerisation organisation*, to adopt necessary organisational and technical measures;
* *users' organisation*, to apply caution and discipline when dealing with information technology;
* *helpdesk*, to answer questions about information security and register incident reports;
* *human resources*, to educate new employees, to have staff sign statements of confidentiality and to set up a sanction policy if rules are broken;
* *sales department*, regarding the conclusion of contracts with third parties;
* *facility management*, to manage the security of buildings and business premises.

In some cases it may be useful to establish an information security steering group, responsible for the monitoring of security regulations. Various organisational units and executive staff can be included in this steering group, such as the security manager, the information managers of organisational units, ICT managers, human resource managers and line managers. Of course, each organisation will have its exceptions to this example.

**The security manager**
It was established earlier that the appointment of a security manager or the creating of a Security Management department may be necessary for the control of the security process. The security manager's tasks include:
* drafting and updating security policy;

* supervising the implementation and observance of security policy, and maintaining and updating the related available knowledge;
* maintaining internal and external contacts in this context;
* serving as project manager in security projects, acting as a manager to project leaders within organisational units;
* coordinating information security with current projects in the organisation;
* executing and initiating risk analyses and small-scale internal audits;
* organising and participating in an information security coordinating committee;
* establishing criteria, norms and standards for the implementation of a security policy and coordinating the activities of people, departments and agencies involved in this implementation;
* collecting and registering information regarding current security measures;
* developing security plans with respect to security measures, and providing support during the execution of the approved plans;
* providing advice (solicited or not) to the management of the organisation and the line managers on necessary measures;
* organising and coordinating internal training sessions on information security for personnel;
* stimulating security awareness and creating, implementing and maintaining a communication plan;
* dealing with security incidents and taking precautionary measures to prevent the recurrence of similar incidents;
* drafting a control plan;
* reporting to the management of the organisation about the implemented policy with respect to information security, the progress of the implementation of new measures, the occurrence of incidents, actions taken, study results and control results;
* staying ahead of new developments regarding security and legislation concerned.

In practice, the security manager must function on the same level as senior line management. In emergencies, the security manager must intervene in a controlled, yet decisive manner. The position is based on confidentiality, as the security manager gets to deal with highly sensitive information. The security manager's senior position means that he or she reports to the executive management of the organisation.

### Policy implementation

Once the policy has been drafted and the corresponding security organisation has been set up, the implementation of the policy in the organisation may commence. The final objective is to create a permanent system of security measures in the organisation, geared to satisfactory risk management. On paper, this appears to be a simple, straightforward operation, comparable to installing a deadbolt lock on your front door. However, experience has shown that the actual situation as regards the implementation of information security policy is far more difficult. For this reason, a few fundamental 'failure factors' must be addressed:

*Security doesn't 'score'*
While a deadbolt lock serves as a visible and physical contribution to the security of your house, most information security measures are not visible to management. In many cases, rather specialised measures in and around the information system are concerned. These measures are not visible to outsiders and therefore not likely to create a good impression.

*Security is tricky*
On the other hand, visible security measures generally cause users a certain amount of inconvenience. Privileges may be taken away, or apparently simple functions must now be carried out in a roundabout way.

*Security is expensive*
Some security measures turn out to be more complex than initially expected. This can increase the costs. In addition, costs involved in information security prior to the implementation process are generally hidden costs. If a clear overview of the total costs of information security is provided during the process, the project may well be opposed by management.

The constant presence of these 'failure factors' makes each security project a considerable challenge that requires a cautious approach and extremely careful preparations. In this context, at least three critical success factors can be identified:

> The security manager must function at the same level as senior management.

*Commitment from senior management*
In order for a security process to be successful, senior management must actively and completely support the policy. If this is not the case, line managers will conclude that security is not a top priority within the organisation.

*Communication*
Optimal communication with all parties involved in security is an absolute necessity before, during and after the process. Insufficient communication will cause parties to feel less involved and will increase resistance within the organisation.

*A structured approach*
The implementation process should take place according to a structured, project-oriented approach. Where necessary, a security plan for each organisational unit can be drafted, indicating when each measure will be implemented. An example of this kind of approach is KPMG's Corporate Information Security programme, which is addressed below.

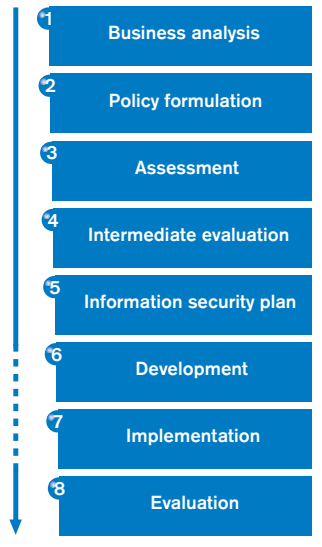



*Figure 2. The phases of the KPMG Corporate Information Security programma.*

## Corporate Information Security

The Corporate Information Security programme consists of a number of steps that are explained in figure 2.

The eight phases of the Corporate Information Security programme are summarised below.

**Phase 1: Business analysis**
During this phase, business processes and the information system within the organisation are analysed, as are the related dependencies and weaknesses. Brief discussions are held with representatives of different organisational units and existing process descriptions are used. The results are summarised in a brief memo.

**Phase 2: Policy formulation**
During this phase, the information security policy is drafted. It should include a description of the desired level of information security. This may be given on the basis of a summarised risk analysis and/or an existing baseline, such as the BS 7799. In addition to clearly formulated strategic and architectural elements of information security, the security policy will contain a description of the minimum level of organisational and technical security measures from the organisation's viewpoint. This 'baseline' is derived from BS 7799 and keyed to the specific situation desired. The policy is co-ordinated by representatives from the various business units during a number of workshops. This phase produces a short draft security policy that is submitted to the management of the organisation for approval. The phase is concluded with a 'go/no-go' moment, when a decision is made regarding the continuation of the project.

**Phase 3: Self-assessment**
During this phase, interviews with representatives from the various organisational units are used to study the extent to which the current system of measures satisfies the baseline level formulated in the previous phase. The results are processed and consolidated centrally and included in a short presentation. This presentation must provide an instantaneous and clear overview of the current situation. The large number of relevant security measures can create a situation in which the managers involved (who often do not have the time to intensively study the material) cannot see the wood for the trees. A simplified graphic representation of the 'IST' situation as a traffic light diagram or a spider web can do wonders (see case 3); however, this must always be presented with caution.

**Phase 4: Intermediate evaluation**
During this phase, the results of the self-assessment are evaluated and discussed with senior management. A moment of reflection and discussion is essential to allow those involved to absorb the results of the self-assessment, so that consensus can be reached on the related implications.

**Phase 5: Information security plan**
In this phase a security plan plan is drafted. It should include a description of the method by which any overdue security measures can be developed and implemented. The security plan must contain a description of the activities that need to be carried out, of throughput time and of the required capacity, as well as a description of the management framework that is to support the security policy. The objective of the security plan is to offer clear points of departure for the successful creation of information security policy by the various business units.

When drafting the plan, it is possible to distinguish between measures that can be adopted in a relatively short time without excessive effort (quick wins) and measures that require a considerably longer time (slow gains). By making this distinction and dealing with the quick wins first, visible results can be achieved rapidly.

Additionally, high priority measures and less urgent measures should be identified, so that the results of the self-assessment do not lead to 'crash actions': measures that must be immediately implemented because the organisation is exposed to unacceptable risks.

If it becomes clear that security is lagging so far behind that implementation of the overdue measures will exceed the available time, money and manpower, an evolutionary development model might be opted for: a long-term plan in which the measures are implemented step by step (not all at once) in order to achieve the desired final situation. This suggests the use of 'plateaus'. A plateau is defined as a stable situation that has proved itself in practice. The transition to the next plateau is only begun when the current plateau functions satisfactorily.

**Phase 6: Development**
During this phase, the overdue organisational and technical measures identified in Phase 4 are developed on the basis of the security plan drafted in Phase 5. The development phase is geared to both organisational and technical measures.

The development of *organisational measures* consists of defining procedures and guidelines that can be recorded in an Information Security Manual and might also be included in an existing Organisation Manual or an Administrative Organisation Manual. The allocation of responsibilities is an essential step in this phase. Finally, attention must be paid to drafting security agreements concerning the information security of third parties, such as suppliers, ICT service providers, customers and other business partners.

The development of *technical measures* consists primarily of the development or selection and purchase of specific security products for such things as logical access security, UPS, network security and encryption. In this context, it should be taken into consideration that costs related to maintenance and administration can often exceed the original investment; total ownership costs can therefore be much higher than just the write-off.

The system of measures should be 'future proof' and be able to continue to function as long as possible. It should be noted that the capacity required for this phase can only be determined after the security plan has been drafted.

**Phase 7: Implementation**
In this phase, the measures developed are formally accepted and implemented in the organisation in accordance with the security plan drafted in Phase 5. Implementation includes the training and education of users and managers as well as an extensive awareness programme. During this phase, it is essential that the 'security message' be transmitted to all managers and staff who were not involved in the previous phases. For this reason, close cooperation takes place with the organisational unit responsible for internal business communication, so that a relevant communication programme can be implemented. Furthermore, intranet solutions are used to an increasing extent as these now play an essential role in business communication within most organisations.

**Phase 8: Evaluation and certification**
In this phase, the security process is formally concluded, evaluated, and, if desired, certified according to the Code for Information Security.

### Experiences

Several variations of the Corporate Information Security programme have been carried out by a large number of organisations. The most important conclusion is that the programme provides an effective approach to the security issue. The straightforward phases of the project, its uniformity and its lack of ambiguity make the Corporate Information Security programme recognisable to management. Furthermore, the process is always completed with physical proof of the effectiveness of the efforts involved.

In practice, BS 7799 has proved to be extremely practical. The increasing acceptance of BS 7799 in the market forms an important factor in its success. The structure of this standard is not always logical, however, and some chapters overlap to a large extent. Nevertheless, it appears that these drawbacks can be overcome in practice. The measures in BS 779 have a great deal in common with other security disciplines, such as security measures for buildings and business premises, measures in the personal arena and ICT audits. It is therefore vital that the departments responsible for these disciplines are closely involved in the security process.

In addition to the general 'failure factors' listed above, only one specific bottleneck can be identified at this time. Commitment is not a problem; in most cases, security awareness is present at all levels of an organisation. Budgetary concerns are a limiting factor in only a small number of cases. A major limitation is that nearly all organisations are currently faced with a shortage of qualified personnel and with a high degree of mobility in the ICT labour market. Both factors contribute to unintentional delays in the security process.

Organisations that initiate a Corporate Information Security programme should know that, although the system may have been certified, it will still contain weak spots that will only emerge at a later date. Given the current state of information technology, this is unavoidable. Yet, it does not spell disaster. The objective is not to fully secure our information environment, but to responsibly manage this environment and the risks that come with it. An organisation that is ready to deal with the inherent weaknesses of information technology quickly and effectively is a step ahead of the pack.

### A word of thanks

Cees Coumou, Paul Overbeek, Ronald Paans and Jan Willem Schoemaker are the conceptual co-founders of the Corporate Information Security programme.

The system of security measures should be 'future proof'.

### Literature

[Roos95]
E. Roos Lindgreen and C.S. Schönfeld, *Maatwerk past information security* (Tailor-made fits information security), Compact/3, 1995.

[Solm97]
R. von Solms, *Can security baselines replace risk analysis?*, Proceedings of the IFIP/SEC Conference 'Information Security in Research and Business', Copenhagen, 1997, pp. 91-101.

*Edo Roos Lindgreen*
(roos.edo@kpmg.nl)
is a partner at KPMG Information Risk Management in Amsterdam, the Netherlands, and teaches ICT & Auditing at the University of Amsterdam. He has a Ph D degree in information security.

*Frank Rizzo*
(frank.rizzo@kpmg.co.za)
is a partner in the Johannesburg office of KPMG's Information Risk Management practice in South Africa. Frank is responsible for Information Security Services in South Africa and has had experience in mainly the Financial Services and Mining industries.

*Allen Zuk*
(allenzuk@kpmg.com.au)
is a senior manager in the Sydney office of KPMG Information Risk Management in Australia. Before this secondment, he has worked in the San Francisco office. Penetration testing, ICT infrastructure controls and Intrusion Detection Systems are his key areas of interest.

*Francois Beaudoin*
(fbeaudoin@kpmg.ca)
is a manager in the Montreal office of KPMG Information Risk Management in Canada. He focuses on Enterprise Security Architectures.

## Case 1: Information Security Assessment using BS7799

KPMG's Information Risk Management department in South Africa recently concluded the first phase of an information security contract for a merchant banking organisation. As the organisation wanted to adopt 'best practice' standards for its information security project, the entire KPMG approach was based on the British Standard on Information Security Management, BS7799. During the process, IRM professionals used KPMG's information security methodology and applied this to the BS7799 requirements.

This case study describes the method used by the IRM specialists during the first phase. The client is a leading South African Merchant Bank with branches in two major cities in South Africa. The Bank is involved in a wide range of merchant banking activities and has assets of approximately USD 2.5 billion.

### Security aspects

The client initiated an information security project halfway through 2000. The project was started in the ICT department, but it soon became clear that Information Security involves more than technology alone. The project was therefore positioned to include all aspects of information security: people, processes and technology.

KPMG were asked to assist the client on account of the organisation's business-driven information security models and methodologies, as well as its access to best practices in the area.

The project consists of the following phases:
* BS7799 assessment;
* detailed analysis and assessment of key initiatives;
* implementation.

The main objectives of the first phase were to:
* create an understanding of the organisation's complex information security environment and information security culture;
* understand the business drivers for information security for each business unit;
* position information security correctly with respect to the business executive team in view of their business unit objectives;
* establish a BS7799 baseline view for compliance and produce a statement of applicability, indicating any opportunities for improvement of the information security level;
* define an accurate and complete action plan to enable the client to reach the required baseline, linking proposed initiatives to their corresponding business drivers.

### Definition

For the purposes of this project, information security was defined as the policies, practices and procedures that help protect information against unauthorised access, modification, or accidental change and that ensure the availability of that information to authorised users (on request).

KPMG's Information Security Capability model was used as a central reference point. This model outlines manageable business and ICT components as regards information security and specifies where attention should be paid to implementation of future controls or security management.

The project got underway with a presentation to the Bank's Executive Committee. The KPMG team also defined a BS7799 Statement of Applicability for the client. This statement shows which controls are relevant to the client and to what extent these need to be applied in order to ensure that information security risks are adequately managed.

### Results

The first phase resulted in the representation shown in figure 3.

The team organised workshops with each of the bank's business units. A risk matrix was set up in these workshops, which was included in figure 3. It turned out that the security level in none of the areas met the BS7799 criteria.

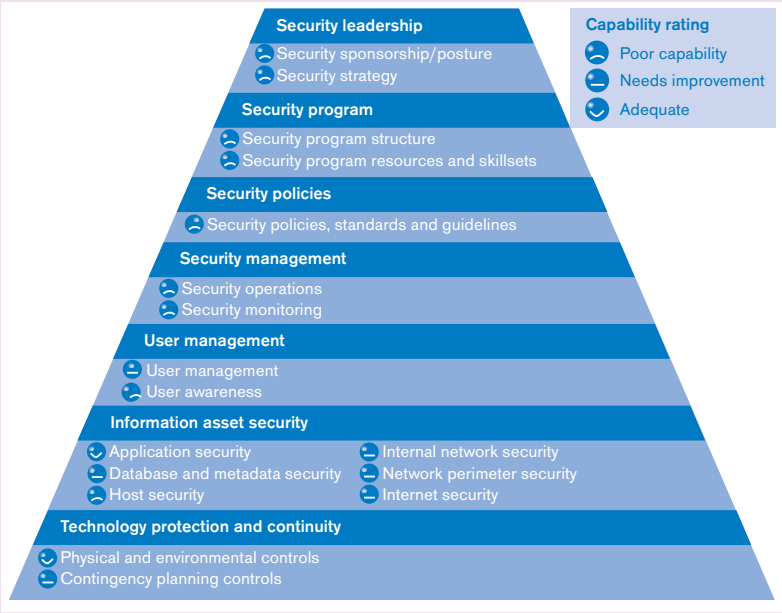



*Figure 3. Information Security Capability Model.*

On the basis of a detailed report that consolidates all KPMG findings, the organisation subsequently decided to address the areas that caused immediate concern. The infrastructural and architectural recommendations were to be addressed in the next phase.

### Case 2: Enterprise Security Architecture

For a number of years now, the Department of Health in Quebec (Canada) has been working on the digitalisation of medical records. These medical records include current patient information as well as the patient's medical history. Ultimately, these digitalised medical records are to be shared by various health care providers, such as hospitals, private clinics, physicians in private practices, pharmacists and so on.

As a first step, the Quebec government has set up a network that links together all hospitals in the province. This private network, called Réseau Télécommunication des Services de Santé (RTSS) (Health Services Telecommunication Network), uses the IP protocol and is connected to the Internet in order to enable external providers to share information. However, before allowing hospitals to connect to the RTSS network, the Quebec government prepared a comprehensive set of strict information security policies that the hospitals must adhere to.

It is within this context that a group of hospitals gave KPMG a mandate to make a complete analysis of their information security systems as well as develop a security architecture that would meet RTSS requirements, as outlined in the government's policies for information security.

The mandate was carried out as follows:
* analysing the current situation ('baseline assessment');
* establishing end state architecture, taking into accounts RTSS requirements and gaps between the current security structure and the desired structure;
* drafting of a transition plan.

#### Analysing current situation

The first objective was to analyse the hospital's current information security provisions. In order to meet this goal, KPMG professionals used the information security assessment methodology. This methodology is based on a 'top down' approach that permits the identification of current security deficiencies as well as root causes. The Information Security Capabilities model, as shown in the previous case study, was used for the assessment phase. In contrast with traditional approaches that generally focus on the identification of technical weaknesses, i.e. the lowest levels in the model, the Information Security Assessment methodology is used as a frame of reference to identify the root causes of these technical deficiencies. Consequently, by looking at the causes, it becomes possible to take direct action and solve problems permanently.

#### Establishing objectives according to RTSS requirements

In Phase II, a perception of information security was developed in conjunction with health care institutions. The objective was to create a security architecture that would enable them to reach their security goals while taking into account their various budgetary, technological and human resources constraints, as well as their obligations to the RTSS network. To achieve this goal, KPMG professionals used the Enterprise Security Architecture methodology.

One of the first objectives was to identify the various risks that the institutions were facing as well as the acceptable level of risk. To reach this objective, KPMG professionals organised several workshops. In addition to achieving their primary purpose, the workshops offered excellent opportunities for participating institutions to share information. As a result, participants in fact established a permanent advisory committee which meets on a quarterly basis and in which KPMG is involved.

Once the risks and the maximum acceptable risk level were established, a concept was developed for a security architecture that corresponds with the best practices within the industry while meeting the RTSS network requirements. Once the security architecture was defined, a gap analysis was conducted of the current ICT security system, as established during Phase I.

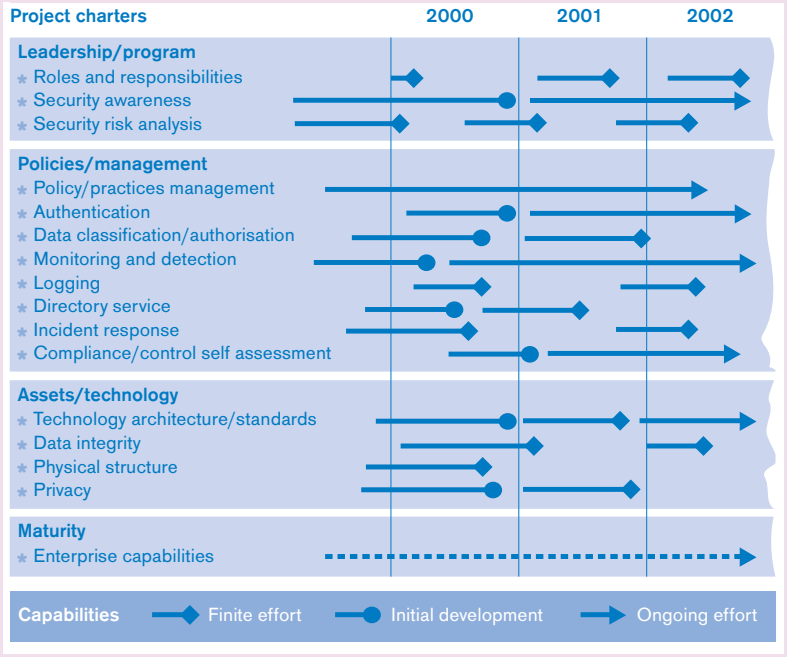
#### Transition Plan

The last phase involved the development of a transition plan. During this phase, KPMG's goal was to provide a road map of all the steps required prior to the implementation of the new security architecture. This action plan, as shown in figure 4, addresses the various components that underlie the architecture's implementation, such as integration with the current technological infrastructure, deployment, training, business processes and so on.

#### Results

The main benefit for the organisation concerns the assessment of its current information security provisions and the development of a security architecture based on best practices within the industry, in compliance with the Quebec government's requirements for the RTSS network. However, some organisations reaped several other benefits from this exercise. In fact, the various workshops held throughout the mandate raised awareness among management and staff who attended the workshops. This helped to make information security a corporate project, rather than simply an ICT project.

*Figure 4. Transition plan and identified security projects.*



### Case 3: Penetration testing

For an Australian organisation, KPMG reviewed the overall security infrastructure of the e-Business environment and perimeter. The objectives of this review were to:

* identify threats associated with the Internet services;
* evaluate the detection and escalation mechanisms employed by the application service provider (website hosting company); and
* make recommendations for any identified weaknesses.

The information provided was limited to network topology, type of systems used, configuration parameters and logical access control policies implemented within the organisation. This means that this penetration attempt is an 'external test with knowledge'. Alternatives are:

* internal penetration test with knowledge;
* internal penetration test without knowledge;
* external penetration test without knowledge.

In several instances, organisations prefer the last option to resemble a hacking scenario, in which the hackers or 'script kiddies' have no prior knowledge of the victim's infrastructure, to see whether access could be obtained to an organisation's back-office systems and internal network from the Internet.

#### Approach

KPMG's approach was designed to present to senior management a summary report identifying the risks and exposures inherent to doing business on the Internet and explaining what these exposures and vulnerabilities represent to an external website. KPMG also aimed to develop action plans with which to address any identified potential weaknesses. The penetration study included the following phases (also shown in figure 5):

* **Phase I: Planning & Preparation –** This phase included development of the engagement objectives, planning and conveying the team's understanding of the terms of the contract. Deliverables included a *Project Plan* and *Rules of Engagement*.
* **Phase II: Identification –** This phase focused on the identification of the various elements of the Fundamental Risk Proposition – risk, value, threats and vulnerabilities. A variety of research methods and investigation techniques were applied to identify potential targets. Deliverables included the organisation's *Security Risk Profile*.
* **Phase III: Exploration –** This phase focused on investigating security risks relevant to the organisation. Indirect techniques were used to identify vulnerabilities within the perimeter of the organisation. Deliverables included the organisation's *Security Vulnerabilities Analysis*.
* **Phase IV: Intrusion –** This phase focused on testing security controls and taking advantage of relevant vulnerabilities. This included the intrusive Internet penetration testing of network gateways, routers (internal/external), firewalls (internal/external) and website servers. Commercial and proprietary tools were used in the attempt to breach the security of devices in the Demilitarised Zone (DMZ) and penetrate the internal network. Deliverables included the organisation's *Intrusion Analysis*.
* **Phase V: Reporting –** This phase focused on the summary and presentation of KPMG's analysis and conclusions. The approach utilised a management presentation. Deliverables included *Management Presentation*, *Summary Report*, and *Detailed Supporting Documentation*.

Other activities employed were:

* 'war dialing' in order to penetrate modems and other remote access connections;
* 'social engineering' to obtain security information from ICT staff;
* penetrating the organisation's networks by first exploiting a business partner, parent company or subsidiary;
* changing or modifying any file or database;
* creating and leaving re-entry paths on any of the penetrated hosts;
* replacing authorised services on compromised hosts with 'Trojan horse' versions of the service;
* attempting attacks on the service to disable the organisation's or provider's services.

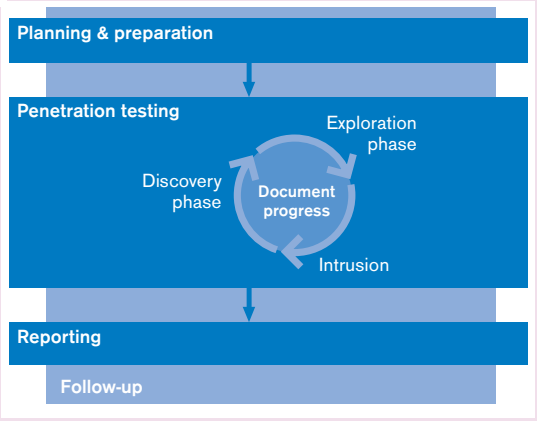



*Figure 5. Penetration study phases (based on model developed by Ruben de Wolf).*

One initial target IP address was supplied and agreed on with client staff before testing commenced. With the initial IP address, the KPMG team was able to obtain IP addresses of additional target devices.

All penetration testing was conducted from an Internet dial-up account using a pool of dynamic IP addresses within a specified range. We provided the client with this information so that the organisation and its provider's staff are able to identify our testing traffic in any relevant security log files.

#### Results

During external penetration testing we were unable to penetrate the organisation's core internal network environment. We were able, however, to obtain access to the pilot website that was still connected to the core production site. This backdoor provided access to the organisation's key web applications and data.

Moreover, the KPMG team made a crucial discovery. The major area of concern relates to the failure of the organisation's service provider to detect our intrusion attempts and initiate an appropriate escalation mechanism. Although the provider's management were aware that the testing was carried out, the key ICT security staff had not been told exactly when testing would occur. At the end of the attempts, KPMG were informed that none of the key ICT security staff at the provider had noticed our testing or had notified the relevant authority.

This represents a significant risk to the organisation if security-related incidents are not detected and responded to in time. Consequently, KPMG was unable to draw any conclusions about the level of effectiveness of the organisation's incident response and escalation procedures as these procedures were not fully developed or included in the SLA (service level agreement) with the provider.

In figure 6, a summary of the security situation is presented, in which an organisation is benchmarked against comparable organisations.

In table 3, an example is shown of a detailed representation of the security situation of all servers that were reached from the Internet.

Other findings included the fact that user names and passwords were obtained by using a brute force password cracking tool, which may result in possible access to the organisation's pilot website from the Internet. In one instance, a password was not required to gain access to the website from the Internet.

The KPMG team discussed these and other results, and management responses with the client. Action plans were drawn up accordingly. The organisation's positive response to the key recommendations that we presented clearly shows that the organisation takes the reduction of potential exposure from e-Business activities seriously. After the report was presented, the client accepted the recommended action plans and began immediate implementation.

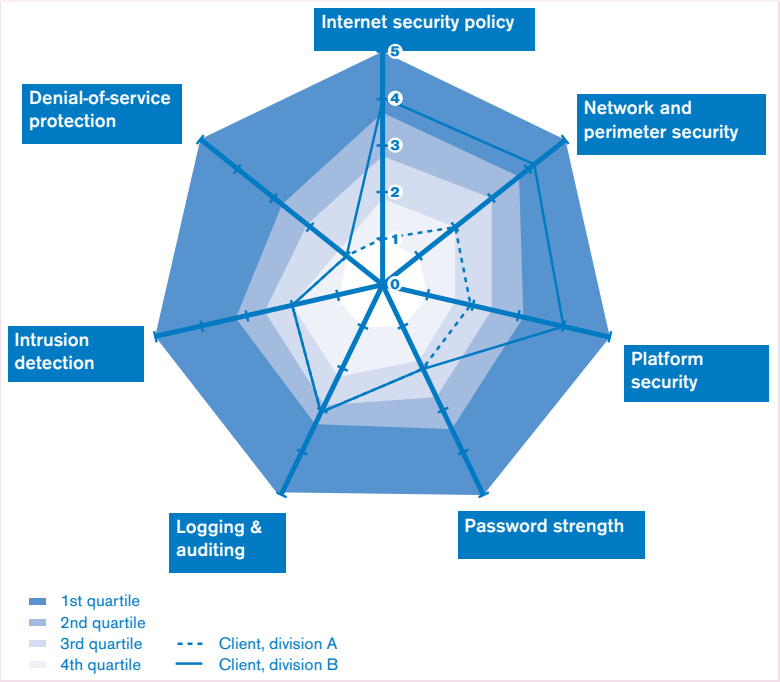



*Figure 6. Sample Internet security benchmarking summary.*

| Vulnerability | Risk | Host |
|---|---|---|
| | | 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 |
| Bind version | Low | |
| DNS server inverse queries | Medium | |
| Guest account enabled | Medium | |
| HTTP server with unresolvable local links | Low | |
| ICMP netmask request response | Low | |
| ICMP timestamp requests | Medium | |
| INN control message vulnerable | High | |
| NetBIOS share found | Low | |
| NNTP posting | Low | |
| NNTP reading | Low | |
| Root dot dot | Medium | |
| Routed append vulnerability allows remote file manipulation | Medium | |
| Shares enumerated through a null session | Low | |
| SMTP EXPN command | Low | |
| SNMP can reveal possibly sensitive information about hosts | Low | |
| SNMP_Get able to guess community name | Low | |
| SNMP_Get able to retrieve public community name | Low | |
| TCP sequence prediction | Medium | |
| Traceroute can be used to map network topologies | Low | |
| Verify account information about users with sendmail | Low | |

*Table 3. Detailed representation of security situation of various servers.*