Information Security at Top Level

Securometer® streamlines management information

A. Buren¹, B. van der Meer², A. Shahim¹, W. Barnhoorn², E. Roos Lindgreen^{1,3}

¹ KPMG EDP Auditors, Burgemeester Rijnderslaan 20, 1185 MC Amstelveen, The Netherlands

² Automatisering Sociale Zekerheid (ASZ), Staalmeesterslaan 411, 1005 CA Amsterdam

³ University of Amsterdam, Postgraduate Accountancy Course, IT & Auditing

E-mail roos.edo@kpmg.nl

Key words: information security, management information, self assessment, web technology, intranet

Abstract: The past few years, information security appears to be receiving increasing attention from senior management. However, unlike the performance of financial and logistics processes, information on the performance of the security process is often reported to senior management in an inefficient and unbalanced manner. This article describes a method and an application for improving reports about security processes to the organisation's senior management.

1. INTRODUCTION

The security of information and information systems is no longer a specialist domain. It is increasingly seen as a normal part of risk management in general, and therefore as a normal responsibility of every organisation's senior management. As with all other aspects of risk management, information security is not a single, non-recurring activity but a system of processes that spans every department in the organisation. All these processes come together at the top of the organisation. In order to have a good insight into how secure the organisation's information and information systems actually are, the management responsible must have a true impression of the quality of each security process, preferably in relation to that process' relative importance for business management and the organisation's continuity.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35575-7_19](https://doi.org/10.1007/978-0-387-35575-7_19)

Information security is increasingly receiving senior management's attention. Management is aware of the risks of information technology and the necessity of dealing with the risks responsibly. However, managers can generally only devote a limited amount of time and attention to information security. This is hardly surprising, considering that the costs of information security are usually no more than a few percent of turnover.

As a consequence, management's attention is often limited to a small group of acute threats and counter measures that happen to relate to the issues of the day. Other security measures are often not paid the attention they deserve. This situation is not only undesirable but also unnecessary. After all, as with the performance of financial and logistics processes, details on the performance of security processes can also be brought to the attention of senior management in an efficient and balanced manner.

This article describes how the information supply relating to information security can be streamlined. The article is arranged as follows. Section 2 describes a general framework for management information concerned with information security. Section 3 provides a general description of Web technology and its application in measuring the performance of security processes. Section 4 discusses the general specifications of such an application, the Securometer. The article concludes with a brief summary.

2. MANAGEMENT INFORMATION

The Code of Practice for Information Security Management [BSI95] is increasingly being used as a basis for setting up information security in organisations. The Code, or BS 7799 as it is commonly called, defines ten categories of security measures that its authors consider to be the minimum requirements.

BS 7799 forms the basis of several structured approaches to the information security challenge. An example of this approach is the Corporate Information Security programme [Roos97]. The essence of the programme is that security measures are developed and implemented on the basis of standardisation, a pragmatic analysis of the current situation and a clear and concise project plan.

2.1 Corporate Information Security

The Corporate Information Security programme consists of a number of steps, which are explained in Figure 1.

Figure 1. The Corporate Information Security programme

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

Phase 1 - Business risk analysis

During this phase, operating processes and the information system within the organisation are analysed, as are the related dependencies and weaknesses. The results of this phase are summarised in a brief memo.

Phase 2 - Policy formulation

During this phase, an information security policy is drafted. 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 as viewed by the organisation. This 'baseline' is typically derived from BS 7799 and is attuned to the organisation's business goals. This phase is concluded with a 'go/no-go' moment, when it is decided whether the project will continue.

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, providing a clear overview of the current situation.

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 and reach consensus on its implications.

Phase 5 - Information security plan

This phase focuses on the drafting of a security plan, which will include a description of the method by which any overdue security measures can be developed and implemented. At a minimum, the security plan must contain a description of the activities to be carried out, the time frame and the resources required, as well as the management framework needed to give shape to 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 considerably more time (slow gains). By making this distinction and dealing with the quick wins first, visible results can be achieved rapidly.

Phase 6 - Development

During this phase, the organisational and technical measures identified as overdue in phase 4 are developed on the basis of the security plan drafted in phase 5. The development phase is geared towards 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, or which can also be included in existing policy manuals. Assigning responsibilities is an essential step in this phase. Finally, attention must be paid to drafting security agreements relating to

the information security of third parties, such as suppliers, IT 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 control, emergency power supply, network security and encryption. In this context, it must be taken into consideration that costs related to maintenance and administration can often exceed the original purchase price of these products; total ownership costs can therefore be much higher.

Phase 7 - Implementation

In this phase, the measures developed are formally accepted and implemented within the organisation in accordance with the security plan drafted in phase 5. Implementation includes training and educating users and managers as well as a broad 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 co-operation takes place with the organisational unit responsible for internal business communication, so that a relevant communication program can be implemented. Furthermore, intranet solutions are being 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 rounded off, evaluated, and, if desired, certified against BS 7799 [Over97].

2.2 Layered audit model

To guarantee the long-term operation and observance of the required measures, the Corporate Information Security Programme provides for a layered audit model, shown in figure 2.

Figure 2. Layered audit model

In this model, the first check of the effectiveness of the measures is made by the member of staff responsible. On the basis of a self assessment, this member of staff reports on the quality of the security measures that fall within his field of responsibility. Besides increasing efficiency, this approach also has the advantage that by recognising the autonomy of the member of staff responsible, it removes a significant psychological barrier that can be an obstacle to the acceptance of a security procedure. After all, who actually enjoys being watched all the time?

A disadvantage of self assessment as an audit instrument is obviously that people often give a more positive reflection of things than is actually the case. The results of the self assessment must therefore also be checked in the second stage of the audit process, by an internal audit department for example. In practice, the people being audited generally understand the need for this extra audit.

Finally, a concluding audit may be carried out by an external expert, such as an EDP auditor. This audit can be conducted within the scope of the audit of the annual accounts, but may also focus on the provision of a Third-Party Report [Velt95] or an official security certificate [Over97].

2.3 Management information

The success of the above audit mechanism depends on the availability of good management information about numerous security processes. Ideally, senior management should be able to see at a glance what the position is regarding the quality of the security measures. In turn, this sets certain requirements for the type and content of the management information on information security.

In practice, the management information often leaves a lot to be desired. This is not just because of the large number of security measures - which may amount to dozens for a medium-large organisation, if not hundreds - but

also because of the varied nature of the measures, which are often the responsibility of various organisational units. Reports therefore often reach senior management along different routes, in different forms and with varying frequencies.

There are various techniques for improving management information about information security. Two of these form the essence of this article.

The first is the use of BS 7799, which is used for setting up a uniform and structured standard report. The fixed and, to many people, familiar chapter headings of the Code help considerably in improving the accessibility and recognisability of the information presented and also help guarantee the report's completeness. Secondly, an integrated audit mechanism based on self assessments can lead to major improvements in the quality of the management information. A mechanism of this kind provides senior management with an instrument for measuring the performance of numerous security processes effectively, efficiently and reliably.

The way in which self assessments are conducted also partly determines how effective they are. Distributing, collecting and consolidating paper questionnaires is still a common practice in many organisations. Others have switched to distributing diskettes with automated questionnaires, but this approach often turns out to make the logistics problem even worse. Nowadays, new media and technologies offer possibilities for conducting self assessments faster and more efficiently.

3. WEB TECHNOLOGY

New media, such as the Internet, intranet and the World Wide Web are now generally accepted. Web technology makes it possible to present information clearly and uniformly. The World Wide Web's low threshold and user-friendly graphical interface is increasingly being used for creating new information systems [Bure97].

3.1 Intranet

Many companies now have advanced intranet applications. In some cases, the intranet is no more than an accessible storage place for a limited collection of general, internal business information, such as forms, regulations, manuals, the telephone directory and a who's who. Other organisations go much further and use the intranet for storing and making available every kind of information conceivable, including links to existing applications for supporting the primary and secondary business processes, but also links to external information sources.

An intranet is relatively simple to build. Because the intranet uses the existing LAN environment, initial costs can be kept low. A major advantage of an intranet is that, by using “active content”, such as Java or ActiveX, the information transfer takes place independently of the underlying client platform by using a platform-independent byte code format. To execute this byte code, the browser has to have an inbuilt Java interpreter. The Java interpreter takes care of the translation for the underlying operating system. Practically all browsers now have an inbuilt Java interpreter, which means the execution of a Java applet is independent of both the operating system and the hardware platform. The user therefore only needs a browser to access management information. This is a welcome feature for organisations, which generally have several hardware platforms, operating systems and workplace PCs that are set up in various ways.

The aforementioned features of accessibility, user-friendliness, platform-independence and the relatively low costs make Web technology perfect for creating a tool for conducting and presenting self assessments. It means the required performance measurements of security measures and the relevant reports to senior management can be largely automated, and set up efficiently, on a permanent basis. An elaboration of this principle has led to the Securometer, which is described below.

4. SECUROMETER

The Securometer is an intranet application for conducting self assessments to review the qualitative status of the security measures that have been taken and to provide the relevant report to senior management. The Securometer was developed by Automatisering Sociale Zekerheid (ASZ), the in-house supplier of information services to the Industrial Insurance Administration Office Group (GAK Group - The Netherlands), in co-operation with KPMG EDP Auditors [Meer97]. The functionality and technical implementation of the Securometer are described below.

4.1 Functionality

Details of the qualitative status of the security measures taken have to be provided by the respondents who are responsible for the set-up and operation of the security measures.

The Securometer works on the basis of the client-server-principle and is independent of the end-user's local computer set-up and any peripheral equipment. The user only needs a browser and access to the intranet. This means there is no installation procedure for the Securometer on the user's

side, which is a welcome detail for managers, who are often already stretched to capacity.

The Securometer has a number of basic functions, which are described below.

4.1.1 Starting

Upon starting, the system determines the user's identity on the basis of a combination of user ID and a password, and determines the associated authorisations. The authorisations relate to the execution of functions and whether or not the user is authorised to retrieve the self assessments of other users. If the user is known to the system, it checks the completion status of previously entered self assessments, indicates the last self assessment that still has to be completed, and possibly also displays screen messages indicating that previous self assessments have not yet been completed or sent.

4.1.2 Self assessment

To obtain an insight into the degree to which security measures have been taken in the organisation, the measures will have to be reviewed periodically. The system formulates questions to this end, and the users supply the answers.

The system contains a central database where all the questions are stored. This list of questions is composed in accordance with the structure of BS 7799, but can be readily altered for other baselines. In view of their position, managers will usually be responsible for only part of the total security measures. Depending on the user's identity, the system therefore only distributes the questions that are relevant to the user or that person's workplace.

The system presents the questions on the basis of a description and characteristics, such the group and the type of question: is it a baseline question or a supplementary question? For each subsidiary subject - the "third level" of the Code - each respondent has to indicate whether a specific measure has been fully implemented, partially implemented or not implemented at all. The answer to the questions is given by clicking on the button relating to the appropriate answer. The questions that have already been answered in the relevant completion period are marked and, depending on the selected menu option ("fill in unanswered questions"), the user may ignore them. The user moves from question to question using navigation buttons. A search button can be used to move to the available question categories (such as those based on the chapter headings of BS 7799). Help

buttons provide additional information, if the user requires a more detailed explanation of the questions or how to operate the system.

The respondent has to confirm a completed self assessment by clicking on a confirmation button, for the answers to be incorporated into the central database. Once incorporated in the central database, the user cannot make any further alternations to the self assessments.

Information exchange on a transaction basis is the chosen method of communication between the client and server. This means the system can always be exited without any loss of information.

4.1.3 Reporting

The Securometer processes registered answers into aggregated, graphical, multidimensional overviews using a weighted average. The status of each security measure taken is also shown by what is known as a “traffic lights diagram”, in which the level of information security is depicted as red, orange or green. “Red” indicates measures that are inadequate; “orange” indicates measures that are either the subject of discussion or that have partially been taken; “green” indicates measures that all the respondents consider to be adequate.

Using a “spider's web diagram”, the set of security measures that has been reviewed can be linked to the predetermined standards (in this case BS 7799). This diagram shows at a glance whether the standards are being observed and thereby provides a quick indication of the general level of security. Figure 3 provides an impression of the design of the screen; the actual screen layout can be readily modified to suit the organisation's house style.

Figure 3. Impression of the design of the Securometer

4.1.4 Trend analysis

Besides retrieving and graphically displaying current self assessments, the system also offers various functions for displaying previous self assessments. Previously completed self assessments can be aggregated for each self assessment completion period by appropriately authorised users, and can be placed in sequence. This provides senior management with a proper insight into the progressive or regressive development of the level of information security.

4.1.5 Management

Besides this functionality for the end user, the Securometer has a separate management module that enables the manager to create and change user names, establish permissions, execute progress controls, make backups of the central database and maintain the questionnaires.

4.2 Technical implementation

The Securometer operates in a Web environment and uses Internet technologies such as TCP/IP and HTTP for the communication between the client and server. The system communicates the information transfer to the user via the intranet, using TCP/IP and the HTTP protocol. The layout and content of the information transfer are marked up in accordance with the HTML format. A new link is set up for every question and answer session.

Web browsers interpret the HTML pages and enable the user to see the page in the layout described. The architecture chosen for the development of the Securometer is known as “thin client” architecture, which limits the client application to navigation functions using a Web browser. This means the Securometer software is centralised on the server, which translates into more efficient performance of management and maintenance work. This architecture also makes it unnecessary to install the Securometer on the user's PC.

The server is linked to a relational database, where the questions are stored. The server acts as a communication port between the Web browser and the Securometer database. The server uses scripts for communicating questions and diagrams (translated into HTML pages) to the Web browser and for processing incoming answers. Figure 4 shows the technical architecture of the Securometer.

Figure 4. Technical architecture of the Securometer

4.3 Practical experiences

At the time of writing, a beta pilot has successfully been completed and the Securometer is being implemented within the ASZ organisation. A number of large organisations have expressed their interest; a demonstration version is available.

Our preliminary experience shows that the implementation trajectory will not be without pitfalls. In fact, it is found that even the minimum effort required to fill in a Securometer questionnaire may still be perceived by line management as unnecessary bureaucracy. Securometer appears to share this fate with other corporate knowledge-management initiatives requiring employees to record their knowledge of products, services, clients, engagements or human resources in a central repository using intranet technology. Indeed, filling the database and keeping it up-to-date are cited as major challenges in such projects. We expect that, with respect to the Securometer, line management will soon delegate this task to the appointed security officers, where the Securometer has met substantial enthusiasm.

An additional advantage of the Securometer is that its application is not restricted to the realm of information security. Instead, its principles are generally applicable to qualitative self assessments in various fields, such as employee satisfaction, quality assurance or customer service evaluation. However, reworking the Securometer to fit these purposes will require additional effort.

5. SUMMARY

Information security is becoming increasingly important as a part of total business management. The necessity of structural improvement calls for a structural approach. To ensure the success of an integrated approach, senior management must have proper management information about the performance of the organisation's security processes.

This management information generally leaves a lot to be desired, owing to the number and variety of security measures. Security measures are often the responsibility of various organisational units. Reports therefore often reach senior management along different routes, in different forms and with varying frequencies.

As part of an integrated approach, a layered report and audit model can be set up consisting of self assessments, and internal and external audit measures. Arranging for decentral management to report regularly about the quality of the security measures will result in an aggregation of reports that can serve as management information for the organisation's senior management. To be able to aggregate this information, it is important to adopt a uniform style of content. The chapter headings of BS 7799 provide a suitable starting point for this.

New technologies offer excellent opportunities for streamlining the production and distribution of management information based on self assessments, also with regard to information security. Using intranet

technology helps simplify the logistics of the audit model; an intranet offers the possibility of making self assessments quicker and more efficient. The accessibility and user-friendliness of Web technology are powerful features used in the Securometer.

The Securometer processes completed self assessments into aggregated, graphical, multidimensional overviews. The status of each security measure taken is also shown separately. The set of security measures that has been reviewed can also be linked to predetermined quality levels, thereby enabling senior management to see at a glance whether the policy standards are being properly observed. Finally, the Securometer provides an insight into the progressive or regressive development of the level of information security.

6. REFERENCES

- [BSI95] British Standards Institution, BS 7799, *A code of practice for information security management*, BSI, ISBN 0 580 23642 0, 1995.
- [Bure97] A.M. Buren, *Multimedia in open omgevingen, de mogelijkheden van het Word Wide Web*, Compact 1997/6.
- [Meer97] B. van der Meer, *Strategisch Plan Securometer en Functioneel Ontwerp Beveiligingsenquête Deelproject 8.7*, 1997.
- [Over97] P.L. Overbeek, *Certificering tegen de Code voor Informatiebeveiliging*, Compact/6, 1997
- [Roos97] E. Roos Lindgreen, *Corporate Information Security - Baselines for Business*, DEC User Group The Netherlands, September 1997
- [Velt95] P. Veltman, *Third party review en -mededeling bij uitbesteding van IT-services*, Compact 1995/3.