Information Security Management Through Measurement

E. VON SOLMS¹, S.H. VON SOLMS²

¹*Department Computer Science and Information Systems
University of South Africa, Pretoria, SA
e-mail: vsolme@unisa.ac.za*

²*Department of Computer Science
Rand Afrikaans University, Johannesburg, SA
e-mail: basie@rkw.rau.ac.za*

Abstract: This paper suggests a model, based on the continuous measuring and monitoring of information security parameters, by which information security management can be made more dynamic and relevant.

1. INTRODUCTION

Securing information is one of the most important aspects in any organization today. Information security's main aim is to protect the organization and its assets (like sensitive information) against attempts of intrusion and corruption. Most organizations in the business world already know the value of information security in the work place. The information security aspects are usually stipulated in the security policy of the organization.

The building blocks of any organization are its policies. The organization is run and ruled with these policies. One of the most important policies are the security policy, this policy must be correctly structured and implemented in an organization. The question that is being asked more frequently now days is, if there is this security policy, why is there still security risks in an organization? The problem of security risks in an organization is often not that the security policy is badly or poorly written, but rather that nobody knows whether the policy is enforced or not. This happens because there are no mechanisms in place, a part form some annual audits, to ensure that they are enforced and complied with on a continuous basis.

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: [10.1007/978-0-387-35515-3_53](https://doi.org/10.1007/978-0-387-35515-3_53)

Internal audits are done once a year to have a closer look if the information security in the organization is working as it should, and that the security policy is enforced. The problem that develops is that during the rest of the year the company is open to security attacks because no one is checking for security problems outside this audit time. The solution to this problem is to go one step further and start measuring and monitoring information security in an organization on a continuous basis. Only through measuring and monitoring information security can an organization find out if the security policy is enforced or not. This idea of measuring and monitoring information security on a continuous basis has many advantages.

One advantage of measuring information security is that results can be obtained on a regular basis. The results can then be used further to detect security risks and solve them before the risks get out of hand. Another advantage is that with measuring and monitoring, statistical and graphical outputs can be obtained at regular intervals. These can be used to support the management of information security. The concept of measurement and monitoring on a regular basis is already implemented in some fields. One of these specific fields is network management.

2. NETWORK MANAGEMENT

A network is a dynamic entity that is always in a state of change. The only way of keeping track of this changing state of a network is through continuous measurement and monitoring on a regular basis. This monitoring and measuring are done from a network management control room, from where the manager can get a corporate wide view of the network status of the company. Table 1 lists some of the aspects that one can find in a typical network environment.

Collect information for the network directly and continuously.
Display the information on a management console.
Drill into specific problems.
Dynamic management based on the collected information.

Table 1: *Aspects of a network management environment.*

The results of this continuous measuring are that the network manager can always be aware what exactly is happening in the network. The results can be displayed statistically or graphically on a monitor. A typical graphical result is depicted in Figure 1A and 1B. The advantage of this type of measuring and monitoring is that the network manager can instantaneously see if something is wrong in the network. The network manager can then immediately address the problem by rerouting the workload or by repairing the connection.

Figure 1A: Network connection

Figure 1B: Network connection down

In this way, through measurement and monitoring, there is a minimum loss of work or inconvenience to clients and users. Without the concepts of measurement and monitoring, the whole idea of dynamic network management will be impossible.

If this concept can be applied to an information security environment, the elimination of many security problems can be done before bigger risks develop. The model that follows is how measuring and monitoring can enhance information security management.

3. A MODEL FOR INFORMATION SECURITY MANAGEMENT THROUGH MEASUREMENT

The question that must be answered now, is how the concepts of measurement and monitoring, and the idea of dynamic network management, can be applied to measure security related activities.

Information security management should therefore be moving in the same direction as network management moved over the last few years. This movement is however much more complex because of the heterogeneity of the underlying systems from which measurement data must be extracted (2). Figure 2 represents a model that can be used to monitor and measure aspects of information security in order to improve management. The proposed model consists of the following components:

- § Security Policy Database
- § User Database
- § Personnel Database
- § Measurement Database
- § Security Manager
- § Statistical output

Each of the components will now be discussed.

Figure 2: A model for measuring security in an organisation.

3.1 Security Policy Database

All organizations in the business world today need to have a security policy in place. This policy will differ from one organization to the next. The reason is that every organization has a different need and level of security. Therefore a security policy can not be directly duplicated from one organization to another one. The basics of the policy can be the same, but most parts of the policy will differ from company to company. Table 2 gives an example of a small clause of a typical security policy.

All users of the company must be security aware.
All passwords must be at least 5 characters.
All passwords must be changed every month.
As soon as an employee resigns, his/her user id and access rights must be deleted from all the company's systems.

Table 2: Part of a security policy.

The Security Policy Database of the model contains the company's information security policy (policies). The information security policy provides the guidelines needed to protect the company's electronic resources. This policy is a physical document, but can also be stored in a database. The policy is written on the

assumption that the employees of the organization will follow the policy in every aspect. One way of knowing if the policy is adhered too by the employees is to start measuring and monitoring.

3.2 Distributed User and Personnel Databases

The information of all the personnel that are currently working in the organization is stored in the personnel database. If an organization does not have a single sign-on facility, the users must have a user id and password for every server he/she wants to logon to. Every server has its own database that stores the ids and passwords of the users that have authority to work on that specific server. The process of multiple logons in an organization must be carefully measured and monitored because security risks can easily develop in this area.

3.3 Measurement System and Database

This measurement database is at the heart of our model for managing security through measurement. This database will be the center point where all the measurement data will be stored.

The measurement database receives its input in two ways. The first is to input data into the database manually. That means transferring information from hard copy into the measurement database – as seen in the model. The information can also come from log files and so on.

The second way in which the measurement database can receive information is to receive the information directly – online - from the relevant systems and databases. All the processing and calculation will be done by the measurement system. The measurement system is directly connected to the measurement database. When observing the monitoring and measuring of information, the measurement system is the active side and the measurement database is the passive side.

This means that the measurement system and database are at the center points of this whole model because the measurement system can access most of the information in the organization. The access level of the measurement system is decided on by the security manager or a higher authority. That means that the measurement system can only access information it has clearance for.

Note that the data from users' passwords are stored in the USER database and not in the measurement database. The measurement system obtains specific information on request from the user's file to measure a specific situation. After the measurement is done and the results are obtained, the information that was obtained from the users database is removed from the measurement database. This is done to prevent sensitive information from being stored in too many places that can lead to a security risk. The measurement database holds the sensitive information just as long as it takes to complete the results.

The whole concept of a measurement system and database is to have one central working unit that constantly measures the security situation in a company, and stores the measurements in the measurement database. The measurement system receives measurement data from different resources, and stores it in the measurement database.

The system then investigates the stored data, for e.g. in comparing it with the specifications in the policy database. Results are then output in different ways, as described below.

After the measurements are received and investigated, the results can be sent to a new database that stores all the results obtained by the measurement system. This is relevant for future use. For example: the result database can compile a whole security profile on all the users – over a time period - in the organizations. That means the security manager does not only measure the security in an organization, but also the employee's security awareness. Another example is that comparisons can be made. This is done to see if an organization's security position has improved over a certain time period or not. Lastly, if the results of a few time periods are compared, it can also help the senior personnel to change the security policy if the results show it to be necessary. The results can also be printed in hard copy. This is shown in Figure 2.

The results can be sent to the Security Manager. The security manager can then have a closer look at the results to determine what the state of the organization's security is. Lastly, the results can be sent to a security web site. This aspect of a secure information security web page is explained later on in the document. But before we go further, let us now consider a few examples of measuring, measurement, data, and results.

3.3.1 Examples

Example 1:

As was mentioned earlier, the security policy is used as a guideline. One of the aspects depicted in Table 2 is that all passwords must be at least 5 characters long and must be changed every month. The measurement system will then compare all the passwords in the user databases to the rule of a minimum of 5 characters. The measurement system can detect which employees are not following the policy. These results can then be send to the security measurement system which can then directly send a message to the user informing him to change his password. The same procedure implies when the system checks if everybody has changed their passwords in a specific month. These actions will all help to properly manage information security in the company.

Example 2:

Another aspect the measurement database can “investigate”, is the clause addressed in the policy that as soon as an employee resigns, his/her user id and access rights

must be deleted from all the company's systems. What the measurement system will then do, is to compare the user database with the personnel database and check if there are any ids and passwords in the user database that do not belong to any present employee of the organization. If there is a user id and a password of an employee that resigned or was fired, the database can forward the results to the security manager. In this way the risk of unauthorized users can be eliminated because the extra id and password can then be deleted immediately.

In this case, the measurement system can operate as follows:

Every night a list of all people who left the company is downloaded onto the measurement database. This list is e-mailed to the operational managers. The next day the user id files of all servers are investigated to see if the relevant ids and passwords have been removed. The status level can then be calculated and passed on to the security manager or to the web site.

3.4 Security Manager

The job of the security manager is to constantly monitor the security situation in the organization. The model will help the manager to measure and monitor the security situation in the organization on a regular basis. As mentioned before, some of the results that are calculated through the measurement system are sent to the security manager. This can be seen in the model. The manager can then immediately see where the security risks are. The manager can then for e.g. go back to these employees and let them know that their passwords are incorrect and that it must be corrected. The manager can then also check if the employee has really changed the password or not. This can be done simply by asking the measurement system to perform the operation that was explained in example 1 again.

All the results produced by the measurement system can then be used to configure statistical figures. These figures must be easy to understand and can be used in meetings with senior personnel.

3.5 Statistical output

The statistical output can be in the form of tables, graphs, charts and many more. These figures are the result of the measured security information and are a reflection of the security situation in the company. The advantage of the results obtained from measurement is that it is available on request at any time. These results are the direct state of the organization's security position because the measurements were done on a regular and continuous basis. The results will be dynamic and will help to secure information in the organization to the maximum.

Figure 3 gives an example of the security situation on passwords. Let's say there are 50 employees. In the first month 12 employees did not change their passwords as stipulated in the policy and from the rest that did change their passwords, 30 of them changed it to an incorrect password.

Figure 3: *Password status of employees*

When looking at these kinds of figures the security manager can immediately see where the security risks are. If the manager wants to see which employees' passwords are incorrect, the following can be done. The manager can ask for the list of the employees with incorrect passwords and send these employees messages to correct the passwords. These results can then be used to identify risk areas and correct them on a regular basis. These results can be shown in many different ways. Another way that can be used is a secure web site.

3.6 The Web as an interface

As mentioned above the results can be shown on the security web site. This security web site is a secure web environment, which means only authorized personnel can access the information shown on the web site. Before the results can be shown it must first be transformed into an easy understandable form. There are a few reasons for this.

The first is that the results are often shown to senior personnel in the organization. These personnel usually have little experience in the security environment. The more user friendly the results are the easier it is for the senior personnel to understand and to make further decisions. By doing this we can see that through monitoring and measuring the security situation in the organization, it is easier to detect risks and make better decisions in the security areas.

The second reason for making results easy to understand is that anyone can immediately see if and where the security risks are. The security manager can then use the results to detect if there are any security problems.

We also mentioned that the one way of looking at security information is to start moving in the same direction as network management. One way of bringing all this together is through the use of a dynamic web site. The security manager can at any time see on the web site where a security risk is. This is to the security manager's advantage because he will see the most up-to-date information on the security situation in the organization on one web site.

One reason of showing these results in a friendly environment is to help the manager manage the security on a minute-to-minute basis and also to help senior personnel make better decisions. In figure 4 the same components were used as in the previously mentioned model. The different servers in an organization can be seen in the figure, in this case there are NT and UNIX servers.

Figure 4: *Security situation in the organization on a specific day*

Figure 4 is showing the results on situations that the measurement system checked. In the figure the white areas are the areas with no security problems. The servers that are marked black have a security problem. If the security manager or anyone else (with clearance) want to know why a server is marked black, they only have to click on the server and further information will be shown. In the case of Figure 4, the NT server is marked black. The reason is that there are 50 users with wrong passwords, 30 users that failed the tutorials and 20 extra user ids and passwords from resigned employees. More specific information can be obtained by double clicking on the specific area. With this way of looking at information security in a secure web environment, information security is made dynamic and therefore more relevant.

4. SECURITY AWARENESS

Another dimension of the measurement model is that it can dynamically address information security awareness. Suppose a web based information security tutorial had been designed, covering all relevant aspects for ex, passwords.

The measurement database can then detect if any employee have an incorrect password for a few months. The system can then send that specific employee a tutorial about passwords. The measurement system can then monitor if the employee did the tutorial and what the results were on the tutorial “test” the employee had to complete in his/her own time. By doing this awareness through the

measurement system, the security manager can keep track of the awareness of each individual employee.

In the pie chart the results of the tutorial can be seen. The conclusion that one can draw from the chart (Figure 5) is that half of the organization have no idea of, or do not care about the security policies. A definitive action must then be launched to make the employees aware of the security issues in the organization. These results of the awareness can then also be added to the web site as we mentioned.

Figure 5: Results of the security tutorials as done by the employees.

5. CONCLUSION

The proposed way of looking at information security is starting to look a lot like the methods used in a typical network management environment. The reality is that information security is dynamic and is constantly changing and reshaping itself. The only way of keeping up-to-date with the security of information is through measuring and monitoring, using a system as described above.

The whole concept of a central measuring facility is starting to grow in organizations. The reason is that only if there is a main measuring facility the security risks and problems can be detected. Some segments of this model are already being implemented in a big organization in South Africa.

The idea of measuring information with a measurement database and system is also starting to expand. The more one knows about the security information in an organization the better information can be managed. One way to find out what the security situation in the organization is, is to measure the security in the organization, this must be done on a regular basis. Only if security is measured on a regular basis can security risk be eliminated that could have been overlooked in an annual audit.

References:

1. Von Solms S.H.1999: "*Information Security Management through Measurement*". Presented as Sec 99, Johannesburg, South Africa.