An Information Security Reporting Architecture for Information Security Visibility

M. Viljoen[1], R. von Solms[2] and M. Gerber[3]
Centre for Information Security Studies, Nelson Mandela Metropolitan University,
Port Elizabeth, South Africa

[1]s20310694@nmmu.ac.za, [2]rossouw@nmmu.ac.za, [3]Mariana.Gerber@nmmu.ac.za

Abstract

The importance of information in business today has made the need to properly secure this asset evident. Information security has become a responsibility for all managers of an organization. To better support more efficient management of information security (IS), timely IS information should be made available to all managers. This paper discusses an Information Security Reporting System Architecture that aims to improve the visibility and contribute to better management of IS throughout an organization by enabling the provision of summarized, comprehensive IS information to all managers.

Keywords

Information security, information security reporting architecture, information security visibility, information security management.

1. Introduction

Information has and will continue to be seen as an extremely important asset in today's business environment (Business Link, 2006; Ernest & Young, 2006). It is, therefore, important that an organization recognizes the critical need to properly protect and secure their information like they would any other valuable asset, for example, their financial assets (Business Link, 2006; ISO, 2006). It is also important that every member of the organization recognize that they play a role and share responsibility for the organizations information security (IS). This is especially true of managers who are responsible for directing and controlling the assets they are answerable for (Whitman and Mattord, 2004). If every member of an organization is to be able to have a share in information security it follows that every person, and especially managers in the organization, should have access to relevant information about the organization's IS. It is therefore important that the appropriate IS reports are available to people at all levels of an organization.

Today there are dozens of tools that can be used to gather and report on IS information (Insecure.org, 2006). Each of these tools have there different strengths and weakness but no single tool is able to completely report on all information security concerns to all levels of the organization. It is, therefore, often difficult for management to see the 'big picture' with regard to information security (B. Robison, 2005).

The objective of this article is to describe and motivate an architecture that makes use of existing network monitoring and reporting tools to enable reporting of IS information to all levels of an organization. This architecture should enable the organizations to have available a customizable, summarized and comprehensive overview of information security. It should enhance the visibility of information security in the organization and should assist managers at different levels of the organization to direct and control appropriate information security concerns more effectively. A prototype has been developed, based on the recommended architecture, as a proof of concept. The prototype system is called the Information Security Reporting System (ISRS). The recommended architecture is referred to as the ISRS architecture.

Before beginning with the description of the architecture, some desirable characteristics for an ISRS architecture that supports efficient information security management will briefly be discussed.

2. Desirable characteristics for ISRF

Managers have the responsibility for directing and controlling the individuals and assets under them in an organization. They will direct (let people know what they have to do) and control (make adjustments as it becomes necessary) these assets in a way that will enable the organization to meet its objectives (Marchewka, 2003). One of the important objectives of an organization should be information security (Whitman and Mattord, 2004). Information security is such an important concern that in many countries a failure to demonstrate due diligence may lead to legal liability (Frazer, 2005; Whitman and Mattord, 2004). Managers should therefore accept responsibility for directing and controlling information security concerns under there sphere of influence. As mentioned above, this is true for managers at all levels of the organization. This includes: staff like CIO, CISO, network and system administrators who work directly with information technology or information security; members of the board and board committees that are responsible for the governance of the organization and managers of other departments of the organization (Corporate Governance Task Force, 2004). The corporate governance task force recommends that there should be a manager in each organizational unit responsible for information security concerns under the control of that organizational unit. They contend that management responsibilities include conducting risk assessments for their units, implementing policies and procedures and testing that information security controls and techniques are being implemented properly for their unit (Corporate Governance Task Force, 2004). If managers are going to have

these responsibilities it follows that they should be equipped with IS information. An architecture that effectively facilitates the reporting of this information will include some of the desirable characteristics mentioned below.

A good reporting system should be configurable to meet the needs of the different managers. Different managers will have different responsibilities and amounts of influence when it comes to information security. For example a manager in the human resource department, a manager in the information technology department and the CEO of an organization are all going to have different responsibilities, amounts of influence and interest in information security. It is therefore important that each manager receives appropriate IS information that pertains to that manager.

Furthermore, it would be of great value if the relevant information for a particular user is presented in a manner that is easy to understand and shows the state of IS as a whole or the state of a particular IS concern at a glance. This will contribute to enabling managers to take corrective actions as they see that things are going wrong.

An ISRS architecture will also be of value if it assists managers to measure how well they comply with internationally accepted IS standards. Standards and policies are essential for the proper management of information security (Whitman and Mattord, 2004; Purser, 2004). Security standards, such as ISO/IEC 17799, prove invaluable in helping managers at the governance level to define information security goals, organizational information security standards and effective management practices (ISO, 2005). It is also valuable for information security policy development.

It would, moreover, be desirable if the ISRS is highly extensible and flexible in that it allow for different tools to be easily integrated with the system. Although security standards, such as ISO/IEC 17799, will provide general guidance, each organization is different, and will make use of different tools and technologies to implement their information security controls. The amount of money that an organization has to spend on information security alone will cause different organizations to have tools and systems that differ widely. Today there are dozens of tools that can be used to gather and report on IS information (Insecure.org, 2006). Insecure.org mentions some of these such as SNORT, Nessus, NetStumbler, Nmap, MBSA. As mentioned before, each of these tools have there different strengths and weakness but no single tool is able to completely report on all information security concerns to all levels of the organization. This often makes it difficult for management to see the ‘big picture’ with regard to information security. Advances in technology will also undoubtedly lead to the development of new and improved monitoring and reporting tools that make new IS information available. There are also organizations that have IS tools that have been custom written for them. The challenge is therefore to develop architecture that easily interfaces with different tools and modules as the need arises to gather information form these different tools and to present it in a useful manner.

It would be beneficial to have an architecture that is scalable and supports large or small heterogeneous distributed environments. Many organizations today have IT infrastructures that incorporate different platforms. For example it is not uncommon

for one organization to run Windows and UNIX operating systems. There is also a lot of work been done in the area of distributed computing. An architecture that allows for interfacing across platforms to gather and report on IS information would therefore be of great value.

Another desirable characteristic of an ISRS is that it will facilitate new ways of correlating and analyzing data. It would be useful to pool information gathered by different tools with different file formats and application programming interfaces such as SNORT, Nessus, NetStumbler, Nmap, MBSA in such a way that allows one to find new relationships between the information form each tool, show the history of the specific information gathered, do new forms of analysis on the combined information etcetera.

In summary it can be said that the desirable characteristics for ISRS architecture should include that it will be standards based, highly extensible, distributable and show the overall, summarized state of information security at a glance.

In the following section an ISRS architecture will be described as an envisioned solution that includes these desirable features.

3. ISRS Architecture

An ISRS architecture has been designed to incorporate the desirable features described above. A prototype system based on this architecture has been developed to test and demonstrate the feasibility of an ISRS that integrates information from different toolsets, and makes it visible to managers at different levels of an organization.

In developing the ISRS architecture the assumption was made that the best approach for an organization would be to link all their information security initiatives to controls specified by best practice standards such as ISO/IEC 17799 or CobiT. Every control is linked to a set of key performance indicators that are used to indicate the measure of compliance with that control. The ISRS accomplishes this by means of a survey component that is based on the SANS Audit Checklist compiled by the SANS institute (Thiagarajan, 2006). The checklist is based on the ISO/IEC 17799:2005 standard. This checklist consists of 11 main categories. These categories are used as security areas or controls in the current prototype implementation of the ISRS architecture. The key performance indicators can be grouped into the following categories: survey results, the progress of tasks or activities, and metrics.

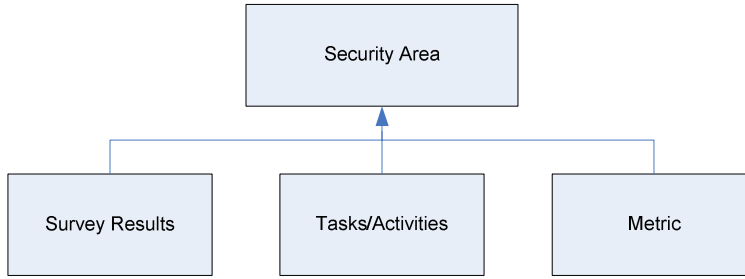

Figure 1: Categories of key performance indicators that are linked to security areas in the current prototype implementation of the ISRS architecture.

Each security area has a number of questions (based on the SANS audit checklist) related to it. In the ISRS system each of these questions can be assigned a weighting to indicate the level of importance that the company assigns to that question. The question also has three other important attributes associated with it. These are: The *"min acceptable"* value. This value indicates the minimum percentage of compliance that is accepted by that company for that specific question. The *"desired value"* to indicate to what level the company would like to have compliance with the question. The "actual value" which indicates to what extent the company is complying with the question.

Besides the questions a security area can also have a number of tasks related to it. With the ISRS system users can be assigned tasks that are related to one or more security areas. The task progress is updated by users to reflect whether the tasks progress is *acceptable*, *good* or *unacceptable*. A task is also assigned as critical or not.

A security area can also have security metrics associated with it. A metric can be gathered by means of available tools, modules or by audit/survey components. To illustrate a metric could be percentage of updates completely installed on machines in an organization. The information for this metric can be collected from tools like MBSA and Nessus by means of web service based modules. A metric could also be percentage compliance with the organizations physical security policy and information for this metric could simply be collected from a completed electronic questionnaire. Like the questions from the SANS audit checklist, a metric has "min acceptable", "desirable" and "actual values" associated with it.

The overall health of a security area is determined by using the weights and values associated with the questions, tasks and metrics associated with that area. The benefit of this approach is that it provides the managers of the organization with a standards-based way to look at IS and enables the level of compliance with controls to be displayed simply. By means of portal software and an operational database it is possible to link specific users to key performance areas and/or to specific metrics. This contributes to making it possible to display the relevant information to different individuals.

Another desirable characteristic of an ISRS is that it will facilitate new ways of correlating and analyzing data. To meet this objective the ISRS architecture makes use of a data warehouse to store the IS information gathered. Within the data warehouse there is a general purpose star schema that can be used to store the general information about metrics. If this general purpose schema does not meet the needs of the metric and information that has to be stored in relation to it another star schema will have to be added to the warehouse. Data warehouses are designed especially so that this type of analysis and can be done efficiently and easily to improve decision support (Kimball and Ross, 2002).

Yet another desirable characteristic of a good ISRS would be that it be extensible and distributable. The ISRS architecture allows for a system that would accomplish this by making use of a service oriented architecture approach. Figure 1.2 depicts the components of the ISRS architecture as described below. Briefly ISRF makes use of web services to interface with and retrieve certain information from existing monitoring and reporting tools. A Data Access web service is used to write the information to a data warehouse and to access information from the warehouse and operational database. A scheduler is a program that queries the operational database for a list of jobs (web service functions) that it must run and information pertaining to the running of these jobs and then makes the necessary calls to the web services that encapsulate the monitoring and reporting tools. Web service interfaces to various visualization tools can be plugged in to facilitate the visualization of the information stored in the data warehouse. The use of web services to encapsulate existing tools makes sense for a number of reasons. Different organizations may for many reasons have a wide array of monitoring tools that collect information security information running in their systems. With this framework, when a new tool becomes available it is easy to retrieve the information it exposes by writing a new web service that can interface with the tool or make use of an existing web service. Which web service should be called, how often this should be done and other information to do with the invocation of this service must then simple be added to the operational database from where the scheduler will retrieve it and invoke the service. The service will in turn have the responsibility of interfacing with the data access web service to store the data in the appropriate place in the data warehouse. As can be seen this approach to gathering information is very extensible because new tools and the metric associated with these tools can easily be integrated into the system as the need arises. Web services are commonly used to provide a standard way of remotely invoking functionality across different platforms (Kalani and Kalani, 2003, p 288-290). This makes the framework highly scalable and flexible since it means that the different tools and web services used can either all be located on a single machine, or they can exist on different virtual machines one a single physical machine (which allows for a box that can be plugged into a machine and with a bit of configuration can be used as a tool to provide information security reports for an organization), or they can be distributed across the infrastructure of an organization.

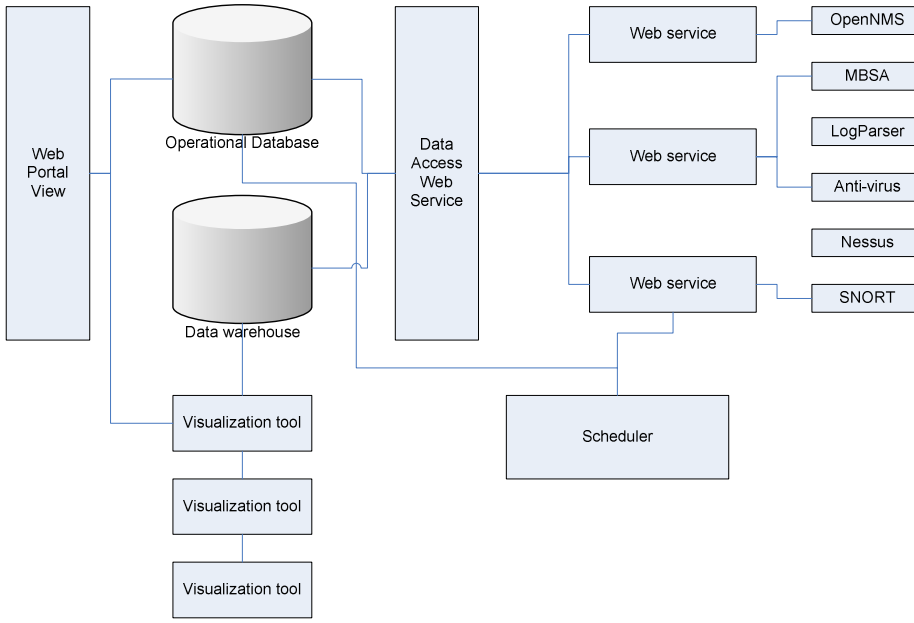

Figure 2: Components of an ISRS architecture.

The following illustrates how this architecture could be used practically. The ISO 17799 control number 6, Communications and Operations Management requires that there are controls implemented to detect, prevent and recover from malicious code. A member of the board may want to know what initiatives and controls are in place to protect the organization against malicious software and to what extent have the controls been implemented. The board may also wish to see evidence that the situation with regard to malicious software is improving over time. Suitable metrics to measure performance in this area might be the percentage of systems with up to date anti-virus patterns installed. The ISRS system should be able to gather information from the anti-virus system (possibly though a web based management interface used by the AV system or maybe from log files created by the AV system). The ISRS system will likely store the information in a data warehouse, and make it visible through a visualization subsystem.

4. Conclusion

The ISRS architecture has several features that make it a desirable approach to follow when implementing an ISRS to improve visibility of information security in the organization and to use as a means to aid in better management of information security throughout an organization.

By following a standards-based approach and making use of technologies such as web services, data warehouses, operational databases and visualization tools the

architecture should be able to be used to enhance the visibility of information security in the organization. It should also allow for a customizable, summarized and comprehensive overview of IS concerns to managers. This should in turn help managers to direct and control IS concerns more efficiently. The principles of service oriented architecture applied in the design of the architecture also make the ISRS extensible, flexible and distributable.

References

Business Link. (2006). Information security best Practice [Online]. URL http://www.businesslink.gov.uk/bdotg/action/printguide?r.l1=1073861197&r.l3=1075406921&topicId=1075406921&r.t=RESOURCES&r.i=1075406928&r.l2=1075408323&r.s=pg

Cisco systems. (2006). Simple network management protocol. [Online] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/snmp.htm

Corporate Governance Task Force. (2004). Information security governance: a call to action [Online]. URL http://www.cyberpartnership.org/
InfoSecGov4 04.pdf

Ernst & Young. (2006). Achieving Success in a Globalized World: Is Your Way Secure? Global Information Security Survey 2006 [online]. URL http://www.ey.com/global/content.nsf/International/Assurance_&_Advisory_-_Technology_and_Security_Risk__Global_Information_Security_Survey_2006

Frazer, A. (2005). Sarbanes-Oxley Compliance Journal. Due Diligence risks in network security. [Online] URL http://www.s-ox.com/Feature/detail.cfm?articleID=1148

Insecure.org (2006). Top 100 network security tools. [Online] URL http://sectools.org/

ISO. (2006). ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management [Online]. URL http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

Kalani, A., Kalani, P. (2003). MCAD/MCSD Developing XML Web Services and Server Components with Visual C# .NET amd Microsoft .NET Framework. USA:Que Publishing.

Marchewka, J.T. (2003). Information technology project management. Providing Measurable Organizational value. USA:John Wiley & Sons.

Purser, S. (2004). A practical guide to managing information security. [Online] URL http://books.google.co.za/books?id=mczgkqHSIXUC&dq=why+are+information+security+standards+so+important&pg=PA147&ots=uY2Zws5uD4&sig=--T3VZUI0Fg4fir6vsc-9MmsztU&prev=http://www.google.co.za/search%3Fhl%3Den%26q%3Dwhy%2Bare%2Binformation%2Bsecurity%2Bstandards%2Bso%2Bimportant%26meta%3D&sa=X&oi=print&ct=result&cd=2#PPR9,M1

Robison, B. (2005). Security dashboard - Are high-level views the answer to getting managers the cybersecurity status information they need to make decisions? [Online] URL http://www.fcw.com/article91327-11-07-05-Print#related

Swanson, D. (n.d.). IT compliance Institute. Ask the Auditor: Who is responsible for information security [Online]. URL http://www.itcinstitute.com/display.aspx?id=1823.

Thiagarajan, V. (2006). SANS Audit Checklist. [Online] URL http://www.sans.org/score/checklists/ISO_17799_2005.pdf?portal=f36013c72bc89932f16f84f4f89245dc

van den Bogaerdt, A. (2006). rrdtutorial. [Online] URL http://oss.oetiker.ch/rrdtool/tut/rrdtutorial.en.html

Whitman, M.E., Mattord, H.J. (2004). Management of information security. Canada:Thomson course technology.