MoVIS: A Model for the Visualization of Network Information Security

(Work-in-Progress Paper)

C. Olivier, R von Solms and N.L.O. Cowley
Faculty of Engineering: Departments of Information Technology and Computer Science & Information Systems
PO Box 77000, Nelson Mandela Metropolitan University, Port Elizabeth, 6031
Tel: +27 41 5043604, Fax: +27 41 5049604
Email: {colivier, rossouw.vonsolms, lester.cowley}@nmmu.ac.za

Abstract – Information has become a very important asset and a standard item on the agenda for most Boards of Directors. More legislation and regulations are introduced internationally on a regular basis to manage and govern information effectively and securely. Thus, information is essential for business well-being at all levels, from the operational/technical level, through the management levels to the corporate/governance level. This paper describes progress made in presenting a novel framework of a model whereby information security related management information can be visualized in such a way as to effectively manage information security.

Index terms – information governance, information security, information security management, information visualization

I. INTRODUCTION

The value of information has grown to become very important to the existence of most organizations today. Information, and its effective utilization, can provide an organization with a competitive advantage, but it can also cause the destruction of the organization if misused or compromised. For this reason, it is imperative that this important asset is protected adequately.

Information security is the process whereby information assets are protected and, because of the criticality of this process, it should be part of corporate governance in every organization. "The road to information security goes through corporate governance." [2] Corporate Governance entails directing and controlling activities carried out by executive management and the board in order to achieve the required outcome of the organization, aligned with its visions and mission and to satisfy the demands of the shareholders.

Thus, information about the protection of business information within the organization is critical to the Board of Directors, at the governance level of an organization, in fulfilling their mandate of directing and controlling the utilization and application of organizational assets.

Further, information security must become an integral part of core business operations. [4] Information is used everywhere in an organization by various employees. Managers, as data owners at the management level of an organization, need to take responsibility for the secure utilization of the data they own. To do this effectively, these managers need to receive information on the data they own and need to secure.

Lastly, operational administrators (network, database, firewall, etc.), at the operational/technical level of an organization, also need to secure information and related IT resources by identifying, implementing and monitoring information security controls. A lot of related information is continuously gathered by the audit logs of most of these resources, providing valuable information about current utilization. This information needs to be interpreted by the information security officer to identify potential information security breaches and to react as soon as possible.

From the above, it can be seen that information security is applied and required on three organizational levels. These levels are the corporate/governance level, the management level and the operational/technical level. Each of these levels requires different sets of information, in different formats, at different time intervals and levels of abstraction.

"As the role of information grows more critical with each passing year, so do the challenges that come with managing it well." [3] Each level of the organization depends on each other. The governance level needs appropriate information at the correct level of abstraction for them to use quickly and effortlessly to determine whether the company is working towards its mission and visions. This will enable the governance level to direct the rest of the organizational structure more effectively to be, and stay, in line with the company objectives. Therefore, in order to effectively manage information security, all levels need visual representations of the relevant information whether in text, graphs, images etc. These will aid in the interpretation, understanding and communication of the information across the three levels in the organization.

"To ensure business continuity the security of corporate information is extremely important." [1] But this will only be effective within the company if all levels of the organization obtained the relevant information in the right format and level of abstraction. Therefore visual representations of that information are a step higher on the 'importance ladder' than just merely securing the information to ensure business continuity.

In the mature financial world, reporting models evolved over many years to ensure that every level within the financial structure has the adequate information in the correct format and level of abstraction. The field of information security is still very immature, but information security and the management thereof is just as important as

security in the financial environment. If information security is compromised, it can have serious consequences as a result. There is therefore a need for a similar visualization and reporting structure to optimize information security management.

The lack of relevant information mechanisms, at the right levels of abstraction and at the right time intervals, is a general problem in all organizations. It impedes an organization in effectively managing and governing the protection of information, at the operational, managerial and governance levels within an organization. [6]

This project aims at addressing this problem by proposing a way to effectively manage and visualise the information within the three levels through a model implementation.

II. PURPOSE OF RESEARCH

The primary objective of this project is to develop a model (MoVIS) that will ensure that information security related information is visualised in such a way that the process of information security management and governance is optimised.

In meeting the primary objective, the following secondary objectives will also be addressed:

1) Identify relevant information sources required to control information security at the operational, managerial and governance levels.
2) Define the levels of abstraction, timely intervals and format of presentation of this information.
3) Develop ways and means of visualising this information in a way suitable to the responsible parties in each of the three levels in the organization.
4) Develop a prototype system, based on the model, to gather, summarise and present information security related information at the various levels of interest.

III. STATUS OF PROJECT

At this stage of the project an established model, Figure 1, was found that will form the basis in representing and proposing the financial reporting and management model. This financial model will be used to infer MoVIS, which will be used to represent the meta-data for the reporting of network information security related information of the different levels. It will be a separate model mapping to the financial reporting model.

The model in Figure 1 represents two views. When viewed from the left to the right it shows an IT perspective, where the focus is on data processing and the state of information to the business. When viewed in reverse, it focuses on business results and the actions and knowledge needed to achieve those results. [5]

From this model, one can derive a financial model, which will have an independent existence, proposing that data resides on the lowest (operational) level of the organization and information and knowledge on the management and governance levels. These are then used for decision making (actions) which will derive from the results that the organization ultimately would like to gain. Unfortunately, because of page restrictions, a visual representation of this complex financial model, which incorporates the three levels as described above, could not be shown in this paper.

This financial model is almost finalized with MoVIS still in its foundation stages.

Figure 1, Information in context [5]

IV. FUTURE WORK

Once the financial reporting model is finalized, MoVIS, which will be based on the financial model and used for the visual representations of the information at the three levels, will be developed as a solution to represent the relevant information at the various levels. The information and knowledge for these visual representations will be gained from studying an existing network.

A prototype system will be developed, based on MoVIS, to demonstrate that it can be implemented and ensure that the information is gathered, summarized and presented to the different levels of concern. An existing system will be used to mine the data that will be used by this system for the visual representations.

This prototype system will support the claim that MoVIS enables effective information security management and governance in any organization. It will also ensure compliance which will assist in the management of network information security.

V. CONCLUSION

A network information security management model is needed to assist in the effective management of information security at the three levels (operational, management and governance) of an organization. Systems based on this model will ensure that all three levels in the organization obtain the required information in the correct format and levels of abstraction in such a way as to ensure effective interpretation, understanding and communication of the visual representations of the security information.

VI. ACKNOWLEDGMENTS

We would like to thank the Telkom Centre of Excellence Programme and the Nelson Mandela Metropolitan University for making this research possible.

VII. REFERENCES

[1] Baxter, G.,R.Marcella, et al. (1999). *Corporate information security management.* New library world **100**(1150): pp213 – 227.
[2] Changepoint. (2004). A White Paper, Governance: The Board's – and the CIO's – Business
[3] EMC Corporation. (2004). Enabling Regulatory Compliance Through Information Lifecycle Management: p1. From http://www.bitpipe.com/ detail/RES/1090346890_635.html. Cited March 31, 2005
[4] Entrust. (2004). A White Paper, Information Security Governance.
[5] Peppard, J., & Ward, J. (2002). Strategic planning for information systems (3rd ed.). New York: Wiley: p207.
[6] von Solms, R. (2005). Business information: Your company's time-bomb? *Infocom*, March 2005.

Carika Olivier received her BTech: Information Technology degree in 2004 from the Nelson Mandela Metropolitan University (NMMU). She is presently doing her MTech: Information Technology degree at the NMMU.