Complexity Reduction in Information Security Risk Assessment

Glourise Haya
Center for Information Systems and Technology
Claremont Graduate University
Claremont, CA USA
glourise.haya@cgu.edu

ABSTRACT
Results of research done by Dlamini et al. [5] clearly show information security was once focused around technical issues. However, over time, that approach transitioned to a more strategic governance model where legal and regulatory compliance, risk management, and digital forensics disciplines became the significant contributors in the domain. This focus has resulted in a proliferation of information security risk assessment models, which on the whole, have not necessarily helped to reduce risks or appropriately respond to security events. This research seeks to develop a new information security risk assessment model through the aggregation of existing models.

Categories and Subject Descriptors
H.1.1 [**Models and Principles**]: Systems and information theory – value of information; C.4 [**Computer Systems Organization**]: Performance of systems – *measurement techniques; Reliability, availability, and serviceability; modelling techniques;* K.6.5 [**Security and Protection**]: Authentication, Invasive software (e.g., viruses, worms, Trojan horses), Physical security, Unauthorized access (e.g., hacking, phreaking).

General Terms
Management, Security, Standardization, Risk

Keywords
Information Security; Risk Assessment; Risk Management

1. INTRODUCTION
Advances in technology and lower costs for storage have allowed organizations to capture and save more information than could have been imagined decades ago. Cyber-criminals have begun to see the value of this information and use it for various motives. Organizations have a fiduciary responsibility to protect information and its associated infrastructure components used to store and transmit it [8] as key assets [2]. "Risk assessments are the first step in determining how to safeguard enterprise assets and reduce the probability that those assets will be compromised [1, p. 344]."

Saleh and Alfantookh [7] reported there were over 200 Information Systems (IS) risk assessment models. This number has been steadily increasing over the years. Reviewing all of these models to find the ideal one for an organization is a daunting task even for a consulting firm. To-date, there has been no aggregation of these models. The complexity, required time commitment, and sheer number of models to be reviewed makes it next to impossible for small and medium-sized organizations to select one that best fits their needs, size, or industry.

"[A]dvancements in the field of technology require more sophisticated decision-making approaches when it comes to security-technology investments as well as data- and digital-asset protection" [3, p. 25]. These advancements put pressure on the domain of information security risk management to ensure risk models are able to address the newest threats and vulnerabilities.

News reports signify the possibility of churches and faith-based non-profit groups becoming the next generation of targets for cyber-criminals. Individual churches may have congregations that range from less than 100 to over 40,000 members. Non-profit faith-based groups may service from hundreds to thousands of people. Regardless of their size, their information security needs are the same or very similar. The skills of decision makers in these groups will vary greatly. Additionally, people move in and out of roles within these organizations frequently as many are volunteers. This scenario calls for a holistic, yet simple and easy to use information security risk assessment model that would span the breath of these institutions. This research seeks to develop a risk management model for churches and non-profit faith-based groups.

2. RELATED WORK
Information security risk assessment models fall within a three-tier classification system: Tier 1) Paper-based or automated model; Tier 2) Qualitative, Quantitative, or Mixed methodology; and Tier 3) Research Goal: Models that compare existing frameworks; Models that add functionality to existing frameworks; or New frameworks. Comparison models have been created specifically to help organizations make a selection between a handful of existing models. Models that add on to existing models seek to enrich the functionality or fill a gap. New models are created when researchers feel none of the existing models meet their needs. As previously stated, there has been no research focused on consolidating existing models in order to reduce complexity.

SIGMIS-CPR '15, June 04-06, 2015, Newport Beach, CA, USA
ACM 978-1-4503-3557-7/15/06.
http://dx.doi.org/10.1145/2751957.2755506

3. RESEARCH QUESTIONS

As stated above, this research seeks to propose a risk assessment model for churches and faith-based groups. This research will answer the following questions:

1. Are there existing risk assessment models that will meet the needs of small and medium sized organizations such as churches and faith-based groups?
2. Can the similarities and differences of existing models be identified, categorized, and combined to make a single holistic model (simplification)? If so, could the design of such a model make it easy to add new research models in the future?
3. Would the structure of the design make it possible to construct an automated, interactive interface that would at a minimum provide a visual comparative display of easy to understand selectable functionality?
4. Could this new model be used by all churches and faith-based groups regardless of size and technical sophistication to protect their assets?

4. METHODOLOGY

A design research approach will be used. Steps in the process include: 1) Perform a literature search to identify potential journal articles for review. 2) Perform an ethnographic content analysis (ECA) [4] to: eliminate articles that will not be included in the study; make an in-depth analysis of the framework in each article to identify taxonomies used, functionality and special features; compare each framework to all other frameworks in the study to identify similarities and differences; and categorize taxonomies, functionalities, special features, etc. 3) Design and develop a database to capture the outputs from Step 2 above. 4) Develop a web-based application using the database that will serve as the end-user interface. 5) Perform a proof of concept with the help of churches and faith-based groups. 6) Document and report results of study.

5. CONTRIBUTION TO EXISTING KNOWLEDGE

From a human perspective, this research addresses the information security needs of small and medium sized organizations such as churches and non-profit faith-based groups. Drucker [6] described three assumptions organizations need to maintain in order to remain relevant. One of the assumptions, mission, is related to how an organization sees itself contributing to the economy and society at large. Churches and faith-based groups exist to contribute to society at large. Undertaking this research project establishes a partnership with these groups and ultimately would contribute to society at large for myself as well as for researchers that will build on it in the future. It provides a feeling of having done something important that goes beyond just the research itself. To-date, there has been no research calling for the simplification and aggregation of information security risk management models. Advantages of simplification include, but are not limited to:

- Bringing the research community together to focus on the improvement of a single model;
- Providing more visibility for academic research in the domain;
- Paving the way to ensure better and more effective information security solutions due to a concentrated focus;
- Providing a visual and interactive interface that will be easy for practitioners in organizations of any size in any industry to use;
- Reducing the number of new information security risk assessment frameworks due to the ability to incorporate new functionality in one model.

6. ACKNOWLEDGMENTS

I wish to thank Dr. Lorne Olfman and Dr. Tamir Bechor for their support and advice.

7. REFERENCES

[1] Atyam, S. Effectiveness of security control risk assessments for enterprises: Assess on the business perspective of security risks. *Information Security Journal: A Global Perspective*, 19, (2010), 343-350. DOI: 10.1080/19393555.2010.514892.

[2] Behnia, A., Rashid, R., and Chaudhry, J. A survey of information security risk analysis methods. *Smart Computing Review*, 2(1), (2012), 79-94

[3] Bojanc, R. & Jerman-Blažič, B. A quantitative model for information-security risk management. *Engineering Management Journal*, 25(2), (2013), 25-37.

[4] Bryman, A. Social Research Methods (4th Ed.) Oxford University Press, Inc., New York, NY, 2012.

[5] Dlamini, M., Eloff, J, and Eloff, M. Information Security: The moving target. *Computers and Security, 28*, (2009), 189-198. doi: 10.1016/j.cose.2008.11.007

[6] Drucker, P. & Maciariello, J. The Theory of Business. In Management (pp. 83-96). Harper Collins, New York, NY. 2008.

[7] Saleh, M. and Alfantookh, A. New comprehensive framework for enterprise information security risk management. Applied Computing and Informatics, 9(2), (2011), 107-118.

[8] von Solms, R. and Niekerk, J. From information security to cyber security. *Computers & Security*, 38, (2013), 97-103.