The House of Security: Stakeholder Perceptions of Security Assessment and Importance

Wee Horng ANG, Vicki DENG, Yang LEE, Stuart MADNICK,
Dinsha MISTREE, Michael SIEGEL, Diane STRONG, Richard WANG

Working Paper CISL# 2007-06

July 2007

Composite Information Systems Laboratory (CISL)
Sloan School of Management, Room E53-320
Massachusetts Institute of Technology
Cambridge, MA 02142

The House of Security:
Stakeholder Perceptions of
Security Assessment and Importance

Wee Horng ANG[1], Vicki DENG[1], Yang LEE[2], Stuart MADNICK[1], Dinsha MISTREE[1], Michael SIEGEL[1], Diane STRONG[3], Richard WANG[1]

[1] Massachusetts Institute of Technology
[2] Northeastern University
[3] Worcester Polytechnic Institute

Abstract

In this paper we introduce a methodology for analyzing differences regarding security perceptions within and between stakeholders, and the elements which affect these perceptions. We have designed the "House of Security", a security assessment model that provides the basic framework for considering eight different constructs of security: Vulnerability, Accessibility, Confidentiality, Technology Resources for Security, Financial Resources for Security, Business Strategy for Security, Security Policy and Procedures, and Security Culture.

We designed and performed a survey of about 1500 professionals in various industries, levels, and functions resulting in a gap analysis to uncover differences (1) between the different constructs and aspects of security, (2) between different enterprise stakeholder roles, and (3) between different organizations. This paper briefly describes the development of the security constructs and some of the preliminary findings.

Introduction

Security is crucial for the success of any organization and many organizations have adopted stringent security policies. Though many of these security policies are valuable, an organization is limited by the amount of resources it can devote to protecting its flows of information. Security costs can be incurred monetarily (e.g., the price of a new firewall) or non-monetarily (e.g., requiring employees to use convoluted passwords or confusing software-protection programs). An organization's goal should be to develop the most cost-effective approach to security, which is further complicated by the different priorities of the various stakeholders in the organization. In addition, as organizations evolve into extended enterprises, which includes ties with suppliers, customers, and other partners, there will be a significant increase in the number of stakeholders and thus a wider range of security requirements.

Purpose of Study

Many scholars have approached the study of security by focusing specifically on the detailed elements of the security systems themselves, such as effectiveness of different cryptographic codes or firewall technologies, or have measured specific events, such as mean-time-to-failure. However, these efforts do not look at security holistically and commonly neglect to consider the members of the organization themselves. They especially neglect to consider the ***perceived needs and security views*** of an organization's members.

In this project, we seek to identify the similarities and differences both within and between different organizations with respect to perceptions of security held by different members of the organization. To accomplish this, there are three major objectives:

- To identify how perceptions both shape and should shape decisions in investments in security systems, with a particular focus on identifying the most important ***constructs of security***, as perceived by the individuals in the organization.
- To identify differences between the importance and assessment of the various security constructs among different organizational systems (e.g., comparing two different companies).
- To identify differences between the importance and assessment of the various security constructs among organizational systems (e.g., comparing the views of mid-level managers to that of the senior management).

The House of Security: Analysis Methodology

Through a comprehensive literature review, web searches, and several surveys, researchers at MIT have identified about 300 security issues. These security issues were found to be grouped primarily into eight meta-groupings, or ***constructs***, as follows: *Good Security* provides Accessibility to data and networks to appropriate users while simultaneously protecting Confidentiality of data and minimizing Vulnerabilities to attacks and threats. *Good Security Practice* goes beyond technical IT solutions. It is driven by a Business Strategy with associated Security Policies and Procedures and implemented in a Culture of Security. These practices are supported by IT Resources and Financial Resources dedicated to Security. These eight constructs form our ***House of Security***, as shown in Figure 1.

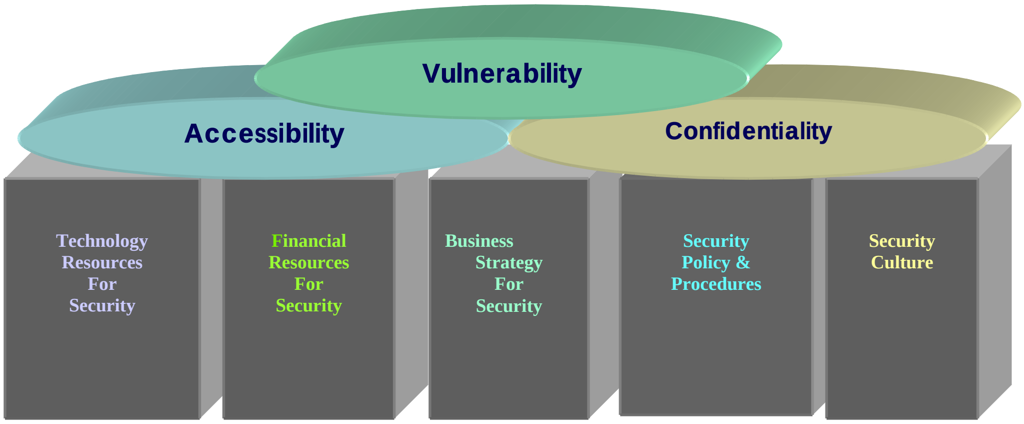
Vulnerability
Accessibility
Confidentiality
Technology Resources For Security
Financial Resources For Security
Business Strategy For Security
Security Policy & Procedures
Security Culture

Figure 1. The Eight Constructs Organized as the House of Security

We chose to use a survey, broadly distributed to an array of members of an organization (from employees to top-level managers across all functional areas), to identify variations in *perceptions* of security. In our survey, respondents are asked to rate a series of statements about their perception of security, specifically:

(1) the current state of that security issue within their organization;
(2) the important of that security issue for their organization;
(3) the current state of that security issue for a partner organization; and
(4) the importance of that security issue for the same partner organization.

A key part of this study involves performing ***gap analyses*** (e.g., how much does the perception of the current state of that security issue in the organization differ from the perception of the importance of that security issue.) Such gaps represent opportunities for improvement and better understanding within the enterprise and across the extended enterprise. When current status is below the desired level, these represent areas for possible improvement. When there are differences in status or gaps perceived among different stakeholders, these represent areas for investigating sources of the differences: the gaps may represent misunderstandings or the gaps may represent differences in local knowledge and needs. While a key goal of this survey is to measure perceptions of the different constructs of security, we also want to understand the causes of these perception variations. For this reason, this survey also asks a series of demographic questions, such as the size of the organization and its industry.

Finally, we evaluated the quality of the survey instrument by measuring the *statistically significance* of the questions and the constructs, the *reliability* of the constructs (by computing Cronbach Alphas) and the *content, convergent* and *discriminant validity* of the constructs.

Preliminary Results of Pilot Study

In our initial pilot survey of about 200 people, interesting results arose in several categories: (1) the individual questions, (2) the constructs, and (3) the construct gaps. Some examples are presented here.

(1) Individual Questions: Respondents were asked to assess whether "people in the organization are aware of good security practices." They were then asked the importance of that issue in the organization. This was to be answered on a 7-point scale (where 1 means "true to a small extent" and 7 means "true to a large extent.") The overall results are shown on the top line of the graph shown in Figure 2. The current assessment (marked MA) is the left part of that line (in yellow) while the importance (marked MI) represents the entire line. The right part of the line (in blue in the top line) represents the gap. In this example, there was a large gap, statistically significant at the 99.99% level. This means that awareness of good security practices falls far short of what is perceived to be needed among the respondents. When comparing individual organizations, such as Company X and Company I, we also observed major differences in assessment, importance, and gap size[1]. One of the goals of this research is to understand these differences.

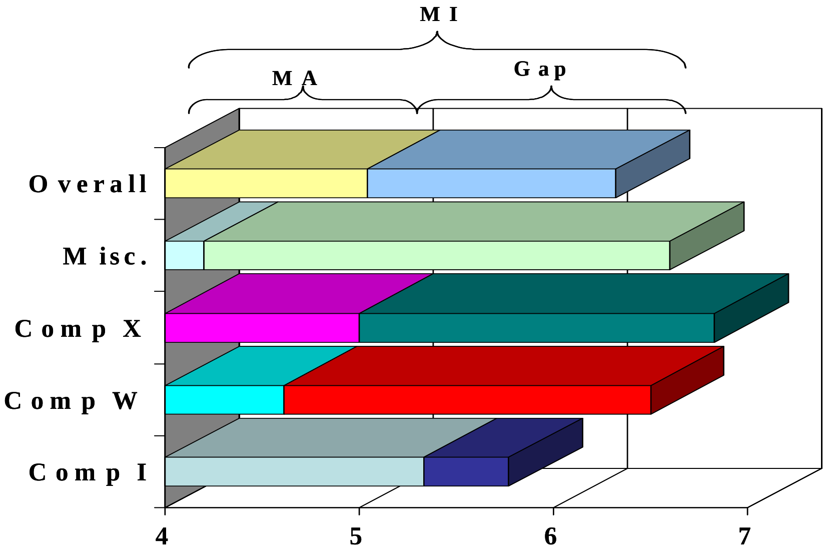

Figure 2. Responses to an Individual Question:
"People in the organization are aware of good security practices."

(2) Constructs: The questions in the survey are aggregated to form the *eight constructs* that constitute our House of Security. An example of the assessment (current situation) for 3 companies (X, W, I) of all 8 constructs can be seen in Figure 3. We can see that for a given company, the assessment values are likely to differ for the eight constructs. Comparing companies, we can see both significant similarities and differences between Company X and Company I. For example, these companies are very similar in their perceptions of "Accessibility" but very different in their perceptions of the state of "Security Policy."

[1] At this point we are not focusing on the specifics of companies X and I, just that there can be considerable differences between companies.

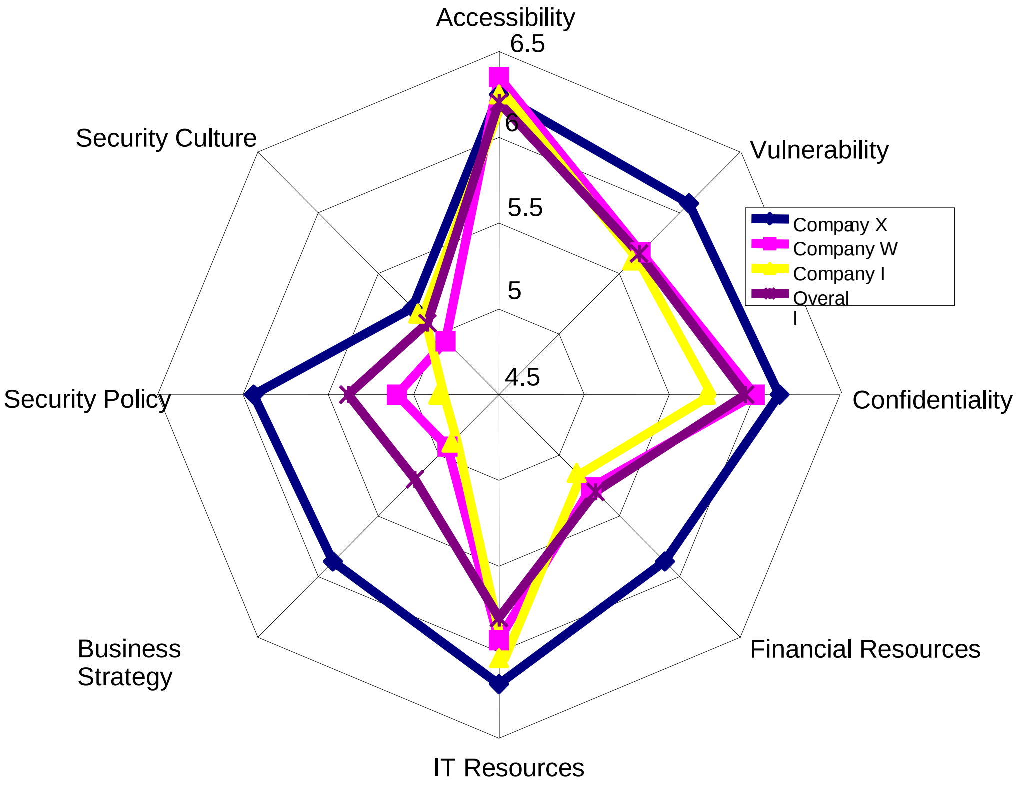

Figure 3. Constructs responses – by company

(3) *Construct gaps:* Although viewing the actual values of each of the constructs provides some insights, it is often more interesting to examine the "gaps." For example, one organization might have an assessment of "5", but if it views that construct as only having an importance value of "5", the gap would be zero and it might be content. Whereas, if another organization had an assessment of "6", but viewed that construct importance as being "7", that is a gap of 1 and might indicate an area for improvement. Some examples of these construct gaps are seen in Figure 4. Comparing companies X and I again, we observed some differences in gaps (which might be considered measures of discontent) in "Accessibility" but much bigger differences in gaps in "Security Culture."

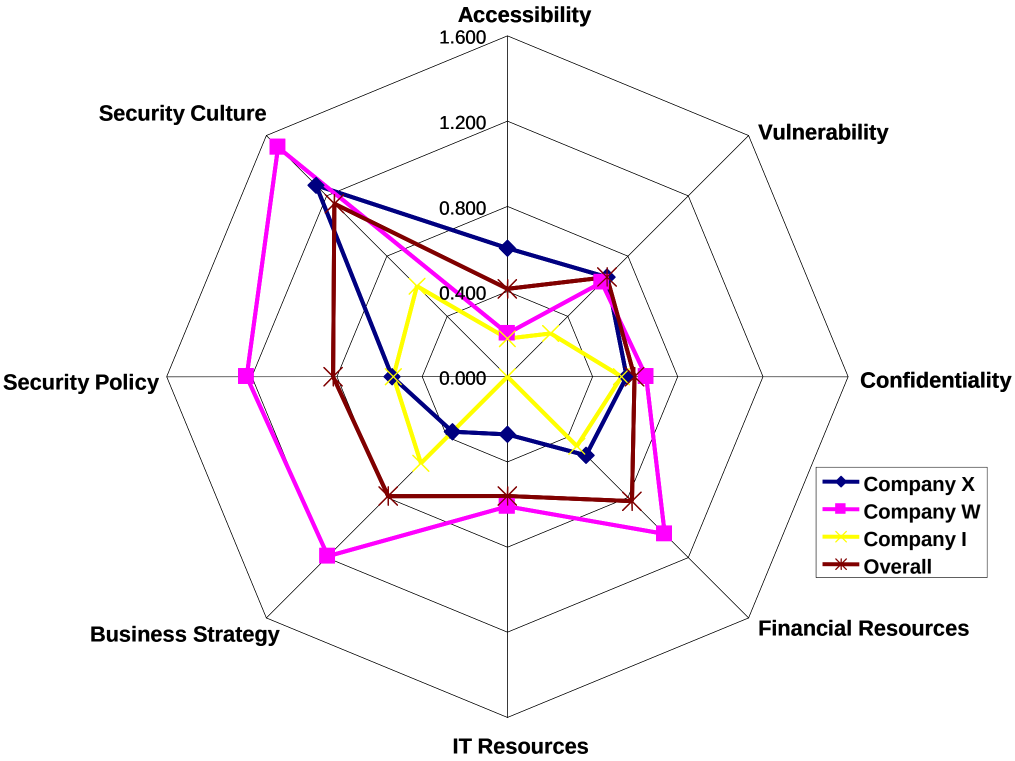

Figure 4. Construct Gaps – by company

Results of Full Scale Study

The pilot study, using about 200 respondents, allowed us to verify the statistical properties of the survey instrument and the constructs. But in order to study other dimensions, such as differences among industries, levels, and functions, a much larger survey was needed. So after some adjustments to the survey instrument were made, a larger scale study was conducted involving some 1500 participants.

Some Findings from Full Scale Study: Variations in Perceptions by Organizational Level

Different people in an organization have different degrees of awareness and perceptions regarding their own company's security. One example of these differences is discussed below.

Security Constructs Assessments

Figure 5 shows the distribution of security perceptions based on the organizational level of the respondent: going from Executive level, to Line Manager, to Professional. Our findings show that top-level Executives (at the CxO level), tend to have a lower perception regarding their own organization's security than middle and lower level personnel. This variation is particularly notable in the areas of business strategy, policy, culture and financial resources.

In general, there is a trend of decreasing confidence in one's own security as organizational seniority increases. This might be attributed to the lack of actual knowledge and personal experience with respect to security as a person approaches executive level work or, alternatively, one's concerns and requirements for security rise as one rises in the organization.

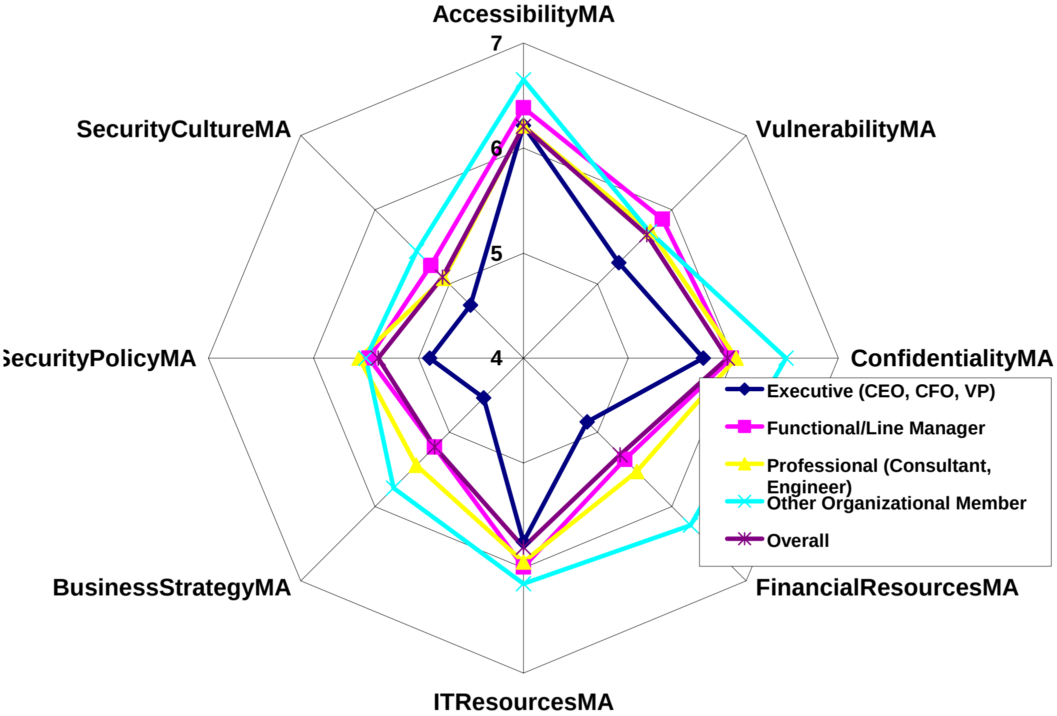

Figure 5. Security Construct Assessment by Level

One possible theory is that different members in different organizational levels may have different attitudes towards security practices as it pertains to their own responsibilities. Since executives are generally responsible for seeing the bigger picture, they may be able to see the overall process better than those functioning within their own silos. The results from the full scale study confirmed that top-level executives have a lower assessment on average than others in an organization. The most notable variations were in the areas of business strategy, policy, culture and financial resources.

Security Constructs Importance

Regardless of their level in the organization, respondents viewed the importance of the various aspects of security to be about the same (as can be seen in Figure 6). This was somewhat surprising given that executives had assessed the security conditions to be significantly worse. There is the possibility that executives do not share the same understanding as others in the organization.

Although ratings of assessment and importance are individually important, the size of the gaps can provide even more insights.

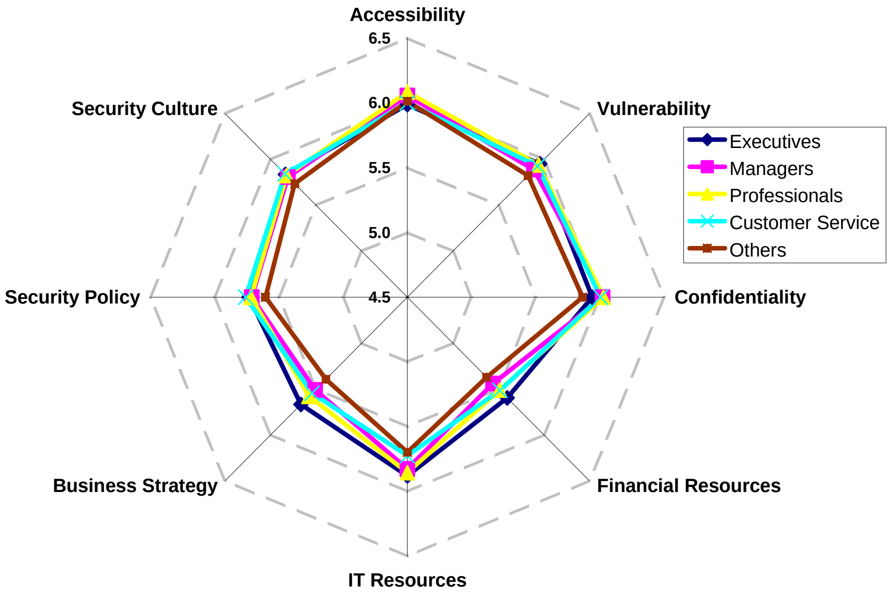

Figure 6. Security Construct Importance by Level

Security Construct Gaps

In our gap analysis of the different organizational levels, we found that the gap size between assessment and importance for top executives were, on average, 60% greater than those of others as shown in Figure 7. The gap sizes for all other levels shared similar trends and took on the same shapes – with the exceptions of the executives. This disparity in perception reiterates the observation that executives appear much more dissatisfied with the situation of security within their own organizations.

Perhaps, executives think situations are worse off than they really are because they do not understand how and if security measures are being correctly implemented. Or alternatively, executives see problems that people in other roles do not see and as a result, their perception of security gap is higher. Follow-up studies and case studies would be needed to understand the actual cause in the significant differences in perception.

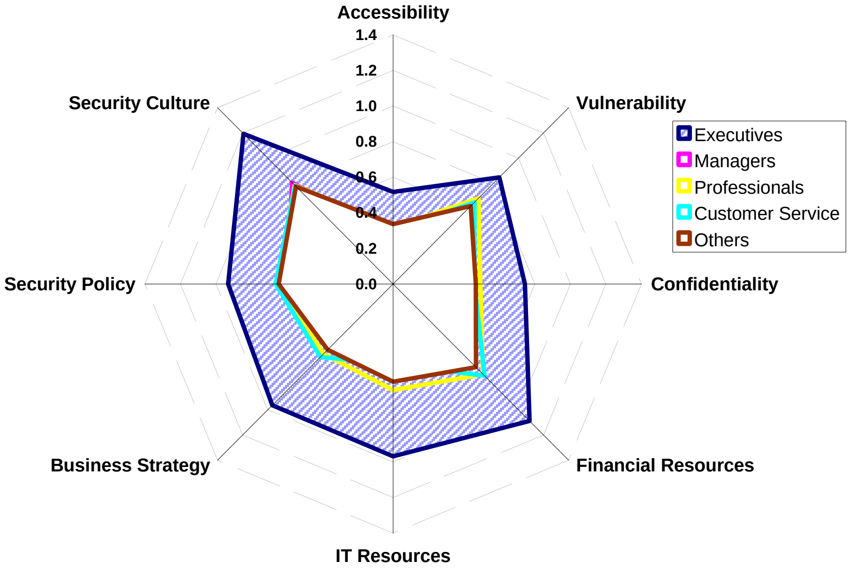

Figure 7. Security Construct Gaps by Level

Conclusion

The security is vital to any organization. In order to identify security strategies and to identify cross-organizational trends, we analyzed perceptions of importance and assessment along eight security constructs. In addition to being a unique way of considering the issue of "security," such an analysis demonstrated the importance of considering perceptions and shed some light on how perceptions shape decision-making in an organization. We believe the results from this work has important implications in a number of areas including assessing an organization's security needs, marketing of security products, and the development of an organization's security technology and policy.

Opportunity to Participate

We welcome you and your organization to participate in our confidential organization benchmarking exercise, similar to organizations X, W, and I shown in Figures 2, 3, and 4. If you would like more information about this opportunity, contact Prof. Stuart Madnick at smadnick@mit.edu

Acknowledgement

The research reported herein was supported, in part, by Cisco Systems, Inc. through the MIT Center for Digital Business.

Bibliography

1. Maxim, P.S., *Quantitative Research Methods in the Social Sciences*. 1999: Oxford University Press, Inc.
2. Hinkle, D., S. Jurs, and W. Wiersma, *Applied statistics for the behavioral sciences*. 2nd ed. 1988, Boston: Houghton Mifflin.
3. Afifi, A.A. and R.M. Elashoff, *Missing Observations in Multivariate Statistics –I. Review of The Literature*. JASA, 1966. **61**: p. 595-604.
4. Hair, J., Joseph F., et al., *Multivariate Data Analysis*. 1998: Prentice Hall.
5. Winch, G., A. Usmani, and A. Edkins, *Towards Total Project Quality: A Gap Analysis Approach.* Construction Management and Economics 1998. **16**(2): p. 193-207.