

HOUSE OF SECURITY: STAKEHOLDER PERCEPTIONS OF SECURITY ASSESSMENT AND IMPORTANCE

Executive Summary¹

Introduction

Security is crucial for the success of any organization. Unauthorized users frequently steal information while hackers constantly disrupt flows of information. In response, organizations have adopted new security policies. It is clear that many of these security policies are valuable, however an organization may be limited in how much of its 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 appropriate approach to security (i.e., a balance between cost and effectiveness). This is further complicated by the fact that there are likely to be different priorities for the various stakeholders in the organization. Furthermore, as organizations evolve towards becoming extended enterprises, including close 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

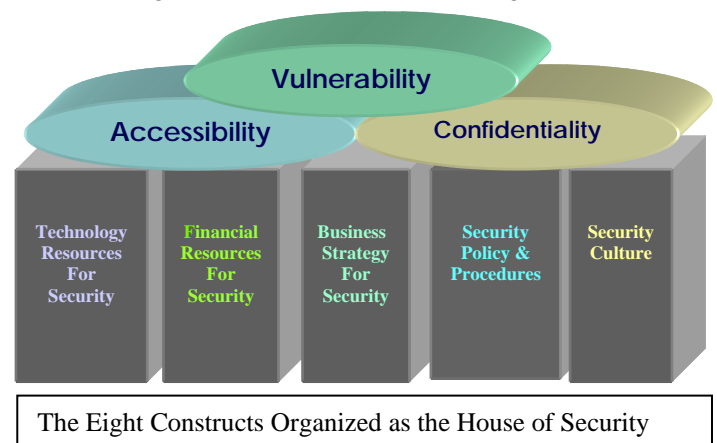
Many scholars have approached the study of security by focusing specifically on the detailed elements of the security systems themselves, such as effectiveness of different cryptographic codes or firewall technologies, or have measured specific events, such as mean-time-to-failure. However, these works 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 take a different approach. We seek to identify the commonalities and differences both within and between different organizations with respect to perceptions of security held by different members of the organization. In order 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



¹ For more information, contact Stuart Madnick (smadnick@mit.edu) or Michael Siegel (msiegel@mit.edu)

Business Strategy with associated Security Policies and Procedures 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*.

The best tool for identifying variations in *perceptions* of security is a survey, broadly distributed to an array of members of an organization (from employees to top-level managers across all functional areas), that addresses both their organization and the extended enterprise. 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.

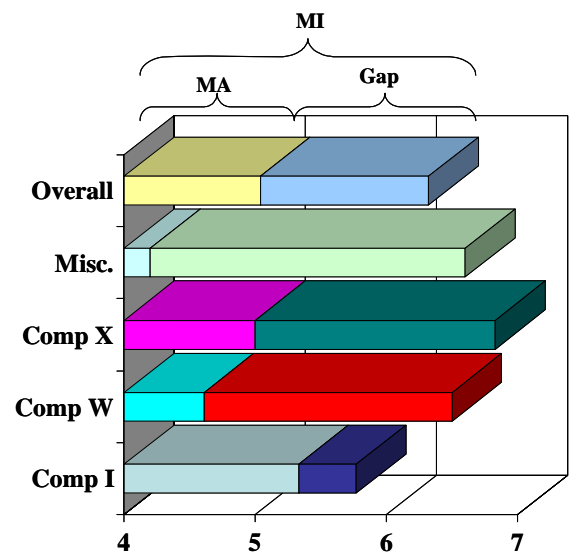
A key part of this study involves performing *gap analyses* (e.g., how much does the perception of the current state of that security issue in the organization differ from the perception of the importance of that security issue.) Such gaps represent opportunities for improvement and better understanding within the enterprise and across the extended enterprise. When current status is below the ideal, 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 evaluate the quality of the survey instrument by measuring the *statistical 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.

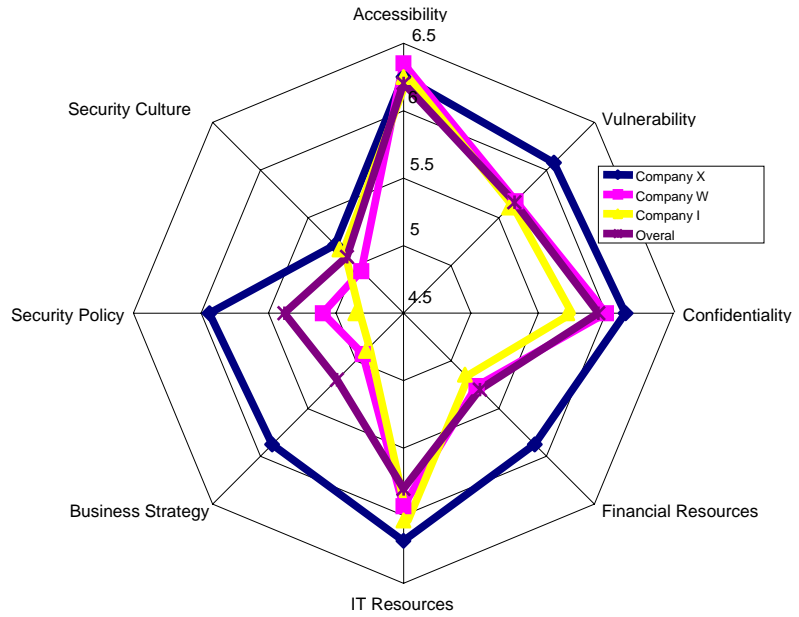
Preliminary Results

In our pilot survey, interesting results have arisen in several categories: (1) the individual questions, (2) the constructs, and (3) the construct gaps. Some examples are presented here.

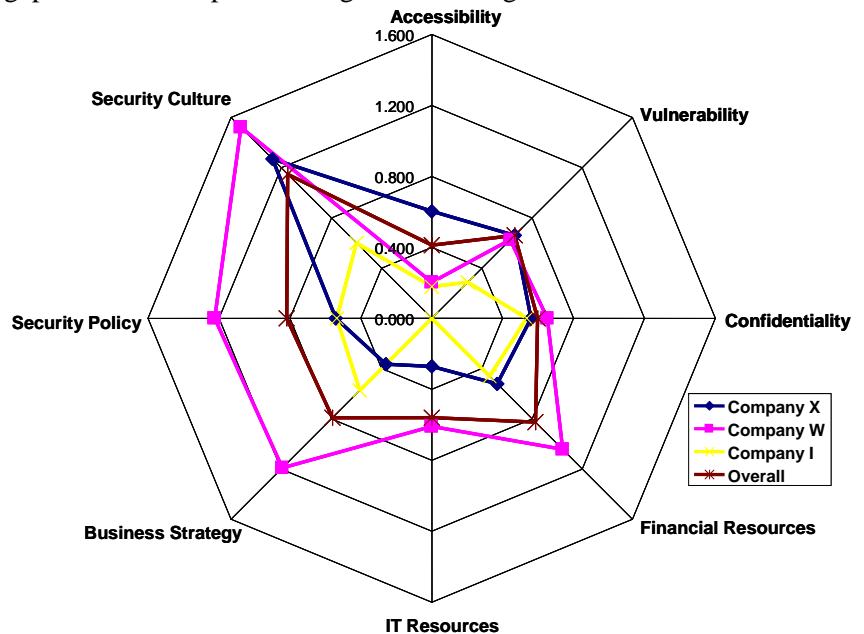
(1) *Individual Questions*: Respondents were asked to assess whether “people in the organization were aware of good security practices.” They were then asked the importance of that issue in the organization. This was to be answered on a 7-point scale (where 1 means “true to a small extent” and 7 means “true to a large extent.”) The overall results are shown on the top line of the graph to the right. 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 suggests 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. One of the goals of this research is to understand these differences.



(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) of all 8 constructs can be seen in the diagram to the right. 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 again. For example, these companies are very similar in their perceptions of “Accessibility” but very different in their perceptions of the state of “Security Policy.”



(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 the diagram to the right. 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.”



Conclusion

The security of information systems is vital to any organization. In order to identify security strategies and to identify cross-organizational trends, we analyze perceptions of importance and assessment along eight security constructs. In addition to being a unique way of considering the “security dilemma,” such an analysis will demonstrate the importance of considering perceptions and may shed some light on how perceptions shape decision-making in an organization. We believe the results from this work will have tremendous 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.