

Enterprise Security Perception and the "House of Security"

September 6, 2006

Professor Stuart Madnick

{smadnick@mit.edu}

Sloan School of Management
Massachusetts Institute of Technology
Cambridge, MA

Differing Perceptions



Picture of old lady or young lady ?

Perceptions are as important as "reality"
(maybe more important)

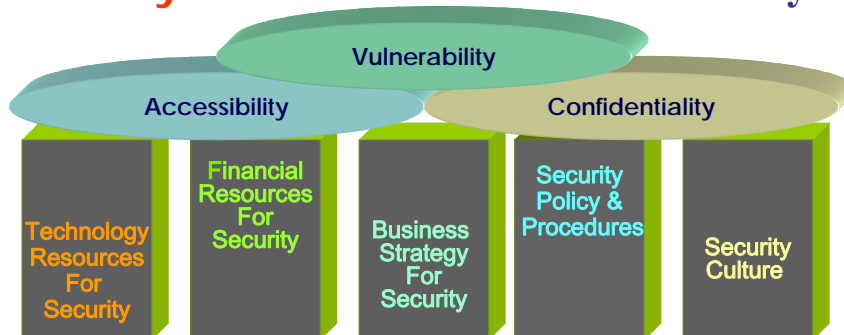
Good Security

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 implemented in a Culture of Security. These practices are supported by IT Resources and Financial Resources dedicated to Security.

Copyright © 2006, MIT

Security Constructs: “House of Security”



Assessment Perceptions: Examples

Who gives lowest “assessment” of these security constructs?

Executives Line Managers Professionals

Which is given highest “assessment” of the constructs?

Own company? “Partner” company? About same?

Copyright © 2006, MIT

Purpose of Gap Analysis

Gap Analysis is to understand
Differences in Perceptions between:

(A) **Security Status Assessment and Security Importance**

(B) **Views of diverse Security Stakeholders**
...within and across the Enterprise

Types of Gaps (examples)

Performance Gaps: Current Status v. Importance

Role Gaps: Business Managers v. IT staff

Rank Gaps: Executive v. Line Manager

Copyright © 2006, MIT



Purpose of Gap Analysis (cont.)

Gaps represent **Opportunities for Improvement**
within the Enterprise and across the
Extended Enterprise

(A) When **Status is below the Needs**,

- Represent Areas for Improvement

(B) When Status among **Stakeholders show differences**, these represent areas for
Investigating sources of the differences

- Gaps may represent misunderstandings
- Gaps may represent differences in local knowledge and needs

Copyright © 2006, MIT



Gap Analysis Questionnaire

- Questionnaire respondents are:
 - Diverse roles (e.g., IT, non-IT)
 - Diverse ranks (e.g., Line managers, Executives)
 - Diverse companies and industries
- Each respondent reports his/her view of actual **assessment** and **importance** of each question for both **his/her organization** and a **partner organization**.

Example Security Questions

Section 3: Security Questions

Assessment Scale:

1= In my view, this security statement is true to a very SMALL extent in my (partner) organization.

7= In my view, this security statement is true to a very LARGE extent in my (partner) organization.

Importance Scale:

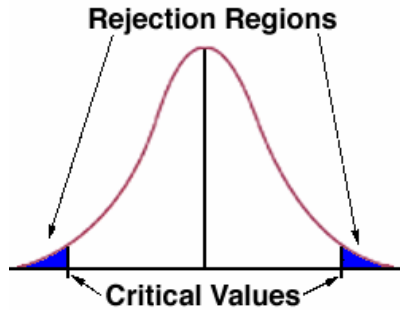
1= In my view, it is NOT at all Important to me that my (partner) organization address this security statement.

7= In my view, it is VERY Important to me that my (partner) organization address this security statement.

Procedurally, you can answer all four columns at once, or, if you prefer, you could answer the first two columns about your organization first and then come back and answer the right two columns about your partner.

	Questions	Your Organization		Partner Organization	
		Assessment	Importance	Assessment	Importance
1	The organization's data and networks are rarely tampered with by unauthorized access.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
2	In the organization, security is adequately funded.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
3	Customers trust the organization not to disclose data about them.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
4	The organization's security strategy sets direction for its security practices.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7
5	Business managers in the organization are involved with IT security policies.	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7	1 2 3 4 5 6 7

Evaluating Statistical Significance



$$t = \frac{(\bar{X} - \bar{Y})}{\sqrt{\frac{n(n-1)}{\sum_{i=1}^n (\hat{X}_i - \hat{Y}_i)^2}}}$$

- where
- n = Number of Respondents
 - \bar{X} = Average of Distribution X
 - \bar{Y} = Average of Distribution Y
 - $\hat{X}_i = (X_i - \bar{X})$
 - $\hat{Y}_i = (Y_i - \bar{Y})$

"My organization" Gaps:
significant @ 99.98%

Partner Gaps:
significant @ 99.97%



Statistically Significant Instrument for Measuring Components of Security Perceptions

Copyright © 2006, MIT

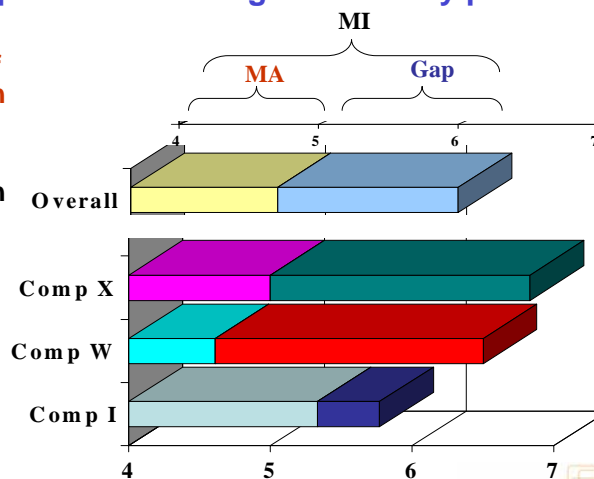
Example Gap Analysis Findings - Different Organizations

Question 33: People are aware of good security practices.

MA = Assessment of "My" organization (5.1)

MI = Importance for "My" organization (6.3)

Gap = difference between Assessment and Importance - for "My" organization (1.2)



Observation: Big differences between companies.

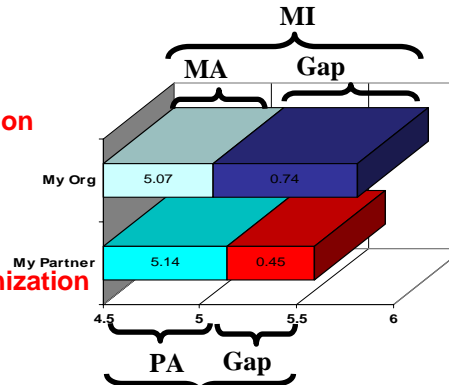
Copyright © 2006, MIT

Example Gap Analysis Findings - Compared with Partner Organization

Question 33: People are aware of good security practices.

Gap between Assessment and Importance – for “My” organization
Overall gap = 0.74

Gap between Assessment and Importance – for “Partner” organization
Overall gap = 0.45



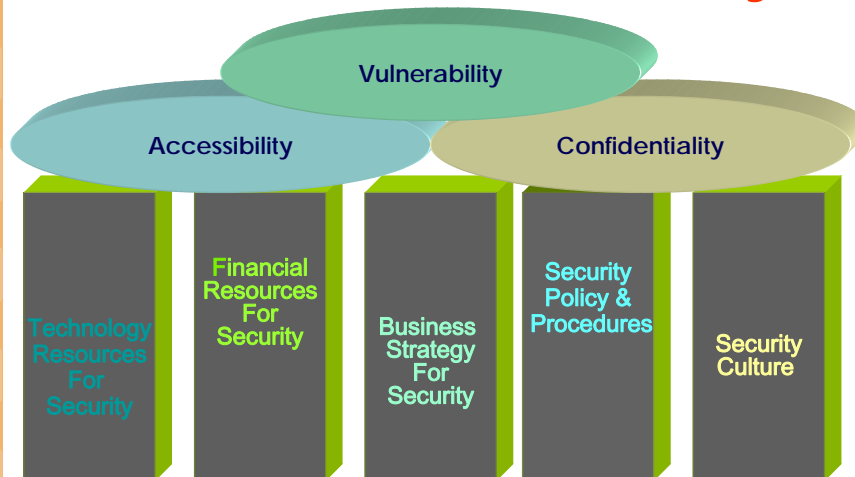
General conclusion:

- View partner as slightly “better” (5.14 v 5.07) PI
- But it is also much “less important” (5.59 v 5.81)

-> So Gap is much less (0.45 partner v 0.74 “my Organization”)

Copyright © 2006, MIT

Dimensions of Security



“House of Security”

Copyright © 2006, MIT

Analysis of Construct Reliability and Validity

Reliability - Cronbach's Alpha Values

	MA	MI
Accessibility	0.90758	0.93701
Vulnerability	0.83714	0.91012
Confidentiality	0.91808	0.94026
FinancialResources	0.91878	0.92768
ITResources	0.91023	0.93680
BusinessStrategy	0.86877	0.89343
SecurityPolicy	0.92184	0.93834
SecurityCulture	0.92188	0.94296

Reliability = produces consistent results

Validity = components are more correlated with others of that construct than another construct

- **Convergent Validity** – form a single construct

- **Discriminant Validity** – not of another construct

For good reliability, want Cronbach's Alpha Values to be >0.6, better if >0.7

Construct Validity - Convergent and Discriminant Validity

	Accessibility	Vulnerability	Confidentiality	Financial Resources	ITResources	Business Strategy	Security Policy	Security Culture
Accessibility	0.96606	0.82730	0.86289	0.72385	0.81193	0.75817	0.75993	0.77299
Vulnerability	0.82730	0.89537	0.85986	0.83791	0.88582	0.83439	0.85439	0.83308
Confidentiality	0.86289	0.85986	0.97320	0.79234	0.86494	0.83070	0.85867	0.85271
FinancialResources	0.72385	0.83791	0.79234	0.97366	0.88814	0.86196	0.86675	0.84406
ITResources	0.81193	0.88582	0.86494	0.88814	0.96623	0.84474	0.87556	0.85137
BusinessStrategy	0.75817	0.83439	0.83070	0.86196	0.84474	0.93056	0.88216	0.85515
SecurityPolicy	0.75993	0.85439	0.85867	0.86675	0.87556	0.88216	0.97341	0.84505
SecurityCulture	0.77299	0.83308	0.85271	0.84406	0.85137	0.85515	0.84505	0.96241

For good Convergent Validity, want diagonals >0.50

For good Discriminant Validity, want all values in columns of each construct to be lower than the diagonals.



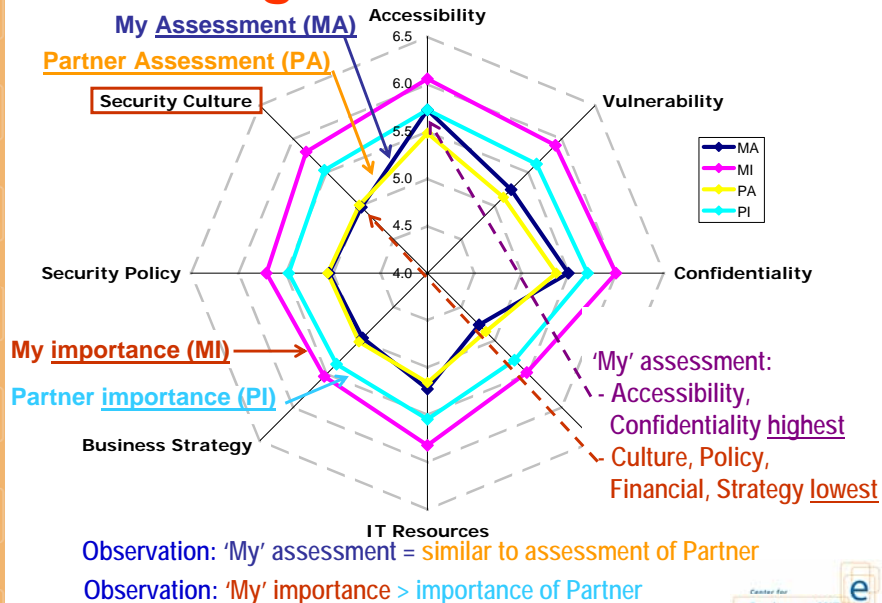
Statistically Reliable & Valid Instrument for Measuring Perceptions of Security Constructs

Copyright © 2006, MIT



13

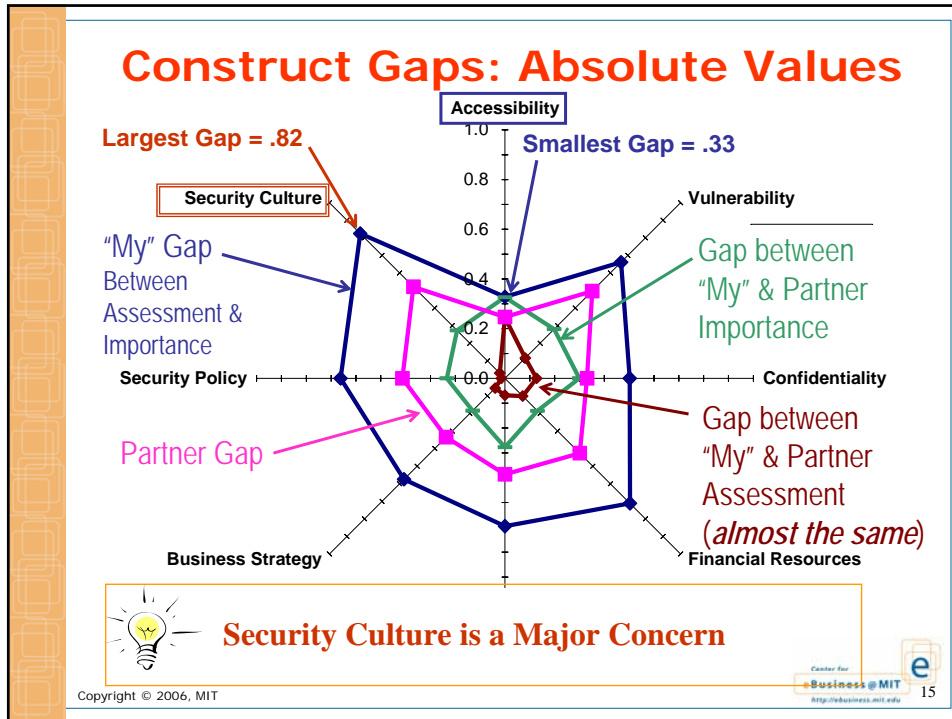
Average Construct Values



Copyright © 2006, MIT

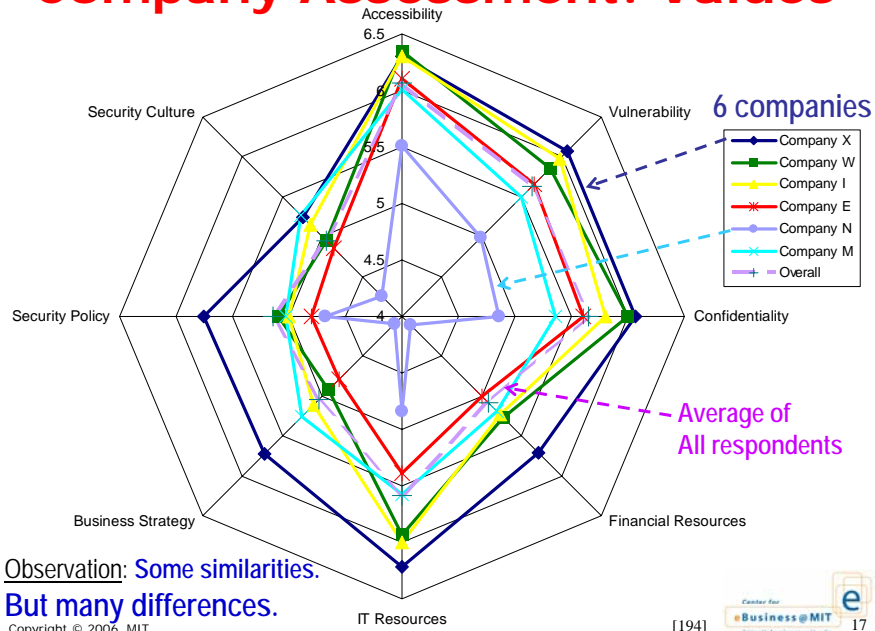


14

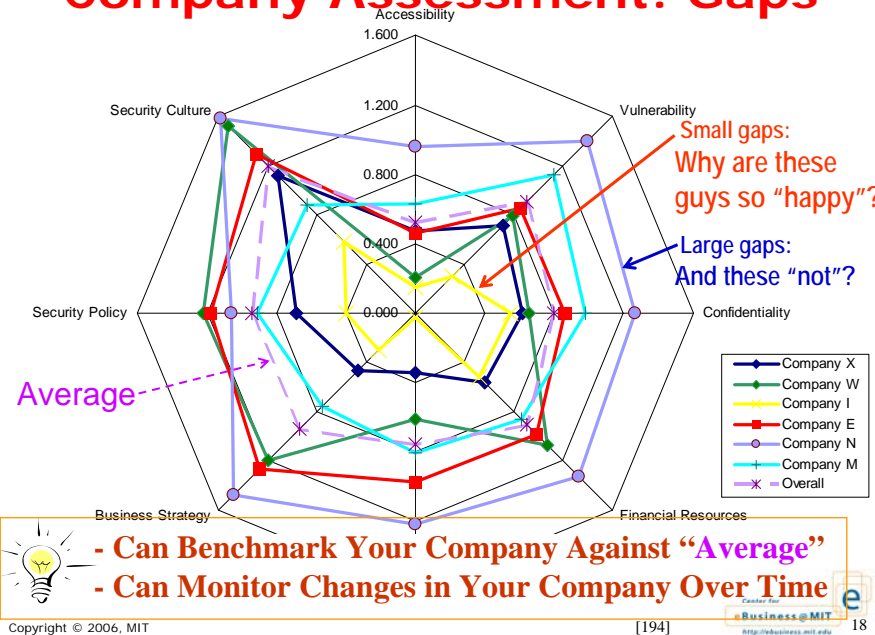


- ## Security Culture Questions
- **Security Practices**
 - In the organization, people are aware of good security practices. [q33; gap=.78]
 - People in the organization are knowledgeable about IT security tools and practices. [q08; gap=.82]
 - People in the organization carefully follow good security practices. [q14; gap=1.08] ← **Largest gap!**
 - **Ethics and Trust**
 - People in the organization can be trusted not to tamper with data and networks. [q21; gap=.69]
 - People in the organization can be trusted to engage in ethical practices with data and networks. [q26; gap=.74]
- Copyright © 2006, MIT
- Center for eBusiness@MIT
http://eBusiness.mit.edu

Company Assessment: Values



Company Assessment: Gaps

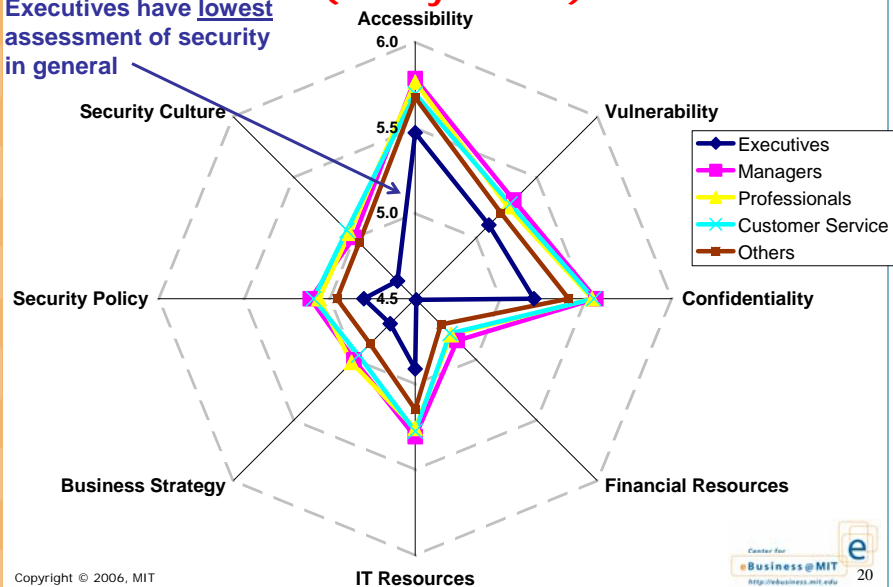


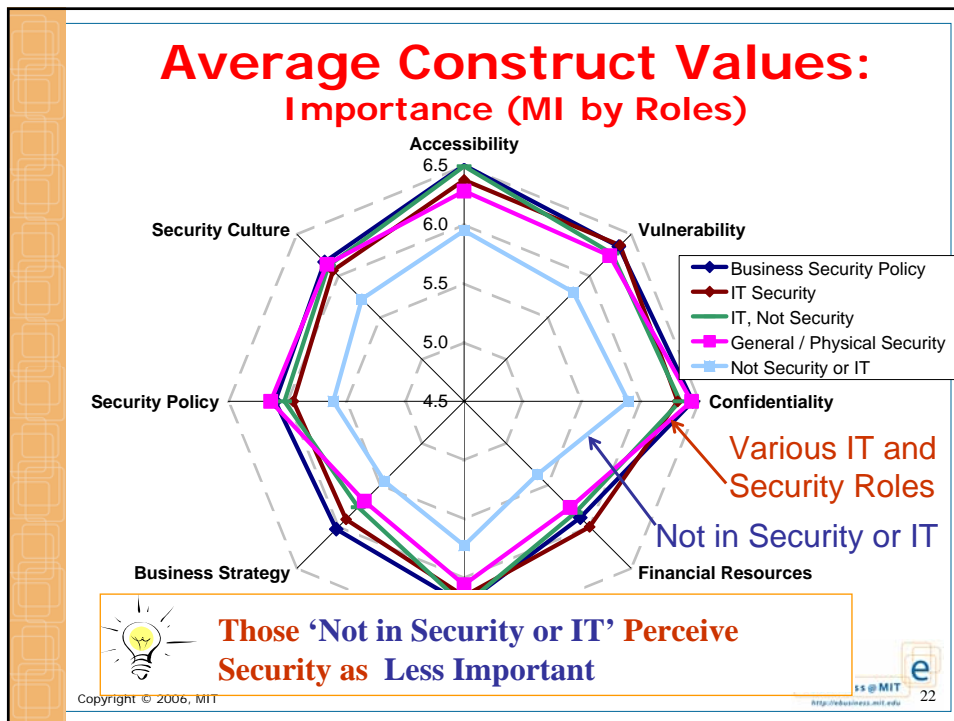
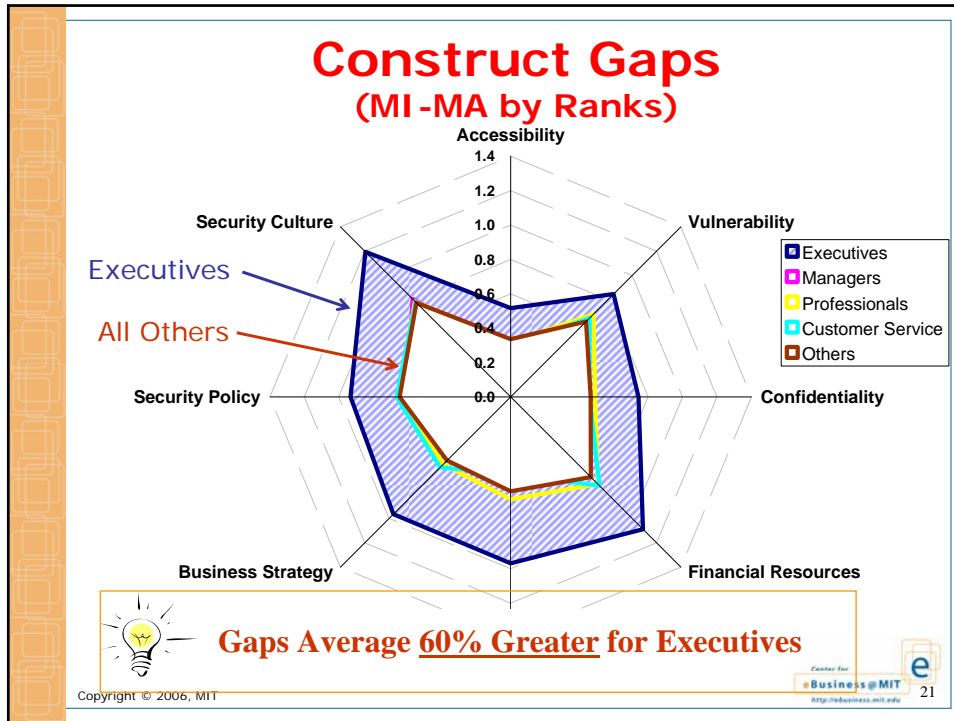
A Closer Look

- Rank Gaps:
 - e.g. Executives v. Professionals
- Role Gaps:
 - e.g. Business Managers v. IT staff
- Industry Gaps:
 - e.g. Healthcare v. Banking

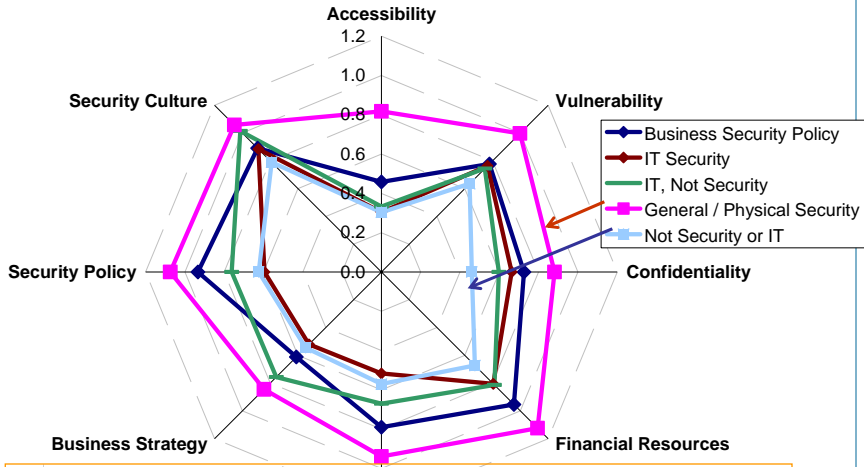
Average Construct Values (MA by Ranks)

Executives have lowest assessment of security in general





Construct Gaps (MI-MA by Roles)

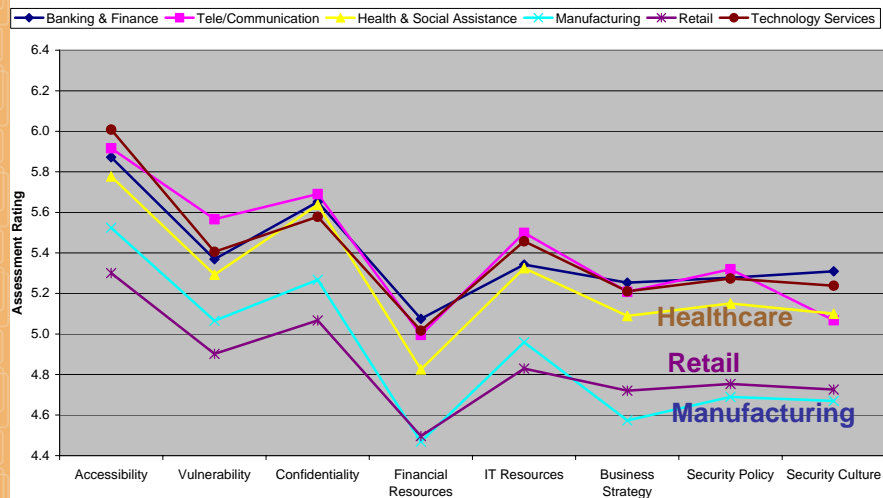


But Even Those 'Not in Security or IT' Still Perceive Significant Security Gaps

Copyright © 2006, MIT

<http://ebusiness.mit.edu> 23

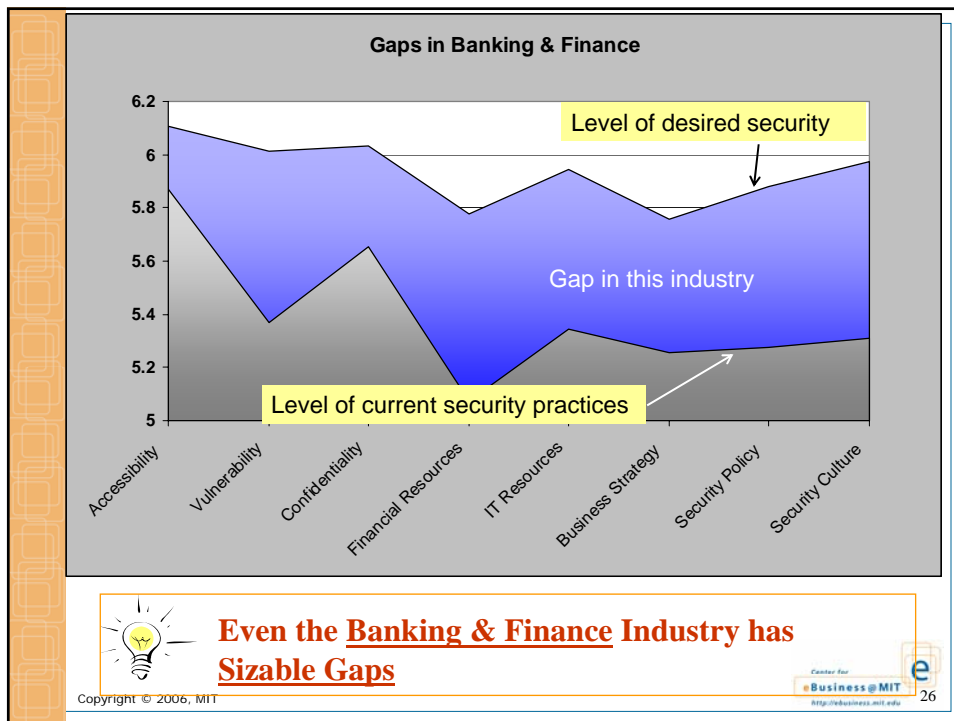
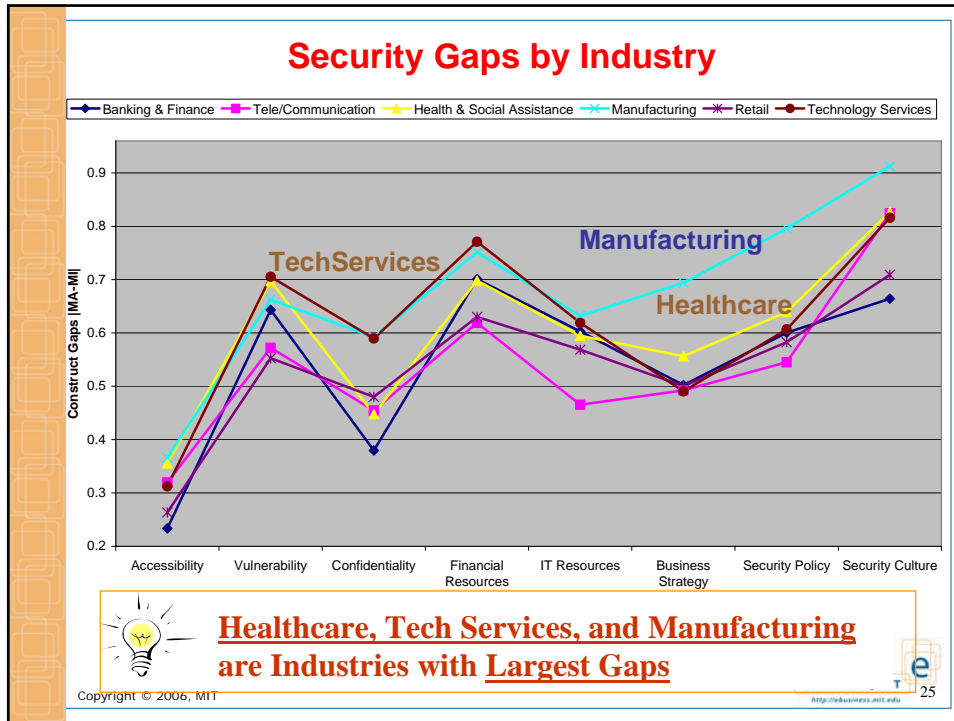
My Assessment of Security by Industry



Healthcare, Retail, and Manufacturing are Industries with Lowest Construct Assessments

Copyright © 2006, MIT

<http://ebusiness.mit.edu> 24



Summary of Key Findings

1. Statistical instrument for measuring perceptions of security
 - Can use to benchmark your company
 - Can monitor changes over time
2. 'Security Culture' is a major concern
 - Needs to be explicitly addressed
3. Healthcare, Retail, and Manufacturing have low assessments and sizable gaps
 - Certain industries to focus on ... *but all need*
4. Executives have lowest assessments of security and largest gaps
5. Those 'not Security or IT' perceive security less important, but still sizable gaps
 - Opportunity/need for communication

Copyright © 2006, MIT

"How Good is your Security?"

It is well known in Consumer Behavior Research that
Perception Is Reality

- Your behavior is based on your perceptions
- We have combined that notion with the discipline of statistics to advance our understanding of Security

More analysis still underway

Stuart Madnick; T 617-253-6671; E-mail: smadnick@mit.edu

Exec Summary: http://ebusiness.mit.edu/research/Briefs/Madnick_Siegel_Security_Brief.pdf

TSQM Survey: <http://web.mit.edu/surveys/tsqm/>

Copyright © 2006, MIT

Next steps:

1. Larger-scale Gap Analysis Study
 - More individual participants
 - More company-specific participation
2. Understand Reasons for Differences
 - More details on the “why?” and “so what?”
 - Detailed company-specific case studies
3. Determine Prescriptive actions
 - More education (what & how best?)
 - More security in specific areas
 - More appropriate security & training
 - Etc ...

Acknowledgement: MIT TEAM

FACULTY

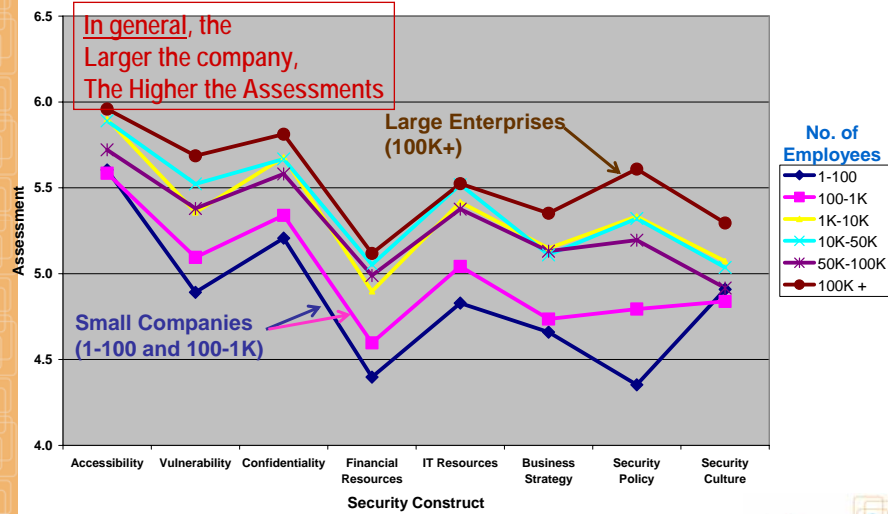
- Yang Lee
- Stuart Madnick
- Michael Siegel
- Diane Strong
- Richard Wang
- Chrisy Yao

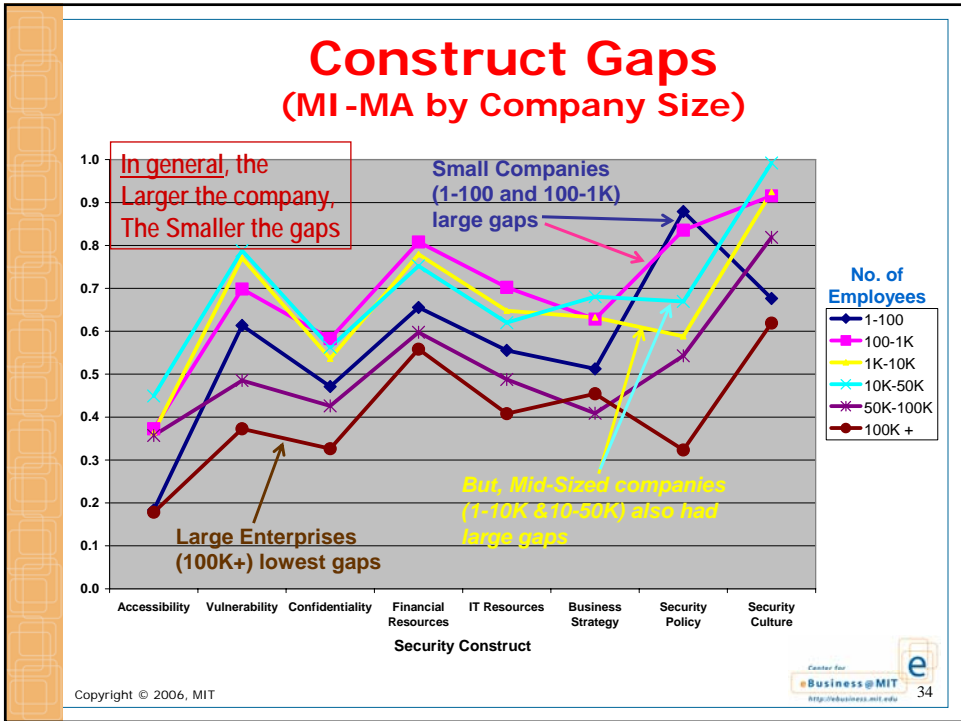
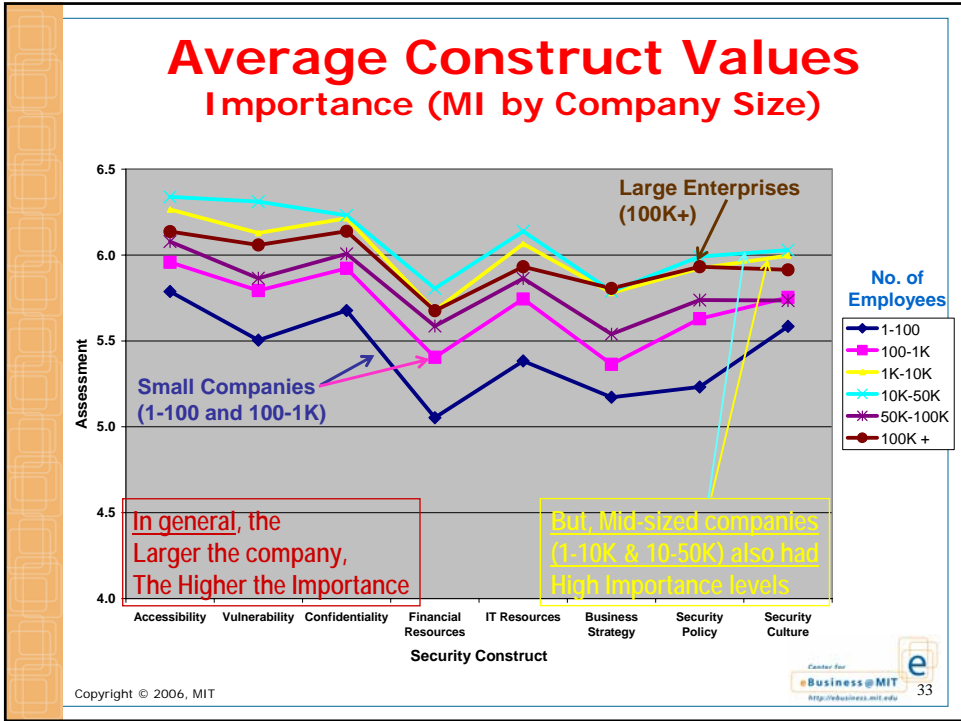
STUDENTS

- Wee Horng Ang
- Vicki Deng
- Desiree Rap
- Dinsha Mistree
- Venkataramana Thummisi

Extra Slides

Average Construct Values Assessment (MA by Company Size)





Vulnerability

- [q01] The organization's data and networks are rarely tampered with by unauthorized access.
- [q05] The organization has adequate safe guards against internal and external threats to its data and networks.
- [q19] The organization improves its security by learning from previous attacks on its data and networks.
- [q31] The organization has a rapid response team ready for action when attacks occur.

Accessibility

- [q04] The organization checks the identity of users before allowing access to data and networks.
- [q11] The organization's data and networks are only available to approved users.
- [q30] The organization provides access to data and networks to legitimate users.
- [q34] The organization's data and networks are usually available when needed.

Copyright © 2006, MIT

Confidentiality

- [q12] The organization has adequate policies for when and how data can be shared.
- [q18] The organization has adequate policies about user identifications, passwords, and access privileges.
- [q20] The organization protects privacy of personal data (for example, customer data, data about employees)
- [q32] The organization provides good protection of confidential corporate data.

IT Resources

- [q03] The organization has enough IT security specialists to cover its security needs.
- [q10] In the organization, the IT group takes security seriously.
- [q13] The organization has adequate technology for supporting security.
- [q17] The organization uses its IT security resources effectively to improve security.

Copyright © 2006, MIT

Financial Resources

- [q09] In the organization, security funds are appropriately distributed based on needs.
- [q16] Security is a funding priority in the organization.
- [q23] The organization has enough security personnel to cover its security needs.
- [q28] The organization makes good use of available funds for security.

Business Strategy

- [q02] The organization's security strategy sets direction for its security practices.
- [q22] Security is a business agenda item for top executives in the organization.
- [q27] In the organization, business managers help set the security strategy.
- [q29] The organization's security strategy is well-publicized in the organization.

Copyright © 2006, MIT

Security Policy

- [q07] The organization has policies for regularly scheduled security audits.
- [q15] The organization has a well-defined and communicated security strategy.
- [q24] The organization has well-defined policies and procedures for data and network security.
- [q25] The organization has procedures for detecting and punishing security violations.

Security Culture

- [q08] People in the organization are knowledgeable about IT security tools and practices.
- [q14] People in the organization carefully follow good security practices.
- [q21] People in the organization can be trusted not to tamper with data and networks.
- [q26] People in the organization can be trusted to engage in ethical practices with data and networks.
- [q33] In the organization, people are aware of good security practices.

Copyright © 2006, MIT