Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity $(IC)^3$

3 Sept 2014

MIT House of Security and Measurement of Security Perceptions in Corporations and Organizations

Professor Stuart Madnick

Massachusetts Institute of Technology

MIT Sloan Management

Measurement of Security Perceptions in Corporations and Organizations

- There are many "concrete" aspects of cyber security that people attempt to measure
  - Number of (known) actual and attempted attacks
  - Mean-time-to-failure , etc …
- Hard to get an *overall* assessment of the state of cyber security for an organization
- The "non concrete" aspects are rarely measured, such as **attitudes** and **perceptions**
  - As many have noted:

"Perception is more important than reality, . . . since people only react to perception because reality is rarely known."

Why is Important to Measure Security Perceptions in Corporations and Organizations?

- The government does not and cannot control all of the cyber infrastructures, so **cooperation and assistance from the private sector is needed**
  - What are their attitudes and perceptions about security?
- Furthermore, even **within the government**
  - We have found that different groups have different attitudes and perceptions
- **We need to understand this better**.

Google blames 'human error' for data leak

(IDG News Service)

- Google is apologizing after it mistakenly e-mailed potentially sensitive business data last week to other users of its business listings service. . . .
- Google provides data on how customers found an ad listing, showing search terms people used before clicking the listing and other data such as the geographic location of someone who looked up driving directions to the business.
- Google sends reports to those businesses who are signed up.
- Early last week, **Google sent the reports to third parties by mistake**. The mistake affected several thousands businesses registered with Local Business Center, of which there are more than a million.

This is what some (maybe many?) in industry think about cyber security

Responsive to oppressive passwords?
Write them on sticky notes and tape to monitor!

Too silly to be believable?

Compliance with Information Security Policies: An Empirical Investigation

IEEE Computer Magazine, Feb 2010

- " ... Writing passwords on sticky notes and leaving them in visible places in the office or at home provides another example. Such careless employee behavior places an organization's assets and reputation in serious jeopardy …"

- "... Several studies have addressed employees' security policy compliance. … While these studies propose interesting principles for increasing information security awareness, none offer empirical evidence to support their principles in practice. … (we need to understand) … why employees do not comply with the organization's information security procedures...."

Approach: Survey security attitudes and Gap Analysis

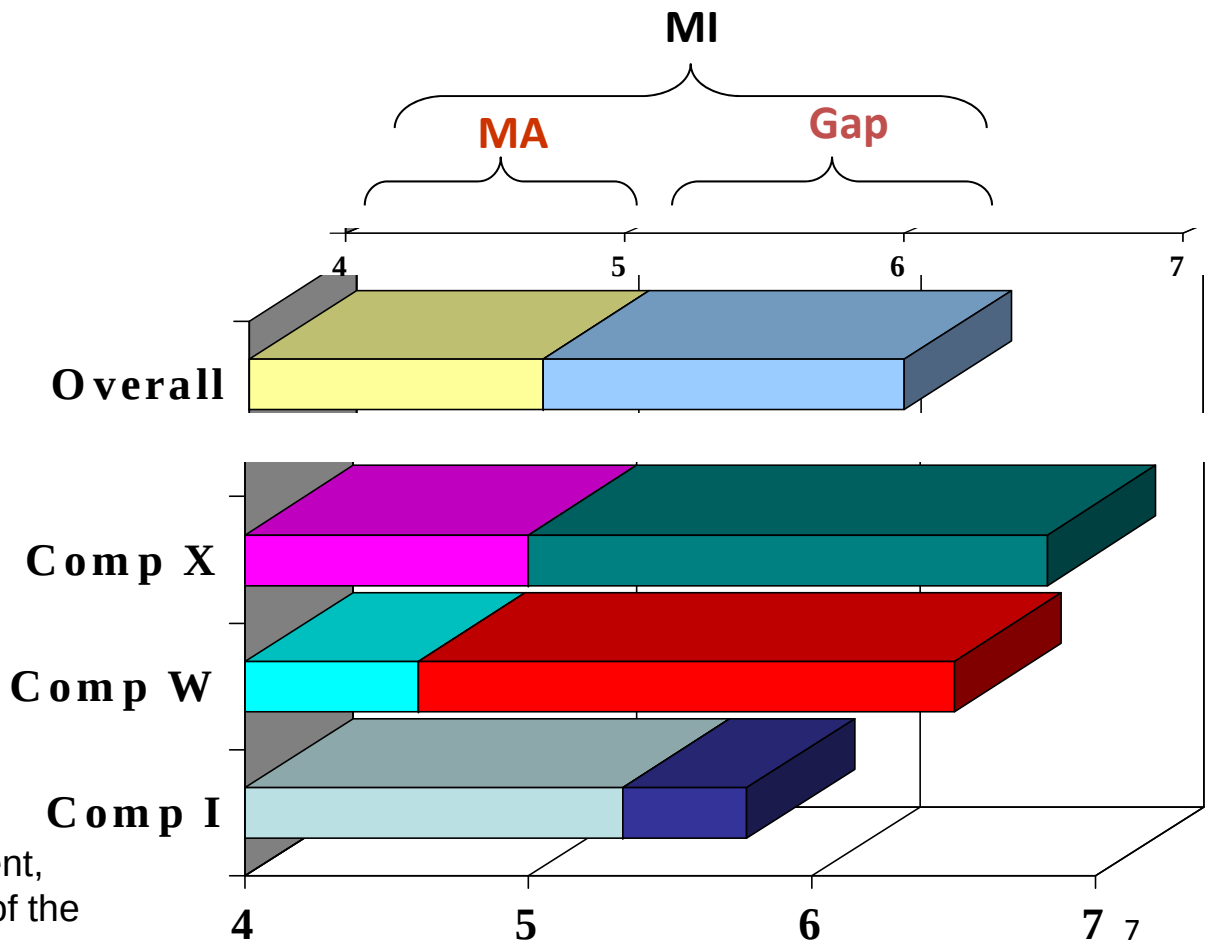
Pilot survey instrument validated[1] and approved.

E.g., Survey Question 33: In our organization, people are aware of good security practices.

MA = Assessment of "My" organization (5.1)

MI = Importance for "My" organization (6.3)

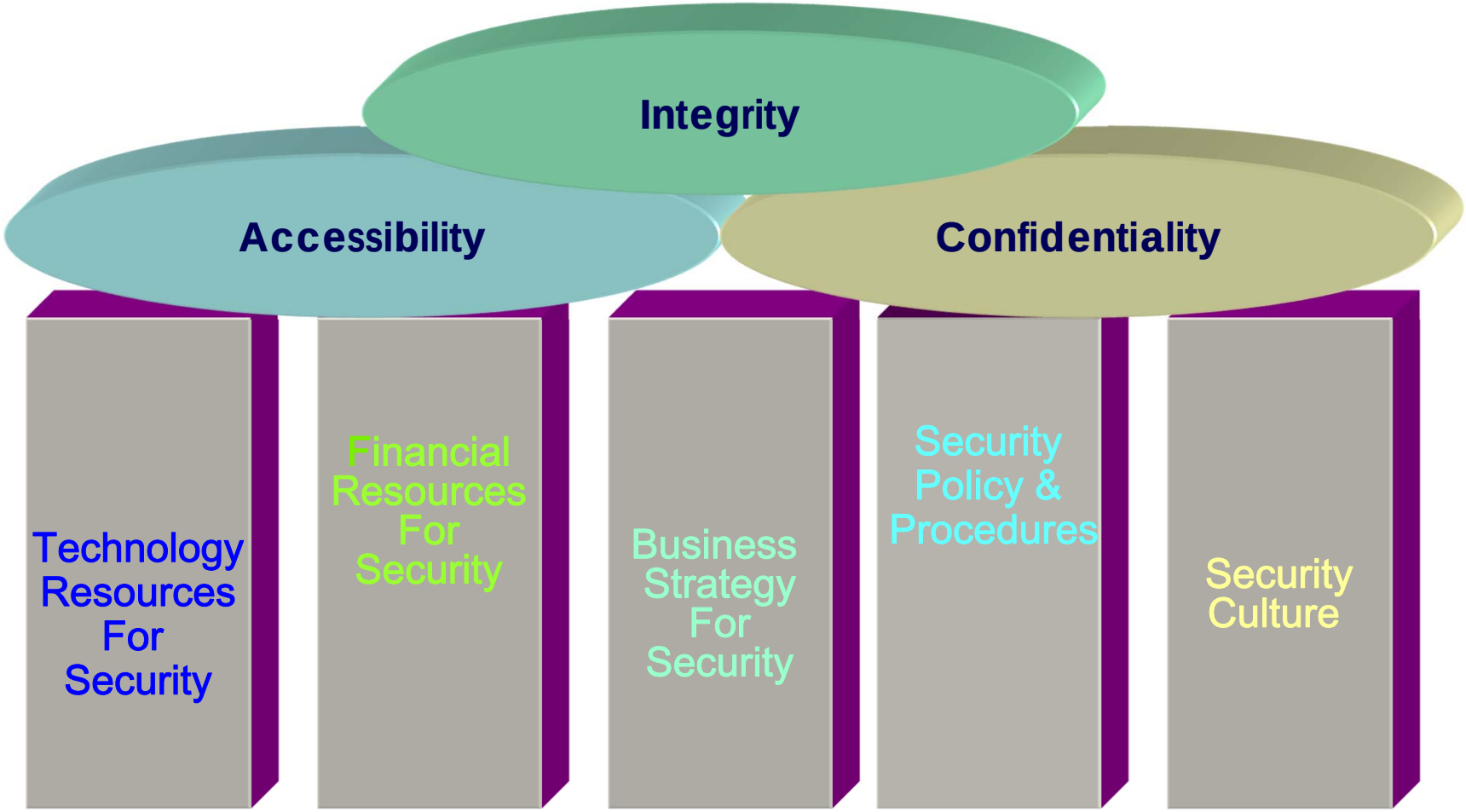
Gap = difference between Assessment and Importance – for "My" organization (1.2)



[1]statistical significance, reliability, content, convergent , and discriminant validity of the constructs.

Observation: Big differences between companies. Why?

Framework: Constructs of Security



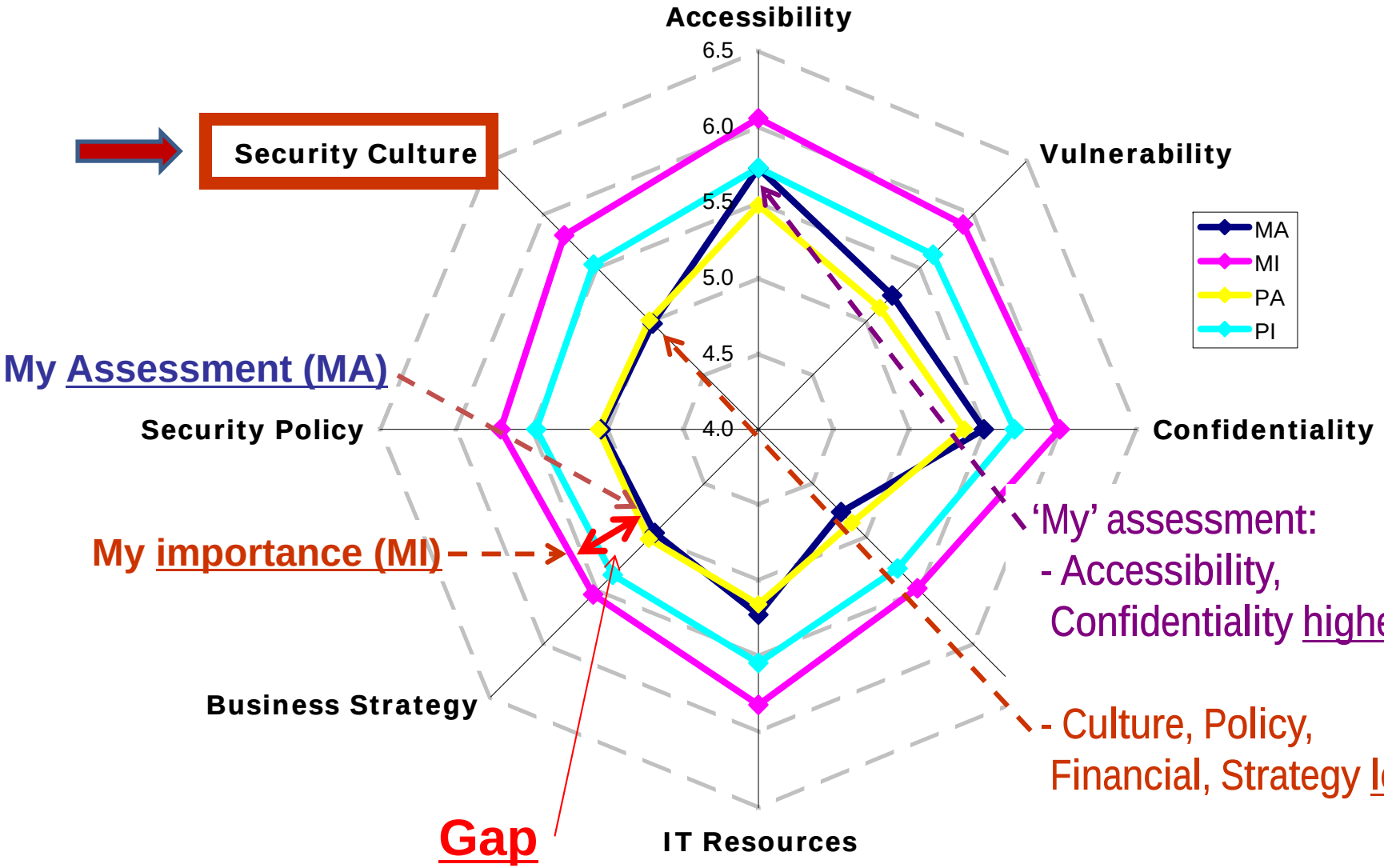
"House of Security"

Statistical Analysis of the Questions and Constructs

Evaluated the quality of the survey instrument and the partitioning into the constructs by measuring:

- Statistically significance of the questions and the constructs
- Reliability of the constructs (by computing Cronbach Alphas)
- Content, convergent and discriminant validity of the constructs.

Average Construct Values

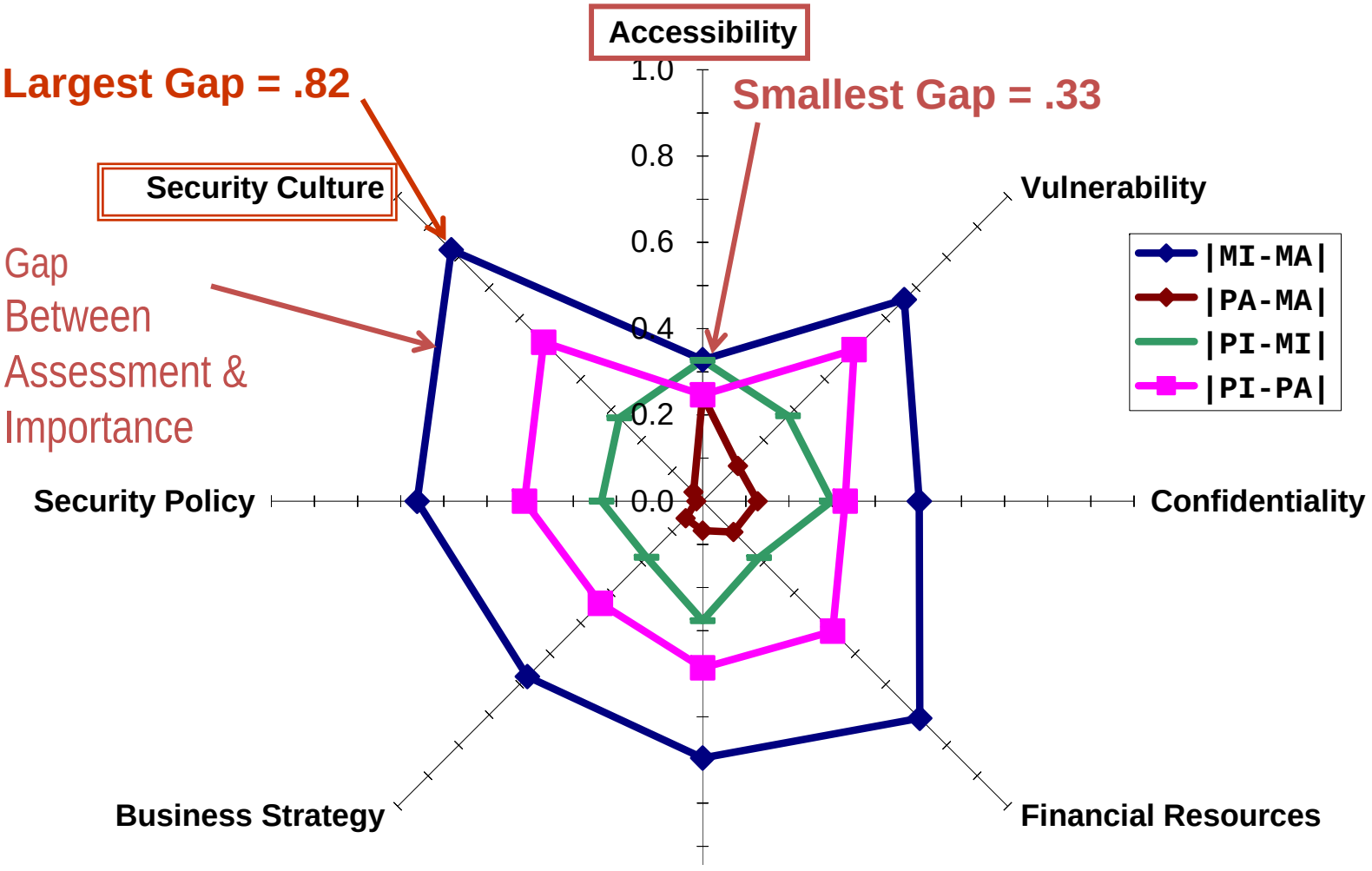


Examples of Security Culture Questions and Results

- **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]

Construct Gaps: Absolute Values



Important to understand if and how the attitudes vary depending on company, industry, country, position, functional area, etc.

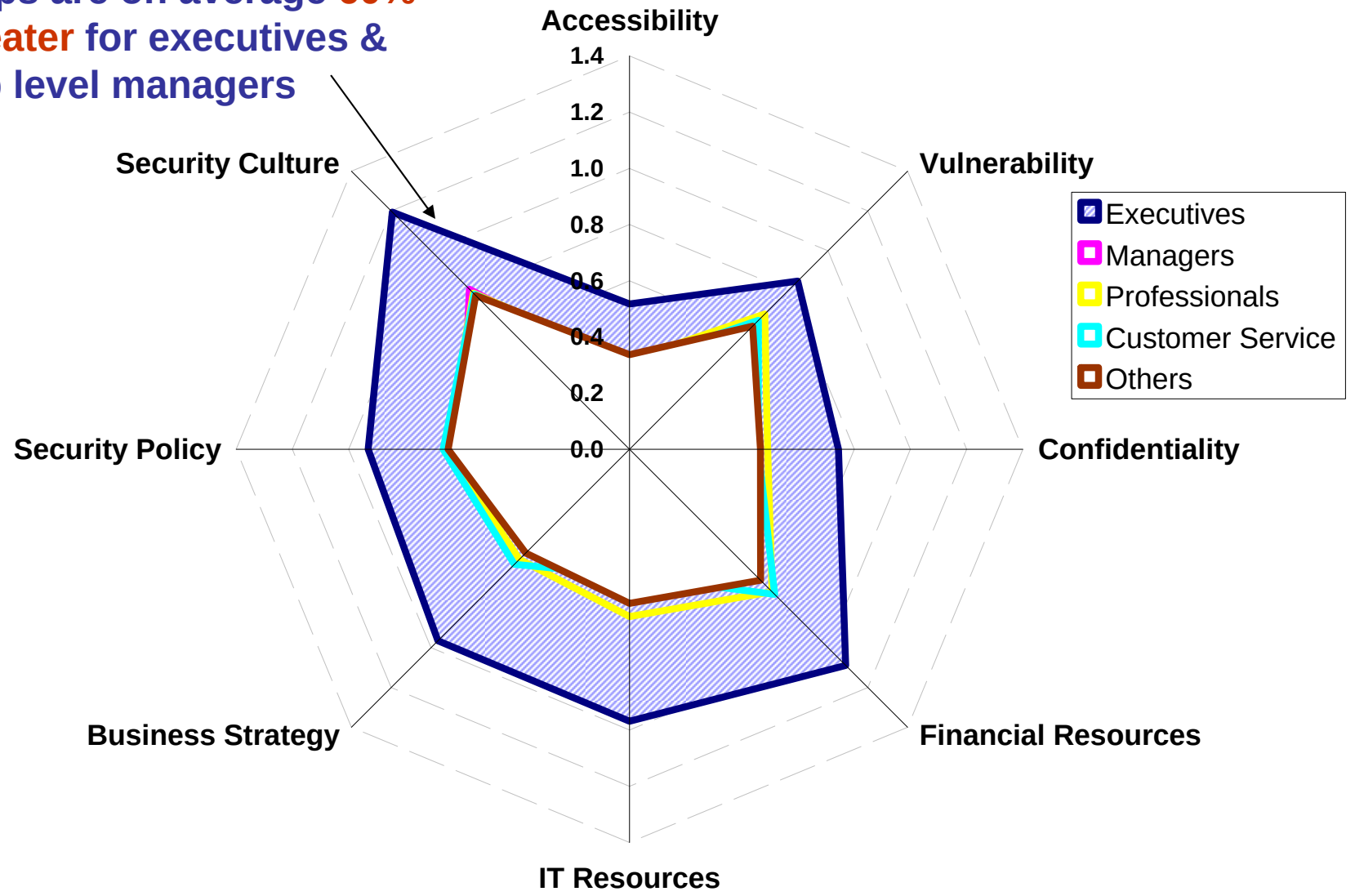
Variation Perceptions

- **Question: Are there variation in perceptions based on different industries, different levels of the organization, different functions by utilizing existing survey data?**
- **Different levels of the organization …**
- **People are which level have the biggest security gaps (differences between where "are" and "should be")?**
  - Top Executives
  - Mid-level Executives (Managers)
  - Professional Staff

Construct Gaps Absolute Values

(MI-MA by Roles)

Gaps are on average 60% greater for executives & top level managers



Future Research Example …

- Revise survey instrument and revalidate and reapprove it
- Identify several other public and private organizations to serve as new survey sites
- Extend to range of organizations in different industries
- Analyze results of survey data
- Explore its use as baseline for organizations (to evaluate improvements) and for industry-wide assessments