Unit 2 Seminar Preparation

User Participation in the Risk Management Process

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Activity

Read the Spears & Barki (2010) article then prepare answers to the following questions:

a. How did the authors use both Qualitative and Quantitative assessment approaches? What benefits did each approach yield?
b. What do the authors list as the advantages of involving users in the risk management process?
c. Based on the findings of the research,

    i. How will the lack of user access affect the risk assessment you will carry out as part of your assessment?
    ii. Will it affect the choice of Qualitative vs. Quantitative assessment methods you utilise?
    iii. How might you mitigate any issues encountered?

You should demonstrate that you understand the topic covered and ensure you use references to academic literature (including journals, books, and reports). This activity will provide evidence of your personal growth and is a component of the e-portfolio, which you can submit at the end of the module.

We will review some of your answers in this week's seminar, as well as covering more on the content of Units 1 and 2. There will also be an opportunity to review your team's progress during the seminar.

---

a) Qualitative approaches were in the form of semi-structured interviews with various "informants with SOX experience [...] identified at a one-day symposium on information assurance and SOX compliance" (Spears & Barki, 2010: 506). There were 11 informants from nine different companies across five industries. Informant positions ranged from IS and audit managers, financial controllers, audit personnel, and accounting personnel.

   Interviews were exploratory, with results used "to gain a better understanding of the process and outcomes associated with business users' participation in IS security projects" (ibid: 507). What resulted were eight hypotheses (please see b)) whose validity were to be explored in the subsequent quantitative analysis.

   The quantitative component measured *user participation*, *organizational awareness*, *control* development, and *control performance*, all of which comprised the relevant hypotheses, and

was meant to “test the validity of the hypotheses that emerged from the exploratory study and to provide triangulation of results from the exploratory study” (ibid: 515).

To test the validity of each hypothesis according to the quantitative measurements, partial least squares (PLS) and AVEs (average variable extracted) were used to measure “the correlation matrix for all constructs, and the composite reliabilities of reflective constructs” (ibid: 516)

The study found that

> the composite reliabilities of organizational awareness, business-aligned SRM, control development, and control performance were .85, .83, .87 and .80, thus supporting reliability. The AVEs of the four constructs were greater than the inter-construct correlations (.74, .71, .69, and .66, respectively), supporting convergent and discriminant validity (ibid: 516),

thus confirming the validity of user participation in IS/SRM in regards to the hypotheses isolated.

b) Advantages of user participation:

i. User participation in SRM raises organizational awareness of IS security risks and controls (Spears & Barki, 2010: 510).

ii. User participation contributes to an alignment between SRM and the business context (ibid: 510).

iii. Business-aligned SRM contributes to greater organizational awareness of IS security (ibid: 511).

iv. User participation contributes to perceived improvements in control development (ibid: 512).

v. Organizational awareness of SRM within a business process contributes to perceived improvements in control development for controls within that business process (ibid: 512).

vi. Organizational awareness of SRM within a business process positively influences the perceived performance of security controls (ibid: 513).

vii. User participation positively influences the performance of security controls (ibid: 513).

viii. Improvements in control development positively influences the performance of security controls (ibid: 513).

c) Based on the findings of the research

i. According to the study, we will be somewhat at a disadvantage without user participation, as “user participation [provides] needed contextual detail of a given business process” (Spears & Barki, 2010: 510) which helps to align security measures with the precise needs of the company.

   One benefit of the assignment is that the business has not yet digitalized, and it is quite small in scope. Needs of the enterprise should comprise of limited network needs, which should allow a comparatively robust risk assessment and security evaluation even without user participation.

ii. Because user participation is qualitative, quantitative analysis will most likely be the main form of data for the assignment – most likely in the form of other similar research studies. These should provide the breadth and depth required to then analyse and evaluate the needs of the assignment’s business.

iii. One nice aspect of the digital age is that there are numbers for everything – if there is not a precise study or statistic that aligns perfectly with the requirements of the assignment business, there will most likely be a similar study that can be used as a proxy to reference. If all else fails, admitting the limitations imposed is always a sound course.

References:

Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Risk Management. *MIS Quarterly* 34(3): 503.