Information Risk Management August 2021

« Collaborative Learning Discussion 1

Doug Leece

Initial Post

347 days ago

3 replies

Last 346 days ago

The journal article for discussion (Spears & Barki, 2010) states user involvement in the development and implementation of security controls may be considered beneficial by people within the security industry but there is little empirical evidence to support that position. The study's authors crafted a survey questionnaire based on information obtained through exploratory interviews with eleven people which resulted in 228 responses suitable for mathematical analysis.

The mixed method approach, supported by multiple fields of scientific study (Hanson, et al., 2005) justifies the study authors combining qualitative and quantitative assessment methods while obfuscating a potential bias flaw in the research. While qualitative assessment often requires limited initial investment and enables unconstrained exploration of matters which researchers may not fully understand, interview participants in this study were limited to a small group and narrow segment of information security (Spears & Barki, 2010). The survey responses provided a data set suitable for mathematical analysis, one of the benefits of quantitative analysis, but the data itself was essentially the opinions of a specific group of information security practitioners.

While the Sarbanes Oxley compliance focus prevents extrapolating security risk management will always benefit from user input, multiple interview respondents acknowledged the value of the contextual business information provided by the users. The concept of incorporating the input of people closest to the problem began gaining momentum in 1978 when IDEO brought design thinking to the market (IDEO, N.D) and has also proven to be successful within cybersecurity (Mohanty, 2019).

The lack of contextual business information prevents the development of customized controls for Acme manufacturing. Solution analysis will need to be based on publicly available research into small business information security requirements, with particular attention to any additional considerations applicable to manufacturing operations.

References

Hanson, W., Creswell, J., Plano Clark, V. & Creswell, J. (2005) Mixed Methods Research Designs in Counseling Psychology. *Journal of Counselling Psychology* 52(2): 224-235.

IDEO. (N.D) Ideo Design Thinking. Available from: https://designthinking.ideo.com/history [Accessed 18 August 2021].

Mohanty, R. (2019) Design Thinking In Cyber Security. Available from: https://www.paladion.net/blogs/design-thinking-in-cyber-security [Accessed 18 August 2021].

Spears, J. & Barki, H. (2010) User Participation in Information Systems Security Risk Management *MIS Quarterly* 34(3): 503-522.

Reply

Maximum rating: 👍 (1)

3 replies

1

Post by **Doug Millward**
feedback

347 days ago

Hi Doug - you make some great points - particularly around basing quantitative analysis on qualitative surveys or feedback (this is a particular bugbear of Hubbard (2009) but of course his views are by no means perfect) and about how to gather evidence to formulate the report. As has been noted elsewhere the intuitive answer is a combination of approaches - looking forward to discussing your views in the seminar.

Reply

2

↑ Reply to  **Doug Millward** from **Doug Leece**

Re: feedback

346 days ago

Hi Doug,

Maybe it just goes with the name but I share Mr. Hubbard's contrary disposition on many points. It actually started when I read "How to Measure Anything" (Hubbard, 2014) which I have found invaluable over the years when quantifying events in log data to identify approaches to fix SIEM rules.

I also located a paper on expert judgement in assessing safety risk (Rae & Alexander, 2017) that drew attention to how people with expertise in a certain area are often assumed to be knowledgeable in other areas as well. The questions in the survey ranged from quantifiable items such as control deficiency count to much more qualitative measures such as user business perspective. I am struggling to see how 238 different people could have similar levels of assessment skill over such a wide range of categories. From my perspective this variability of input jeopardizes the integrity of the mathematically derived output.

References

- HUBBARD, D. W. (2014). *How to measure anything: finding the value of "intangibles" in business*. 3rd ed. Hoboken, N.J., Wiley.
- Rae, A. & Alexander, R. (2017) Forecasts or fortune-telling: When are expert judgements of safety risk valid?. *Safety Science 99(B): 156-165*

Reply

Maximum rating: 👍 (1)

3

Post by **Doug Millward**
Hubbard

346 days ago

Generally, the Hubbard material seems very 'marmite' - love it or hate it. I feel it is excellent reading material - and the 'Failure of Risk Management' (link in the module resources) book poses a lot of questions and makes you think - which for me is always the mark of a good book :) However, I also think it's worth tempering with more up-to-date and academic resources - and then forming your own opinion :).

Reply

Add your reply

Your subject

Type your post

Choose Files No file chosen

Submit

Use advanced editor and additional options

Older discussion

Initial Post

Newer discussion

A few thoughts