Assignment 3: Applicability of Risk Management

Robert Salter

Stockholm University

Risk Management (RIMA)

Love Ekenberg

HT 2021

1. Introduction

The paper aims to critically reflect Cox's 2009 paper regarding issues with hazard-ranking systems and preferential alternatives to this approach. An analysis of Cox's 2011 commentary on the terms "accurate" and "small uncertainties" concerning the definition of scientific uncertainty in a risk management context follows before an evaluation of the appropriateness of Cox's arguments is considered in relation to previous assignments.

2. Critical Reflection of the Articles

2.1 What's wrong with Hazard-Ranking Systems?

The paper examines the shortcomings of hazard-ranking systems and his reasons why priority ranking systems achieve a sub-optimal allocation of resources for risk remediation. Hazard-ranking systems also include the terms risk-scoring methods or priority-scoring systems, which, as stated by Cox (2009), are used by many organisations to rate, rank or score different sources of risk, or risk-reducing opportunities.

Cox's primary argument is that risk scoring methods are unsuited to correlated risks. He finds that "common elements in multiple risky systems create correlated vulnerabilities, criticalities, consequences and threats" and that priority lists do not generate effective risk management decisions. Cox proposes considering risk in terms of a portfolio of risk-reducing opportunities that can achieve "significantly greater risk reductions for resources spent".

Cox finds that priority-based risk management systems are suitable when a collection of risk-reducing measures are independent with normally distributed values. In such cases, funding of risk reduction opportunities should be selected in order of decreasing priority to maximise total expected utility. Where costs are not

identical, the total certainty of a collection of risk-reducing activities should guide decision making, selecting the portfolio of activities with the highest certainty.

Cox raises the credible issue that additive scoring systems do not differentiate between the different elements and the decision maker's preferences towards reducing some aspects of the model, only taking the ranking score as the conclusion. To illustrate this point, an organisation that allocates risk-mitigating resources using a formula of event probability x lack of preventability would prioritise a risk with a high event probability (⅘) that can be prevented with certainty (lack of preventability 0/5) as equal to a risk with a moderate event probability (⅖) and a moderate lack of preventability(⅖). The fact that one risk can be prevented with certainty must surely make the first alternative preferential. In this case, using a multiplicative model would reflect a more optimal priority scoring system to negate this.

Cox states that the risk-scoring methods are sub-optimal for both the classification of risk and treatment of risks if uncertainties about the size of the risks are correlated. He finds that risk scoring systems rank the attributes of individual opportunities rather than considering correlations among several risk-reducing opportunities. In support of his argument, he provides numerous examples which, whilst reasonable in theory, are challenging to understand in a real-world context. The example of a decision problem in which a vulnerability-scoring system ignores opportunities for coordinated defences illustrates this point. The preferred solution by Cox is to protect half of the machines with certainty, which results in a lower number of expected successful attacks. Whilst this example may have been relevant in 2009, the example lacks context in 2021 under a background of ransomware attacks and prioritisation of cyber security by organisations. The decision-maker would indeed have a range of alternatives available.

The final example states that priority scoring ignores aversion to large-scale uncertainties. Cox's analysis is interesting in that the optimal choice for the decision-maker for small scale impacts is to take an uncertain intervention that, if successful, reduces the impact from 10% to 0% and for large-scale uncertainties, a certain intervention that reduces the impact from 10% to 5%. This example is

interesting in that Cox argues that using a priority scoring system would recommend the first choice suitable for a small number of targets yet be applied to a large number of targets and potentially result in excessive tail risk exposure.

Whilst Cox's analysis of the shortcomings of the priory-scoring systems in some cases is theoretical and confined to narrow examples, his conclusion that the application of investment portfolio optimisation principles can create better portfolios of risk-reducing activities is interesting. The crux of the paper is that priority-scoring systems ignore information about correlations amongst risks such as common vulnerabilities. This, in turn, introduces uncertainty to the effectiveness of risk-reducing measures.

2.2 Clarifying Types of Uncertainty: When Are Models Accurate, and Uncertainties Small?

Cox's paper responds to Professor Avens's paper of the clarifying of terms such as "scientific uncertainty" for use in risk management and the challenges of defining the terms "accurate" and "small" concerning risk models and input uncertainties. The original paper, according to Cox (2009), "proposes that scientific uncertainty should be considered greatest when no accurate prediction model can be established and least when one can be and when uncertainties about its inputs are "small" in some relevant sense."

This statement leads to the paper's motivation to understand the terms "an accurate prediction model" and "small uncertainty in its inputs".

In Cox's first example, the larger input uncertainties create smaller output uncertainties in a classification model as the range for classifying a value is proportionally extremely small. This example clarifies that certainty of inputs should not infer a greater certainty of outputs in predictive modelling.

The more relevant question that Cox raises is, when is a prediction model accurate? He raises whether a model that correctly describes an epidemic's evolution with

perfect accuracy makes it an accurate prediction model. Cox states his answer as "no", yet a prediction model must indeed be judged, in some respects, by the quality of its predictions and its usefulness as a prediction tool.

The second question is whether the same model with the same input data can be an accurate prediction model for some scientific or risk management decision purposes but an inaccurate one for others. The author agrees with Cox that a model may be an accurate predictor over short periods yet inaccurate over more extended periods or under conditions that differ from the input data. However, this must surely be the case for all models, given the constantly changing uncertainties in the world and the challenges of forecasting future events. Cox also compares just two alternative initial conditions, which seems narrow and unrealistic given the task of predicting an epidemic.

The challenge of analysing any risk model based on accuracy is that the absence of an event or failure to forecast successfully does not necessarily demonstrate that the model's conclusions are inappropriate. Models can be used to forecast potential states of the world from which risk mitigation measures can be derived. If the event does not happen, does this mean that the model was inaccurate and risk mitigation controls were unnecessary? The outcome should not solely gauge whether a decision was appropriate.

Cox finally questions whether an accurate risk prediction model should be causal. His example of replacing the component of a machine based on empirical actuarial techniques is a proactive example of risk control which confirms his reasoning that an accurate risk model need not be causal. The author finds that when attempting to answer such a complex question, there will be examples that confirm the need for causality and models performing accurate predictions without casualty.

3. Application to Assignments One and Two

Previous assignments have outlined a risk management process for a mobile payment project implemented by a Nordic commercial bank.

The bank developed a mobile contactless payment solution that works within Apple Wallet, Samsung Pay or Google Pay, allowing customers to make payments with their mobile phones. A risk management process focusing on the operational risks impacting the project was implemented using a project risk register which rated risks by impact and likelihood and including actions to be taken by the project managers to mitigate risk. The second assignment defined three risk analytical methods; a bow-tie analysis, SWOT analysis and the Delphi method, before concluding that the bow tie analysis was the most suitable for the mobile payments project.

Cox's insight raises interesting implications to the classification of risk in both analyses. Risks in the project risk register rated risks in terms of likelihood and magnitude before concluding an overall rating and next steps.

Risk Index	Risk Description	Current level of risk			Action to be taken
		Likelihood	Magnitude	Overall Rating	
1	Data leakage through the sharing of sensitive customer data with external suppliers.	Low	High	Medium	• Implementation of the company handbook/framework regarding outsourcing of operations, in partnership with the legal department.
2	IT system failure/crashes during the product launch.	Medium	Medium	Medium	• Staggered launch schedule. • Beta testing. • Soft launch product with no marketing preceding the full launch.
3	Poor customer service knowledge of new products.	Low	Medium	Medium	• Implement workshops and training for customer service. • Customer service included in beta testing.
4	Project delayed due to a lack of specialist IT knowledge.	Low	Low	Low	• Assessment of IT competencies • Recruit specialist consultants

5	Project over budget.	Medium	Medium	Medium	● Scrum teams. ● Project management team oversees the budget.
6	Delayed approval of outsourcing by the Financial Regulator (FR).	Low	High	Medium	● Partner with the compliance department to expedite application to FR.
7	Risk of IT issue between banking app and Samsung/Google /Apple app.	High	High	High	● Members of the banking app team to work on the project. ● Increased testing before launch.

Table 3.1: Selected risks from the project risk register (assignment one)

Cox's 2009 paper implies that this rating of the risks would lead to a sub-optimal allocation of risk resources due to the correlation of likelihood and magnitude and the correlation of the risk-reducing consequences. Whilst Cox presented his idea under a threat-vulnerability-consequence context, the correlation between likelihood and magnitude in the project risk register is unclear.

The correlation between risk-reducing activities (or actions to be taken) has more significant applications to the problem. There may be a correlation between the assessment of IT competencies (risk 4) and the project being over budget (risk 5). Assessment of IT competencies could improve the efficiency of IT resources which in turn may reduce the risk of the project coming in over budget. Similarly, finding a correlation in the impacts of a bow-tie representation may produce a more effective implementation of response controls.

Considering the interdependencies amongst the project risks, such as how they impact one another, how risk mitigation can positively or negatively impact other risks, and even in the context of the organisation and the broader risk register, is beneficial to an organisation. Cox's rank scoring insights would have wider implications for the bank's broader risk register and the bank's approach to internal risk measurement, where risks are evaluated in terms of exposure, probability of loss event, and the event's severity (BIS 2001). Considering correlations between risks would benefit the bank, and treating the risks in terms of a portfolio of risks would be a suitable strategy.

Regarding the implications of considering the accuracy of the risk register or uncertainty of the inputs, the qualitative analysis does not have the same complexity as a forecasting model. However, accuracy is essential to the thorough implementation of the risk management process. Inaccuracies regarding the classification of risks and remediating action can lead to the growth of unknown risks and incorrect or inadequate treatment, which could critically affect the project's success.

4. Conclusion

Cox's insight into the suboptimal outcomes for priority-scoring systems in risk management raises questions about its suitability throughout many industries. It is concluded that Cox's analysis of correlated risks and risk-reducing activities should be considered when classifying risks and considering mitigation strategies, yet the examples used in the papers are narrow and lack real-world context.

5. References

BIS., (2001). *Consultative Document Operational Risk* [online]. BIS [Viewed 16 September 2001]. Available from: https://www.bis.org/publ/bcbsca07.pdf

Cox Jr., L. (2009). *What's wrong with hazard-ranking stems? An expository note: Perspectives.* Risk Analysis, 29(7), 940-948.

Cox Jr., L. (2011). *Clarifying Types of Uncertainty: When Are Models Accurate, and Uncertainties Small?*. Risk Analysis: An International Journal, 31(10), 1530-1533.