Chapter 43
Factors Comprising Effective Risk Communication, Decision-Making, and Measurement of IT and IA Risk

Ricardo Daza
University of Fairfax, USA

Kathleen M Hargiss
University of Fairfax, USA

ABSTRACT

This article focuses on factors that comprise effective risk communication, decision-making, and measurement of information technology (IT)/ information assurance (IA) risk. A review of the extant literature provided the basis for the formulation of research questions. The sample population consisted of senior IT/IA practitioners from Florida chapters of information security professional organizations. Results of this study found that decision making, and measurement are all factors in effective risk communication of IT/IA risk to non-IT personnel. This research has implications for both IT/IA practitioners and recipients of risk communication through the identification of factors which influence IT/IA professionals in how and why IT/IA risk communication take place, and consequently, how to simplify and improve its effectiveness.

INTRODUCTION

For years the information technology (IT) department, and by extension, the information assurance (IA) department, has been perceived by board members and senior management as "someone who is managing back-office technology" (Wysopal, 2015). This is in part due to the inability of the departments to communicate using a common language. The IT/IA department speaks geek and managers speak business. According to Wysopal (2015), Chief Information Security Officers (CISOs) need to communicate the

DOI: 10.4018/978-1-7998-1760-4.ch043

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

level of risk in terms that board members can understand, namely using numbers not acronyms. This study examined the challenges of how to effectively communicate IT/IA risk information to an extra-departmental audience. The effectiveness of that communication is judged by both the quality of the information relayed in the message and the decisions they affect.

Background

Information Security can be thought of as an economics problem. According to Sowell (2014) economics is the study of the allocation of scarce resources to satisfy an infinite demand. Organizational governance entails the allocation of resources (human resources, financial capital), across the organization's various departments. No organization has sufficient resources to satisfy every request by every department. Therefore, those entrusted with organizational governance (typically senior management or a board of directors) must make difficult decisions on how best to allocate scarce resource to most effectively achieve organizational goals.

IT/IA departments are required to communicate to extra-departmental stakeholders about the risks to the organization from the use of information technology. According to Gigerenzer (2015), the best way to ensure risk-savvy decision-making, is through the introduction of knowledge about risk. If the objective is to perform effective risk communication, then IT/IA practitioners or anyone interested in effective communication of risk information must consider what makes effective versus ineffective risk communication. The most obvious factor might be decision quality, but that assertion necessitates further exploration regarding what constitutes a good decision versus a bad one. It may be tempting to say the quality of the outcome, but we are talking about decisions regarding risk, and thus, necessarily have a component of uncertainty.

Much of the literature in the decision sciences relies on gambling decisions to illustrate concepts and one is leveraged here. When a decision-maker bets with lower odds of success, and thus a higher payoff, regardless of the outcome of the wager, poor decision-making is likely because the statistical probability of winning is so low. The measure of a good decision regarding risk then is not solely about the outcome, but also the thought processes and logic used by the decision-maker, which brings us back to the information that was communicated, in what format was it presented, and how it was collected. The quality of those aspects should also be considered, such as the risk message content, its accuracy, complexity, clarity, and ability to overcome counterproductive natural human tendencies to make poor risk judgment (Cho, Torsten, & McComas, 2015). Evaluating the risk message in this last aspect is particularly challenging as no two people react the same way to identical risk information. Factors such as cultural background, education, professional training, age, gender, and racial identity can influence how risk is judged and highlights the importance of knowing one's audience (Cho et al., 2015).

The recipient of a given risk message can present an unknown quantity in most situations; unless the message is intended for only one recipient and that individual's identity and message profile is known in advance of message construction. If the intended audience is a heterogeneous group, the challenges are not only the influences of individuals making up the group such as gender, racial identity, age, et cetera, but also each individual's preconceived notions. Research demonstrates that media exposure informs many of our perceptions about risk and thus can influence decision-making (Bodemer, Müller, Okan, Garcia-Retamero & Neumeyer-Gromen, 2012). Information about risk from the media can distort risk beliefs as media outlets have different goals from the IT/IA practitioner and their stakeholders. Media has the objective of selling something, and sensationalism is the tool of choice, statistical accuracy is a decidedly low priority.

18 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/factors-comprising-effective-risk-communication-decision-making-and-measurement-of-it-and-ia-risk/245485

Related Content

Are the Payments System and e-Banking in India Safer than in other SAARC Members?
Rituparna Das (2020). *Start-Ups and SMEs: Concepts, Methodologies, Tools, and Applications (pp. 1646-1663).*
www.irma-international.org/chapter/are-the-payments-system-and-e-banking-in-india-safer-than-in-other-saarc-members/245530

AHP-Driven Knowledge Leakage Risk Assessment Model: A Construct-Apply-Control Cycle Approach
Haley Wing Chi Tsang, Wing Bun Leeand Eric Tsui (2020). *Start-Ups and SMEs: Concepts, Methodologies, Tools, and Applications (pp. 218-237).*
www.irma-international.org/chapter/ahp-driven-knowledge-leakage-risk-assessment-model/245453

Capacity Building in SMEs
Stephen M. Mutula (2010). *Digital Economies: SMEs and E-Readiness (pp. 248-264).*
www.irma-international.org/chapter/capacity-building-smes/36114

Optimizing Virtual Communities in Tourism to Facilitate Development of Small and Medium-Sized Enterprises
Silvena Dencheva Yordanova (2020). *Start-Ups and SMEs: Concepts, Methodologies, Tools, and Applications (pp. 1023-1041).*
www.irma-international.org/chapter/optimizing-virtual-communities-in-tourism-to-facilitate-development-of-small-and-medium-sized-enterprises/245495

Sources of Innovation and Success in the Food Service Industry
A.T. Juntunen (2013). *Small and Medium Enterprises: Concepts, Methodologies, Tools, and Applications (pp. 1790-1804).*
www.irma-international.org/chapter/sources-innovation-success-food-service/76044