Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Effect of network infrastructure factors on information system risk judgments

Jennifer A. Cowley [a,**,1], Frank L. Greitzer [b,*], Bronwyn Woods [a]

[a] Carnegie Mellon University/Software Engineering Institute, Pittsburgh, PA 15213, USA
[b] PsyberAnalytix, Richland, WA 99352, USA

ARTICLE INFO

Article history:
Received 31 July 2014
Received in revised form
21 April 2015
Accepted 25 April 2015
Available online 5 May 2015

Keywords:
Network security
Risk perception
Risk judgment
Information system risk
Vulnerability
Security metric
Network topology
Network risk assessment
Risk management

ABSTRACT

Little is known about how perceived network topology factors, which are common components of information system risk metrics, impact human judgments of risk. Using a half-fractional factorial design, this study experimentally manipulated five perceivable network topology factors (*network partitioning*, *network diversity*, *wireless status*, *network footprint* and *connectivity*) to assess the relationship between these factors and network risk judgments. The consistency of network risk ratings and rankings were evaluated for each of the 16 network topologies across a sample of 55 network security professionals who reviewed these topologies. Three robust significant main effects (*network partitioning*, *wireless status*, and *connectivity*) and one significant interaction (*network partitioning* X *wireless status*) were found. While some topologies were consistently rated and ranked as significantly more risky than others, there was some variability in ratings at each main effect level as well as the spread of the mean ratings between the two main effect levels (e.g., *wireless* and *wired*). We discuss the implications of our findings with respect to network risk metric rigor.

1. Introduction

Risk to information systems, which includes *network risk*, arises from threats to information systems that can cause the loss of data confidentiality, integrity, or availability and includes the adverse impacts to organizational operations (e.g., mission, functions, image, or reputation), organizational assets, individuals, or other organizations (NIST SP 800-53, 2013). The measurement of network risk in particular is important for a variety of reasons. First, networks are integral to communications between computers in an information system, thus they enable access to critical vulnerabilities that attackers seek to exploit. Effort spent to reduce risks through secure network configuration can limit access to those vulnerabilities, thus reducing overall system risks. Second, the measurement of network risk is important because organizations use risk metrics to prioritize how to spend their limited resources to secure their information systems (Elky, 2006; NIST, 2012). In current practice, an organization's network risk can be assessed with any of these metrics: Operationally Critical Threat, Asset, and Vulnerability

* *Corresponding author*. Tel.: +1 509 539 4250.
** *Corresponding author*.
E-mail addresses: jcowley@cert.org (J.A. Cowley), Frank@PsyberAnalytix.com (F.L. Greitzer).
[1] Tel.: +1 412 268 4461.
http://dx.doi.org/10.1016/j.cose.2015.04.011
0167-4048/

Evaluation (OCTAVE) (Alberts and Dorofee, 2001); NIST SP 800-30Rev1 (NIST, 2012) and the NIST CVSS V2.10 network risk measure; CORAS (Aagedal et al., 2002); and Risk Management Framework (RMF) (Verdon and McGraw, 2004).

Rigorous risk metrics are difficult to validate because they depend upon the composition of human perceptions of physical elements (e.g., computers, software, firewalls, etc.) and non-physical abstractions (e.g., adversary type, subjective security levels, etc.). We identified two critical issues that must be addressed to improve the rigor of network risk metrics in light of these challenges. First, neither the risk research community nor network security practitioners have converged on an empirically validated definition of network risk (Renn, 1998) involving the objective and subjective components of network risk. Consequently, if practitioners are not using the same definition of risk, then miscommunications results (Fischhoff, 2009) that leads to confusion, incorrect assumptions or inaction. Second, the subjective component of network risk metrics (e.g., the NIST CVSS V2.10), introduces variance in human risk judgment. If these metrics include factors (e.g., availability, integrity, etc.) with high disagreement about the risk level of those factors, then the metric's underling model may have too much variance and suffer reliability and validity reductions. Due to the lack of published research on metric generation and validation for network risk metrics, it is unclear how much variability in the underlying metric model can be attributed to human judgments of subjective factors, such as availability. In addition to human perceptions of the network environment, other factors also impact human judgment such as memory lapses, personal experiences, attitudes and opinions, and perceptual biases (e.g., Pamula et al., 2006; Gilovich et al., 2002).

To address these issues, we conducted an empirical investigation of the impacts of experimentally manipulated network topology factors (network partitioning, network diversity, wireless status, network footprint and connectivity) on expert judgments of network risk. Through both exploratory and quantitative analyses of risk rating and ranking data, we sought to identify those factors that were important for network risk judgments and to assess the variability among expert ratings and rankings of network risk. This study therefore examined characteristics that are potentially important to consider in any model of network risk and which should inform efforts to standardize subjective ratings used in network risk assessment.

This paper is organized as follows: Section 2, reviews related research and theory on the challenges of network risk metrics; Section 3, presents the research questions; in Section 4, we present the experimental method and procedure, including the participant sampling and study materials used; Section 5 reports the results of exploratory and statistical modeling of the data obtained; and finally Section 6 discusses the results, implications and limitations of the study, and possible future research.

2. Related work

In this section, we first review the phenomenology of risk before we review research from the social sciences on how perception can influence judgment as it pertains to risk, and how the measurement of judgments is challenging.

Risk is a socially constructed phenomenon (Kukla, 2000): its meaning and how it is represented is based on a degree of agreement among the parties affected, each of whom has the ability to modify and evolve this meaning over time. For example, people have different opinions of what happiness is and how it is visually represented. In contrast, physical height is not socially constructed; its measurement does not entail the subjective interpretation of what height is; however, the interpretation of tall vs. short is socially constructed and is relative to individual experiences. Because happiness is identified through subjective interpretation of visual cues that differs across group cultures (Diener, 2000), no single representation of happiness theoretically exists. The class of psychometrics that measure socially constructed phenomena is not designed to reduce the importance of the subjective judgments; the subjective judgment is the foundation of this class of psychometrics. Like happiness, the socially constructed concept of network risk is likely based on idiosyncratic interpretations of what network risk is and how it is identified. Yet, network risk publications (Longstaff et al., 2000; Pamula et al., 2006) often try to minimize the subjective component of risk metrics to improve their objectivity. This impacts metric validity because the concept of risk is based on group consensus. Therefore, we question the validity of network risk metrics that are designed from a single person's (the metric designer) vantage point given that one this single view point may run counter to the perspectives of the population of network risk professionals. Our research approach exclusively focuses on the subjective interpretation of network risk in order to understand how network risk is socially constructed.

Prior research identified the term *risk* as a psychological construct (Cronbach and Meehl, 1955), typically represented by the aggregation of *dimensions* (e.g., likelihood of adversarial penetration, impact of a lack of network resilience, etc.). Arguably, dimensions could be considered types of risk (e.g., financial risk, availability risk, competing-mission risk, etc.) but grounded analysis research is required on human network risk judgment to determine the degree of orthogonally between *dimensions* and *types of risk*. Furthermore, dimensions are based on perceived, tangible cues in the network environment that we call *factors* (e.g., zero redundant connections to the internet). We conjecture that a relationship exists between a person's definition of network risk, their own dimensions that they believe are important to risk, and the factors that they perceive and consider for risk judgment. To our knowledge, there is no agreement about how the term risk is defined and what dimensions constitute risk (Bauer, 1960; Crespo et al., 2009; Dowling, 1986; Fischhoff, 2009; Gemünden, 1985; Haimes, 2009; Ingene and Hughes, 1985; Ross, 1975). The term network risk suffers the same lack of agreement (Renn, 1998). We know from prior research that network risk judgments are based on perceptions of network vulnerabilities, threats (e.g., adversaries, natural disasters, etc.), asset importance, resilience, and counter measures (Alberts and Dorofee, 2001; Ghandi and Lee, 2011; see also DOD Instruction 8500.2 available at, http://fas.org/irp/doddir/dod/d8500_2.pdf). However, we do not know the degree of