Government Information Quarterly 32 (2015) 108–117

Contents lists available at ScienceDirect

Government Information Quarterly

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

'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection

Kevin Quigley [a,*], Calvin Burns [b], Kristen Stallard [a]

[a] School of Public Administration, Dalhousie University, 6100 University Avenue, PO Box 15000, Halifax, Nova Scotia, Canada B3H 4R2
[b] Department of Human Resource Management, Strathclyde Business School, University of Strathclyde, Graham Hills Building, 50 Richmond Street, Glasgow, UK G1 1XU

ARTICLE INFO

Available online 26 March 2015

Keywords:
Cybersecurity
Risk perception
Availability heuristic
Management gurus
Rhetoric
Critical infrastructure

ABSTRACT

This paper draws on the psychology of risk and "management guru" literature (Huczynski, 2006) to examine how cybersecurity risks are constructed and communicated by cybersecurity specialists. We conduct a rhetorical analysis of ten recent cybersecurity publications ranging from popular media to academic and technical articles. We find most cybersecurity specialists in the popular domain use management guru techniques and manipulate common cognitive limitations in order to over-dramatize and over-simplify cybersecurity risks to critical infrastructure (CI). We argue there is a role for government: to collect, validate and disseminate more data among owners and operators of CI; to adopt institutional arrangements with an eye to moderating exaggerated claims; to reframe the debate as one of trade-offs between threats and opportunities as opposed to one of survival; and, finally, to encourage education programs in order to stimulate a more informed debate over the longer term.

1. Introduction

There is a tension at the centre of our relationship with technology. On the one hand, there is incredible optimism that information technology can simultaneously improve service delivery and cut costs (Layne & Lee, 2001; Sharif, 2008). On the other hand, there is burgeoning IT security literature that warns that our increasing dependence on technology is becoming a liability because the technology can be so easily attacked by those with malicious intent, and the critical infrastructure and services that depend on it can be so easily discontinued (Clarke & Knake, 2010). Our paper is particularly interested in the latter claim. Much of the research on computer security and critical infrastructure protection, however, focuses on the ways in which organizations secure their networks and information in the supply chain (Faisal, Banwet, & Shankar, 2006; Kolluru & Meredith, 2001; Von Solms & Van Niekerk, 2013). Less attention has been paid to how organizations construct and understand cybersecurity risks. Our failure to do so constitutes a risk in itself. It is not enough for systems to be secure; they have to seem secure (Bertot, Jaeger, & Grimes, 2010).

There are three purposes to this paper. The first is to provide an understanding of how cybersecurity risk is constructed. We will draw on the psychology of risk literature to show that people have numerous biases that prevent them from drawing reliable inferences in the face of uncertainty. Following this, we examine 'management gurus' literature, which explains how consultants, academics and authors who profit from selling solutions to complex organizational issues persuade audiences of the usefulness of their ideas. Secondly, we use the techniques Nørreklit (2003) employed in her rhetorical analysis of *The Balanced Scorecard* to analyze cybersecurity discourse in ten recent publications. The publications range from popular print media to TED Talks to academic and technical articles. We are particularly interested in examining the extent to which cybersecurity specialists are using management guru techniques and manipulating common cognitive limitations in order to over-dramatize and over-simplify cybersecurity risks.

Finally, using a cybernetic understanding of control (information gathering, standard setting and behaviour modification), we examine the policy challenges that emerge as a result of the present framing of cybersecurity risks. The ultimate goal will be to question the effectiveness of how we talk about and raise awareness of cybersecurity issues in general and what policies we should adopt to address potential weaknesses in governance of cyberspace that are aggravated further by the present cybersecurity discourse.

2. The psychology of risk and the techniques of management gurus

2.1. The psychology of risk

Burns (2012) argues it is important to understand risk perception for two reasons. First, risk perception helps us to understand and predict people's behaviour. Secondly, awareness of how perceptions are

* Corresponding author.
E-mail addresses: kevin.quigley@dal.ca (K. Quigley), calvin.burns@strath.ac.uk (C. Burns), kstallard@amans.ca (K. Stallard).

http://dx.doi.org/10.1016/j.giq.2015.02.001
0740-624X/

constructed helps to improve communication between technical experts and laypersons. The psychometric paradigm draws on the work of cognitive psychologists such as Slovic, Fischhoff, and Lichtenstein (1982) to conceptualize risks as personal expressions of individual fears or expectations. In short, individuals respond to their perceptions whether or not these perceptions reflect reality. The study of risk perception has grown significantly over recent decades and has constituted a significant challenge to rational actor approaches to risk (see for example Arrow, 1971; Jaeger, Renn, Rosa, & Webler, 2001; Lachlan & Spence, 2010; Pachur, Hertwig, & Steinmann, 2012; Pennings & Grossman, 2008; Pratt, 1964; Slovic, 1987). The psychology of risk literature has identified several biases in people's ability to draw inferences in the face of uncertainty. Risk perception can be influenced by properties such as personal control (Langer, 1975), familiarity (Tversky & Kahneman, 1973), exit options (Starr, 1969), equitable sharing of both benefits and risks (Finucane, Slovic, Mertz, Flynn, & Satterfield, 2000) and the potential to blame an institution or person (Douglas & Wildavsky, 1982). It can also be associated with how a person feels about something, such as a particular technology or a disease (Alhakami & Slovic, 1994). People also show confirmation bias (Wason, 1960), which suggests they seek information to confirm how they feel, not to challenge it.

A central finding of the risk perception literature is that perceptions are often, in fact, faulty, when we consider consequence *and* probability (Slovic et al., 1982). Risk cannot be directly observed; rather, it is constructed by people based upon their understanding of hazards in everyday life. People often make judgments about risk using incomplete or erroneous information. They also rely on judgmental biases or heuristics to comprehend complexity. Heuristics are cognitive tools people use to analyze risk and complexity (Slovic et al., 1982). In some ways, they are helpful; heuristics allow people to render simplistic understandings of complicated subjects. However, they can also oversimplify or distort our understanding. Heuristics fall along two primary dimensions: the unknown factor and the dread factor. The unknown factor influences people to be more concerned with risks that are not observable or known to science (Slovic et al., 1982). On the other dimension, the dread factor influences people to be more concerned with risks that are not controllable and pose potentially catastrophic consequences (Slovic et al., 1982).

One of the most common heuristics is *availability*. Under the influence of the availability heuristic, people tend to believe that an event is more likely to occur if they are able to imagine or recall it easily (see for example Betsch & Pohl, 2002; Folkes, 1988; Maldonato & Dell'Orco, 2011; Slovic, Fischhoff, & Lichtenstein, 1979; Tversky & Kahneman, 1973). For instance, fear of shark attacks increased dramatically after the release of the movie *Jaws*, despite the fact that there was no empirical evidence to suggest that shark attacks had suddenly become more probable (Slovic et al., 1979). By contrast, availability can also lull people into a false sense of security regarding the risks associated with everyday tasks, such as in the workplace or the home. Availability is considered to be one of the most important heuristics for understanding risk perception (Sjöberg, 2000). For instance, the availability heuristic influences people to be concerned about terrorist attacks despite the fact that – like other many high-profile risks – it is considered to be extremely unlikely (Gierlach, Belsher, & Beutler, 2010). This phenomenon is referred to as 'probability neglect' (Slovic, Peters, Finucane, & Macgregor, 2005). When probability neglect is at work, "people's attention is focused on the bad outcome itself, and they are inattentive to the fact that it is unlikely to occur" (Sunstein, 2003, p. 122). In other words, people tend to overemphasize the consequences of risks while minimizing or even ignoring the probabilities.

2.2. Management gurus

The term 'management guru' refers to the authors, publishers, editors, consultants, managers, commercial seminar organizers and professors who offer advice on business and management (Kieser, 1997). The field is primarily interested in "how management knowledge is created, processed into saleable products and services, how it is marketed, communicated to customers, and how it is consumed by them" (Huczynski, 2006, p. 2). The field has also attracted business and management academics critical of the ambitious prescriptions offered by management gurus. The management guru literature can therefore be understood as both a reaction against and response to the popular literature on business and management.

There are three key themes in the management guru literature: how guru ideas become popularized, their unique appeal to managers and common techniques.

Management gurus are considered to be influential because they inspire managers to implement their solutions to solve complex organizational problems (Huczynski, 2006). A key finding of the literature is that these cures come and go over time. Kieser (1997) likens the rise and fall of management trends to the fashion industry. He notes that "at the start of the fashion, only a few pioneers are daring enough to take it up. These few are joined by a rising number of imitators until the fashion is 'out' and new fashions come on the market" (Kieser, 1997, p. 51). In addition to explaining the rise and fall of management trends, this metaphor is helpful for capturing the influential role that aesthetics play in management trends as well. Røvik (2011) argues that the rise and fall of management trends can also be compared to the lifecycle of a virus. The virus theory helps to explain what happens to organizations once they have been 'infected' with a new organizational idea. Organizations typically go through the stages of "infectiousness, immunity, replication, incubation, mutation, and dormancy" before the next fad takes hold (Røvik, 2011, p. 635). Finally, organizations do not build immunity to management fads over time. Despite the fact that guru ideas have only a modest impact on actual working life, managers always seem prepared to entertain the next trend.

One of the central questions of the literature is why managers are particularly susceptible to guru ideas, especially given their limited practical results. Ahonen and Kallio (2009) argue that guru ideas are a form of cultural expression. From this perspective, the management model is the Holy Grail "to which all seemingly good values and ideas have been projected" (Ahonen & Kallio, 2009). Much like the quest for the Holy Grail, the search for the ideal management model is more important than the model itself. It also represents many ideals in liberal Western democracy, such as the never-ending quest for "efficiency, success, and welfare" (Ahonen & Kallio, 2009, p. 433). As such, the search for the best management ideas serves a therapeutic role for managers and gurus alike. Other researchers explain the appeal of gurus through their impressive performances. Clark and Salaman (1996) liken these performances to that of a witchdoctor since gurus give "a 'dramatic realization' in which the performer conveys to an audience that which they wish to express" (p. 91).

The literature also accounts for how popular management ideas become influential. One of the fundamental findings is that rhetoric is a common and influential technique. For example, Hood and Jackson (1991) argue that persuasion fuels organizational change more often than objective facts. In their view, speakers attempt to establish their theories as the most credible, not necessarily the most truthful. To this end, Hood and Jackson (1991) identify six salient features of administrative arguments: their universal appeal, contradictory nature, instability, use of recycled ideas, reliance on soft data and logic, and competition with rival ideas through aesthetics rather than evidence. Berglund and Werr (2000) support Hood and Jackson's (1991) typology, adding that management gurus rely on the use of contradictory business myths or ideas to adapt their arguments to suit any need or audience. Furthermore, Keulen and Kroeze (2012) bring attention to the way management gurus frame their arguments using historical narratives or anecdotes to express the soundness of their ideas. The use of anecdotes is also a persuasive method to position management gurus as the purveyors of practical knowledge in contrast to the theoretical