Introduction

Michael Workman

Nathan M. Bisk College of Business,
Florida Institute of Technology,
150 West University Blvd.,
Melbourne, Florida, USA
E-mail: workmanfit@yahoo.com

Biographical notes: Michael Workman received his PhD from Georgia State University and came to academic life in 2001 with nearly 30 years of experience in the computer industry where he began as a Software Engineer, then moved into management and executive management. He is currently a Full Professor with the Florida Institute of Technology, and he has published over 40 manuscripts and proceedings.

The ability to spread information and misinformation over the internet in blogs and social media websites has become accompanied by the growing pattern of cyber harassments against professionals and corporations. In many cases, harassments may arise from a process of critical discourse or from differences of opinion, but increasingly such harassments have more malevolent motives. In the latter case, the attack – we may call cyber smearing – is deliberately contrived to harm or extort from the legitimate financial interests of companies, and may include as its weapons harassment, defamation, tort interference, or other offences that can damage corporate valuation.

To illustrate, in 2007 a company had produced a new information integration and visualisation technology, and they had begun negotiation to sell the company to a suitor. The company's product had been purchased by many domain knowledgeable experts at several multi-billion dollar companies and several government agencies worldwide, all of whom had carefully inspected the technology and considered their returns on investment. However, the prospective suitor told the board of directors that the valuation of the company had been significantly diminished as the result of 'attacks' by a single blogger using many *self-promoting* web pages and on *trash-talk* blogs and website linkages used to elevate the attack visibility from internet search engines.

In these attacks, the blogger proclaimed himself: 'An expert in information visualisation' even though his academic education was in the unrelated field of *religion studies*. The blogger had never developed any commercial software product or published any reviewed scholarly research. Yet, the blogger not only dogmatically attacked the company's product, but also people associated with it, including their customers and even academic researchers who the blogger claimed were vested in the company because they had published favourable original studies of the information visualisation method. In these attacks, the blogger took out of context bits of personal e-mail messages sent to him by some of his victims who made attempts to be conciliatory, to clarify, and point out some of his incorrect statements, and he manipulated them and distributed the fabrication in what he called a 'newsletter' and posted it online with his stated intention to *prevent the company from selling its product* (Workman, 2010).

The financial damages associated with cyber smears such as illustrated in the previous example are difficult to come by partly because of the under reporting of the incidents and partly because of the scope of the problem. Nevertheless, the costs to businesses are noteworthy (Casarez, 2002). Some corporations, with significant financial resources, use what are commonly called strategic lawsuits against public participation (SLAPP) to dampen the spread of negative information. However, as was noted by Riley and Vance (2011) about the 2011 Sony Online Entertainment security breach, such a tactic may backfire by popularising the very information the company is trying to suppress. Also, because these attacks take place over the internet, recourse through civil litigation may be complicated and expensive, or made difficult in pursuing attackers from abroad or circuitous routes. This leaves the victim in a vulnerable state. As with other types of internet attacks, the attacker relies on this vulnerability to exploit for personal gain. Consequently, other approaches companies have used to deal with this problem have included attempting to ascertain the motives of those who harass corporations to determine whether to ignore them, or make attempts to defend against them in some other fashion such as using reputation management services and techniques, or try to placate the attacker by acceding to the attacker's demands.

Because the problem of harassment has been primarily studied in relation to proximal (e.g., in the office) incidents, or in relation to school children online, there is little in the body of academic literature to guide management decision-makers regarding cyber harassment or smearing against professionals and corporations. Thus, the aims of this special issue of the *International Journal of Management and Decision Making* are to open the discussion and begin the examination of the conflicts between free speech and due process, the psychological makeup of cyber harassers, motives for cyber smearing, and present some of the impacts to businesses and available countermeasure options to inform management decision-making.

References

Casarez, N.B. (2002) 'Dealing with cybersmear: how to protect your organization from online defamation', *Public Relations Quarterly*, Vol. 47, No. 2, pp.40–45.

Riley, M. and Vance A. (2011) 'The company that kicked the hornet's nest', *Business Week*, May, pp.35–36.

Workman, M. (2010) 'A behaviorist perspective on corporate harassment online: validation of a theoretical model of psychological motives', *Computers & Security*, Vol. 29, No. 8, pp.831–839.