Emerging developments in organizational risk

Kurt J. Engemann
Center for Business Continuity and Risk Management, Iona College, New Rochelle, New York, USA

Received 18 March 2019
Revised 18 March 2019
Accepted 19 March 2019

Abstract

Purpose – Unforeseen crises can result in significant losses for unprepared organizations. A paradigm for risk management discloses that threats can lead to crisis events which can have immense negative consequences. Analyzing risks and making appropriate decisions regarding them is very challenging but crucial. Emerging developments in organizational risk reveal similar characteristics among evolving threats. Effective risk management requires insightful leadership and is essential for an organization to achieve security. The paper aims to discuss these issues.

Design/methodology/approach – The authors explore some emerging developments in organizational risk, by highlighting evolving concerns and identifying their common characteristics. The authors then discuss key resources and recommend approaches in managing organizational risk.

Findings – Evolving concerns in organizational risk include: infrastructure risk, enterprise risk, information security risk, supply chain risk and new technologies risk. The most troubling threats to an organization tend to have some risk characteristics in common. These attributes are useful in identifying further threats.

Originality/value – Managing risk is an enormous challenge that all organizations encounter. Understanding the common characteristics of evolving risks that are currently under scrutiny can provide insight into identifying further threats to organizations. With these common characteristics understood, the primary resources of solid leadership, risk analytics and professional business continuity management can aid in the recognition of additional obscured but growing risks and be beneficial in providing security for an organization.

Keywords Leadership, Risk, Technology, Supply chain

Paper type Research paper

Challenges in managing risk

Managing risk is an enormous challenge that all organizations encounter. Unexpected crises can unleash incalculable deleterious consequences, as failing to plan appropriately can not only be injurious to humans but can also drastically affect the entire venture. Risk management includes assessing risks, evaluating alternatives and implementing strategies.

Various approaches to defining risk add to our acumen of risk. Basically, risk may be defined as the possibility of experiencing an event characterized by probability and impact (Engemann and Henderson, 2012). Some descriptions handle risk objectively while others consider it subjectively. The risk viewpoint chosen influences the manner in which risk is analyzed and has significant implications for risk management (Aven, 2012).

A basic principle of risk management is that while risk cannot be eliminated, it can be controlled to some extent. The main objective of risk management is that of safety and protection of life. Examining potential risks and selecting suitable courses of action is very demanding but essential. Deciding on a risk management strategy includes balancing costs and benefits. Management must offer leadership and guidance regarding strategy selection and determine the organization's acceptable level of risk tolerance.

In this paper, we explore some emerging developments in organizational risk, by highlighting evolving concerns and identifying their common characteristics. We then discuss key resources and recommend approaches in managing organizational risk.

Evolving concerns

Some risk events arise from natural threats such as: earthquakes, fire, floods, hurricanes, tornadoes, tsunamis and Winter storms. A multitude of other situations also threaten

Continuity & Resilience Review
Vol. 1 No. 1, 2019
pp. 26-35

2516-7502
DOI 10.1108/CRR-03-2019-0011

organizations, including: accidents, crime, cyber-attacks, energy shortages, financial crises, infrastructure failure, power outages, strikes and terrorism. Management is charged with the duty of preparing for disasters which includes: safeguarding life, caring for the environment, protecting assets and continuing operations. Risk assessment includes determining event probabilities and estimating potential losses, both of which are quite difficult given the infrequency and breadth of these events.

Evolving concerns in organizational risk include: infrastructure risk, enterprise risk, information security risk, supply chain risk and new technologies risk. These risks are discussed below, with some examples provided in each category for illustrative purposes. These risks are not disjointed, but intersect with one another, however, for simplicity each will be briefly discussed separately.

Infrastructure risk

Infrastructure is the foundation upon which organizations function. Crucial infrastructure includes: banking, electricity, emergency services, gas, oil, telecommunications, transportation and water. Infrastructure is susceptible to decay and damage from disasters. Some natural disasters may provide forewarnings and therefore permit time for preparations to be made. Some disasters occur without notice, for example accidents or malicious acts. Additionally, the political climate may have negative implications of civil unrest for a location, resulting in infrastructure destruction. Economic security depends upon the critical infrastructure that provides the framework for business continuity (Engemann and Miller, 2009).

An epic single infrastructure point-of-failure is the global financial system. Organizations discover how dependent they are on the banks when the threat of banking crisis appears imminent. The transportation system is at risk of disruptions in many ways. Modern civilization depends upon the electric grid and threats exist that can substantially impact the electric grid over extended periods of time, with some consequences being extreme (Miller and Engemann, 2015).

Infrastructure risk is inherent in densely populated areas, and with the complexity of urban functions comes vulnerability to disruption of communication, power, utilities and transportation. Harmful effects of chemicals and ecosystem deterioration present potential risks to human health (Marolla, 2016). The strength of society and the economy are dependent on public health.

When disaster strikes at the infrastructure, local immediate response is necessary, often without the direction of centralized authorities. The initial leaders in a disaster may not be members of an organized response structure. The framework for assessment of resilience is inferred from self-organization in complex chaotic environments (Lalonde, 2004). A shift to disaster resilience is a more proactive expression of community engagement (Cutter *et al.*, 2010).

Flooding is a threat to the infrastructure in many areas. Vulnerability to disruptions arises because of insufficiency of preparation, and some forecasts indicate that flooding is expected to further increase in severity (Bannock, 2005). Damage to infrastructure and the ensuing business closures may hamper recovery efforts of local communities and affect the society at large (Tierney, 2007).

Immediate infrastructure for an organization includes buildings and equipment. Every location is susceptible to threats which can disrupt a business and those threats need to be assessed relative to the organization's tolerance level. The type of building construction should be examined based upon the potential disasters. Recent innovations in earthquake resistant construction may allow a building to survive the resultant shaking from certain magnitude earthquakes, however buildings may remain vulnerable to resultant flooding.

Enterprise risk

Risk management challenges are faced by organizations in every industry, whether it is banking, education, energy, healthcare, insurance, manufacturing or transportation.

The primary focus of enterprise risk management is that of risks to the organization's resources, with special attention given to safety, environmental, compliance, governance, security and financial risks.

Operations, marketing and finance are the principal functional areas of an organization and are closely interrelated, where: operation is responsible for producing services and goods; finance is responsible for the organization's financial assets; and marketing is responsible for creating and fulfilling demand. The various areas of an organization are affected by changes elsewhere. Rapid technological changes have created opportunities and risks for organizations, especially regarding the use of information systems for the processing of financial and accounting data.

Accounting information systems process transactions through an organization and are vital in tying an enterprise together to ensure its proper functioning. Investment in these enterprise systems provides responsiveness in decision making and enables built in controls, thereby reducing internal weaknesses (Morris, 2011). As accounting information systems continue to evolve, they become more engrained into the organization's operations but also become increasingly complex. It is this complexity of enterprise systems that itself poses exposure to a multitude of additional risks. The validity of the output is compromised if the initial data provided are not accurate. There is a risk that the programmer did not precisely comprehend the intended calculations and created a logical error in the system. Some risks related to an organizations' accounting information systems include: access risk, business interruption risk, change management risk, control risk, cyber-security risk, legal risk and reliability risk. There is also a risk that auditors introduce control risk which involves the material misstatements of the firm's internal controls.

White-collar crime can be attributed to the failure of corporate governance by key players in the organization. Yeoh (2016) advocates that decision-makers should be held more accountable for criminality resulting from their negligence. There is a growing awareness that organizations must prepare for the crises emanating from white-collar crime. White-collar crime, which includes bribery, corruption, embezzlement, and fraud, can lead to criminal prosecution and significant fines. The destruction of organizational integrity can extinguish an organization's legitimacy and is a crisis event that can challenge an organization's viability. Some businesses break down when the organization is struck by a white-collar crime crisis (Soltani, 2014).

Information security risk

Threats challenging information security have become more complex and insidious. Conventional security measures, placing emphasis on boundaries, are no longer effective, while the violation of integrity can lead to severe negative consequences. The extensive presence of software systems mandates security to be a significant matter. The complexity of systems, along with growing sophistication and vast interconnectivity and applications, creates serious concerns.

Data center risk is a concern because computing and telecommunication technologies depend on data centers. Crisis events include physical disruptive events and logical intrusions, such as denial of service attacks (Engemann and Miller, 2019). The role of disaster recovery and information security should be viewed in the context of the applications, hardware and telecommunications that affect the organization. Disaster recovery focuses on restoring the systems and communication capabilities of an organization after a disaster.

The continuing trend of growing computing services has expanded the requirement that data centers be continuously operating (Engemann *et al.*, 2005). Evolving business requirements for ubiquitous computing, immediate access and more data analytics have created demand for instantaneous information. This affects expectations for data centers,

during regular operations and when disasters strike. Failure to sufficiently address these matters can lead to significant losses.

Vulnerability is intensified by most organizations' rising dependence on computing and telecommunications technologies, and with trends toward integrating suppliers and business operations (Miller *et al.*, 2006). Because measures to address information security are themselves new technologies which affect systems, operations, and other organizations, additional risks arise.

System security failure may not merely present a risk of financial loss. Unsecured software can negatively impact an organization's customers, employees and investors. It can damage an organization's reputation, and in fact can be life threatening. Disruptions diminish services and increase costs; additionally, compromised software can migrate through enormous networks and damage widespread systems.

Supply chain risk

Globalization has created supply chains that are increasingly vulnerable to severe disruption from far-off events. The importance of supply chain resilience has been made more apparent with current events involving earthquakes, fires, hurricanes, market disruptions and tsunamis (Zsidisin and Wagner, 2010; Munoz and Dunbar, 2015). In addition to natural and man-made disasters, disruption in supply chains can be caused by a multitude of factors including product recalls, supplier bankruptcy, and financial, operational, or strategic exposures. New categories of risks that are outside the perimeter of the organization and its direct business partners have resulted from global supply chains.

Supply chain risks may be categorized in three groups: systemic, environmental and social (Fiksel, 2003). Systemic risks relate to the supply chain itself, resources supporting it, and its related infrastructure. Environmental risks relate to the natural environment and how it affects the supply chain. Social risks relate to social and organizational systems that are external to the organization.

As businesses strive for larger market share and economies of scale globally, they are faced with unintended consequences and new categories of risks that are outside the perimeter of the organization (Sheffi, 2007). Global competition fosters an increase in the outsourcing of operations, thus increasing dependence on more complex supply chains. Concentration of capacity outside an organization's control creates a single point-of-failure risk. Risks of supply disruption increases with greater dependency on raw materials being transported from distant suppliers. Suppliers, who provide a large proportion of commodities, pose a risk of demand interruption outside the influence of the organization.

The cost of products in global supply chains are impacted by financial markets; therefore, organizations must effectively manage foreign exchange risk. Currency rate volatility poses risks for businesses involved in global supply chains and can significantly affect profitability, organizational cash flow and the ability to competitively price products (Burnside, 2012).

Requirements for supply chain resilience grow greater as also do those for supply chain sustainability. As with resilience, customer expectations have driven supply chains to become more sustainable, along environmental, economic and social responsibility dimensions. Supply chain resilience and supply chain sustainability appear to be conflicting concepts, but they are mutually supportive in many ways (Miller and Engemann, 2018).

New technologies risk

Rapid advances in technology have caused organizations to reassess the implications that these changes have on their business. The increased complexity of new technologies is associated with new risks, suggesting that risk may increase with more economic activity (Abrahamsen *et al.*, 2018). This relationship between risk, new technology and economic activity is of great concern, as it relates to safety.

Ample energy production is a key component of a strong infrastructure and involves a host of technologies. Although fracking has existed for decades, new technologies of fracking are associated with additional risks for which the industry is still developing mitigation techniques. Oil and gas operations by their nature involve environmental risks, which are normally well managed, but new fracking operations, with intensive use of water resources, are causing much debate (Drake, 2018). The challenges are an amalgamation of dynamics where nature can initiate technological disasters and technology can intensify natural instabilities.

Consider the inherent risk of financing oil fracking in a free market. The free market permits great volatility in price depending on supply and demand. Although price may be a good signal regarding when to expand capacity, it does not indicate how much to expand. Invariably, excess capacity is generated which eventually distresses the industry. Oil frackers additionally face the risk created by the short length of time their wells produce compared to conventional oil wells (Nersesian, 2018).

The economy is principally driven by fossil energy resources, although there are enthusiastic proponents encouraging the switch to renewable resources. To decrease dependence on fossil energy, industry is expanding the use of fuel from sustainable biomass. Exploitation of plants for energy is encouraging their cultivation, and to further protect the environment, multiple utilization of the same resource prior to its life cycle end is being practiced, leading to more complex production (Kircher, 2012). Organizations in this emerging bioeconomy are experiencing new risks associated with variations in quality and availability of material.

Given the complexity of many new technologies, and concern over possible negative unintended consequences, the precautionary principle has been used when formulating controls and regulations. Because many technologies once thought safe have been found to be hazardous, the logic behind applying some level of the precaution makes sense. However, complications occur when decision are made based on insufficient evidence (Miller and Engemann, 2019).

Discussion

Traditional methods of recognizing and managing organizational risk are often ineffective in increasingly complex chaotic environments. Understanding the common characteristics of evolving risks that are currently under scrutiny can provide insight into identifying further threats to organizations. With these common characteristics understood, the primary resources of solid leadership, risk analytics and professional business continuity management can aid in the recognition of additional obscured but growing risks and be beneficial in providing security for an organization.

Risk characteristics

The most troubling threats to an organization tend to have some risk characteristics in common. These attributes express the essence of the risks previously discussed and describe the factors that are innate to the risk. These attributes are useful in identifying further threats, as in general, the more an event, process, product, resource, setting, system, venture, etc. can be described, with a negative connotation, using these terms, the greater the inherent risk. Themes that permeate emerging risks are:

(1) Scope/scale:

- vast, massive, enormous;
- insufficient, inadequate, unsatisfactory;
- outside span-of-control, extra-organizational; and
- single point-of-failure, unique, irreplaceable.

(2) Complexity/dependency:
- complex, complicated, intricate;
- simple, sparse, redundant;
- dense, concentrated, clustered; and
- interconnected, reliant, dependent, entrenched.

(3) Environment/changes:
- degraded, unstable, erratic;
- disintegrating, eroding, fluctuating;
- rapid technological changes; and
- new categories of risks.

(4) Knowledge/uncertainty:
- unaware, naïve, inexperienced;
- large potential negative consequences, strong downside;
- unknowns, undiscoverable, incomprehensible; and
- unintended consequences, increasing vulnerability.

(5) Precision/readiness requirement:
- perfection, exactness;
- faultless, impeccable;
- instantaneous response; and
- always-on, immediate.

Leadership

Risk characteristics are useful in identifying threats to an organization and can be used by leaders and other stakeholders in that regard. The Board of Directors has ultimate responsibility for an organization's performance, with senior management having direct responsibility for an organization's resiliency. Management is subject to intense scrutiny during a crisis, and a mishandled event can reveal weak leadership, thereby challenging an organization's viability. Solid leadership with clearly defined roles is paramount, especially because judgment plays a critical role in crisis decision-making.

A decisive response from leadership is required during a crisis, when all facets of an organization are subject to concentrated scrutiny. A crisis is a unique negative event for which there is no suitable prearranged response (Leonard, 2009). Leaders need to have requisite knowledge to guide an organization to survive a crisis event. Core values of organizations quickly become evident in crisis decisions because the time pressure of these events do not allow the opportunity for explicit discussions about values.

Crisis decision making is challenging, particularly for those situations involving human life and safety. The assessment of strategies should reflect the attitude of the decision maker, which in turn is influenced by the safety climate of the organization. Within the framework of the risk attitude chain, safety climate can be regarded as influencing risk attitude (Engemann and Engemann, 2017). A high safety climate is reflective of a cautionary style and is consistent with a risk attitude that puts more emphasis on possible negative consequences. A low safety

climate echoes an uncritical opinion of unsafe behavior and is consistent with a risk attitude that predicts that matters will go very smoothly.

Knowledge is a valuable resource capable of empowering coordinated action and change. High reliability organizations operate within very ambiguous and frequently hazardous situations. High reliability organizations are distinctive because they continue a dialogue among members, capturing collective learning from success and failure. Studying the role of knowledge in organizations that function in these dynamic environments, from the perspective of risk and uncertainty, is providing valuable lessons to aid an organization in managing risk (Engemann, 2018).

Judgment plays a vital role in crisis decision-making, where effectiveness depends upon the decision maker's knowledge in the decision domain. Relying on intuition in decision-making is contrasted with analytical processes, with intuitive decision-making often being regarded as more natural. Depending on intuition-based decisions in crisis events may be inevitable, especially when pressing actions are needed and inadequate data are available (Kahneman and Klien, 2009). The need for a quick intuitive decision should not be conflated with the preference for intuitive decisions above analytical decisions, because of the severe disadvantages of relying too heavily on intuition. Intuition may be relatively effective when a decision maker has both knowledge and experience in the domain in which the decision is being made, however, advances in risk analytics and artificial intelligence promise to modify intuition's role, as decision-makers enhance their use of algorithms, even in immediate crisis situations.

Risk analytics

Analyzing risk can be challenging because it involves anticipating extraordinary events that have unidentified implications. Risk analytics play a vital role in understanding this situation and in selecting a strategy to implement. Data analysis techniques are available to assist in determining relationships in uncertain conditions, and decision models can support decision-making in a risky environment.

A decision model should reflect the attitude of the decision maker. Immediate probabilities amend typical probabilistic knowledge with information about the payoffs, mediated through attitudinal information of the decision maker (Yager *et al.*, 1995). The resulting probabilities are a modified formulation of the perception of probabilities in effect at the time of the immediate decision. Risk decision approaches are available that include attitudinal summary measures for both central tendency and dispersion (Engemann *et al.*, 2005). Decision models using attitudinal and fuzzy modeling, which incorporate sensitivity analysis of the decision maker's attitude, are valuable in the selection of risk strategies (Engemann and Miller, 2015).

The information required in a decision model is complex, and often inexact and impossible to attain precisely. Nevertheless, computational intelligence, using fuzzy rule constructions, is promising. Perception based granular probability distributions are valuable in modeling the uncertainty profiles of alternatives, and new techniques for assessing rule-based decision functions, while incorporating perception-based uncertainty profiles, continuously emerge (Yager, 2018).

Explicitly integrating the decision maker's attitude into the decision model addresses a deficiency in applying the precautionary principle. Extreme risk aversion often becomes a default frame of reference, yet maximum risk aversion need not be accurate, as there are multiple risk postures that a decision maker may assume. Advances in decision modeling provides more granularity surrounding this frame of reference and can support decision makers in making decisions that are more robust (Miller and Engemann, 2019).

While the precautionary principle has traditionally used the concept of regret as its primary outcome measure, a new measure of satisfaction, known as comfort is emerging. Comfort is defined as the difference between the payoff received by selecting a strategy and the worst payoff that could have been received under the manifestation of the same state-of-nature.

Several methods of aggregating an alternative's individual comforts across the different states-of-nature, incorporating various types of information about the uncertainty associated with the states-of-nature, have been proposed. The Comfort Decision Model is used to determine the value of alternative risk strategies utilizing attitudinal measures of the decision maker (Engemann and Yager, 2018).

Using simulation modeling, organizations can analyze complex strategies. Simulation models are very useful tools to analyze risk, for example, in studying how disasters affect supply chains (Miller and Engemann, 2008). Drawing on concepts from reliability theory and capacity analysis, the model is used to examine various scenarios, including examining correlation among node locations; the effectiveness of disaster recovery plans; and dual sourcing. Using simulation modeling creates the opportunity for an organization to study their specific supply chain to establish strategies to best prepare for possible crises (Miller and Engemann, 2014).

Business continuity management

Business continuity management is a management process that identifies organizational threats and their potential impact, and provides a framework for building resilience. Successful business continuity management raises the likelihood of uninterrupted operations, and promotes mindfulness for methodical risk management. Organizations are implementing recommended risk management procedures with holistic risk assessment and employing enhanced risk controls. Business continuity typically focuses on matters such as speedy recovery of information technology, essential services and supply chain. This outlook is rooted in the development of the profession whose primary objective was to ensure consistency in the operation of critical activities. This is principally the case in sectors such as banking, finance, energy and healthcare which have substantial regulatory requirements and significant impact on the populace.

The value of business continuity management has generally been recognized by its role in focusing on operational issues as to opposed strategic initiatives. Gradually, business continuity professionals have been taking on more comprehensive concerns. The character of the profession of business continuity management in corporate governance has changed from a technological responsibility into an all-inclusive business service.

Institutes that certify professionals in business continuity management promote the importance of application of the field to activities at all levels of the organization. The profession proposes an array of perspectives, from anticipative, handling the readiness of business activities, to strategic, positioning an organization in the market. International standards organizations and professional groups have provided an approved set of standards and practices to ensure thorough and consistent application of the principles of the profession.

Conclusion

In this paper, we explored some emerging developments in organizational risk, by highlighting evolving concerns and identifying their common characteristics. We then discussed key resources and recommended approaches in managing organizational risk.

An effective risk management program is essential for an organization to provide itself security from crises. A risk management program should raise awareness of threats and provide a comprehensive approach to identify risk and to develop solutions to manage risk. Underlying threats may be known or unknown, and how those threats become manifest in a complex environment is often unpredictable. With this mindset, consideration should be given to choosing strategies that are robust and effective, spanning across many scenarios.

As the boundaries for organizations endlessly transform, contemporary risk management must recognize threats from anywhere. Nevertheless, the proper blend of awareness, methods, practices, policies and technology can effectively support organizational risk management.

Risk professionals now have a substantial body of knowledge available from which to obtain direction. Fundamental principles and theories on the subject have evolved, for example, the traditional approach that risk is predominantly negative is yielding more recently to an inclusion of the positive aspects that risk may yield. Likewise, while early practitioners focused on physical risk, modern professionals also place emphasis on more comprehensive strategic organizational goals.

References

Abrahamsen, E.B., Asche, F. and Dahl, R.E. (2018), "Safety and economic activity", in Engemann, K.J. (Ed.), *The Routledge Companion to Risk Crisis and Security in Business*, Routledge, New York, NY and London, pp. 434-440.

Aven, T. (2012), "The risk concept – historical and recent development trends", *Reliability Engineering and System Safety*, Vol. 99, pp. 33-44.

Bannock, G. (2005), *The Economics and Management of Small Business: An International Perspective*, Taylor & Francis Routledge, London.

Burnside, C. (2012), "Carry trades and risk", in James, J., Marsh, I. and Sarno, L. (Eds), *Handbook of Exchange Rates*, Vol. 2, John Wiley & Sons, Hoboken, NJ, pp. 283-312.

Cutter, S., Burton, C. and Emrich, C. (2010), "Disaster resilience indicators for benchmarking baseline conditions", *Journal of Homeland Security and Emergency Management*, Vol. 7 No. 1, pp. 1-22.

Drake, F. (2018), "Risk society and anti-politics in the fracking debate", *Social Sciences*, Vol. 7 No. 11, pp. 1-22.

Engemann, K.J. and Henderson, D.M. (2012), *Business Continuity and Risk Management: Essentials of Organizational Resilience*, Rothstein Associates, Brookfield, CT.

Engemann, K.J. and Miller, H.E. (2009), "Critical infrastructure and smart technology risk modelling using computational intelligence", *International Journal of Business Continuity and Risk Management*, Vol. 1 No. 1, pp. 91-111.

Engemann, K.J. and Miller, H.E. (2015), "Risk strategy and attitude sensitivity", *Cybernetics and Systems*, Vol. 46 No. 3, pp. 188-206.

Engemann, K.J. and Miller, H.E. (2019), "Business continuity management in data center environments", *International Journal of Information Technologies and Systems Approach*, Vol. 12 No. 1, pp. 52-72.

Engemann, K.J. and Yager, R.R. (2018), "Comfort decision modeling", *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 26 No. S1, pp. 141-163.

Engemann, K.J., Miller, H.E. and Yager, R.R. (2005), "Disaster management of information resources using fuzzy and attitudinal modeling", *International Journal of Technology, Policy and Management*, Vol. 5 No. 4, pp. 388-406.

Engemann, K.N. (2018), "Knowledge in high reliability organizations: a review of interrelated perspectives", in Engemann, K.J. (Ed.), *The Routledge Companion to Risk Crisis and Security in Business*, Routledge, New York, NY and London, pp. 80-90.

Engemann, K.N. and Engemann, K.J. (2017), "Risk attitude chain: safety climate, risk attitude and risk decisions", *International Journal of Business Continuity and Risk Management*, Vol. 7 No. 4, pp. 211-221.

Fiksel, J. (2003), "Designing resilient, sustainable systems", *Environmental Science and Technology*, Vol. 37 No. 23, pp. 5330-5339.

Kahneman, D. and Klien, G. (2009), "Conditions for intuitive expertise: a failure to disagree", *American Psychologist*, Vol. 64 No. 6, pp. 515-526.

Kircher, M. (2012), "The transition to a bio-economy. National perspectives", *Biofuels, Bioproducts and Biorefining*, Vol. 6 No. 3, pp. 240-245.

Lalonde, C. (2004), "In search of archetypes in crisis management", *Journal of Contingencies and Crisis Management*, Vol. 12 No. 2, pp. 76-88.

Leonard, A.M. (2009), *Managing Crisis; Responses to Large-Scale Emergencies*, CQ Press, Washington, DC.

Marolla, C. (2016), *Climate Health Risks in Megacities: Sustainable Management and Strategic Planning*, Vol. 1, CRC Press, Boca Raton.

Miller, H.E. and Engemann, K.J. (2008), "A Monte Carlo simulation model of supply chain risk due to natural disasters", *International Journal of Technology, Policy and Management*, Vol. 8 No. 4, pp. 460-480.

Miller, H.E. and Engemann, K.J. (2014), "Using reliability and simulation models in business continuity planning", *International Journal of Business Continuity and Risk Management*, Vol. 5 No. 1, pp. 43-56.

Miller, H.E. and Engemann, K.J. (2015), "Threats to the electric grid and the impact on organizational resilience", *International Journal of Business Continuity and Risk Management*, Vol. 6 No. 1, pp. 1-16.

Miller, H.E. and Engemann, K.J. (2018), "Resilience and sustainability in supply chains", in Zsidisin, G. and Henke, M. (Eds), *Revisiting Supply Chain Risk*, Springer, pp. 25-263.

Miller, H.E. and Engemann, K.J. (2019), "The precautionary principle and unintended consequences", *Kybernetes*.

Miller, H.E., Engemann, K.J. and Yager, R.R. (2006), "Disaster planning and management", *Communications of the International Information Management Association*, Vol. 6 No. 2, pp. 25-36.

Morris, J.J. (2011), "The impact of enterprise resource planning systems on the effectiveness of internal controls over financial reporting", *Journal of Information Systems*, Vol. 25 No. 1, pp. 129-157.

Munoz, A. and Dunbar, M. (2015), "On the quantification of operational supply chain resilience", *International Journal of Production Research*, Vol. 53 No. 22, pp. 6736-6751.

Nersesian, R. (2018), "Financial risk inherent in oil fracking", in Engemann, K.J. (Ed.), *The Routledge Companion to Risk Crisis and Security in Business*, Routledge, New York, NY and London, pp. 328-350.

Sheffi, Y. (2007), *The Resilient Enterprise*, MIT Press, Cambridge, MA.

Soltani, B. (2014), "The anatomy of corporate fraud: a comparative analysis of high profile American and European corporate scandals", *Journal of Business Ethics*, Vol. 120 No. 2, pp. 251-274.

Tierney, K. (2007), "Businesses and disasters: vulnerability, impacts, and recovery", in Rodriguez, H., Quarantelli, E.L. and Dynes, R.R. (Eds), *Handbook of Disaster Research*, Springer, New York, NY, pp. 275-296.

Yager, R.R. (2018), "Intelligent rule-based risk modeling for decision making", in Engemann, K.J. (Ed.), *The Routledge Companion to Risk Crisis and Security in Business*, Routledge, New York, NY and London, pp. 457-468.

Yager, R.R., Engemann, K.J. and Filev, D.P. (1995), "On the concept of immediate probabilities", *International Journal of Intelligent Systems*, Vol. 10 No. 4, pp. 374-397.

Yeoh, P. (2016), "Corporate governance failures and the road to crime", *Journal of Financial Crime*, Vol. 22 No. 1, pp. 216-230.

Zsidisin, G.A. and Wagner, S.M. (2010), "Do perceptions become reality? The moderating role of supply chain resiliency on disruption occurrence", *Journal of Business Logistics*, Vol. 31 No. 2, pp. 1-20.

Further reading

Ho, W., Zheng, T., Yildiz, H. and Talluri, S. (2015), "Supply chain risk management: a literature review", *International Journal of Production Research*, Vol. 53 No. 16, pp. 5031-5069.

Corresponding author
Kurt J. Engemann can be contacted at: kengemann@iona.edu