A WEIGHTED MEAN MODEL FOR OPERATIONAL RISK ASSESSMENT

YUNDONG HUANG,
L MURPHY SMITH & DAVID DURR

Assessing operational risk, particularly related to internal control, is increasingly important to business firms. This is especially the case for publicly-traded companies that are engaged in multinational operations, which involve additional complexity and risk. In the United States, for example, the Sarbanes-Oxley Act requires public companies to document adequate internal control in their annual report. However, there is no standard or uniformly accepted solution for internal risk analysis. Several complex methods have been introduced in the academic field. These complex methods, while theoretically sound, may be problematic in practice due to the necessity of sufficient historical data. When insufficient data are available for measuring operational risk, most of the models, which are based on probability theory, do not work. As a consequence, in most companies' annual reports, the internal risk disclosure is still rather ambiguous and intuitive. In this paper, we will present a simple weighted mean model that can be used for internal risk assessment. This weighted mean model offers an approach that is relatively easy to use and overcomes deficiencies of more complex models. This model can be a viable alternative to empirical or intuitive methods.

INTRODUCTION

In recent years, managing operational risk (OR) has become increasingly important to business managers, government regulators, investors, and lenders. Operational risk has been identified as the top-risk coverage priority by chief audit executives (IIA 2013). Interest in OR increased subsequent to some highly-publicised and costly financial scandals in the late 1990s and early 2000s, such as the NASDAQ odd-eighths pricing scandal (Christie and Schultz 1994) and the bankruptcy of Barings Bank (Brown and Steenbeek 2001). Corporate operations are always at risk, due to unethical behavior such as fraud, mismanagement, and corruption. Unethical behavior has led to massive financial losses as well as regulatory fines and penalties (Smith et al. 2012, Okafor et al. 2013, Blazovich and Smith 2011).

Assessing operational risk, particularly concerning internal control, is increasingly important to business firms, especially those engaged in multinational operations, which involve more complexity and more risk. In the United States, for example, the *Sarbanes-Oxley Act* requires companies to document adequate internal control in their annual report. Uncertainty and risk are two components essential to a decision-making framework. The usual application of these terms characterises uncertainty as incomplete knowledge and risk as unknown consequences. Probability is typically employed to quantify random uncertainty and statistical models used to approximate statistical risks (Sage and White 1980).

For this study, subjective adjustments are examined and numbers are used in phases to represent operational risks with uncertainty. We distinguish between different types of uncertainties. Last, we provide a weighted mean model for calculating ORs faced by companies or other business entities. We provide calculation cases regarding operational risk and computer security to exhibit model rationality.

THEORY AND LITERATURE REVIEW

Operational risk has been defined as the risk of loss ensuing from inadequate or failed internal processes, people or systems (Lockamy 2011). An overall theory that encompasses operational risk, and management thereof, is systems theory, which generally is viewed as a group of 'compound-structure elements' that specifically represent plan, control and evaluation (Jebrin 2012). Under the umbrella of systems theory, quantifying operational risk provides a rational and systematic approach for business managers to document and assess risks facing company operations. In addition, quantifying operational risk, particularly regarding internal control, can be helpful to internal and external auditors in their risk assessment efforts (Mascha and Miller 2010, Chandra and Calderon 2009).

Cerchiello and Giudici (2012) assert that uncertainty, potentially imprecise and inaccurate data, and the difficulty in observing and measuring a phenomenon, make it difficult to manage and construct operational risk models. The authors propose a fuzzy logic approach to risk modeling and apply their model using information technology operational risk data. This approach transforms qualitative variables into quantitative ones, and creates an alternative predictive regression model for operational loss.

Ergashev (2012) developed a framework for integrating scenario losses into operational risk models. He advocates the ordering of scenarios and asserts that only worst-case scenarios be modeled. It is only the worst-case scenarios that contain valuable information about the tail behavior of operational losses. Ergashev presents five alternative approaches for integrating the scenarios into the operational risk models.

Feng-ge and Zhang (2012) develop an operational risk model to address operational uncertainty in the Chinese banking system, where huge operational losses have already occurred. The authors construct a conditional value at risk (CVaR) model and apply the model to commercial banks in China. The CVaR model improves on the VaR model often used to assess operational risk as it includes measurement of tail losses of loss distribution. The model can produce a relatively precise value estimate of operational loss, thus allowing bank managers to plan for adequate capital reserves.

Following losses resulting from OR, the Basel Committee on Banking Supervision implemented a new minimum capital charge for OR as part of the Basel II Capital Accord (Basel Committee 2005), and large financial institutions are creating three measurement methodologies to estimate the OR capital charge, with the most advanced being the use of sophisticated measurement models incorporating bank-specific risk measurements. There is an expanding literature on quantitative modeling for OR. Research by de Fontnouvelle et al. (2003) applied loss amounts to data on operational loss events. Findings of their study were that capital requirements for operational loss events frequently exceed capital requirements for market risk at major banks. Research by Allen and Bali (2007) offered quantitative results regarding the magnitude of operational losses, based on monthly stock price data. These studies demonstrate that OR is significant.

Research by Cummins et al. (2006) quantified the market value impact of OR events, using an events study of US banks and insurers. A model, created by Wei (2006), combines 'high frequency, low severity' internal data and 'low frequency, high severity' external data to approximate operational loss. Chavez-Demoulin et al. (2006) demonstrate use of copula-based methods to formulate stress tests for dependence structures within OR.

BACKGROUND ON COMPUTER SECURITY

Businesses involved in e-commerce face a number of operational risks associated with electronic business transactions. E-commerce has been defined as business transactions that include the electronic transfer of money; however, e-commerce is widely considered as any electronic transaction concerning a purchase by cheque, phone or some other means. There are two categories of e-commerce, those that include retail trade between business and consumers (B2C) and those that include business-to-business (B2B) trade (Smith 2008).

E-commerce has played a major role in the globalisation of business. The beginnings of e-commerce are connected to the original electronic computers of the 1950s. Yet, it was the creation of the World Wide Web in the 1990s that led to the dramatic expansion of e-commerce. Exhibit 1 provides a timeline of major events concerning the Internet and e-commerce (Smith et al. 2011).

Exhibit 1. Historical Timeline Pertaining to the Web and E-Commerce

1946 -	The first electronic computer, ENIAC, is constructed at the University of Pennsylvania.
1958 -	To counter Soviet technological advances, the U S forms the Advanced Research Projects Agency (ARPA), with the Department of Defense, to develop U.S. prominence in science and technology applicable to the military.
1969 -	ARPANET, the forerunner of the Internet, established with four nodes: UCLA, Stanford, UC-Santa Barbara, and University of Utah.
1970 -	First applications of electronic data interchange (EDI).
1984 -	Science fiction author William Gibson coins the term ‘cyberspace’ in his novel, Neuromancer. Internet host computers exceed 1,000.
1988 -	Internet worm disables 6,000 of 60,000 Internet hosts. The worm was created by a Cornell University graduate student; infected computers were connected through ARPAnet and other E-mail networks in the Internet loop. Some of the US’s top science and research centers were affected.
1991 -	Tim Berners-Lee, working at CERN in Geneva, develops a hypertext system to provide efficient information access. He posts the first computer code of the World Wide Web in a relatively innocuous newsgroup, “alt.hypertext.” Later, people refer to the Internet itself as the Web.
1994 -	Inception of business to consumer (B2C) e-commerce. Pizza Hut sells pizza on its website. First Virtual, the first cyberbank, opens.
1995 -	The Bottom Line is Betrayal authored by K T Smith, D L Crumbley and L M Smith: the first business educational novel focused on international trade, global marketing and emerging technologies.
1997 -	Inception of business-to-business (B2B) e-commerce. US Postal Service issues electronic postal stamps.
2009 -	Internet host computers (i.e. computers with a registered IP address) exceed 200 million. Users in over 150 countries are connected.

Source: Katherine T Smith, L Murphy Smith and Jacob L Smith, ‘Case Studies of Cybercrime and Its Impact on Marketing Activity and Shareholder Value’ (2011) 15(2) *Academy of Marketing Studies Journal* 67, 67–81.

E-risk has been defined as the potential for financial and technology problems to occur as a consequence of e-commerce. Changes in technological, economic, industrial and regulatory environments lead to new problems for business operations. Regarding technology, cyberspace is accessible to villains who seek ways to exploit business computer systems. Hackers are a particular problem, in which persons external to a company gain unauthorised access to a company’s online computer system. When access is achieved, the hacker can potentially create major problems by deleting or modifying operational data. This is just one example of an e-risk, which is a category of operational risk facing all companies engaged in e-commerce. Other e-risks connected to e-commerce include the following (Smith 2008):

- The changing e-commerce environment alters risks, so old solutions may no longer work.
- International business activity expands the scale and scope of risks.
- Computing power, connectivity, and speed can spread viruses, facilitate system compromise, and compound errors in seconds, potentially affecting interconnected parties.
- Hackers never stop devising new techniques; thus, new tools mean new vulnerabilities.

The complexity of modern business is associated with increased operational risk. Technology has enabled the creation of the virtual business, which is a modular structure of multiple individual business firms linked by computer technology, as illustrated in Exhibit 2. The individual businesses that make up a virtual business are networked, making it possible for them to share skills, costs, and access to markets. Each individual business supplies its core competencies to the overall virtual business (Smith 2008).

Exhibit 2. Virtual Business

Source: L Murphy Smith, Katherine T Smith and S Gordon, Essentials of Accounting Information Systems (Leyh Publishing, Austin, Texas, 2003).

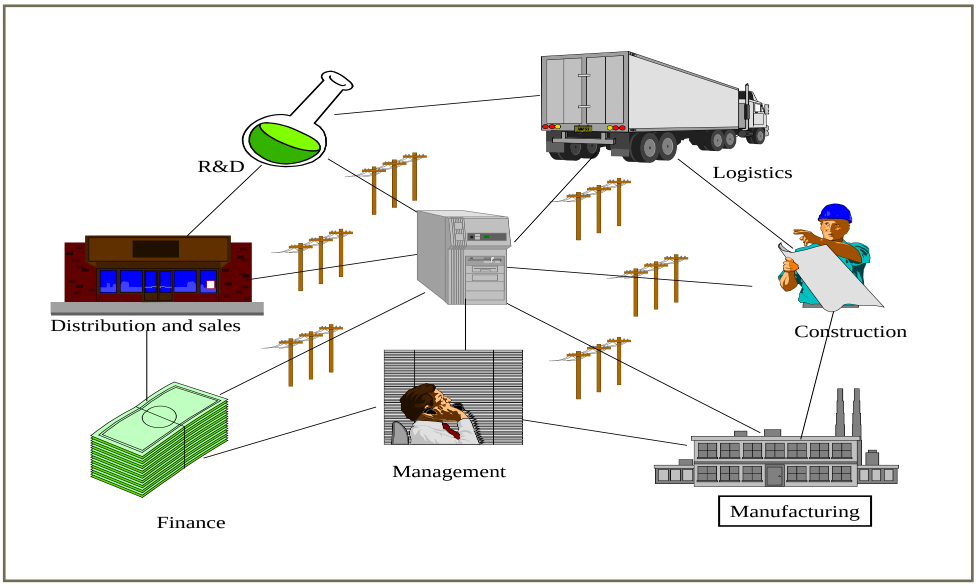
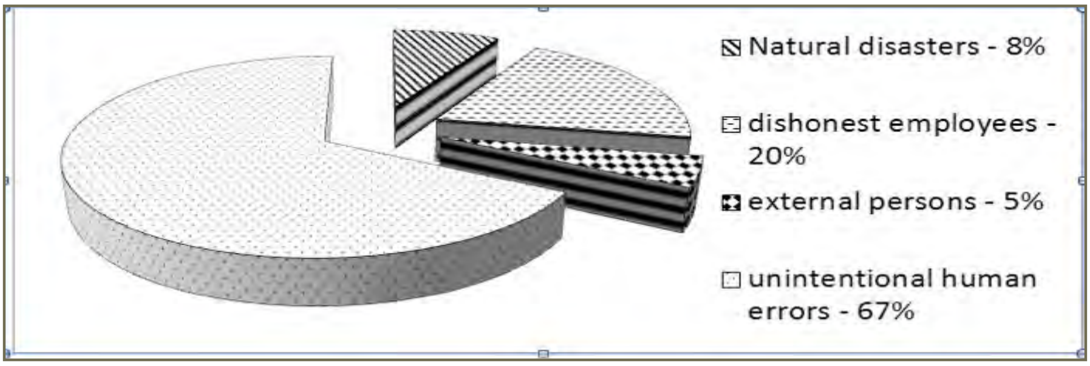


Exhibit 3. Threats to Computer Security

Stanley H Kratchman, Jacob L Smith and L Murphy Smith, 'Perpetration and Prevention of Cyber Crimes' (2008) 23(3) Internal Auditing 3, 3–12.



Whether a company is engaged in e-business on a large scale or not at all, all companies must manage their operational risks. Publicly-traded companies are legally required to have adequate internal control structure, due to the *Foreign Corrupt Practices Act* (Smith et al. 2012). What is adequate internal control structure varies from company to company due to size, industry type, extent of e-commerce activity, and span of geographic operations. Failure to properly carry out specified control procedures leads to operational risk. One of the roles of a company's internal auditors is to ensure that designated internal control procedures are working as described in company policies.

Establishing an effective internal control structure regarding computer security is a challenge for all types of businesses. Often reported in the media are cases involving hackers external to the company or fraudsters internal to the company. However, the most significant threat to accurate and reliable data in business computer systems is actually unintentional human errors. Threats to computer security can be summarised into four categories, as follows: (1) natural disasters, (2) dishonest employees, (3) persons external to the organization (e.g. hackers), and (4) unintentional human errors and omissions by employees. The extent that each of these threats is actually realised is shown in Exhibit 3 (Kratchman et al. 2008).

OPERATIONAL RISK DEFINED

Many companies have devoted attention to the discussion of business risks in general, but quantifying OR is often an ongoing challenge. As interest in OR began increasing in the 1990s, the definition of OR was still in flux. For financial institutions, OR was defined by the Basel Committee (2003) as 'the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.' Thus, the meaning of OR is built on a foundational hierarchy of OR causes comprised of four categories: people, processes, systems and external events. The definition incorporates legal risk, but omits reputation, strategic and systemic risk, as well as market risk and credit risk (Huang 2009).

Generally, risk is quantified using a formula such as Eq. (1) or Eq. (2). Consequently, OR is typically measured using statistical modeling.

$$\textit{Risk} = \textit{Probability} \times \textit{Impact} \qquad (1)$$
$$\textit{Risk} = \textit{Probability} \times \textit{Consequence} \qquad (2)$$

In the Advanced Measurement Approach (AMA) per Basel Accord II, OR is formulated as shown (Basel Committee 2005):

$$OR = \sum_{i,j} \gamma(i,j) \times EI(i,j) \times PE(i,j) \times LGE(i,j) \qquad (3)$$

where *i* represents operation type, *j* is risk type, $\gamma(i, j)$ is expected loss (*EL*) conversed into capital requirements, which is established by supervisory department based on operation loss data of the overall industry, *EI(i, j)* the OR exposure of *(i, j)*, *PE(i, j)* the resulting probability of loss on *(i, j)*, and *LGE(i, j)* the loss degree at the time events occur on *(i, j)*. The lender-bank would internally estimate the three parameters *EI(i, j), PE(i, j), and LGE(i,j).*

UNCERTAINTIES PERTAINING TO OPERATIONAL RISK

An example of OR in the aviation industry involves human factors linked to interactions of physiological and psychological factors related to decision-making in emergency response situations. Case studies are used to evaluate judgment, training, resource management, aero-medical physiology, and stress awareness and management. The case approach facilitates evaluation of aviation professionals who operate, maintain and support aircraft, and the impact on safety outcome of emergency response operations (Huang 2009).

In the OR identification process, the following should be evaluated: the total range of possible OR; the external and internal setting in which the company carries on operations; the company's long-term goals; the services or goods produced by the company; the company's unique situation; external and internal changes; and the rate of those changes. After being recognised, ORs could be analysed to ascertain which are intolerable. These should be reduced or eliminated. Usually this is attained by estimating the probability that the OR will materialise, evaluating causes of the OR, and assessing its effect, prior to application of control strategies (Huang 2009).

The possible effect of ORs should be considered not only in financial terms but more broadly with consideration of the possible impact on attainment of company goals. When a company wishes to improve in quantifying ORs, reliable data on operational loss events (by types of risk) and possible sources of operational loss must be accumulated. The company can then create a model to quantify each risk type. Quantifying OR involves three critical phases: the internal and external environment, the company's long-term goals, and management activities (Huang 2009).

A major source of errors between actual ORs and results from traditional probability models is ambiguity. To make things easier in quantifying OR, this study emphasises evaluating phases in OR and approximating risk level. Doing so affords a novel approach to approximating OR without probability.

UNCERTAINTY ESTIMATION

OR results from uncertainties in the phases for OR identification. For this situation, we assume that a company can control its actions to avoid OR. In other words, if a company is aware that an activity will result in losses, it can cancel that activity. We assume that there is no loss in general but that there are *n* phases in OR identification,

$S_1, S_2, \ldots, S_n$. Therefore, OR can be represented by Eq. (4).

$$OR = F(S_1, S_2, \ldots, S_n) \qquad (4)$$

In the *i*th operation type, and the *j*th risk type, if the company can determine expected loss $\gamma(i, j)$, exposure $EI(i, j)$, probability of loss events $PE(i, j)$, and loss degree $LGE(i, j)$, the function *F* can be formulated, as described earlier, by Eq. (3).

If uncertainties within a phase cannot be formulated mathematically, a simple but effective method for quantifying an uncertainty is to assign a number in [0, 1] for the uncertainty. Thus, if there is adequate knowledge and data to define a phase, the uncertainty is 0. Alternatively, if a phase is so unusual that no one has any history with it, the uncertainty is 1.

When an uncertainty is 0, then a company has no OR for that assumption, that is, the company can control its activity to avoid OR. On the other hand, if an uncertainty is 1, then the company has the maximum OR, as the company cannot alter its activity to avoid the OR.

A SCENARIO OF OPERATIONAL RISK IN A PHASE

Consider a scenario in which OR depends on a phase *S*. The demise of Britain's Barings Bank in 1995 is a classic story of financial risk that resulted from a phase carried out by an unscrupulous employee, in this case, Nick Leeson, head derivatives trader in Singapore. The bank's difficulty was measuring OR by application of a traditional probabilistic approach. On the other hand, had the bank evaluated the employee's activities in light of the potential downside, the bank could have identified the risk. The less reliable the employee, the greater the risk the bank faced (Huang 2009).

Assume that $U(S)$ is be the uncertainty of the phase which defines OR. The assessment of $U(S)$ is stated as [0,1]. Assuming that the company is able to control its activity to avoid OR, then OR is formulated as in Eq.(5).

$$OR = U(S) \qquad (5)$$

Consequently, in the case of Barings Bank, the employee's uncertainty at the time of the unauthorised trading is *U* (Employee) =1; its OR is 1.

AN EXAMPLE OF OPERATIONAL RISK IN TWO PHASES

Assume that OR depends on two phases, S_1, S_2. To illustrate, for the majority of companies, OR is a consequence of the combined action of miscarried internal procedures and a hostile external environment. Thus, the phase involving the internal procedures is S_1, and the other involving the external environment is S_2. For a company in the retail industry, having an online computer system lacking appropriate access controls will be secure only if there are no hackers in the external environment. For the most part, the effect of S_1 to OR is larger than S_2. We assign weights W_1 and W_2 to differentiate them. Assume $U(S_1)$ and $U(S_2)$ are the uncertainties of phases S_1 and S_2, respectively. The most basic methodology to approximating OR with two phases S_1, S_2 is shown in Eq.(6).

$$OR = \frac{W_1 U(S_1) + W_2 U(S_2)}{W_1 + W_2} \qquad (6)$$

A manager might contend that, for an online computer system C, and an external environment E, if there is 99 per cent confidence that access controls can prevent hackers, i.e., $U(C)$=0.01, and 20 per cent confidence that there are no new hackers in the external network targeting the company's online system, i.e., $U(C)$=0.2, and correspondingly, weights are W1 =0.9 and W2 =0.1, then, according to Eq.(6), approximately, we have:

$$OR = 0.9 \text{ x } 0.01 + 0.1 \text{ x } 0.2 = 0.029$$

OR IN MULTIPLE PHASES: A CASE APPLICATION

For a retail firm's online computer system, risks to computer security were identified above, as follows: natural disasters, dishonest employees, persons external to the organisation, and unintentional human errors by employees. This concept of risk suggests that a retail firm has an idea of its expected losses for the different areas of risk. Such notions are founded on past experience about the future external environment on the one hand and the retailer's future internal computer security controls on the other.

Let the computer security OR of a retail firm depend on the following four phases, S_1, S_2, S_3, S_4:

S_1: Disaster recovery procedures by Ben;
S_2: Internal controls preventing unauthorised data manipulation by dishonest employees by Jacob;
S_3: Access controls preventing access by external hackers by Sam;
S_4: Internal controls preventing or correcting unintentional errors by Tracy.

We suppose that

- Ben is superlative at designing disaster recovery procedures. There will be nothing lacking in his work, i.e., $U(S_1)$=0;
- Jacob is new at the job with little experience. Let $U(S_2)$=0.7;
- Sam is an exemplary employee in most respects. However, she has not stayed up-to-date regarding recently developed hacking techniques. Thus, $U(S_3)$=0.2;
- Tracy is a leading expert, but recently has been distracted by personal financial problems. Let $U(S_4)$=0.1.

In addition, we assume that

a) Recovery from disaster, if it occurs, is a necessity; therefore, we assume that the weight of S_1, in degree of importance, written as W_1, is 0.1;
b) The internal controls preventing unauthorised data manipulation by dishonest employees are well designed. Let W_2=0.1;
c) Access controls are deemed effective. However, if hackers break into the online system, then potential damage is considerable. Let W_3=0.2;
d) The greatest threat to computer security is unintentional human errors. Let W_4=0.4.

Summarily, we have:
$U = \{U(S_1),U(S_2), U(S_3),U(S_4)\}=\{0,0.7,0.2,0.1\}$

$W = \{W1, W2, W3, W5\}=\{0.1,0.1,0.2,0.6\}$

Finally, in the case of that there is no interaction between Ben, Jacob, Sam, and Tracy, applying Eq.(10), we have:

$$OR = \frac{W_1U(S_1)+W_2U(S_2)+W_3U(S_3)+W_4U(S_4)}{W_1+W_2+W_3+W_4}$$

$$= \frac{0.1\times 0+0.1\times 0.7+0.2\times 0.2+0.6\times 0.1}{0.1+0.1+0.2+0.6}$$

$$=0.17$$

CONCLUSIONS

Operational risk has drawn great attention in recent years, especially after the *Sarbanes-Oxley Act* in 2002. In the case of online computer security systems, operational risk may result from natural disasters, dishonest employees, persons external to the organisation, and unintentional human errors by employees. Oftentimes, a company may lack detailed historical data for the probabilities regarding operational risk. Further, operational risk may be nebulous as there may be alternative viewpoints of an identical assessment result and alternative viewpoints concerning what is tolerable. As a result, methodology for assessing OR based on traditional statistical models can be problematic in practice.

As an alternative to traditional statistical models, the OR model, described in this paper, is based on subjunctive judgment of uncertainties on phases for operational risk identification. The OR model extends a viable alternative to traditional probabilistic models. An uncertainty in which representation by a function is problematic, can be represented by a number [0,1]. The example OR calculation case regarding computer security operational risk, related to natural disasters, dishonest employees, persons external to the organisation, and unintentional human errors, illustrates that the proffered OR model is practical and relatively simple to use, benefiting from the non-statistical approach. Such a methodology can be beneficial to business managers, auditors, and others for assessing operational risks in settings where use of traditional statistical models is problematic.

REFERENCES

L Allen and T G Bali, 'Cyclicality in Catastrophic and Operational Risk Measurements' (2007) 31(4) *Journal of Banking & Finance* 1191, 1191–235.

Basel Committee, *Sound Practices for the Management and Supervision of Operational Risk* (2003), Bank for International Settlements, Basel, Switzerland.

Basel Committee, *International Convergence of Capital Measurement and Capital Standards: A Revised Framework* (2005), Bank for International Settlements, Basel, Switzerland.

J Blazovich and L Murphy Smith, 'Ethical Corporate Citizenship: Does it Pay?' (2011) 15 *Research on Professional Responsibility and Ethics in Accounting* 127, 127–63.

Stephen J Brown and Onno W Steenbeek, 'Doubling: Nick Leeson's Trading Strategy' (2001) 9(2) *Pacific Basin Finance Journal* 83, 83–99.

P Cerchiello and P Giudici, 'Fuzzy Methods for Variable Selection in Operational Risk Management' (2012) 7(4) *Journal of Operational Risk* 25, 25–41.

Akhilesh Chandra and Thomas G Calderon, 'Information Intensity, Control Deficiency Risk, and Materiality' (2009) 24(3) *Managerial Auditing Journal* 220, 220–32.

V Chavez-Demoulin, P Embrechts, and J Nešlehová, 'Quantitative Models for Operational Risk: Extremes, Dependence and Aggregation' (2006) 30(10) *Journal of Banking & Finance* 2635, 2635–58.

W G Christie and P H Schultz, 'Why Do Nasdaq Market Makers Avoid Odd-Eighth Quotes?' (1994) 49(5) *Journal of Finance* 1813, 1813–40.

J D Cummins, C M Lewis and R Wei, 'The Market Value Impact of Operational Loss Events for US Banks and Insurers' (2006) 30(10) *Journal of Banking & Finance* 2605, 2605–34.

Patrick de Fontnouvelle, Virginia Dejesus-Rueff, John Jordan and Eric Rosengren, 'Capital and Risk: New Evidence on Implications of Large Operational Losses' (Working Paper 03-5, Federal Reserve Bank of Boston, Boston, Massachusetts, 2003).

B A Ergashev, 'A Theoretical Framework for Incorporating Scenarios into Operational Risk Modeling' (2012) 41(3) *Journal of Financial Services Research* 145, 145–61.

Y Feng-ge and P Zhang, 'The Measurement of Operational Risk Based On CVaR: A Decision Engineering Technique'

(2012) 4 *Systems Engineering Procedia* 438, 438–47.

Ali Hadi Jebrin and Abdalla Jamil Abu-Salma, 'Conceptual Knowledge Approach to Operational Risk Management (A Case Study)' (2012) 7(2) *International Journal of Business and Management* 289, 289–302.

Yundong Huang, 'A Naïve Uncertainty Model for Measuring Operational Risks Faced by Financial Institutions' (2009) 23(4) *Stochastic Environmental Research and Risk Assessment* 507, 507–16.

IIA (Institute of Internal Auditors), 'Poor Evidence, Deficient Audits' (2013) 70(1) *Internal Auditor* 13, 13, 15.

Stanley H Kratchman, Jacob L Smith and L Murphy Smith, 'Perpetration and Prevention of Cyber Crimes' (2008) 23(2) *Internal Auditing* 3, 3–12 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1123743>.

Archie Lockamy, 'Benchmarking Supplier Risks Using Bayesian Networks' (2011) 18(3) *Benchmarking: An International Journal* 409, 409–27.

Maureen Francis Mascha and Cathleen L Miller, 'The Effects of Task Complexity and Skill On Over/Under-Estimation of Internal Control' (2010) 25(8) *Managerial Auditing Journal* 734, 734–55.

Collins L Okafor, Murphy Smith and Nacasius U Ujah, 'Kleptocracy, Nepotism, Kakistocracy: Impact of Corruption in Sub-Saharan African Countries' (2013) *International Journal of Economics and Accounting*, forthcoming. Available at SSRN: <http://ssrn.com/abstract=1839968>.

A P Sage and E B White, 'Methodologies for Risk and Hazard Assessment: A Survey and Status Report' (1980) 10(8) I*EEE Transactions on Systems, Man and Cybernetics SMC* 425, 425–46.

Katherine T Smith, 'An Analysis of E-Commerce: E-Risk, Global Trade and Cybercrime' (Working Paper, 2008). Available at SSRN <http://ssrn.com/abstract=1315423> or <http://dx.doi.org/10.2139/ssrn.1315423>.

Katherine T Smith, L Murphy Smith and Jacob L Smith, 'Case Studies of Cybercrime and Its Impact on Marketing Activity and Shareholder Value' (2011) 15(2) *Academy of Marketing Studies Journal* 67, 67–81.

L Murphy Smith, Karyl M Van Tassel and Philip Innes, 'Current Developments Regarding the Foreign Corrupt Practices Act' (2012) 27(1) *Internal Auditing* 31, 31–37.

L Murphy Smith, Katherine T Smith and S Gordon, Essentials of Accounting Information Systems (Leyh Publishing, Austin, Texas, 2003).

L Murphy Smith, L C Smith, William C Gruben and Leigh Johnson, 'A Multinational Analysis of Corruption and Economic Activity' (2012) *Journal of Legal, Ethical and Regulatory Issues*, forthcoming.

R Wei, *Quantification of Operational Losses Utilising Firm-Specific Information* (PhD Dissertation, The Wharton School, University of Pennsylvania, Philadelphia, 2006).

AUTHOR PROFILES

Yundong Huang is a doctoral student at Texas A&M International University in Laredo, Texas, USA.
Email: hydmail2000@gmail.com

Dr. L. Murphy Smith is the David and Ashley Dill Distinguished Professor of Accounting at Murray State University. Dr. Smith's academic record includes numerous professional journal articles, research grants, books, professional meeting presentations, and awards teaching and research.
Email: msmith93@murraystate.edu

Dr. David Durr is the Arthur J Bauernfeind Endowed Chair in Business and Investment Management at Murray State University. Dr. Durr has an extensive record of teaching, research, and service. He holds designations of Certified Financial Planner and Chartered Financial Analyst. Dr. Durr has served as a Teaching Scholar in Residence for the University Center for Teaching and Learning.
Email: ddurr@murraystate.edu