2008

IS-Related Operational Risk: An Exploratory Analysis

James Goldstein
Syracuse University, jcgoldst@syr.edu

Michael Benaroch
Syracuse University, mbenaroc@syr.edu

Anna Chernobal
Syracuse University, annac@syr.edu

IS-Related Operational Risk: An Exploratory Analysis

James Goldstein
Martin J. Whitman School of Management
Syracuse University
jcgoldst@syr.edu

Michel Benaroch
Martin J. Whitman School of Management
Syracuse University
mbenaroc@syr.edu

Anna Chernobai
Martin J. Whitman School of Management
Syracuse University
annac@syr.edu

ABSTRACT

Past research concerning information systems (IS) risk has mainly focused on development risk. However, the impact of any risk event that occurs once the system is operational can be far more extensive. Such events are due to what has been termed *operational risk*. Our research is concerned with operational risk that involves an IS – or *IS-related operational risk* – which has received little attention in the academic literature. Specifically, we seek to offer a comprehensive exploratory analysis of IS-related operational risk based on a database documenting hundreds of actual IS-related operational risk events. Our findings could help managers and researchers to achieve a better understanding of the risk exposure associated with operational ISs in their current business environment and with new information technology (IT) investments under consideration. This research could also assist organizations in achieving a higher level of strategic and economic alignment, through the use of a systematic IS risk management approach.

Keywords

Information systems risk, operational risk, business process risk

INTRODUCTION AND LITERATURE REVIEW

Stories abound concerning organizations that have lost millions of dollars in information system (IS) implementations gone wrong, but ISs that have successfully made it past the implementation phase can have catastrophic effects on the organization as well. The impact of risk events that occur during system development are generally limited to increased project costs or the loss of invested resources. By contrast, the impact of risk events that occur once the system is operational can be far more extensive, because operational ISs are increasingly embedded in the business process environment that they support. Recent IS-related failures demonstrate the far-reaching impacts that operational risk events can have on organizations:

- In June 2007, United Airlines suffered a shutdown of a mission-critical system that lasted for two hours. As a result, the company was forced to cancel more than twenty flights and ground over 250 more. An industry consultant estimated the overall loss to be in excess of $10 million.
- In 2005, over 40 million credit card accounts at MasterCard International were compromised due to a computer security breach.
- During much of 2006, a trader at Paris-based bank Société Générale had been exploiting weaknesses in the IT systems in order to establish fake trading positions that would go unnoticed from supervisors. Poor IT security has been partially blamed for the $7.2 billion loss.

There has been much interest in operational risk in recent years mainly due to new regulatory standards and catastrophic events, such as the September 11th terrorist attacks. The Basel Committee on Banking Supervision (BCBS), which establishes standards that set risk-based capital requirements for financial institutions, defines *operational risk* as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events" (BCBS, 2001). The ramifications of inadequate or failed ISs to business processes with which they are integrated have been recognized by regulatory agencies and practitioner-based frameworks. A good example is the Control Objectives for Information and related Technology (COBIT) framework developed by the IT Governance Institute (ITGI, 2007a), which believes that the BCBS definition of operational risk should be considered in light of IT management (ITGI, 2007b).

It is easy to build on the BCBS definition and define *IS-related operational risk* as any operational risk that involves an information system, but it is important to clearly position IS-related operational risk in relation to operational risk and IS risk in general. IS-related operational risk includes any form of operational risk arising directly due to an IS failure (e.g., software

bugs, hardware malfunction) or indirectly from a failure in the work supported by an IS within a business process. Importantly, in including failures in the work supported by an IS we are implicitly targeting failures due to flawed systems and IS-enabled process designs lacking proper controls (e.g., intentional or unintentional user data entry errors, security bridges) as well as failures due to poor system implementation and ongoing management procedures (e.g., inadequate data refresh cycles, backup procedures, user training). What makes such risks IS-related is the fact that they can be controlled, at least to some degree, by adequately designing and implementing an IS and its work environment. As to IS risk in general, IS-related operational risk includes any form of IS risk that arises only once an IS becomes operational, as opposed to during IS development and implementation. For practical IS management purposes, however, our discussion thus far clearly suggests that operational IS risks may be of great relevance even during IS development and implementation.

Despite growing interest in operational risk, Hinz (2005) observed that "research on identifying and mitigating the operational risk associated with IT is still quite immature in theory and in practice, leaving managers without sound decision support." Indeed, based on their extensive survey of the literature on IS risk and risk management, Alter and Sherer (2004) note that the majority of studies focused on risks in the context of developing and implementing new ISs as opposed to systems in operation. Even the relatively limited research relevant to IS-related operational risk has focused mainly on *computer crime* involving "the use of computerized systems to perform illegal acts" (Alter, 2002) and on *IS security threats* presented as IS vulnerabilities that could result in undesirable consequences (Im and Baskerville, 2005; Neumann, 1995). Within this research stream we were able to identify five key works that developed IS threat taxonomies which include other types of IS-related operational risk (Alter, 2002; Baskerville, 1996; Im and Baskerville, 2005; Loch et al., 1992; Whitman, 2004). Unfortunately, these taxonomies are limited in their ability to provide much insight into IS-related operational risk events experienced by organizations. Two were survey-based (Loch et al., 1992; Whitman, 2004) rather than based on actual events, and one was not tested at all (Alter, 2002). Additionally, even though they accounted for non-computer crime events, those taxonomies that were tested still had a sparse representation of such events.

This ongoing research seeks to offer an exploratory analysis of IS-related operational risk based on a close examination of hundreds of actual IS-related operational risk events (ISOREs) documented in a commercially available database. Our research has two main objectives. The first is to develop a better understanding of the types of ISOREs experienced by organizations. This includes identification of the types of ISs and IS-enabled processes that give rise to these events, examination of the magnitudes of associated losses, and investigation of the varying impacts of these events over time and across countries. A more fundamental objective that follows is the identification and formulation of testable research hypotheses concerning ISOREs.

Our findings could help managers and researchers to achieve a better understanding of the risk exposure associated with operational ISs in their current business environment and with new IT investments under consideration. In addition, our research could assist organizations in achieving a higher level of strategic and economic alignment, through the use of a systematic IS risk management approach.

RESEARCH APPROACH & METHODOLOGY

Data

The primary goal of our research is to conduct an exploratory analysis of the IS-related events collected in the Algo FIRST database, which is maintained by Algorithmics Inc., a member of the Fitch Group. This commercial database documents thousands of operational risk events that have been reported in public sources such as reports and press releases from regulatory agencies (e.g., SEC filings) and the media (e.g., *Wall Street Journal*) from 1920 to the present day. We recognize that the FIRST database may be biased toward larger loss events of the kinds that make their way into public sources, especially since many of the events have occurred in the financial services sector. We are hence sensitive to this limitation and its effect on the generalizability of our research findings. Nevertheless, the kinds of events in the database are likely to be of prime management concern since they could cause the greatest damage to an organization. More importantly, since no study to date has examined actual IS-related operational risk events, research based on the FIRST database can still offer useful and novel insights as well as foundations for follow-up research on IS-related operational risk.

The FIRST database contains for each event a narrative description, along with more structured information consisting of over 20 specific attributes of the event (e.g., firm at which the event occurred, geographical region, loss amount, and date of occurrence). An important attribute classifies events by *event trigger*, or what Algorithmics defines as "the primary cause of an event," of which there are five categories: (1) people, (2) relationship, (3) process, (4) technology, and (5) external.

We searched the FIRST database to identify the ISOREs most relevant to our study. We applied several filters to the data. First, all events classified within the event trigger "technology" were selected. Additionally, as an ISORE may not necessarily be classified within the "technology" event trigger, the database was searched for key words within the detailed

event description narrative For example, an employee input error may be classified in the "people" event trigger, but would still be an ISORE that could have been prevented by building appropriate controls into the IS. Therefore, the key words we used to search for ISOREs outside the "technology" category include "computer", "electronic", and "information systems". Overall, we identified 777 events for review against our definition of IS-related operational risk. Finally, events reported in 2007 were removed from this sample because data in 2007 may be under-populated due to the extended duration of many events: it could take time for all relevant information about an operational risk event to be discovered. Our final sample consists of 416 events that occurred globally up until the end of 2006.

ISORE Classification

We classified the 416 identified ISOREs based on the taxonomy of risk categories defined in Table 1. Most of these risk categories come from the "system threats" taxonomy proposed by Alter (2002). Beyond his categories, we found it necessary to use two additional categories provided in the FIRST database: "New Technology Failure" and "Systems Integration (Merger Related)". These two categories were deemed to provide necessary distinction for the relevant events, and did not map to any categories identified in the literature. Lastly, an "Unspecified System Failure" category was created for those events where it was not apparent whether the failure took place due to hardware or software issues. In most cases, the database categories very closely matched those proposed by Alter. However, the narratives for all events were carefully reviewed to ensure conformance with category definitions.

Computer Crime	**Use of computer systems to perform illegal acts**
Theft	Includes: (1) Theft of software and computer equipment, (2) Unauthorized use of access codes and financial passwords, (3) Theft by entering fraudulent transaction data, (4) Theft by stealing or modifying data, (5) Internet hoaxes for illegal gains, (6) Theft by modifying software
Sabotage & Vandalism	Attempt to invade or damage system hardware, software, or data
Non-Computer Crime	**ISOREs that are not due to Computer Crime**
Software Bugs	Flaw in a program that causes it to produce incorrect or inappropriate results
Hardware Malfunctions	Flaw or failure of computer hardware that causes it to produce incorrect or inappropriate results
Operator Error	Combination of inattention, nonconformance to procedures, or other error by participants in a system
Inadequate System Performance	System cannot handle the task that is required of it
Damage to Physical Facilities	System disruption or failure due to a wide range of environmental threats and external events
Data Errors	System disruption or failure due to an incorrect data source
New Technology Failure	Newly implemented system causes business process disruption/failure due to (1) flaws within the system itself, (2) flaws within the implementation process, and/or (3) system incompatibility with business process environment
Systems Integration (Merger Related)	Systems from merged entities fail to properly operate together in newly merged business process environment
Unspecified Systems Failure	System disruption or failure that cannot be attributable to hardware or software (provided information not detailed enough)

Table 1. ISORE Categories

PRELIMINARY DATA ANALYSIS AND DISCUSSION

Number of ISOREs over Time

Figure 1 shows that the number of ISOREs has increased dramatically since 1970, which was their first appearance in the database.

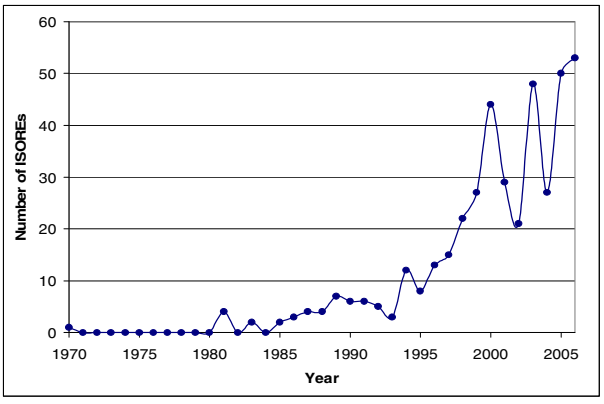

Figure 1. Number of ISOREs by Year

The number of events reached an all-time high in 2006, the last year included in our analysis. The data shows a steady upward trend in the number of events with a sharp increase in the trend around the mid 1990s. Moreover, the data does not indicate that the trend is associated with any subset of the types of ISOREs in Table 1 or any specific subset of countries.

While the growth pattern we observed is interesting in itself, it is important to understand what could be the causes underlying this pattern and whether the effect of those causes is likely to persist over time. Could it be that the growth in the number of ISOREs is simply a function of the increased presence of IT within organizations? Or, is it due to business cycles? Or perhaps due to shifts in the global IT environment, such as the Internet and the influx of new technologies and applications that it brought about? We are in the process of examining, formalizing and testing these and other plausible explanations for the observed pattern. For example, we are looking to determine whether the number of ISOREs **normalized** by the level of IT investment over time exhibits the same growth pattern. Another example is to determine whether the dramatic increase before 2000, and the subsequent downturn, can be explained by the dot com investment bubble. These are some directions that we are exploring in line with our objective to identify hypotheses concerning ISOREs that are testable and potentially insightful.

Prevalence and Severity of ISORE Types

Table 2 details the categorization of the 416 ISOREs. Some interesting observations emerge from this preliminary analysis of the data. First, although they have received less attention in the literature than computer crime events, more non-computer crime events were present in our sample. The second observation deals with the nature of loss impact. The FIRST Database distinguishes between *direct losses*, being "the financial repercussions of an event", and *indirect losses*, being "non-financial impacts, such as reputational damage, loss of market access or ratings downgrades" (Algorithmics, 2006). Only 25% of the ISOREs had a direct loss impact. Those same ISOREs also made up the great majority of the events with a stated loss amount in the database. This is not surprising considering that indirect losses can be more challenging to quantify. This observation suggests additional research questions, such as: (1) Why do certain ISORE types (e.g., New Technology Failure) more often result in indirect losses than others (e.g., Hardware Malfunctions)? and (2) What types of systems (e.g., customer-facing vs. backoffice-support) are more likely to be associated with ISORE types that more often result in indirect losses? The answers to such questions could have important implications on whether and how organizations should consider certain ISOREs and for the way they can be managed from the moment a new system is proposed and its associated IT investments are being evaluated.

A third observation concerning ISOREs from Table 2 is that the 65 non-computer crime events with stated loss amounts resulted in a much higher overall average loss than the 43 computer crime events: $53.2M versus $16.2M, respectively. In fact, although Theft ISOREs were the highest occurring event type, they had a much lower average loss than the second most occurring event type, Software Bugs. This revealing figure emphasizes the importance of differentiating between events of low/high frequency and events of low/high severity and could have implications on the way organizations allocate resources for lowering risk due to low-impact events such as security threats and high-impact events such as software bugs.

	Number of ISOREs	Number of ISOREs with Direct Loss Impact	Percentage of ISOREs with Direct Loss Impact	Number of ISOREs with Stated Loss	Average Loss ($ Millions)
Computer Crime					
Theft	139	33	23.7%	27	3.5
Sabotage & Vandalism	51	7	13.7%	16	37.6
	190	**40**	**21.1%**	**43**	**16.2**
Non-Computer Crime					
Software Bugs	90	27	30.0%	28	60.8
Operator Error	27	9	33.3%	9	58.3
Inadequate System Performance	24	9	37.5%	8	52.4
Damage to Physical Facilities*	21				
Unspecified System Failure	18	5	27.8%	6	26.8
New Technology Failure	16	9	56.3%	9	48.7
Hardware Malfunctions	16	1	6.3%	1	3.2
Systems Integration (Merger Related)	12	3	25.0%	3	66.8
Data Errors	2	1	50.0%	1	7.4
	226	**64**	**28.3%**	**65**	**53.2**
	416	**104**	**25.0%**	**108**	**38.4**

*** Events in this category contain losses that relate to damages outside the ISORE alone (i.e. loss of life) - Therefore, losses are not included for purposes of this analysis**

Table 2. Sample Descriptive Statistics of ISORE Data (1970-2006)

ISOREs by Geographical Region

Some interesting patterns also begin to appear when ISOREs are examined across the three geographical regions with the greatest number of events: North America, Europe, and Asia (contain over 90% of all events). Theft, Software Bugs, and

Sabotage & Vandalism are the top three most frequently documented ISORE types in each geographical area. Yet, there are some striking differences among these regions. For example:

- Of the three regions, North America has the greatest number of events but the lowest overall average loss amount, while Asia has the least number of events but the highest overall average loss amount
- Theft and Sabotage & Vandalism events appear to result in much higher losses on average in Asia.
- The average loss for Operator Error events is significantly higher in Asia, and those occurring in Europe are almost ten times higher than those in North America.

These findings clearly indicate that there are differences both in the prevalence of ISOREs and their loss severity across geographical regions. Here, too, there are numerous plausible root cause explanations that we are looking to examine and formalize as testable hypotheses. A good example is the potential link between the level of regulation in a particular region and the characteristics of ISOREs that organizations experience in that region.

	Asia		Europe		North America	
	No. of ISOREs	Avg. Stated Loss ($ Millions)	No. of ISOREs	Avg. Stated Loss ($ Millions)	No. of ISOREs	Avg. Stated Loss ($ Millions)
Theft	10	9.9	49	0.7	66	4.4
Software Bugs	8		31	83.6	45	57.3
Sabotage & Vandalism	6	111.8	13	31.1	28	2.8
Operator Error	6	170.5	2	73.0	19	7.5
Inadequate System Performance	1		6		17	52.4
Damage to Physical Facilities	2			75.0	18	
Unspecified System Failure	2		7	3.2	7	3.5
Hardware Malfunctions	1		4	56.6	11	
New Technology Failure			4		12	44.7
Systems Integration (Merger Related)	3		2		7	66.8
Data Errors					1	7.4
Grand Total	**39**	**69.0**	**118**	**43.7**	**231**	**33.9**

Table 3. Number of ISOREs and their Severity (in USD) by top three Geographical Regions

CONCLUSION

Past IS research has paid little attention to operational risk and its relation to IS development, implementation and management. Yet, because ISs are often tightly embedded within organizational business processes, the failure of operational ISs could also result in significant losses. Increasing dependence of the corporate and financial sectors on IT in recent decades increases their exposure to this type of IS risk. This research uses a database of publicly reported events to analyze the types of IS-related operational risk events (ISOREs) that occur within organizations. The goal of this ongoing research is to identify and formulate testable research hypotheses concerning these events, with the hope that it will provide managers a better understanding of IS-related operational risk both in their existing business environment and in potential IT investments.

We believe that the rich level of detail within the FIRST database will greatly assist us in reaching this goal. For example, the events included in the database can provide insight into important issues such as the behavior of computer crime incidents versus non-computer crime events over time. This type of observation would allow management to better assess the level of resources to be spent on both types of exposure. From preliminary analysis of the database, the information it contains could also shed light on the types of ISOREs experienced by particular business units within organizations. Additionally, the database classifies the impact of events within a different direct loss and indirect loss categories, and also attempts to identify factors which affect an event's likelihood to occur or its level of severity. Analyzing such information, as well as other database attributes, will contribute greatly to what we currently understand about this little-explored dimension of IS risk.

ACKNOWLEDGMENTS

This research was supported by a research grant from the Brethen Institute for Operations Research, Whitman School of Management, Syracuse University.

REFERENCES

1. Algorithmics (2006) *Fitch Risk FIRST User Manual*, Version 3.05.
2. Alter, S. (2002) *Information Systems: The Foundation of E-Business*, 4th edition, Upper Saddle River, NJ, USA, Prentice Hall.
3. Alter, S. and Sherer, S. (2004) A general, but readily adaptable model of information system risk, *Communications of the AIS*, 14, 1-28.
4. Basel Committee on Banking Supervision (BCBS) (September 2001) Working paper on the regulatory treatment of operational risk, http://www.bis.org.
5. Baskerville, R. (1993) Information systems security design methods: Implications for information systems development, *ACM Computing Surveys*, 25, 4, 375-414.
6. Baskerville, R. (1996) A taxonomy for analyzing hazards to information systems, in S. Katsikas and D. Gritzalis (Eds.) *Information Systems Security: Facing the Information Society*, London, UK, Chapman & Hall, 167-176.
7. Charette, R.N., Adams, K.M. and White, M.B. (1997) Managing risk in software maintenance, *IEEE Software*, 14, 3, 43-50.
8. Chernobai, A., Rachev, S. T. and Fabozzi, F.J. (2007) *Operational Risk: A Guide to Basel II Requirements, Models, and Analysis*, Hoboken, NJ, USA, John Wiley and Sons, Inc.
9. Hinz, D.J. (2005) High severity information technology risks in finance, *Proceedings of the 38th Hawaiian International Conference on System Sciences*, Hawaii.
10. Im, G.P. and Baskerville, R.L. (2005) A longitudinal study of information system threat categories: The enduring problem of human error, *The DATABASE for Advances in Information Systems*, 36, 4, 68-79.
11. IT Governance Institute (ITGI) (2007a) *IT Assurance Guide: Using COBIT*, Rolling Meadows, IL, USA.
12. IT Governance Institute (ITGI) (2007b) *IT Control Objectives for Basel II*, Rolling Meadows, IL, USA.
13. Loch, K.D., Carr, H.H and Warkentin, M.E. (1992) Threats to information systems: Today's reality, yesterday's understanding, *MIS Quarterly*, 16, 2, 173-186.
14. Markus, M.L. (2000) Toward an integrative theory of IT-related risk control, in R. Baskerville, J. Stage, and J. DeGross (Eds.) *Organizational and Social Perspectives on Information Technology*, Boston, MA, USA, Kluywer Academic Publishers, 167-178.
15. Sherer, S. and Alter, S. (2004) Information systems risk and risk factors: Are they mostly about information systems?, *Communications of the AIS*, 14, 2, 29-62
16. Smith, H.A., McKeen, J.D. and Staples, D.S. (2001) Risk management in information systems: Problems and potential, *Communications of the AIS*, 7, 13, 1-29.
17. Straub, D. W. and Welke, R.J. (1998) Coping with systems risk: Security planning models for management decision making, *MIS Quarterly*, 22, 4, 441-469.
18. Whitman, M.E. (2004) In defense of the realm: Understanding the threats to information security, *International Journal of Information Management*, 24, 43-57.