Journal of the Association for Information Systems

JAIS

Research Article

An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories

James Goldstein
Canisius College
goldste3@canisius.edu

Anna Chernobai
Syracuse University
annac@syr.edu

Michel Benaroch
Syracuse University
mbenaroc@syr.edu

Abstract

Organizations' growing exposure to IT operational risk, or the risk of failures of operational IT systems, could translate into significant losses. Despite this, there are notable theoretical and empirical gaps in the literature on IT operational risk. We propose the "resource weaknesses" framework, which extends the resource-based theory of the firm, as a theoretical lens for investigating IT operational risk and its impacts. We also theorize about and empirically examine the impact differences of two categories of IT operational failures: ones resulting in the disclosure, misuse, or destruction of data assets, and ones resulting in the loss of availability or the mis-operation of functional IT assets responsible for the handling of data assets. Whereas the former, data-related failures have had some coverage in the literature, little is known about the latter, function-related failures. We apply an event study analysis with a well-balanced data set of IT operational failure events that occurred in U.S. financial service firms over a 25-year period. We find that function-related events have a substantially larger negative wealth effect than data-related events, and that firm characteristics such as firm size and growth potential greatly influence the degree of wealth effect. We conclude with important implications for practice and research.

Keywords: *IT Risk, Operational Risk, IT Security, Event Study.*

* Robert Fichman was the accepting senior editor. This article was submitted on 29th June 2010 and went through two revisions.

Volume 12, Issue 9, pp.606-631, September 2011

An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories

1. Introduction

As information technology (IT) systems are increasingly embedded in business processes, failures of these systems are exposing organizations to significant economic losses. The following are examples of such failures:

1. *In August 2008, HSBC Bank suffered a failure of its core banking computer system due to a corrupted disk in its Amherst data center, resulting in four million customers experiencing a significant interruption in services for nearly a week.*

2. *In June 2005, more than 40 million credit card accounts at MasterCard International were compromised due to a computer security breach.*

3. *United Airlines suffered a shutdown of a mission-critical system in 2007 that caused the cancellation of more than 20 flights and the delay of 250, resulting in an overall loss exceeding $10 million.*

4. *EBay's servers crashed in 1999, costing the company $2 million a day in losses.*

The above failures are manifestations of what we term *IT operational risk*. The Basel Committee on Banking Supervision (BCBS) defines *operational risk* as "the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events" (BCBS, 2001, p. 2). While given for use by financial firms, this definition is equally applicable to non-financial firms. *IT operational risk* is a specialized subset of operational risk and centers around potential failures in operational IT systems and/or business processes that they support.

The main objective of this paper is to theoretically investigate and empirically examine the impact differences of two broad classes of IT operational risk events. The distinction we make between the two classes is motivated primarily by the fact that extant research has focused on one class while being virtually silent on the other. We characterize these classes here and will define them formally later. At the core of our distinction is the recognition that an IT system comprises *functional IT assets* (hardware, software, telecommunications, end-users, system operators, and system management procedures), which are responsible for creating, processing, transporting, and storing *data assets*. For the purpose of this study, we respectively distinguish between the following two classes of IT operational risk events.

Class 1: IT operational risk events that result in disclosure of confidential data assets to unauthorized parties, misuse of data assets, or destruction of data assets.

Class 2: IT operational risk events that result in loss of availability, or are the result of the mis-operation, of functional IT assets responsible for the handling of data assets.

These characterizations recognize that data has no intrinsic functional or operational capability and that data is only indirectly affected by class 2 events. Also, class 1 events may occur even if functional IT assets operate properly, and class 2 events may or may not impact data assets. In this light, for lack of better terms, we will refer loosely to IT operational risk events in classes 1 and 2 as *Data* and *Function* events, respectively.

Extant research on IT operational risk has two critical shortcomings that are of interest to this study. First, extant studies lack adequate theoretical grounding. The hypotheses they test rest mostly on anecdotal evidence, surveys of IT managers, and past empirical results. A suitable theoretical framework is crucial to the ability to theorize about IT operational risk and to conduct meaningful empirical research. Second, extant work is unbalanced in its treatment of Data-related and Function-related risks. It has concentrated on Data events, primarily ones due to malware and hacking attacks,

and yielded mixed results on the impact of these events (e.g., Campbell, Gordon, Loeb, & Zhou, 2003; Cavusoglu, Mishra, & Raghunathan, 2004; Acquisti, Friedman, & Telang, 2006; Kannan, Rees, & Sridhar, 2007). Even work that has paid attention to Function events has used small data sets and focused on denial-of-service (DOS) and virus attacks that compromise the availability of IT assets (e.g., Campbell et al., 2003; Hovav & D'Arcy, 2003; Cavusoglu et al., 2004). Thus, completely overlooked are incidents where functional IT assets mis-operate due to such common factors as software bugs, network failures, user input errors, and operator errors.

In this light, the goal of this paper is two-fold. First, we propose the *resource weaknesses* framework (West & DeCastro, 2001; Arend, 2004) as a theoretical lens for reasoning about IT operational risk and its subtypes. This framework extends the resource-based view (RBV) of the firm (Wernerfelt, 1984) by recognizing that firms often develop organizational weaknesses in conjunction with the development of resource strengths that lead to competitive advantage. Although the IT literature has dealt with strategic advantages arising from IT resources (e.g., Bharadwaj, 2000; Wade & Hulland, 2004), it has not explicitly addressed capability weaknesses arising from these same resources. Such weaknesses manifest as IT operational risk events. Our second goal is to theorize about and empirically test the impact of Data and Function events on the market value of firms experiencing them. To achieve this purpose, we use the event study methodology with data from a commercial proprietary database called Financial Institutions Risk Scenarios Trends (FIRST). FIRST is a comprehensive repository of thousands of publicly reported operational risk events occurring worldwide, with a strong representation of events in financial services firms. Our primary focus is, therefore, on the financial services industry. This industry is sufficiently large in its own right for our results to be of value to a wide audience. Nonetheless, since the financial services industry is so heavily reliant on IT (Berger, 2003), we expect our findings to apply to other IT-intensive industries.

This paper makes two important contributions to the IT risk literature. It is the first to propose a theoretical lens for conceptualizing IT operational risk, where the predictions we make based on this theoretical lens concerning the impacts of various subtypes of this risk are validated by our empirical results. Moreover, by using the most varied data sample to date, the paper's results offer novel insights into a little-explored but important class of IT risk. Like past research on operational risk, in general (Cummins, Lewis, & Wei, 2006), we find that IT operational risk as a whole has a negative wealth effect. More importantly, we observe that only Function events result in a statistically significant drop in firm market value, and that the drop is substantially larger than that observed for all events combined and for Data events, in particular. Last, we find that the firm characteristics of size, growth potential, and financial subsector impact the degree of market reaction to IT operational risk events. These findings have important implications for practice and research, as our discussion will show.

The paper proceeds as follows. Section 2 formally defines IT operational risk and reviews related literature. Section 3 presents the theory of resource weaknesses and formulates our research hypotheses. Section 4 describes the data and methodology used to test the hypotheses and presents the results. Section 5 discusses our main findings, their limitations, and their implications for research and practice along with directions for future research. Section 6 offers concluding remarks.

2. Background and Literature Review

This section discusses the notion of operational risk in general, defines IT operational risk and two of its subtypes, and reviews the extant literature on IT operational risk.

2.1. Operational Risk and IT Operational Risk

The increased interest in (general) operational risk in recent years is attributed to new regulatory capital and compliance requirements for financial institutions, which came as a counter-measure to numerous high-visibility operational risk events. By one estimate, about 40 percent of all firms that experience high magnitude operational risk events are out of business within three to five years (Croy, 2008). However, even more common, non-catastrophic operational risk events are of significant concern. For example, a study of operational risk in banking found that "large,

internationally active banks typically experience between 50 and 80 losses, each exceeding $1 million per year" (Rosenberg & Schuermann, 2006, p. 591). Overall, there is a clear recognition that operational risk events can have severe impacts "on earnings, share price volatility, and potentially even solvency" (Cummins et al., 2006, p. 2606).

Under recently imposed regulatory standards, financial institutions, primarily depository institutions, are required to track their operational risk exposure within seven risk categories as defined by the Basel Committee (BCBS, 2001). These categories are defined in Table 1.

Table 1. BCBS Operational Risk Categories

Basel Operational Risk Category	Illustrative IT Operational Risk Events (from the FIRST database)	Primary IT assets Affected (Data or Functional)
Internal Fraud: acts to defraud, misappropriate property, or circumvent regulations, the law, or company policy, by employees	Employee sold proprietary information, which was used to make counterfeit checks	Data
	Rogue trader exploited loophole in IT system to hide trading losses	Functional
External Fraud: acts to defraud, misappropriate property, or circumvent the law, by external parties	Computer hackers obtained personal data on thousands of customers	Data
	Computer worm attacked phone, Internet, and banking networks, leading to a breakdown in services	Functional
Employment Practices and Workplace Safety: acts inconsistent with employment, health or safety laws, or agreements	Employees took valuable client information prior to taking a position at a rival firm	Data
Clients, Products, and Business Practices: failures to meet a professional obligation to specific clients or from the nature or design of a product	Trading brokerage violated regulatory trading rules due to faulty system	Functional
	Bank failed to implement systems compliant with regulatory anti-money laundering provisions	Functional
Damage to Physical Assets: loss or damage to physical assets from natural disasters or other events	Burst steam pipe shut down building cooling system, leading to the inability to use computer systems	Functional
Business Disruption and System Failure: disruption of business or system failure	A "keystroke error" lists a multi-million share IPO on Nasdaq for $0.01 per share rather than the original price of $19.50 per share	Data
	Website failure led to inability of customers to conduct online trading	Functional
Execution, Delivery, and Process Management: failures in transaction processing or process management	Company fined by regulatory agency for failing to comply with data retention policies	Data
	Computer system incorrectly reported transactions due to a software bug (leading to regulatory penalties)	Functional

While IT operational risk is only a specialized subset of operational risk, it cuts across all seven Basel-defined categories. This is consistent with the IT Governance Institute view (ITGI, 2007a) and supported in Table 1 using examples of IT operational risk events (second column) extracted from the FIRST database that we used to construct our data sample. Such extensive representation of IT risk events across the spectrum of operational risk in financial institutions does not come as a surprise, considering that financial services have ranked within the top 10 most IT intensive industries in the U.S. since the mid-1990s (Triplett & Bosworth, 2002).

2.2. IT Operational Risk Defined

Straub and Welke (1998) define "systems risk" as uncertainty related to using computer-based systems and interpret this risk to be "broadly construed to mean modification, destruction, theft, or lack of availability of computer assets such as hardware, software, data, and services" (p. 442). This interpretation is consistent with Loch, Carr, and Warkentin's (1992) earlier recognition that IT operational risk could result in the disclosure, modification, destruction, or denial of use of IT resources. It also coincides with the Confidentiality-Integrity-Availability (CIA) framework commonly used to benchmark the security of an organization's data and information assets in terms of risks surrounding the confidentiality, integrity, and availability of these assets (Campbell et al., 2003; Cavusoglu et al., 2004; Kannan et al., 2007). Together, these three views offer a solid basis for our next definition of IT operational risk; although we need to further clarify that computer assets, or what we call IT assets, include hardware, software, telecommunication, data, users, system operators, IT management procedures, and IT infrastructure services (Weill & Broadbent, 1998). Accordingly, we offer the following adaptation of Straub and Welke's (1998) definition:

> ***IT operational risk*** *is any threat that may lead to the improper modification, destruction, theft, or lack of availability of IT assets.*

We distinguish between two types of IT operational risk events -- Data and Function events -- based on the primary IT assets being affected. (Table 1 characterizes the samples of IT operational risk events accordingly.) This distinction recognizes that data assets have no intrinsic function, as even the meaning of data comes about from the context in which the data is used. All other IT assets provide the functions needed to handle – create, process, transport, and store – data assets (Longo, 2009), and can, hence, be termed functional IT assets. Another notion at the core of this distinction is that IT operational risk events may *directly* impact either data assets or functional IT assets.

Data events directly impact data assets. They may be due to malware or hacker attacks (phishing, Trojans, viruses, and worms) or computer crime activities by internal personnel. They can result in the extraction of private sensitive data, the deletion of data files, theft of passwords and access codes, or website defacement. Data events may also be due to accidental factors, such as loss of computer equipment containing confidential data, unintentional posting of sensitive data on a firm's website, or erroneous mailing of sensitive customer information to the wrong parties.

> ***Data-related IT operational risk*** *is any threat to the confidentiality of data assets that can result in the disclosure, misuse, or destruction of these assets.*

Function events directly impact functional non-data IT assets by affecting either their integrity (i.e., correct operation) or availability (Cavusoglu et al., 2004; Kannan et al., 2007). Events that result in loss of availability of functional IT assets can be due to technical problems (e.g., hardware, software, network, or power outages), natural phenomena (e.g., floods), malicious activities (e.g., DOS attacks or vandalism), or human errors. Events that compromise the integrity of functional IT assets can be due to viruses that delete programs, software bugs and processing errors, or user input errors. Like Data events, Function events can be malicious and externally initiated, but they are more often accidental and originate from within the firm.

> ***Function-related IT operational risk*** *is any threat to the availability or to the integrity of functional IT assets (that may eventually affect data assets).*

2.3. Research on IT Operational Risk

The IT risk literature has recognized the importance of IT operational risk but only to a limited extent. A comprehensive survey confirms that the primary focus of this literature is on risks arising in the development of IT systems (Sherer & Alter, 2004). Some work recognizes that IT development risk and IT operational risk interact and highlights the need to integrate their treatment (e.g., Lyytinen & Hirschheim, 1987; Markus & Keil, 1994; Markus, 2000). In this vein, researchers have called on

system developers to consider how system design and development practices affect the potential for human operator errors (Brown & Patterson, 2001), maintenance errors (Charette, Adams, & White, 1997), and computer crimes (Baskerville, 1993).

There is much work on IT operational risk in the context of information security, but this work largely concentrates on Data-related risks. Straub and Welke (1998) explain that information security is a subset of what they call "systems" risk, as it is concerned only with the protection of data and information assets (Smith, 1989; Ryan & Bordoloi, 1997). In fact, according to a review of more than 1,280 information security research papers published from 1990 to 2004 (Willison & Siponen, 2007), the bulk of these papers address the nature and prevention of data privacy violations and other Data-related threats (e.g., viruses and hacker attacks), and far fewer specifically address Function-related threats.

Relatively few empirical studies have addressed IT operational risk. These studies analyze the impact of IT operational risk events on firm value using the event study methodology, except for Ko and Dorantes (2006), who use a matched-sample comparative analysis. Table 2 provides details on these studies, the types of events (Data and Function) they analyzed, and their main findings.[1]

Table 2. Summary of Extant Empirical Studies

Study	Sample Period	Num. of Events	Num. of Events and Risk Event Target *Data-Function Classifications*		Basis for Tested Hypotheses	Key Relevant Findings and Observations
			Data	Function		
Campbell, et al. (2003)	1995-2000	43	• 11 data security Breaches • 4 website defacing attacks • 4 viruses	• 8 DOS attacks • 2 service interruptions • 2 traffic re-direction • 2 flaws in email systems • 10 worms (self-propagating email attachments that overwhelm email servers)	• Anecdotal Evidence • Academic / Practitioner Surveys	• Negative market reaction found only for breaches involving confidential data • All Function events and only about half of Data events involved non-confidential data
Hovav and D'Arcy (2003)	1998-2002	23		• 23 DOS attacks	• Anecdotal Evidence	• No negative market reaction to DOS attacks is observed, except for Internet companies
Cavusoglu, et al. (2004)	1996-2001	66	• 32 data security breaches	• 34 DOS attacks	• Resource-Based Theory • Information Transfer Theory • Anecdotal Evidence	• Negative market reactions found for both Data and Function events, without differences between types of attack • Stronger market reaction observed for Internet and small firms • Market reaction increases over time
Acquisti, et al. (2006)	2000-2005	79	• 67 data security breaches • 12 data loss		• Other Empirical Studies of Security Breaches	• Negative market reaction observed for Data events, with a stronger reaction for retail firms and for smaller firms

[1]We exclude Bharadwaj, Keil, and Mahring (2009). This study explored the impact of IT development failures and operational IT failures without clarifying the nature of the operational IT failures their data covered.

Table 2. Summary of Extant Empirical Studies (continued)

Study	Sample Period	Num. of Events	Num. of Events and Risk Event Target *Data-Function Classifications*		Basis for Tested Hypotheses	Key Relevant Findings and Observations
			Data	Study		
Ko and Dorantes (2006)	1997-2003	19	• 12 security breaches of confidential data • 7 other security breaches		• Other Empirical Studies of Security Breaches	• Financial performance of firms with Data breaches over four consecutive quarters was somewhat lower than that of non-breached firms in a matched sample
Kannan, et al. (2007)	1997-2003	72	• 12 data security breaches • 39 viruses • 11 website defacing attacks	• 4 DOS attacks • 6 website outages	• Other Empirical Studies of Security Breaches • CIA Framework	• No negative market reaction found for either Data or Function events, except when events from the months right after "9/11" are included in the sample • No differences in market reaction for Data and Function events, or for events occurring in different industries • Smaller reaction found for larger firms
Leung and Bose (2008)	2007 and Prior	2,994	• 2,994 phishing attacks		• Anecdotal Evidence	• No negative market reaction found, except for a few industries (financial but non-banking firms and IT and telecommunication firms)

From Table 2, four main gaps in the literature are apparent:

1. Most work has focused on Data events. Four studies that address Function events narrowly focus on DOS attacks, and two also analyze website outages and disruptive viruses (Campbell et al., 2003; Kannan et al., 2007). No work addresses Function events due to such factors as hardware and software failures, although IT managers rate those among the top threats to operational IT systems (Whitman, 2004).

2. This work provides inconclusive evidence on the impact of IT operational risk events. Four studies of Data events find that such events result in a drop in firm market value, and two find a similar result only for narrow contextual settings. Three of the four studies addressing Function events observe a drop in firm market value for only narrow contextual circumstances (Hovav & D'Arcy, 2003; Cavusoglu et al., 2004; Kannan et al., 2007), and one finds no market reaction (Campbell et al., 2003).

3. The data sets used by the studies cover limited four to six year periods, and most overlap with the dot-com bust and the time subsequent to the September 11, 2001 attacks (9/11), two problematic periods that may distort findings. For instance, Kannan et al. (2007) find no market reaction to the events that they study once events from the six months post-9/11 are excluded.

4. The studies lack theoretical foundation for the origin and nature of impact of IT operational risk. All but two studies rest their hypotheses solely on anecdotal evidence,

surveys of IT professionals, and past empirical studies. And only Cavusoglu et al. (2004) rely narrowly on resource-based theory and information transfer theory to theorize about the impact of the tested events on larger firms and security firms, respectively.

3. Theory and Research Hypotheses

This section introduces the theoretical lens used to investigate the impact of IT operational risk and its Data and Function subtypes. Like other studies using the event study methodology, our research hypotheses concern the impact of IT operational risk events on the equity prices of firms experiencing those events.

3.1. Theoretical Framework: Resource Weaknesses

Powell and Arregle (2007, p. 59) argue that "firms compete on two axes: the axis of competitive advantage, where performance is driven by the inimitable resources and capabilities of high-performing firms; and the axis of errors, where performance is driven by failures to attend to the activities, resources and opportunities that are equally available to all firms." The first axis concerns things that firms do uniquely well and lead to competitive advantage and to the generation of value. By contrast, the second axis concerns things that firms do poorly and lead to the erosion of competitive advantage and to the destruction of value. Others have labeled the second axis resource weaknesses (West & DeCastro, 2001), organizational liabilities (Arend, 2004), or competitive disadvantages (Powell, 2001).

The strategy and IT literature have paid great attention to the first axis, or to resource strengths. In particular, the resource-based view (RBV) of the firm ascribes competitive advantage to a firm's idiosyncratic resource strengths and capabilities used to implement firm strategies (Wernerfelt, 1984; Barney, 1991). Such resources are strategic when they are scarce, inimitable, non-substitutable, and appropriable. Drawing on RBV, much IT research has argued and demonstrated empirically that IT can be a source of competitive advantage when: (a) the firm possesses IT resources that are valuable, rare, and costly to imitate; or (b) the firm uses IT to realize the full competitive potential of non-IT resources through complementarity and co-specialization with these resources (e.g., Bharadwaj, 2000; Wade & Hulland, 2004; Melville, Kraemer, & Gurbaxani, 2004; Ray, Muhanna, & Barney, 2005; Ravinchandran & Lertwongsatien, 2005; Aral & Weill, 2007).

Much less attention has been given to the second axis, or resource weaknesses (West & DeCastro, 2001; Arend, 2004). Resource weaknesses are more than the failure of or the non-existence of resource strengths, "but rather the failure even to satisfy the minimum success requirements … required of any firm" (Powell, 2001, p. 877). This recognizes, consistent with RBV, that a firm generally must also invest in resources that are neither rare nor difficult to imitate in order to maintain competitive parity. Because resource weaknesses "destroy value in a firm rather than simply failing to add any," they can produce performance variations that are attributable to competitive disadvantages (Arend, 2003, p. 280). Like strategic resource strengths, a resource weakness can be strategic if it has three characteristics (Arend, 2004). First, it is costly – destroys value and reduces firm performance, either directly or by intervening in the generation of value through the use of strategic resources or by introducing the opportunity cost associated with loss of competitive position. Second, it is scarce and inconvertible – uncommon to the entire industry and cannot be economically converted to a benign form (West & DeCastro, 2001). Third, it is appropriated – paid for by the firm with no economic way of avoiding its associated costs.

Based on this expanded perspective, we summarize a dynamic view of strategy development in Figure 1 (adapted from West & DeCastro, 2001). Traditional perspectives, including that of the RBV, tend to view strategy as being related to building distinctive competences via the development and enhancement of unique resource strengths (path A). The expanded theoretical perspective, in addition, recognizes that resource weaknesses and inadequacies may be developing concurrently with strengths and competences (path B). Therefore, it posits that enhancing a competitive position

also lies in overcoming or counteracting resource weaknesses (Path C). Moreover, firms that do not do so will see their resource weaknesses persist and may also experience a loss of strategic advantage as a result of erosion in (or imitation of) their resource strengths (path D). Persistence of resource weaknesses could, in addition, constrain the ability of a firm to develop new related resource strengths as part of strategic renewal (path E).

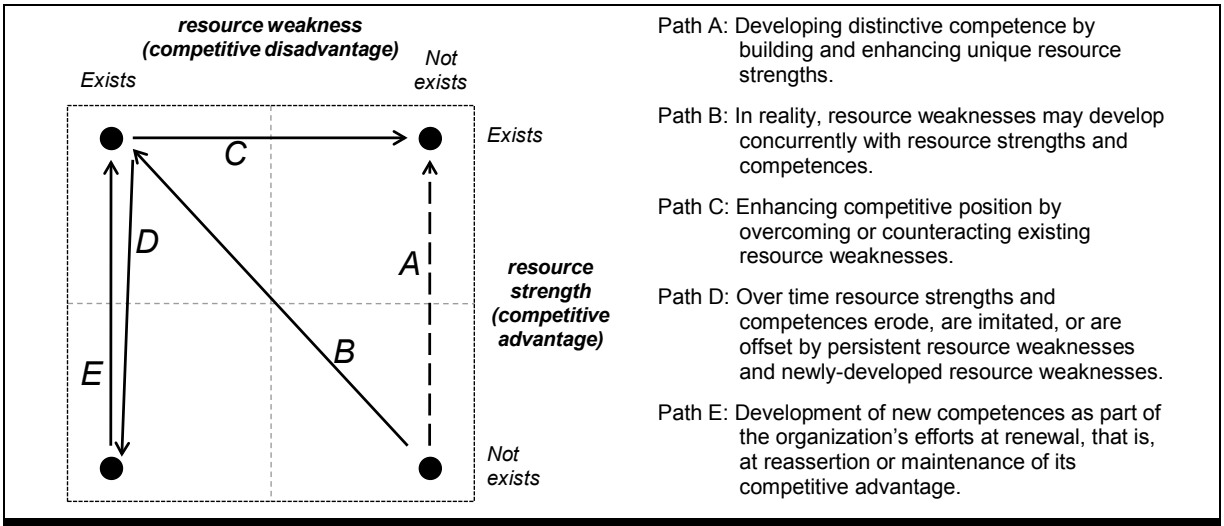

Figure 1. Expanded View of (Resource-Based) Strategy Development

Our context fits well with the theory of resource weaknesses. If imperfectly implemented, the same IT resources that endow a company with a strategic competitive advantage when they are coupled with complementary non-IT resources could also create the risk that their own operational failure would mean a failure of their co-dependent non-IT resources (Alter, 1999). Thus, IT resource weaknesses could be a direct concurrent by-product of investment in the creation, support, or use of strategic IT resource strengths (Arend, 2004). IT resource weaknesses may also arise from the natural evolution of strategic IT resource strengths (Arend, 2004). Over time, specialized IT assets that may endow some firms with a competitive advantage often become commoditized and readily available to all firms and, therefore, do not offer a distinction to any firm (Clemons, 1991; Carr, 2003). Ongoing reliance on such commoditized IT resources is a business necessity, and a failure to manage their associated weaknesses as well as the risks that arise with continued investment in the support and use of such resources would put a company at a competitive disadvantage. In either case, such IT resource weaknesses are at the root of exposure to IT operational risk.

3.2. Hypotheses Formulation

When actual IT operational risk events occur, they signal to the market that IT resource weaknesses are present within the affected firm. To investors, the presence of IT resource weaknesses signaled by such an event is more important than the direct monetary impact of the event itself, since these resource weaknesses are strategic and can erode the competitive position of a firm.

To begin with, IT resource weaknesses are scarce. As previously stated, they are idiosyncratic (firm-specific) because they are often the by-product of investments in scarce, idiosyncratic IT resource strengths. And, since they cannot be separated from those resource strengths, imitable solutions to those weaknesses do not exist in the competitive environment (West & DeCastro, 2001). The implication is simple: when IT resource strengths erode over time, their associated weaknesses persist and continue to expose the firm to IT operational risk (akin to a move along path D in Figure 1). Moreover, just as it takes time to develop strategic IT resource strengths, "the dismantling of resource weaknesses becomes an expensive and time-consuming affair" (West & DeCastro, 2001, p. 426). This reality could limit the ability of a firm to rid itself of IT resource weaknesses as a way to enhance its competitive position (akin to a limited ability to move along path C in Figure 1).

IT resource weaknesses can also be costly. They may result in significant losses that are mainly appropriated by the firm. Given firms' increased reliance on IT resources in daily operations, IT resource weaknesses could distract the generation of rents by the strategic IT resources embodying them (West & DeCastro, 2001). In particular, these weaknesses could diminish (current and previously created) IT-based competitive advantages by creating inefficiencies, or non-optimal processes and systems, which inhibit a firm's best potential performance with its current resource strengths (Arend, 2004). This view is consistent with some of the empirical results of studies summarized in Table 2.

In this light, IT resource weaknesses can place a firm at a competitive disadvantage. On the premise that IT operational risk events signal the presence of strategic IT resource weaknesses, our first hypothesis is:

> ***H1****: Firms that experience IT operational risk events suffer negative abnormal changes in their market value.*

Arend (2004) argues that firm performance deteriorates as the strength of a resource weakness increases in any of its definitional traits (scarcity, costliness, and appropriation). On this basis, we posit that Function events signal the presence of more significant IT resource weaknesses than Data events. To clarify why, we first discuss Data events separately from Function events and then contrast the two.

IT resource weaknesses at the root of Data events are characterized by a degree of scarcity, costliness, and appropriation. These resource weaknesses are unlikely to be scarce or unique to the affected firm. Although the business specifics of data assets affected by Data events may vary from firm to firm, the methods of data storage and protection are common across firms. Standardized solutions to respective resource weaknesses exist due to extensive research and practice work on information security (e.g., encryption and firewalls). As to the costliness of Data events, short-term costs are mainly attributable to the recovery effort (e.g., notifying customers of private data loss and reconstituting affected data assets). Also relevant are potential legal liability costs and regulatory penalties, but the magnitude of such costs could be uncertain and pending at the time of the event's occurrence. Long-term costs are relevant for Data events involving loss of scarce confidential data (e.g., proprietary firm data and custodial customer data). They include reputational damage, loss of customer trust, and regulatory restrictions. In this sense, these IT resource weaknesses can ultimately erode the ability of a firm to build, and to generate value (rents) from, strategic data assets.

IT resource weaknesses at the root of Function events have a greater degree of scarcity, costliness, and appropriation. The functional IT assets linked to Function events are often highly specific to the firm experiencing the events. Even if firms employ similar functional IT assets (e.g., SAP enterprise resource planning system), these assets are configured to fit firm-specific business requirements, business processes, and IT architecture. Therefore, respective IT resource weaknesses would be equally unique to an organization. This means that effective solutions to these weaknesses would also be scarce rather than readily available. As to costliness and appropriation, these are a function of the short-term and long-term costs of Function events. Short-term direct costs include losses that are substantial and highly visible, in terms of lost productivity and lost transactions (Paquette, Jaeger, & Wilson, 2010). These losses will lower the firm's profitability, as they will be evident on the firm's books and records. The recovery cost from a Function event is also substantial. For events that result in loss of availability of functional IT assets, or Availability-type Function events, reconstituting those IT assets may be relatively quick, but the processing of "lost" or delayed transactions must be done in parallel with ongoing business operations[2] similar to a parallel conversion approach from an old to a new IS (Dennis, Wixom, &

[2] Personal communication with Cathy Burrows, Director of Marketing Services, Royal Bank of Canada, and Scott Overby, VP of Decision Support, Discover Card Inc. Symantec's IT Risk Management Report from 2008 offers the following clarification (2008, p. 15): *"... when they occur, availability and performance disasters can be nightmare scenarios: transaction processing at a crawl on the busiest shopping day of the year or during a market crash, failures cascading through backup systems during a site or regional disaster, or essential services missing when they're needed most. Worse, Availability and Performance disasters are often irrecoverable over the short term."*

Tegarden, 2005). For events involving the lack of integrity of functional IT assets (e.g., faulty processing due to a software bug), or Integrity-type Function events, recovery involves additional challenges. Full detection and repair of root causes requires more highly skilled and slack IT staff, solid insight into the original system design, and rapid software maintenance and testing. Since all this is done under time and resource pressure, this could cause negative rippling effects including new sources of IT operational risk (Charette et al., 1997). Long-term costs are more significant and tie directly with IT resource weaknesses at the root of Function events. In a nutshell, these resource weaknesses are challenging to overcome and will distract a firm from the generation of rents via the strategic IT resources with which they are coupled. Specifically, these weaknesses result in severe inefficiencies and inhibit a firm's best potential performance with its current resources; such inefficiencies are an important source of a resource weakness' cost (Arend, 2004). Relative to Integrity-type Function events, relevant resource weaknesses include inadequate IT capabilities for the acquisition, development, deployment, accreditation, and maintenance of functional IT assets (ITGI, 2007b). Relative to Availability-type Function events, relevant resource weaknesses include inadequate IT capabilities for performance and capacity planning, definition of service level agreements, and configuration and infrastructure management, among other weaknesses (ITGI, 2007b). Most importantly, such IT resource weaknesses diminish a crucial source of value attributed to investment in IT – business growth opportunities associated with idiosyncratic IT resource strengths (Bharadwaj, Bharadwaj, & Konsynski, 1999).

On balance, when compared to Data events, Function events signal the presence of more severe IT resource weaknesses. To begin with, IT resource weaknesses at their root have greater scarcity and cost more to resolve. And since "higher costs of conversion and transference imply that a firm is less likely to ever rid itself of the liability [weakness]" (Arend, 2004, p. 1010), a firm is more likely to reach a semi-permanent state of resource weakness (Wernerfelt, 1984) with respect to Function-related resource weaknesses. Function events are also likely to result in higher direct, reportable costs that lower profits and weaken firm performance. Moreover, relative to long-term indirect costs, resource weaknesses at the root of Function events erode IT-based competitive advantages more severely than do Data events (akin to a move along path D in Figure 1), especially since they can constrain more severely the development of new related IT competences as part of a firm's efforts at strategic renewal (Rumelt, Schendel, & Teece, 1995) (akin to an inability to move along path E in Figure 1). In this light, investors would react more strongly to Function events than to Data events. Hence, our second hypothesis is:

> ***H2**: Firms experiencing Function events suffer greater negative abnormal changes in their market value than firms experiencing Data events.*

4. Data, Analysis, and Results

This section explains the data and methodology used to test the research hypotheses and presents the analysis results.

4.1. Data Source and Sample Selection

Our data source is a commercial operational risk events database, called Financial Institutions Risk Scenario Trends (FIRST), marketed by Algorithmics Inc. Events in the FIRST database are gathered from a variety of public sources such as regulatory filings (e.g., the Securities and Exchange Commission), court resolutions, and the media (e.g., Reuters and the Wall Street Journal).[3] These events occurred globally in a variety of industries. A significant portion of the events occurred in the financial services industry and spans 25 years from 1985 to 2009. This is attributable to this industry being subject to greater regulatory scrutiny and more stringent reporting requirements. FIRST's data have been used in several empirical studies on operational risk (e.g., Cummins et al., 2006; Rosenberg & Schuermann, 2006). We are the first to use it in the IT context.

[3] Because of the public nature of the data sources used to populate the FIRST database, it is safe to assume that information about all events in FIRST was available to investors directly from those same sources at the time the events first became public.

The majority of events in FIRST were reported by third parties rather than the firms that experienced the events. This reduces the chances that our data are contaminated by self-selection bias. However, this may also indicate some bias toward greater magnitude events, which firms have greater difficulty hiding, an issue that we will revisit later. Nevertheless, higher magnitude events are likely to be of prime concern to management.

FIRST offers a multi-item description of each operational risk event. Of importance to our study are: (1) the firm where the event occurred; (2) the event date; (3) a detailed event narrative; (4) a list of source documents for the narrative details (e.g., court filings and news articles); (5) the "event trigger" or primary cause (People, Technology, Process, and Relationship); and (6) the event mapping into Basel's risk categories (see Table 1).

Other data we use include market data on daily stock prices from the University of Chicago's CRSP database and accounting data from the Standard & Poor's Compustat database. All the variables we use are measured in U.S. dollars and adjusted for inflation to January 2010 using the Consumer Price Index. These variables are listed and defined in Table 7, Section 4.3.

Table 3 details the process we used to construct the data sample. We determined the event date, denoted as "day 0" hereafter, to be the first press-cutting date on which an event was announced to the media. We cross-checked these dates against the Dow Jones Factiva and the LexisNexis business news databases. We excluded events potentially contaminated by confounding events, such as earnings announcements, new CEO appointments, mergers and acquisitions, and major lawsuits. To ensure robustness of the results, following Kannan et al. (2007), we also excluded events that occurred in the six months after 9/11 and all events following the August 2008 financial market meltdown. The final sample contains 142 events.

Table 3. Data Sample Construction Methodology

Phase 1: Identify source database	• FIRST database containing **9,005** publicly reported operational risk events as of January, 2010.
Phase 2: Narrow events to U.S. publicly traded firms	• Excluded events from U.S. private firms and non-financial firms and events occurring in foreign firms. • Kept events that occurred in publicly traded U.S. companies – **2,508** events.

Phase 3: Identify ***initial*** data sample	• Identified events that may have occurred due to IT operational risk – **1,120** events:
	  ○ Selected events having "Technology" and "Processes" as their *Event Trigger;*
	  ○ Selected events whose *narrative* contains one or more of the following keywords: "data," "computer," "electronic," "information," "system," "technology/technical," "security," "software," "hack," "phishing," "access," "code," "password," "data," "network," "transaction," "error/erroneous," "hard drive," "outage," "volume," "internet," "interrupt," "breach," "cyber," "virus," "attack," "glitch," "steal/stole," "confidential," "process," "e-mail," "private account/information/record," and "privacy".
	• All pre-selected events were then independently checked by the three authors, who reviewed the detailed narratives provided for each event in order to identify IT operational risk events – **195** events.

Phase 4: Produce the ***final*** data sample	• Excluded **28** events involving confounding factors that occurred within a week from the event date:
	  ○ Searched for firm-specific news in the Dow Jones Factiva database and the LexisNexis database of business news articles.
	  ○ Eliminated events that occurred around the time of earnings announcements, CEO appointments, mergers and acquisitions, tender offers, and other major news releases.
	  ○ Removed IT operational risk events that occurred within the same firm and had overlapping event windows.
	• Excluded **20** events that occurred during the 6 months after 9/11 (**7** events) and after August 2008 (**13** events), when the financial meltdown began.
	• Excluded **5** events for which market data was unavailable.
	• A total of **142** events were retained.

All three authors independently classified the 142 events in the sample. Each event was classified as either a Data or a Function event. Of the 142 events, 67 are Data events and 75 are Function events. We further categorized the Function events into the Integrity and Availability subcategories: 52 compromised the integrity of functional IT assets and 23 compromised the availability of such assets. Both classifications achieved inter-rater reliability levels close to 1.0.

We further classified our events by sub-industry using U.S. Standard Industry Classification (SIC) codes. Almost 80 percent of the events occurred within firms classified as Depository Institutions (2-digit SIC code of 60) and firms classified as Security and Commodity Brokers, Dealers, Exchanges, and Services (2-digit SIC code of 62). Depository Institutions made up 44 percent of the sample (29 Data and 34 Function events), and Security and Commodity Brokers, Dealers, Exchanges, and Services made up 35 percent (18 Data and 32 Function events). The remainder of our events occurred within firms that fell into other financial sub-industries.

Our analysis of how each of the events map into Basel's categories of operational risk suggests that Function events are as prevalent as Data events. Data and Function events in our sample are similarly distributed across all seven categories (see Table 4). There are slightly more Function events in the two categories most visibly linked to IT operational risk, namely the *Business Disruption and System Failure* and the *Execution, Delivery, and Process Management* categories (27 and 21 versus 20 and 17, respectively). We note that about 40 percent of all events in our sample actually fall into the remaining five categories, with the bulk (25.4 percent) falling into the *External Fraud* category. Table 4 also parallels our earlier discussion of Table 1.

Table 4. Breakdown of IT Operational Risk Events by Basel II Event Type Category

Basel II Event Type Category	Distribution of Sample ITOR Events: Number (Proportion)		
	All Events	Data	Function
Internal Fraud	6 (4.2%)	3	3
External Fraud	36 (25.4%)	19	17
Employment Practices and Workplace Safety	3 (2.1%)	3	0
Clients, Products, and Business Practices	11 (7.7%)	5	6
Damage to Physical Assets	1 (0.7%)	0	1
Business Disruption and System Failure	47 (33.1%)	20	27
Execution, Delivery, and Process Management	38 (26.8%)	17	21
Total:	**142 (100%)**	**67**	**75**

Figure 2 illustrates the time series of the Data and Function events in our sample. It shows a generally increasing trend of the total number of events over time; the low number of events around 2001 and 2008 is partly attributable to our sample selection (see Table 3, Phase 4). Moreover, both event types are relatively evenly distributed in each year. Hence, there is no evidence that either type of event has greater prevalence over the other in any particular period or in general.

We also inspected the (measurable) loss amounts recorded in FIRST for Data and Function events, since they may inform about differences in the magnitude of events as a potential source of bias in the market reaction to different events. The data on loss amounts was available only for 59 (or 42 percent of the 142) events in our sample, and we present their descriptive statistics in Table 5. Compared to Data events, all statistics are greater for Function events, suggesting that loss magnitudes of Function events may be higher. However, the null hypothesis of the population means of losses being equal could not be rejected (p-value=0.1015), probably because of the small subsample with available loss data. In any case, we are not able to control for the event magnitude in our econometric models due to limited availability of loss data in our sample. This is not a problem, however. Consistent with our theory, from a value perspective, the point is not the size of an event as much as the fact that the event signals the presence of deeper resource weaknesses. With this said, one still cannot dismiss the possibility that loss size plays a role in Data events being more frequently disclosed to the public than Function events, and, thus, that our results may be biased in this sense.

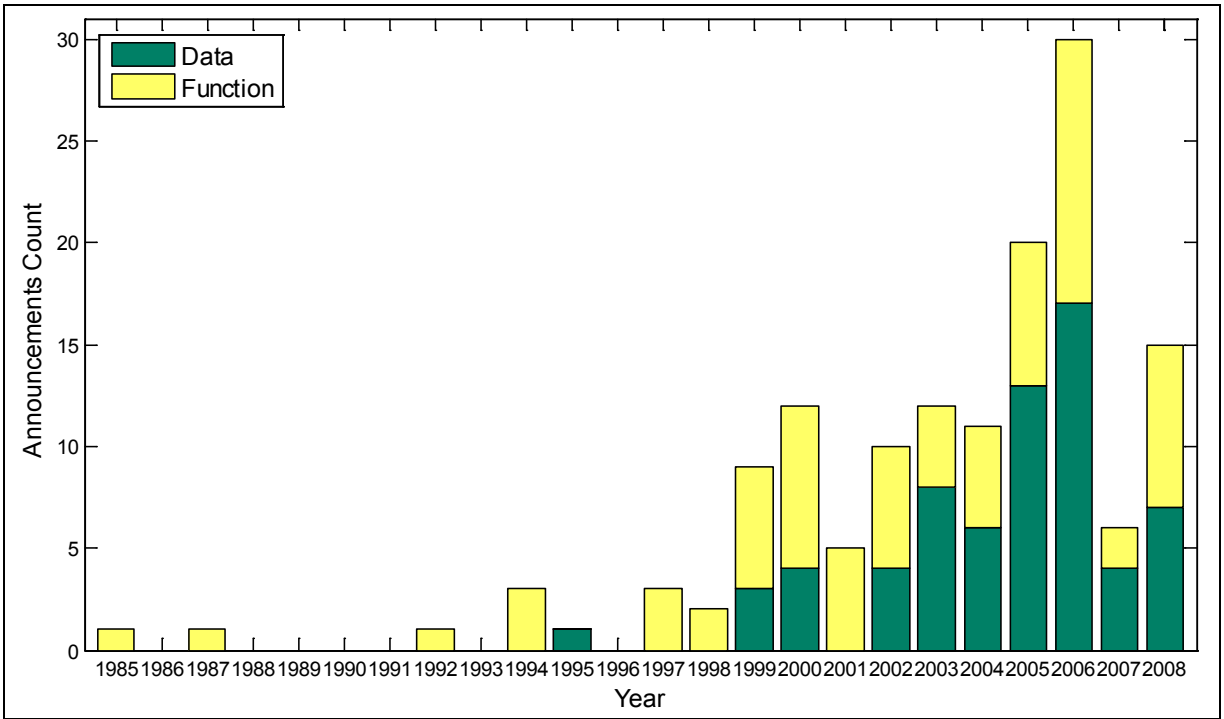

Figure 2. Time Series of Data and Function Operational Risk Events

Table 5. Loss Descriptive Statistics by Event Type

	Mean	Median	25 perc	75 perc	N	*t*-test for $\mu_D - \mu_F$: *t*-stat [*p*-value]
Data	4.56	0.62	0.05	3.08	18	-1.6645
Function	28.09	4.55	0.30	12.87	41	[0.1015]
Total:	**20.91**	**1.89**	**0.23**	**11.48**	**59**	
All dollar amounts are in USD millions.						

4.2. Event Study Analysis and Univariate Results

We use the event study methodology to test whether the market value of a firm is sensitive to IT operational risk event announcements. This methodology postulates that the market takes into account all available information in determining security prices (McWilliams & Siegel, 1997). Hence, when an unexpected event that brings new information is announced, if such event is value relevant, the market reaction to the event will be observed over an event window [T1,T2] that overlaps with the event's first press-cutting date. Where the event date is denoted day 0, following convention, we tried various event windows starting three days before day 0 (T1=3) to account fo r a possible leakage of information prior to the announcement, and extending up to three days after day 0 (T2=3) to give stock prices time to adjust to the event.

We estimate the market reaction to an event using two steps. The first step estimates normal stock returns. Expected returns for a firm *i* at date *t* are estimated through the single index market model:

$$R_{it} = a_i + b_i R_{mt} + e_{it} \qquad (1)$$

where R_{it} is firm *i*'s return on the common stock on day *t*, and R_{mt} is the return on a market index on day *t*. Following many financial studies, R_{mt} in our study is the equal-weighted return index from the CRSP

database estimated over 255 trading days prior to the announcement date, during [-301, -46]. The second step computes the daily abnormal returns (AR) during the event window for firm *i* on day *t*:

$$AR_{it} = R_{it} - (\hat{a}_i + \hat{b}_i R_{mt}) \quad (2)$$

where $\hat{a}$ and $\hat{b}$ are the OLS estimates from the market model. Abnormal returns are then accumulated for each event window to form cumulative abnormal returns (CARs).

For our study, the *a priori* expectation is that IT operational risk event announcements would generate negative abnormal returns. Hence, where CARs are averaged across all firm-events to produce the mean CARs, denoted as $\overline{CAR}_{[T_1,T_2]}$, the null hypothesis is: $\overline{CAR}_{[T_1,T_2]} \geq 0$. We test this hypothesis using a one-tail test of Patell's (1976) standardized Z-statistic (Brown & Warner, 1985).

Table 6 shows mean CARs for the event groups and univariate tests of our hypotheses. The results support H1 and H2. Based on column (1), H1 is supported. In general, the market value of firms experiencing an event drops, on average, by 0.26 percent on day 0, and it continues to drop up to day 2. Moreover, the mean CARs range between -0.52 percent and -0.82 percent, depending on the event window, and most are statistically significant at the 1 percent to 5 percent level. The remaining columns lend strong support for H2. In column (3), mean CARs for Function events are substantially negative and statistically significant near or below the 1 percent level for all event windows; the maximum mean CAR is -1.48 percent for event window [-1, 2]. By contrast, mean CARs for Data events are smaller and not significant for all event windows. Based on column (6), the univariate test of the difference between the mean CARs for Function and Data events formally confirms H2. Compared to Data events, mean CARs for Function events are up to an additional 1.54 percent lower. These results are statistically significant at the 5 percent level. Thus, Function events have a more adverse market reaction than Data events. Finally, columns (4)-(5) and (7)-(8) show the comparable results for the Integrity and Availability types of Function events. Based on columns (4) and (5), each subcategory on its own shows similar results to those for all Function events, except that the mean ARs and CARs are notably smaller for Availability-type events. As such, column (7) shows that mean CARs for Data events are not significantly different than for Integrity-type Function events, for the most part, whereas column (8) shows them to be significantly higher than for Availability-type Function events.

4.3. Multivariate Hypothesis Testing

We estimate regression models that further test H2 and help explain some of the variation in the market reaction to IT operational risk events. The variables are described in Table 7. The dependent variable is CAR[-1,2] because the [-1,2] event window has the largest negative mean CARs for most event groups (Table 6). The independent variables are dummy variables denoting the type of event.

We also included four control variables in the model. First is firm size (measured by the natural logarithm of total liabilities). It has been found to influence the market reaction to IT operational risk events in other studies (Acquisti et al., 2006; Cavusoglu et al., 2004; Kannan et al., 2007). Second is firm growth (measured by the Tobin's *q* ratio). Studies have shown that high growth firms are more negatively affected by operational risk events than those with fewer growth opportunities, "consistent with the view that such firms may have to forego attractive projects following an operational loss event" (Cummins et al., 2006, p. 2,631). The last two control variables account for possible industry effects. Earlier studies (Acquisti et al., 2006; Leung & Bose, 2008) have noted that industry differences can affect the market reaction to certain IT operational risk events. We add two dummy variables to control for the firms with a 2-digit SIC code of 60 (depository institutions) and 62 (security and commodity brokers, dealers, exchanges, and services) that constitute the majority of our sample. Table 7 summarizes the definitions and constructions of the variables used in this study.

Table 6. Mean ARs and CARs for IT Operational Risk Event Groups

	(1)		(2)		(3)		(4)		(5)		(6)	(7)	(8)
	Hypothesis: H1		Hypothesis: H2										
	All ITORs (N=142)		Data (D) (N=67)		Function (F) (N=75)		Integrity (I) (N=52)		Availability (A) (N=23)		($\mu_F - \mu_D$)	($\mu_I - \mu_D$)	($\mu_A - \mu_D$)
Day / Event Window	Mean CAR (%) (*z*-statistic) [*p*-value]	% (<0)	Mean CAR (%) (*z*-statistic) [*p*-value]	% (<0)	Mean CAR (%) (*z*-statistic) [*p*-value]	% (<0)	Mean CAR (%) (*z*-statistic) [*p*-value]	% (<0)	Mean CAR (%) (*z*-statistic) [*p*-value]	% (<0)	Mean CAR diff. (*t*-statistic) [*p*-value]	Mean CAR diff. (*t*-statistic) [*p*-value]	Mean CAR diff. (*t*-statistic) [*p*-value]
-3	0.14 (1.460) [0.928]	49	0.04 (0.370) [0.644]	51	0.23 (1.660) [0.952]	47	-0.11 (0.521) [0.699]	48	1.01 (2.214) [0.987]	43	0.19 (0.482) [0.685]	-0.15 (-0.343) [0.366]	0.97 (1.720) [0.956]
-2	0.11 (1.557) [0.940]	49	0.25 (1.865) [0.969]	49	-0.02 (0.379) [0.648]	49	0.06 (0.087) [0.535]	46	-0.20 (0.554) [0.710]	57	-0.27 (-0.738) [0.231]	-0.19 (-0.488) [0.313]	-0.45 (-0.815) [0.209]
-1	0.07 (0.076) [0.530]	54	0.26 (0.507) [0.694]	49	-0.11 (-0.375) [0.354]	57	-0.17 (-0.663) [0.254]	62	0.02 (0.320) [0.626]	48	-0.37 (-1.040) [0.150]	-0.43 (-1.218) [0.113]	-0.24 (-0.418) [0.339]
0	**-0.26 (-1.366) [0.086]***	**53**	**0.12 (0.126) [0.550]**	**48**	**-0.61 (-2.000) [0.023]****	**57**	**-0.32 (-1.467) [0.071]***	**58**	**-1.25 (-1.406) [0.080]***	**57**	**-0.73 (-1.991) [0.024]****	**-0.44 (-1.159) [0.124]**	**-1.37 (-2.940) [0.002]*****
1	-0.32 (-1.969) [0.025]**	55	-0.17 (-0.514) [0.304]	54	-0.46 (-2.223) [0.013]**	56	-0.48 (-1.728) [0.042]**	52	-0.42 (-1.417) [0.078]*	65	-0.29 (-0.674) [0.251]	-0.31 (-0.637) [0.263]	-0.25 (-0.619) [0.269]
2	-0.24 (-1.066) [0.143]	57	-0.15 (-0.488) [0.313]	52	-0.31 (-1.005) [0.157]	61	-0.10 (-0.720) [0.236]	60	-0.79 (-0.733) [0.232]	65	-0.16 (-0.426) [0.336]	0.05 (0.166) [0.566]	-0.64 (-1.235) [0.110]
3	0.13 (0.668) [0.748]	46	0.12 (-0.231) [0.409]	51	0.13 (1.137) [0.872]	43	0.29 (1.881) [0.970]	38	-0.22 (-0.775) [0.219]	52	0.01 (-0.042) [0.517]	0.17 (0.467) [0.679]	-0.34 (-0.843) [0.201]
[-1, 1]	-0.52 (-1.882) [0.030]**	56	0.21 (0.069) [0.528]	49	-1.18 (-2.655) [0.004]***	61	-0.97 (-2.227) [0.013]**	60	-1.65 (-1.445) [0.074]*	65	-1.39 (-2.227) [0.014]**	-1.18 (-1.761) [0.040]**	-1.86 (-2.585) [0.006]***
[-1, 2]	**-0.75 (-2.163) [0.015]****	**53**	**0.06 (-0.184) [0.427]**	**45**	**-1.48 (-2.802) [0.003]*****	**60**	**-1.06 (-2.289) [0.011]****	**58**	**-2.43 (-1.618) [0.053]***	**65**	**-1.54 (-1.999) [0.024]****	**-1.12 (-1.448) [0.075]***	**-2.49 (-2.506) [0.007]*****
[-1, 3]	-0.63 (-1.636) [0.051]*	49	0.18 (-0.268) [0.394]	42	-1.35 (-1.998) [0.023]**	55	-0.78 (-1.206) [0.114]	54	-2.65 (-1.794) [0.036]**	57	-1.53 (-1.760) [0.040]**	-0.96 (-1.041) [0.150]	-2.83 (-2.507) [0.007]***
[0, 1]	-0.58 (-2.358) [0.009]***	57	-0.05 (-0.274) [0.392]	52	-1.07 (-2.986) [0.001]***	61	-0.80 (-2.259) [0.012]**	58	-1.66 (-1.996) [0.023]**	70	-1.02 (-1.767) [0.040]**	-0.75 (-1.168) [0.123]	-1.61 (-2.830) [0.003]***
[0, 2]	-0.82 (-2.541) [0.006]***	55	-0.20 (-0.506) [0.307]	52	-1.37 (-3.019) [0.001]***	57	-0.90 (-2.260) [0.012]**	56	-2.45 (-2.053) [0.020]**	61	-1.17 (-1.703) [0.045]**	-0.70 (-0.947) [0.173]	-2.25 (-2.874) [0.003]***
[0, 3]	-0.69 (-1.867) [0.031]**	50	-0.08 (-0.554) [0.290]	49	-1.24 (-2.046) [0.020]**	51	-0.61 (-1.017) [0.155]	48	-2.67 (-2.165) [0.015]**	57	-1.16 (-1.496) [0.069]*	-0.53 (-0.623) [0.267]	-2.59 (-2.782) [0.003]***

CARs are market model-adjusted abnormal returns (measured in percentages), defined from an industry market model estimated over 255 trading days prior to day 0, during [-301, -46]. The industry index is constructed from a portfolio of equal-weighted equity returns. Columns labeled "% (<0)" indicate the proportion of events with a negative mean AR or CAR. Patell's*z*-test statistics in columns (1)-(5) are in round brackets. *p*-values(in square brackets) are based on a left-tailed test. ***, **, and * denote significance at 1%, 5%, and 10% levels, respectively.

Table 7. Model Variables and their Definitions

	Variable Name	Definition and Calculation	Source
Dependent Variable	*CAR[-1,2]*	Cumulative abnormal return over the [-1, 2] event window, measured in percentages	Event study model; market data from CRSP
Independent Variables	*D_Function*	Dummy variable equal to one if an event is of Function type	Event description
	D_Integrity	Dummy variable equal to one if an event is of Integrity type	Event description
	D_Availability	Dummy variable equal to one if an event is of Availability type	Event description
Control Variables	*FirmSize*	Ln(total liabilities), where total liabilities are measured in USD billions; firm size was found to influence the reaction to IT operational risk events (Acquisti et al., 2006; Cavusoglu et al., 2004; Kannan et al., 2007).	Compustat
	FirmGrowth	Tobin's *q* ratio: (market value of equity plus book value of debt)/ (total assets), both measured in decimal; growth firms may suffer greater losses, as has been seen for general operational risk events (Cummins et al. 2006).	Compustat
	D_SIC60, D_SIC62	Dummy variable equal to one if the 2-digit SIC code is 60 or 62, respectively; the effect of industry differences have been observed by two studies (Acquisti et al., 2006; Leung and Bose, 2008).	Compustat

All dollar values are adjusted for inflation to January 2010 using the Consumer Price Index. Data for the index was obtained from the Federal Reserve Bank of St. Louis' FRED database.

The Pearson pair-wise correlation matrix is shown in Table 8. CAR[-1,2] is strongly and negatively correlated with FirmGrowth. A high correlation also exists between FirmSize and FirmGrowth, as high growth firms tend to be smaller (Cabral 1995; Lang, Ofek, & Stultz, 1996). Further, these two variables are functionally related; the measure of FirmSize, total liabilities, is highly correlated with one of the inputs to the measure of FirmGrowth, total assets, since financial services firms typically have high leverage ratios (e.g., Mansfield, 1962). Finally, high correlations also exist, by definition, between dummy variables.

Table 8. Pearson Correlation Matrix

	CAR [-1,2]	D_Function	D_Integrity	D_Availability	FirmSize	FirmGrowth	D_SIC60	D_SIC62
CAR[-1,2]	1							
D_Function	-0.1666 [0.048]**	1						
D_Integrity	-0.0507 [0.549]	**0.7184** **[0.000]***	1					
D_Availability	-0.1594 [0.058]*	**0.4155** **[0.000]***	**-0.3342** **[0.000]***	1				
FirmSize	0.0941 [0.266]	0.0789 [0.351]	0.1294 [0.125]	-0.0623 [0.461]	1			
FirmGrowth	**-0.3962** **[0.000]***	0.0298 [0.725]	-0.0230 [0.786]	0.0704 [0.405]	**-0.5505** **[0.000]***	1		
D_SIC60	0.0458 [0.588]	0.0206 [0.808]	-0.0609 [0.471]	0.1076 [0.203]	0.2235 [0.008]***	-0.2605 [0.002]***	1	
D_SIC62	-0.0510 [0.547]	0.1386 [0.100]*	0.0749 [0.376]	0.0899 [0.287]	-0.2010 [0.017]**	0.0934 [0.269]	**-0.6381** **[0.000]***	1

Pair-wise correlation coefficient estimates and *p*-values for model variables. Superscripts ***, **, and * denote significance at 1%, 5%, and 10% levels, respectively.

We use three regression model specifications. Model 0 contains only control variables. Model 1 adds a dichotomous variable D_Function to capture the difference in market reaction to Function events and Data events. Model 2 replaces D_Function with D_Integrity and D_Availability, to capture the difference in market reaction to the two subcategories of Function events compared to Data events. We estimate the three models using a cross-section ordinary least squares (OLS) regression. The distribution of the dependent variable shows no significant deviations from the normality assumption, and the Chow test (Chow, 1960) of the coefficients of the control variables being different across the Function and Data subsamples is negative. Hence, a pooled regression is well justified.

We present the regression results in Table 9. A negative coefficient associated with an explanatory variable means a greater negative market reaction for higher values of that variable. Model 1 supports H2, confirming our earlier univariate test results. The coefficient of D_Function is negative and statistically significant (p=0.0278), indicating that the market value of firms experiencing a Function event drops, on average, an additional 1.1577 percent compared to a Data event. Model 2 similarly shows the coefficients of both D_Integrity and D_Availability to be negative, with the former having a weak statistical significance level (p=0.0979) and the latter a strong statistical significant level (p=0.0386). Compared to Data events, the market value of firms experiencing an Integrity-type or Availability-type Function event drops, on average, an additional 0.8596 percent and 1.8906 percent, respectively. In all three models, the variance inflation factors (VIF) for our variables ranged from 1.05 to 1.83, well below the VIF value of 10 commonly used as a minimum threshold for multicollinearity to be a concern.

Table 9. Determinants of CARs – Regression Results

	Predicted Sign	Model 0	Model 1	Model 2
		Coefficient (*t-statistic*)	Coefficient (*t-statistic*)	Coefficient (*t-statistic*)
D_Function	(–)		-1.1577 (-1.93)**	
D_Integrity	(–)			-0.8596 (-1.30)*
D_Availability	(–)			-1.8906 (-1.78)**
Control Variables:				
FirmSize	(+)	-0.4194 (-2.86)***	-0.3708 (-2.69)***	-0.3852 (-2.74)***
FirmGrowth	(–)	-3.8247 (-3.56)***	-3.6844 (-3.56)***	-3.6470 (-3.48)***
D_SIC60	(+/–)	-1.1546 (-1.67)**	-0.9131 (-1.42)*	-0.7296 (-1.15)
D_SIC62	(+/–)	-1.1686 (-1.01)	-0.8118 (-0.73)	-0.6777 (-0.65)
Intercept		7.0617 (3.65)***	7.0264 (3.83)***	6.9340 (3.68)***
Number of Observations		142	142	142
F-statistic [*p*-value]		4.88 [0.0020]***	5.22 [0.0006]***	3.86 [0.0029]***
R^2		0.1893	0.2039	0.2092
ΔR^2		n/a	+0.0146	+0.0199

The *t*-statistics (in round brackets) are based on heteroskedasticity-robust standard errors, clustered by firm. Superscripts ***, **, and * denote significance at 1%, 5%, and 10% levels, respectively. Significance levels are based on a one-tailed test, depending on the sign. ΔR^2 is defined as $R^2 - R^2_0$, where the subscript "0" refers to Model 0.

A comparison of Models 0, 1, and 2 suggests that the control variables explain more of the variation in the market reaction to IT operational risk events than the independent variables. The regression coefficients for FirmSize and FirmGrowth are negative and statistically significant at the 1 percent level in all three models. However, the high R-squared of 0.1893 in Model 0 is largely attributable to the FirmGrowth variable. (In fact, if FirmGrowth is removed from Model 0, the R-squared reduces to merely 0.0100.) The coefficient of FirmGrowth indicates that the market reaction is more punitive to higher growth firms. Likewise, the market reacts more negatively to events in larger firms,

suggesting that after accounting for growth and industry, the market is more surprised to see an IT operational risk event in firms with more well-established and diverse business operations. Finally, of the industry dummies, only the first one (2-digit SIC code of 60) is mildly significant, indicating that the market reaction is slightly more pronounced for depository institutions than for other financial firms, likely because the market is more surprised to see events in more regulated firms.

5. Discussion and Future Research

This section discusses our main results and contributions, limitations of our study, and the implications for research and practice. It also outlines directions for future research.

5.1. Contributions and Main Findings

This paper is the first to present the framework of resource weaknesses as a theoretical lens for conceptualizing IT operational risk and examining its impact on firm performance. This framework supplements another theory that has been used extensively in IT research, the RBV of the firm. More importantly, our empirical results indicate that the predictions of this theoretical framework correspond well with reality.

Some of our empirical findings are the first of their kind and offer novel insights into the wealth effect of IT operational risk. Specifically, in examining the impact of IT operational risk events on public U.S. financial services firms, we find that firms experiencing these events suffer a (statistically) significant negative drop in their market value when such events are first announced. This result is consistent with earlier studies on operational risk, in general (Perry & de Fontnouvelle, 2005; Cummins et al., 2006; Gillet, Hübner, & Plunus, 2010). The more important insights, however, pertain to the impact of the Data and Function subtypes of IT operational risk. We find that firms experiencing Function events suffer, on average, a 1.48 percent drop in their market value, compared with a 0.75 percent drop for IT operational risk events, in general. Moreover, only Function events have a (statistically) significant wealth effect, and this wealth effect is substantially more negative than that of Data events. On average, Function events result in an additional market value drop of 1.157 percent compared with Data events. Of the Function events, those that specifically impair the availability rather than integrity of functional IT assets result in an additional drop in value of 1.89 percent compared with Data events. These results provide ample motivation for researchers and practitioners to revisit and test any existing perceptions that Function-related IT operational risk is any less detrimental than Data-related risk.

For the most part, our results contrast with those of past studies (see Table 2). Contrary to our results, past studies either observed no significant market reaction to Function events (Campbell et al., 2003) or observed a market reaction only under narrow circumstances (Hovav & D'Arcy, 2003; Kannan et al., 2007). Likewise, contrary to our result, the majority of past studies found varying degrees of market reaction to Data events (Campbell et al., 2003; Cavusoglu et al., 2004; Acquisti et al., 2006; Leung & Bose, 2008). A key reason for this divergence in results may be that our data sample also contains types of Data and Function events not considered in past studies, namely, events that are accidental in nature and originate within the firm. Additionally, our sample is restricted to events in the financial services industry, while other studies pooled events from a wide range of industries. Future research that accounts for these differences may help reconcile our resulting differences with past studies.

Our results also show some firm-specific characteristics to be more important predictors of the degree of negative wealth effect of IT operational risk events than the types of events themselves. The negative market reaction tends to be the greatest for high growth firms. Moreover, for any two firms with identical growth potential, and holding all else constant, the larger firm is expected to experience a more negative wealth effect. Last, having focused on the financial services industry, we find the negative wealth effect to be slightly stronger for depository institutions than for other institution types.

5.2. Limitations

All this said, we recognize that our study is subject to limitations. To begin with, our results may be limited to public U.S. financial services firms. Although the financial services industry is sufficiently large in its own right for our results to be of value to a wide audience, generalizing our results is important. It is necessary to analyze IT operational risk data that are much broader in nature while controlling for industry- and country-specific factors such as the regulatory and macroeconomic environment. In any event, it is important to keep in mind two things. First, our findings about Data events are likely to extend to other prominent industries facing equally strong regulatory restrictions on data security (e.g., the medical industry and patient privacy under HIPPA). Second, the financial services industry is a good representative of IT-intensive industries, and so, Function events may be equally detrimental in those other industries.

Another potential limitation is that the two categories of IT operational risk events we analyzed are broad. This choice was motivated by a desire to shed light on the category of events least studied to date. Future research should also examine more granular event subcategories. In particular, since past research has concentrated on Data events that are malicious in nature and arise from external sources (see Table 2), future research ought to be sensitive to the intent of events (malicious vs. accidental) and to their source (internal vs. external). Understanding differences between more granular subtypes of IT operational risk events could help firms better manage their efforts to identify, assess, and manage different subtypes of this risk. Another useful distinction could be the firm's IT sourcing mode. For example, vendor-supplied software is one of the most common reasons for trading system outages in financial institutions (Chorafas, 2004). Examination of this aspect alone may have important implications for IT outsourcing decisions, on how vendors are selected, and on contracting practices.

Third, as we indicated earlier (in Section 4.1), we could not control for the size or magnitude of events in our data sample. Not only is it possible that our results are sensitive to the size of events, but another potential consequence is that our results may be biased toward larger Function events. Since there are laws that mandate disclosure of Data breaches but no laws that mandate disclosure of Function events, it could be that only higher-magnitude Function events make their way to the public eye. If so, the occurrence of Function events and the significance of their ensuing impact may be more surprising to investors. Hence, a potential bias could exist between the two risk types concerning the impact of publicly disclosed IT operational risk events. However, even if this bias does indeed exist, it does not change our conclusion that Function events, on average, result in a greater negative wealth effect. Rather, it may mean that Function events are more damaging not because they are the result of intrinsically stronger IT resource weaknesses but rather because they are likely to be brought to light only when they are sufficiently significant. Regardless, the overall message of this research remains valid: Function-related IT operational risk should receive more attention from both research and practice than it has in the past.

5.3. Implications for Research and Practice

Our findings have implications for IT practice and research. For practice, the implications are straightforward – IT operational risk is a major hazard that cannot be ignored. Firms must make the necessary efforts to understand, identify, and manage this risk. Firms must also examine their exposure to specific subtypes of this risk and determine which subtypes deserve more attention. And, perhaps most importantly, the average firm ought to view Function-related risk at least as seriously as Data-related risk.

More broadly, firms must examine IT operational risk and its implications from a resource weakness perspective. Despite their high cost, the generation of IT resource weaknesses is often overlooked by firms in the pursuit of strategic advantage. As IT resource weaknesses arise over time in conjunction with IT resource strengths, they may not be evident (West & DeCastro, 2001). If a firm has difficulty detecting its IT resource weaknesses, these weaknesses will eventually manifest as IT operational risk events, which inform the world of the presence of the weaknesses and the firm's inability to properly manage them.

One broad implication for research stems from the fact that our paper and its results highlight how little we know about IT operational risk. A crucial need exists to develop approaches and methods for understanding

and managing different types of this risk. These approaches and methods must incorporate IT operational risk considerations into areas fertile for future research. We summarize below three main areas.

First and foremost, the resource weaknesses theoretical lens that we have presented is the first attempt (known to us) that seeks to close a serious theoretical gap in the literature. This theory supplements the resource-based theory of the firm, which has been used extensively in IT research. As such, it may offer another powerful way to theorize about IT resources and their associated operational risk. Nevertheless, it remains to be seen if this theory is sufficiently developed to enable the investigation of aspects of IT operational risk not considered in this study, such as the intent of risk events (malicious vs. accidental) and their initiation source (external vs. internal).

Moreover, this theory offers broader propositions that deserve an examination and empirical evaluation in the IT context. For example, the theory recognizes that investments for building resource strengths and dismantling resource weaknesses are ultimately undertaken in order to improve the competitiveness of a firm, but an open question remains about which of these investments is more effective (West & DeCastro, 2001). Likewise, on the premise that "efforts to reduce stocks of resource weaknesses will take more time and greater investment than will efforts made to build stocks of resource strengths," and because the effectiveness of investments made to reduce stocks of resource weaknesses may be more difficult to assess, the theory postulates that firms often prefer taking the route of building and maintaining competitive advantage through investments in multiple resource strengths (West & DeCastro, 2001, p. 434). If this assertion is accurate, the consequences of IT operational risk should be clear. "By concentrating only on the development of strengths, firms could actually lay a foundation for losing advantage due to inattention to emerging weaknesses and inadequacies" (West & DeCastro, 2001, p. 419). Put another way, by acting in this manner, firms divert management attention and discretionary investments away from dismantling IT resource weaknesses, resulting in a diminished strategic position. All this leads to a fundamental IT management question: Is there an optimal balance between investment in creating stocks of IT resource strengths and investment in reducing stocks of IT resource weaknesses? Any attempt to address such a question would go to the heart of the problem of managing IT operational risk.

A related and more practical area is IT system development and maintenance. System design decisions that are better informed about the impact of IT operational risk can reduce exposure to this risk.[4] For example, better system design can simplify and improve IT system maintenance, which itself is a source of IT operational risk (Charette et al., 1997; Chorafas, 2004). Another key issue is the design of IT controls, which can be built into the technology itself or into the IT-supported business work environment (Juergens, Maberry, Ringle, & Fisher, 2006). For Function-related risk, examples include IT controls for business continuity, disaster recovery, and prevention of user input errors. For Data-related risk, examples include IT controls for handling and disseminating data, segregating duties, and manually reconciling system output. A third issue is how investments in IS development and IS maintenance are evaluated and budgeted for. In particular, it may be necessary to take into account how such IT investments are expected to affect the organization's overall operational risk exposure. A primary challenge is to measure this exposure from a long-term perspective and balance it against short-term IT investment goals and constraints.

Another related area that lies at the intersection of both earlier areas is the examination of IT resource weaknesses in terms of the root causes of IT operational risk events. Detailed narrative descriptions of IT operational risk events may reveal the risk factors associated with different subtypes of these events (Keil, Cule, Lyytinen, & Schmidt, 1998). These risk factors can then be tested against the severity of events and their subtypes. The results may highlight specific factors that contribute most crucially to the

[4] Chorafas (2004, pp. 95-96) offers a highly illustrative example: *"In classical 'electronic data processing' (EDP), the same information element is entered up to seven times. The average number of re-entries used to be 3.5. Now the average is 2.8. This is still too high, let alone the error in transcription which comes into the IT system through multiple entries made in incompatible formats and addressing heterogeneous files […]. No wonder that data entry costs and subsequent clearance of embedded errors have been consuming 20-25% of the IT budget in many companies. The best policy is one entry, many uses, but its implementation demands a deal of organization and self-discipline. Both are lacking from the majority of IT operations in the banking industry, with the result that operational risks are ballooning."*

presence of IT resource weaknesses and exposure to IT operational risk. This may also bring us closer to the ability to balance trade-offs between long-term exposure to IT operational risk and short-term IT investment goals and constraints.

The strong relevance of these research venues to the effective management and use of IT resources highlights the need to expand the relatively limited extant research on IT operational risk. We are confident that the theoretical basis we have presented and our findings on the economic significance of some types of IT operational risk will motivate researchers to follow up on our present work and pursue these research venues.

6. Conclusion

As IT systems are increasingly embedded in the business process environments that they support, failures of these systems can lead to significant consequences for organizations. Despite this, there are significant gaps in the research concerning IT operational risk. To explore these gaps, we define two broad categories of IT operational risk for the purposes of this paper, which are based on the types of assets comprising IT systems. *Data-related IT operational risk* is any threat to the confidentiality of data assets that can result in the disclosure, misuse, or destruction of these assets. *Function-related IT operational risk* is any threat to the availability or to the integrity of functional IT assets (that may eventually affect data assets). Extant research has primarily focused on Data events, while little analysis exists concerning Function events. Additionally, we apply the organizational liability framework, which is an extension of the resource-based value theory, to the concept of IT operational risk.

We examine the economic impact of these two categories and of IT operational risk, in general, by using the event study methodology. The data we use consists of a balanced mixture of publicly reported operational risk events in the two categories of interest. Our results show that IT operational risk events are value relevant in the sense that they impose a strong negative impact on the market values of organizations that experience such events. More importantly, these results are largely driven by Function events, as Data events do not result in a significant effect on firms' market value. We control our analysis for certain firm characteristics and find that some are important predictors of the market reaction to IT operational risk events. Our findings indicate that IT operational risk and, especially, Function-related risk are areas of IT risk that warrant close attention from researchers and practitioners. They may also indicate the need for research and practice to, perhaps, guard against the over-emphasis of Data-related risk at the expense of Function-related risk.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *Proceedings of the Twenty-Seventh International Conference on Information Systems (ICIS 2006)*. Milwaukee, USA.

Alter, S. (1999). A general, yet useful theory of information systems. *Communications of the Association for Information Systems, 1*(3), 1-69.

Aral, S., & Weill, P. (2007). IT assets, organizational capabilities & firm performance: How resource allocations and organizational differences explain performance variation. *Organization Science, 18*(5), 763-780.

Arend, R. J. (2003). Revisiting the logical and research considerations of competitive advantage. *Strategic Management Journal, 24*(3), 279-284.

Arend, R. J. (2004). The definition of strategic liabilities, and their impact on performance. *Journal of Management Studies, 41*(6), 1003-1027.

Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management, 17*(1), 99-120.

Basel Committee on Banking Supervision (BCBS) (2001). *Working paper on the regulatory treatment of operational risk*. Bank for International Settlements. Retrieved from: www.bis.org.

Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys, 25*(4), 375-414.

Berger, A. N. (2003). The economic effects of technological progress: Evidence from the banking industry. *Journal of Money, Credit and Banking, 35*(2), 141-176.

Bharadwaj, A. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly 24*(1), 169-196.

Bharadwaj, A., Keil, M., & Mahring, M. (2009). Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems, 18*(2), 66-79.

Bharadwaj, A. S., Bharadwaj, S. G., & Konsynski, B. R. (1999). Information technology effects on firm performance as measured by Tobin's Q. *Management Science, 45*(6), 1008-1024.

Brown, A. B., & Patterson, D. A. (2001). To err is human. *Proceedings of the First Workshop on Evaluating and Architecting System Dependability (EASY '01)*. Göteborg, Sweden.

Brown, S., & Warner, J. (1985). Using daily stock returns: The case of event studies. *Journal of Financial Economics, 14*(1), 3-31.

Cabral, L. (1995). Sunk costs, firm size and firm growth. *Journal of Industrial Economics, 43*(2), 161-172.

Campbell, K., Gordon, L., Loeb, M., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.

Carr, N. G. (2003). IT doesn't matter. *Harvard Business Review, 81*(5), 5-12.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104.

Charette, R. N., Adams, K. M., & White, M. B. (1997). Managing risk in software maintenance. *IEEE Software, 14*(3), 43-50.

Chorafas, D. N. (2004). *Operational risk control with Basel II: Basic principles and capital requirements*. Oxford, UK: Butterworth-Heinemann Publishing.

Chow, G. C. (1960). Tests of equality between sets of coefficients in two linear regressions. *Econometrica, 28*(3), 591-605.

Clemons, E. K. (1991). Evaluating strategic investments in information systems. *Communications of the ACM, 34*(1), 22-36.

Croy, M., & Laux, D. J. (2008). *Are we willing to take that risk? 10 questions every executive should ask about business continuity*. Bloomington, IN: iUniverse.

Cummins, J. D., Lewis, C. M., & Wei, R. (2006). The market value impact of operational loss events for U.S. banks and insurers. *Journal of Banking and Finance, 30*(10), 2605-2634.

Dennis, A., Wixom, B., & Tegarden, D. (2005). *Systems analysis and design with UML*. Hoboken, NJ: John Wiley & Sons, Inc.

Gillet, R. L., Hübner, G., & Plunus, S. (2010). Operational risk and reputation in the financial industry. *Journal of Banking and Finance, 34*(1), 224-235.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review, 6*(2), 97-121.

IT Governance Institute (ITGI) (2007a). *IT control objectives for Basel II: The importance of governance and risk management for compliance*. Rolling Meadows, IL: ISACA. Retrieved from: http://www.isaca.org.

IT Governance Institute (ITGI) (2007b). *COBIT 4.1 framework*. Rolling Meadows, IL: ISACA. Retrieved from: http://www.isaca.org.

Juergens, M., Maberry, D., Ringle, E., & Fisher, J., (2006). *Global technology audit guide: Management of IT auditing*. Altamonte Springs, FL: The Institute of Internal Auditors.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69-91.

Keil, M., Cule, P. E., Lyytinen, K., & Schmidt, R. C. (1998). A framework for identifying software project risks. *Communications of the ACM, 41*(11): 76–83.

Ko, M., & Dorantes. C. (2006). The impact of information security breaches on financial performance of the breached firms: An empirical investigation. *Journal of Information Technology Management, 17*(2), 13-22.

Lang, L., Ofek, E., & Stulz, R. M. (1996). Leverage, investment, and firm growth. *Journal of Financial Economics, 40*(1), 3-29.

Leung, A., & Bose, I. (2008). Indirect financial loss of phishing to global market. *Proceedings of the Twenty-Ninth International Conference on Information Systems (ICIS 2008)*. Paris, France.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

Longo, E. C. (2009). The knowledge management role in mitigating operational risk. *Proceedings of the European Conference on Intellectual Capital*, Inholland University of Applied Sciences, Haarlem, The Netherlands.

Lyytinen, B. P. , & Hirschheim, R. (1987). Information systems failures – A survey and classification of the empirical literature. In P. I. Zorkoczy (Ed.), *Oxford surveys in information technology* (pp. 257-309). Oxford, UK: Oxford University Press.

Mansfield, E. (1962). Entry, Gibrat's Law, innovation, and the growth of firms. *American Economic Review, 52*(5), 1023-1051.

Markus, M. L. (2000). Toward an integrative theory of IT-related risk control. In R. Baskerville, J. Stage, & J. DeGross (Eds.), *Organizational and Social Perspectives on Information Technology* (pp. 167-178). Boston, MA: Kluywer Academic Publishers.

Markus, M. L., & Keil, M. (1994). If we build it they will come: Designing information systems that users want to use. *Sloan Management Review, 35*(4), 11-25.

McWilliams, A., & Siegel, D. (1997). Event studies in management research: Theoretical and empirical issues. *The Academy of Management Journal, 40*(3), 626-657.

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly, 28*(2), 283-322.

Patell, J. (1976). Corporate forecasts of earnings per share and stock price behavior: Empirical tests. *Journal of Accounting Research, 14*(2), 246-274.

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010), Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly, 27*(3), 245-253.

Perry, J., & de Fontnouvelle, P. (2005). Measuring reputational risk: The market reaction to operational loss announcements. Working Paper, Federal Reserve Bank of Boston, Boston, MA.

Powell, T.C. (2001). Competitive advantage: logical and philosophical considerations. *Strategic Management Journal, 22*(9), 875-888.

Powell, T.C., & Arregle, J. L. (2007). Firm performance and the axis of errors. *Journal of Management Research, 7*(2), 59-77.

Ravinchandran, T., & Lertwongsatien, C. (2005). Effect of information systems resources and capabilities on firm performance: A resource-based perspective. *Journal of Management Information Systems, 21*(4), 237-276.

Ray, G., Muhanna, W. A., & Barney, J. B. (2005). Information technology and the performance of the customer service process. *MIS Quarterly, 29*(4), 625-652.

Rosenberg, J. V., & Schuermann, T. (2006). A general approach to integrated risk management with skewed, fat-tailed risks. *Journal of Financial Economics, 79*(3), 569-614.

Rumelt, R. P., Schendel, D. E., & Teece, D. J. (1995). Fundamental issues in strategy. In R. P. Rumelt, D. E. Schendel, & D. J. Teece (Eds.), *Fundamental issues in strategy: A research agenda* (pp. 1-54). Boston, MA: Harvard Business School Press.

Ryan, S., & Bordoloi, B. (1997). Evaluating security threats in mainframe and client/server environments. *Information & Management, 32*(3), 137-146.

Sherer, S. A., Alter, S. (2004). Information system risk and risk factors: Are they mostly about information systems? *Communications of the Association for Information Systems 14*(2), 29-64.

Smith, M. (1989). Computer security – Threats, vulnerabilities, and countermeasures. *Information Age, 11*(4), 205-210.

Straub, D. W., & Welke, R. J. (1998), Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Symantec (2008). *IT risk management report 2: Myths and realities*. Sunnyvale, CA: Symantec Corporation. Retrieved from: www.symantec.com.

Triplett, J.E., & Bosworth, B. P. (2002), Baumol's disease has been cured: IT and multifactor productivity in U.S. services industries. Working Paper, The Brookings Institution, Washington, DC.

Wade, M., & Hulland, J. (2004). Review: The resource-based view and information systems research: Review, extension, and suggestions for future research. *MIS Quarterly 28*(1),107-142.

Weill, P., & Broadbent, M. (1998). *Leveraging the new infrastructure: How market leaders capitalize on information technology*. Boston, MA: Harvard Business School Press.

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal, 5*(2), 171-180.

West, G. P., & DeCastro, J. (2001). The Achilles heel of firm strategy: Resource weaknesses and distinctive inadequacies. *The Journal of Management Studies, 38*(3), 417-442.

Whitman, M. E. (2004). In defense of the realm: Understanding the threats to information security. *International Journal of Information Management, 24*(1), 43-57.

Willison, R., & Siponen, M. (2007). A critical assessment of IS security research between 1990-2004. *Proceedings of 15th European Conference on Information Systems* St. Gallen, Switzerland.

About the Authors

James GOLDSTEIN is an Assistant Professor of Accounting Information Systems in the Wehle School of Business at Canisius College in Buffalo, NY. He earned his Ph.D. from the Whitman School of Management at Syracuse University and his M.B.A. from the Stern School of Business at New York University. His research interests include the assessment and management of operational risk, Enterprise Risk Management, and the business case presentation of proposed IT systems. Prior to his academic career, he held positions in a public accounting firm, in a major investment bank on Wall Street, and in the finance division of a regional retail bank.

Anna CHERNOBAI is an Assistant Professor of Finance at the M.J. Whitman School of Management at Syracuse University, NY, USA. The focus of her research is operational risk, default risk, stochastic processes, and applied statistics. She is an author of the book "Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis," has been an FDIC research fellow and JP Morgan Chase faculty fellow. Anna Chernobai earned her Ph.D. is statistics and applied probability from the University of California at Santa Barbara in 2006. She also holds a Master's degree in finance from the Warwick Business School at the University of Warwick, UK, and a bachelor degree in economics from Sophia University, Japan.

Michel BENAROCH is a Professor in the Accounting and Information Systems Department at the M.J. Whitman School of Management, Syracuse University, USA. His research focuses on the management of IT investments and IT investment risk in an IT portfolio context, and in the design of declarative ontology-centered modeling formalisms for information systems development. He has published extensively in such outlets as *MIS Quarterly*, *Information Systems Research*, *IEEE Transactions on Software Engineering*, *IEEE Transactions on Knowledge and Data Engineering*, *International Journal of Economic Dynamics and Control*, *International Journal of Human-Computer Studies*, *Decision Sciences*, and *Decision Support Systems*. Michel earned his Ph.D. from the Stern School of Business at New York University.