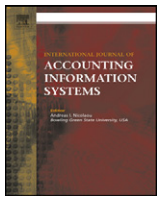
International Journal of Accounting Information Systems 13 (2012) 357–381

Contents lists available at SciVerse ScienceDirect

International Journal of Accounting Information Systems



An internal control perspective on the market value consequences of IT operational risk events

Michel Benaroch [a,*], Anna Chernobai [b], James Goldstein [c]

[a] Department of Accounting and IS, Whitman School of Management, Syracuse University, United States
[b] Department of Finance, Whitman School of Management, Syracuse University, United States
[c] Department of Accounting, Canisius College, United States

ARTICLE INFO

Article history:
Received 27 June 2011
Received in revised form 27 February 2012
Accepted 5 March 2012

Keywords:
IT control weaknesses
IT operational risk events
Internal control objectives
Regulatory environment
Confidentiality, integrity and availability of IT assets
Financial services
Event study

ABSTRACT

IT internal controls are an important component of an organization's arsenal of internal controls. Upon conceptualizing failures of operational IT systems, or what we call *IT operational risk events*, as signals of IT internal control weaknesses, we theorize about these events' impact on internal control objectives in general and about how this impact is influenced by the regulatory environment in particular. We then perform an event study to examine the economic impact of a diversified sample of IT operational risk events from the U.S. financial services industry during 1985–2009. We specifically test the impact of contextual factors on the degree of this effect, including the events' target (confidentiality, integrity, or availability of IT assets), the source of disclosure (regulatory or voluntary), the enactment of the Sarbanes–Oxley Act, and firm-specific attributes. We find that investors penalize firms most strongly for experiencing events that compromise the availability of IT systems, consistent with our prediction that these events more negatively impact the reliability of financial reporting and the efficiency and effectiveness of operations. This result contrasts extant empirical studies that are predominantly concerned with information and security breaches. We find also that investors' penalty is the strongest for firms experiencing IT operational risk events that occurred after the passing of the Sarbanes–Oxley Act or were disclosed by a regulatory body. Finally, the market reaction is shown to be stronger for firms with high growth potential, firms that are larger, riskier, and are in the banking sector. Implications for research and practice are discussed along with directions for future research.

© 2012 Elsevier Inc. All rights reserved.

* Corresponding author.
E-mail address: mbenaroc@syr.edu (M. Benaroch).

1467-0895/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.accinf.2012.03.001

1. Introduction

A growing research stream on information technology (IT) internal controls is motivated by the 2002 Sarbanes–Oxley Act (SOX), which requires firms to disclose internal control weaknesses (ICWs) over financial reporting. Broadly, *IT controls* refer to "the management, operational and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information" (NIST, 2010, p. 3). The importance of IT controls has come hand in hand with greater dependence of business processes on IT systems and a tendency to build into these systems' automated managerial controls. Indeed, studies of SOX-disclosed IT control weaknesses find that many of the causes of financial misstatements relate to ineffective IT controls (Messier et al., 2004), that firms with IT control weaknesses have less accurate management forecasts (Li et al., 2008), and that IT deficient firms report significantly more non-IT ICWs and financial misstatements (Klamm and Watson, 2009) and experience eight of the top-ten most common accounting errors more frequently (Grant et al., 2008). These studies are part of a broader body of work showing that firms with general (non-IT) SOX-disclosed ICWs have more accounting errors, lower quality financial reporting, more earning restatements, and a negative stock price reaction to reported material ICWs (Doyle et al., 2007; Krishnan and Gnanakumar, 2007; Beneish et al., 2008; Chan et al., 2008; Ashbaugh-Skaife et al., 2009; Hammersley et al., 2010). Overall, this research stream offers ample evidence on the impact of SOX-disclosed ICWs – whether IT-related or not – albeit in the limited context of control over financial reporting.

While SOX-reported IT control weaknesses are informative, they may or may not materialize into actual control failures, unlike IT operational risk events that signal the actual materialization of IT control weaknesses. IT operational risk events are manifestations of "loss of internal control" (Mensah and Velloci, 2006, p. 83) or "consequences of a weak internal control environment" (Chernobai et al., 2011, p. 3). They stem from actual failures of operational IT systems (software, hardware, networks, users, etc.) and/or the data assets that these systems record, process, transport, and safeguard (Markus, 2000). The impact of IT operational risk events has been studied by numerous researchers from areas related to accounting information systems (e.g., Campbell et al., 2003; Zhou, 2004; Anthony et al., 2006; Bolster et al., 2010; Gatzlaff and McCullough, 2010) and management information systems (e.g., Garg et al., 2003; Hovav and D'Arcy, 2003; Cavusoglu et al., 2004; Ko and Dorantes, 2006; Kannan et al., 2007; Goldstein et al., 2011).[1] This stream of studies complements the SOX-centered research stream by not being limited to SOX disclosures of IT control weaknesses over financial reporting. Nevertheless, it has some notable shortcomings. One is that, unlike SOX-centered research, this stream does not build on rich accounting literature that can inform about the impacts of IT operational events from an internal control perspective. Rather, most of the hypotheses tested by this stream rest predominantly on anecdotal evidence, business surveys, and past empirical results. A second shortcoming is the narrow focus on a single type of IT operational risk events, namely information and computer security breaches that compromise the *confidentiality* of data assets. IT operational risk events can also compromise the *integrity* and *availability* of operational IT systems, and can occur due to software bugs, hardware failures, and user errors (Whitman, 2004); software bugs alone cost the U.S. economy about $60 billion annually (NIST, 2002). The third shortcoming is the mixed inconclusive empirical results these studies offer. Nearly half the studies find no market reaction to the announcement of data and security breach events, while the rest find a negative market reaction or a reaction only under certain specific conditions.

The present study seeks to address these inter-related shortcomings of research on IT operational risk events. *First*, we use accounting literature on internal controls to frame IT operational risk events as realizations of IT control weaknesses and to reason about likely impacts of these events on internal control objectives. In a related paper, Goldstein et al. (2011) employ the resource-based view of the firm to frame IT operational risk events as the result of strategic IT resource weaknesses (Stoel and Muhanna, 2011). Their strategy-oriented perspective seeks to inform MIS researchers and managers about strategic concerns surrounding IT operational risk. For example, one strategic concern is the balance between deploying IT

[1] The latter studies are part of a broader IT research stream that is concerned with the impact of IT risk on firms' market value, usually from the perspective of transaction cost economics and the resource-based view of the firm (e.g., Oh et al., 2006; Dewan and Ren, 2007; Benaroch and Appari, 2011). Unlike this broader research stream, our interest in examining the impact of IT operational risk events from the perspective of internal control weaknesses that give rise to such events.

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات