Linking Operational IT Failures to IT Control Weaknesses

Full Paper

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

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

Abstract

Operational IT failures have significant negative impacts on firms but little is known about their origins. Building on accounting research linking adverse operational events to SOX-disclosed control weaknesses (CWs) over financial reporting, we study the origins of IT failures in relation to IT-CWs. We use a sample of 212 operational IT failures where the confidentiality, integrity, or availability of data assets and functional IT assets (hardware, networks, etc.) has been compromised. We find that IT failures are linked to a relatively small set of IT-CWs, where each IT failure type is linked to a distinctly different subset of IT-CWs. Moreover, IT failures that are more harmful to the firm are found to be associated with IT-CWs that are more severe in the sense that they are more difficult to remediate.

Keywords

Information systems risk, operational IT failure, IT control weaknesses, CobIT.

Introduction

Operational Information Technology (IT) risk manifests itself as failures of operational IT systems (Carr 2003). Any such failure could compromise the *confidentiality*, the *integrity,* or the *availability* of data assets and/or functional IT assets (software, hardware, etc.) that create, record, process, transport, store, and safeguard data assets (Benaroch et al. 2012).

How operational IT failures affect firms has been studied extensively, but little is known about their origins. The IT literature focuses on how these failures affect firm value (e.g., Garg et al. 2003; Cavusoglu et al. 2004; Ko and Dorantes 2006; Goldstein et al. 2011). Accounting Information Systems (AIS) research is more concerned with how these failures affect the quality of financial reporting (e.g., Bolster et al. 2010; Campbell et al. 2003; Gatzlaff and McCullough 2010). Collectively, this work agrees on the adverse effects of operational IT failures. Some studies further report that failures compromising the integrity and/or availability of data and functional IT assets are more consequential than confidentiality failures involving data and security breaches (Garg et al. 2003; Kannan et al. 2007; Goldstein et al. 2011; Benaroch et al. 2012). Yet, the literature has been silent on the root causes of IT failures.

We investigate the origins of operational IT failures in relation to weaknesses in internal IT controls. While coverage of operational IT failures is sparse in the IT literature, accounting and AIS research has extensively studied the link between adverse operational events (e.g., fraud, financial misstatements) and SOX-disclosed weaknesses in IT and non-IT controls over financial reporting. Building on this research, we study the link between operational IT failures and IT control weaknesses (IT-CWs). IT controls are management and technical safeguards or countermeasures prescribed to protect the confidentiality, integrity, and availability of a system and its information (ITGI 2007). We specifically hypothesize that: (1) different types of operational IT failures are associated with different IT-CWs, and (2) more consequential operational IT risk events (availability and integrity failures) are associated with more severe and difficult to remediate IT-CWs. We test our hypotheses using a sample of 212 operational IT failures for which detailed narrative descriptions are available. We map each failure to weaknesses in CobIT controls; CobIT is a practice-oriented IT control framework (ITGI 2007). We assess controls' remediation difficulty based on input/output dependencies between CobIT controls and social network analysis measures of centrality. Our analysis confirms both hypotheses and identifies specific IT-CWs prevalent in our data.

This paper makes several contributions to the IT and AIS literatures. Being first to investigate and empirically link operational IT failures to specific IT-CWs, the patterns we identify may be useful for theory development on the connection between IT failures and weaknesses in IT controls. In particular, our results suggest that the negative impact of IT failures on firm performance may also be a function of the specific IT control weaknesses linked to IT failures (based on how market investors react to the revelation of IT failures), a line of inquiry common in accounting research. Second, the paper highlights opportunities and challenges for scholarly research in a relatively understudied area that is of importance to theory and practice. In particular, we identify accounting research concepts and methods that may not be applicable in the IT failures context (e.g., entity-level controls, analysis based on matched samples), suggesting a need to explore other disciplines for additional guidance and/or develop new methods for collecting and analyzing data on IT failures. Lastly, our results pinpoint a relatively small set of IT-CWs that firms ought to avoid in order to lower exposure to operational IT risk.

Background: Internal CWs as Origins of Operational IT Failures

Internal controls are "policies, procedures, practices, and organisational structures designed to provide reasonable assurance that business objectives will be achieved and *undesired events will be prevented or detected and corrected*" (ITGI 2007). Enterprises establish a system of internal controls to mitigate probable events posing risk to their objectives (COSO 2004). Due to the multitude of such events, enterprises design controls for events posing the most risk. Hence, when a risk event materializes, or an operational failure occurs, it is taken to signal weaknesses in the system of internal controls – deficient controls and/or missing controls (Grant and Miller 2007; Canada et al. 2009; Stoel and Muhanna 2011).

Accounting research documents extensively the link between internal SOX-disclosed CWs and adverse operational events. Firms with SOX-disclosed CWs have more accounting errors and financial reporting quality, leading to such events as earning restatements (Ashbaugh-Skaife et al. 2009; Beneish et al. 2008; Chan et al. 2008; Doyle et al. 2007; Krishnan and Gnanakumar 2007). Firms also suffer a negative stock price reaction to disclosure of CWs (Hammersley et al. 2008). Focused on IT controls, AIS research asserts that SOX-disclosed IT-CWs have a pervasive impact on financial reporting. Firms with SOX-disclosed IT-CWs have more financial misstatements, significantly more non-IT-ICWs, more of the most common accounting errors, less accurate management earnings forecasts, and are slower to remediate non-IT-CWs (Messier et al. 2004; Grant et al. 2008; Klamm and Watson 2009; Klamm et al. 2012; Li et al. 2012). Stoel and Muhanna (2011, p. 285) add that "material weakness in IT internal controls can adversely impact both the underlying business operations … as well as the production of reliable financial reports." Furthermore, "companies with material IT control weaknesses have significantly lower ROA, ROS, and growth compared with companies with no weaknesses and even companies with non-IT control weaknesses" (Boritz and Lim 2007, p. 21).

Accounting research also shows CWs to vary widely on their severity and remediability. On severity it distinguishes between account-level and entity-level CWs. Account-level controls raise no serious concern to the reliability of financial reporting, whereas entity-level controls are over the financial reporting process and may signal an inability to prepare accurate financial reports (Doss and Jonas 2004). Entity-level CWs are more severe and associated with lower accrual quality, auditors' going concerns, and lower market returns, while account-level CWs are not (Doyle et al. 2007; Hammersley et al. 2012; Klamm et al. 2012). As to remediability, investors react more negatively to disclosures of difficult to remediate CWs (Hammersley et al. 2012). Moreover, companies failing to remediate CWs pay higher audit fees and are more likely to miss filing deadlines and experience decreased bond ratings (Hammersley et al. 2012).

In summary, though limited to SOX-reported CWs over financial reporting, accounting research documents a strong link between adverse operational events and CWs, especially more severe CWs.

Research Hypotheses

Building on existing literature, we posit that the occurrence of operational IT failures is linked to the existence of IT-CWs. We next develop two hypotheses in relation to the nature of IT-CWs associated with different IT failure types.

Different types of operational IT failures are expected to be linked to different IT-CWs. For example, Kerr and Murthy (2007) identify critical controls that are responsible for reliability of financial reporting, and Kim et al. (2006) identify "foundational" controls affecting firm performance on security and IT

operations; both findings are based on surveys of senior IT managers and IT audit experts. The internal controls that enterprises choose to implement are designed to mitigate specific adverse events (COSO 2004). By extension, IT controls are designed to fulfill well-defined functions: provide security, monitor software changes, ensure continuous service delivery, comply with regulations, and so on. This explains, in part, the existence of multiple IT control frameworks that vary on their focus and, therefore, the granularity and type of IT controls they define (Parent and Reich 2009). In this light, we hypothesize as follows:

> **Hypothesis 1**: *Availability, Integrity, and Confidentiality operational IT failures are associated with different IT-CWs.*

More consequential IT failure types are expected to be linked to more severe IT-CWs. As we said earlier, accounting research links more severe, entity-level CWs to lower quality financial reporting and lower firm performance. On the same grounds, knowing that firms suffer greater abnormal returns when experiencing Integrity and Availability failures than Confidentiality failures (Garg et al. 2003; Kannan et al. 2007; Goldstein et al. 2011; Benaroch et al. 2012), the former failures types should be associated with more severe IT-CWs. One explanation for the difference in abnormal returns, based on the resource-based view of the firm, links all operational IT failures to the existence of 'IT resource weaknesses' in the experiencing firms (Goldstein et al. 2011), and more consequential failures to IT resource weaknesses that are more difficult to overcome and dismantle. The link with IT-CWs should be clear. IT governance has oversight and *control* responsibilities over the acquisition of new IT resources and utilization of IT resources in business operations (Webb et al. 2006); it is responsible for designing and enforcing controls over IT resources. If some IT resource weaknesses are more difficult to dismantle, IT controls at their root must have weaknesses that will be as difficult to remediate. On this ground, availability and integrity failures would be associated with more difficult to remediate IT-CWs. Remediation difficulty could depend on the number of IT-CWs linked to an IT failure and their degree of interdependence with other IT controls. This parallels what accounting research terms "pervasive" controls – controls that cut across multiple components of the internal control system and/or interacts with multiple other controls (Hammersley et al. 2012). It is also consistent with a recognition that certain IT controls are more critical than others (Guldentops et al. 2002; Kerr and Murthy 2007; Kim et al. 2006) by virtue of the number of additional IT controls they affect (ITGI 2007). In this light, we hypothesize as follows:

> *Hypothesis 2: Compared to confidentiality IT failures, availability and integrity IT failures are associated with more severe IT-CWs.*

Data and Analysis

Sample Selection

Our data source is Financial Institutions Risk Scenario Trends (FIRST), a commercial operational risk events database marketed by IBM. The bulk of events is in financial services firms. Data about them is collected from public sources (SEC filings, court decisions, Reuters, newswire, etc.). We focus on incidents that occurred between 1985 and 2011 in publicly traded U.S. financial services firms.

We pre-selected candidate events via an electronic auto-search for over 50 IT-related keywords (computer, software, email, etc.). Then, each author independently examined the detailed narrative of each pre-selected event and classified it as a confidentiality, integrity, or availability failure. This has yielded 212 IT failures with inter-rater reliability measured close to 1.0. We ended up with 86 Confidentiality failures, 95 Integrity failures, and 31 Availability failures.

Linking IT Failures to IT-CWs

We proceed to test Hypothesis 1, which states that different IT failure types are associated with different IT-CWs. To test this hypothesis, we need to map IT failures to IT-CWs using a suitable taxonomy of IT controls.[1] Since our data sample covers all types of IT failures, CobIT's broad nature and comprehensive

[1] We considered other taxonomies. Those commonly used in the literature distinguish IT application controls from general IT controls (Bellino and Hunt 2007), or between SOX categories of IT controls over financial reporting (Boritz and Lim 2007; Li et al. 2012). Practice-oriented IT control frameworks are more comprehensive but they are each narrowly focused either on information security (ISO17799), IT services (ITIL), auditing ISs (SAC), or another distinct aspect of IT (Parent and Reich 2009).

coverage of IT controls makes it appropriate for this study (Parent and Reich 2009). CobIT provides an end-to-end reference model for all processes normally found in IT's traditional responsibility areas (CobIT 2007). It defines 34 IT processes in four domains: Plan & Organize (PO), Acquire & Implement (AI), Deliver & Support (DS), and Monitor & Evaluate (ME). CobIT also defines 350 IT controls over those processes. Input/output relations between the controls govern how the effectiveness of one IT control may impact, or be impacted by, one or more other IT controls.

IT failures in our sample were mapped to IT-CWs using the detailed failure descriptions provided in the FIRST database. The detailed description field of every IT failure was uploaded into Excel, one per row, and searched using text functions for the presence of over 600 stemmed words in CobIT's 350 controls. Matches flagged candidate IT controls implicated in each IT failure by text in the description field. Using this information one author and two MBA students with over five years of experience in CobIT implementation independently identified IT control weaknesses linked with each IT failure and coded them as CobIT processes (e.g., AI.7) and CobIT controls (e.g., AI.7.2). Inter-rater reliability exceeded 0.9, based on Krippendorff's alpha. All differences were reconciled upon discussions among the three.

Table 1 offers a count breakdown of our sample IT failures by CobIT domain and IT process, and by IT failure type. Many events were mapped to more than one CobIT control. On the whole, IT failures are linked mostly to CWs over IT processes in the AI and DS domains – 127 and 195 instances, respectively. Distinct patterns emerge from the mapping. Confidentiality failures are predominantly linked to IT-CWs in the DS domain, and concentrated in IT processes DS2, DS5, and DS11. Integrity failures are linked to IT-CWs mostly in the AI domain and some in the DS domain. Availability failures are linked to IT-CWs in select IT processes in the DS and AI domains. Intersingly, the top-five most implicated IT processes in our data (AI2, AI6, DS4, DS5, and DS11) are singled out by three surveys of senior IT managers and IT audit experts (Guldentops et al. 2002, Kerr and Murthy 2007, Kim et al. 2006). These surveys corroborate the concentration of weaknesses in IT controls over the selected IT processes we identified.

IT Failure Type / CobIT Domain and Process	Number of IT-CWs (%)		
	Confidentiality	**Integrity**	**Availability**
PO (Plan & Organize)	**2 (1.8%)**	**3 (1.8%)**	**0 (0%)**
PO4 (Define IT Processes, Organization & Relationships)	2	1	0
PO7 (Manage IT Human Resources)	0	1	0
PO10 (Manage Projects)	0	1	0
AI (Acquire & Implement)	**5 (4.5%)**	**103 (62.4%)**	**19 (35.2%)**
AI2 (Acquire & Maintain Application Software)	1	38	4
AI3 (Acquire & Maintain Technology Infrastructure)	0	1	0
AI4 (Enable Operational Use)	0	3	0
AI5 (Procure IT Resources)	0	0	1
AI6 (Manage Changes)	1	6	3
AI7 (Install & Accredit Solutions & Changes)	3	55	11
DS (Deliver & Support)	**105 (93.8%)**	**55 (33.3%)**	**35 (64.8%)**
DS2 (Manage Third Party Services)	22	6	2
DS3 (Manage Performance & Capacity)	0	6	5
DS4 (Ensure Continuous Service)	0	5	12
DS5 (Ensure Systems Security)	57	9	8
DS7 (Educate & Train Users)	1	7	0
DS8 (Manage Service Desk & Incidents)	0	2	1
DS9 (Manage the Configuration)	0	1	1
DS10 (Manage Problems)	1	5	2
DS11 (Manage Data)	23	14	0
DS12 (Manage the Physical Environment)	1	0	4
ME (Monitor & Evaluate)	**0 (0%)**	**4 (2.4%)**	**0 (0%)**
ME3 (Ensure Compliance with External Requirements)	0	4	0
Total	112 (100%)	165 (100%)	54 (100%)

Table 1: Breakdown of IT-CWs Mapped to Operational IT Failures

We are now ready to test Hypothesis 1 in a multivariate setting. To examine the probability that an observed IT failure is of a particular type as a function of specific IT-CWs in our data, we estimate three multivariate logistic models. The response variable equals 1 if an IT failure is of type Confidentiality, Integrity, or Availability, respectively, and 0 otherwise. The explanatory variables capture the presence of

weaknesses in controls over specific IT processes; excluded are IT processes with too few ($n \leq 3$) instances of IT failures. We estimate the three models simultaneously using a Seemingly Unrelated Regressions (SUR) model.

The results are depicted in Table 2. Regression coefficients are reported along with the predicted (conditional) probability's sensitivity measures for each independent variable.[2] Weaknesses in controls over IT processes DS2, DS5, and DS11 have a significant link with Confidentiality IT failures. For example, the probability that an observed IT failure is a Confidentiality type failure increases by 58.83% if weaknesses in controls over process DS2 are observed, and the same probability drops by 14.84% if weaknesses in controls over process AI2 are observed, holding other variables constant. Likewise, conditional on the occurrence of an IT failure, weaknesses in controls over processes AI2, AI7, and DS7 are primary indicators of Integrity type failures, and weaknesses in controls over processes AI6, DS3, and DS4 are primary indicators of Availability type failures. Our results strongly support Hypothesis 1, by demonstrating a highly significant association between distinctly different IT-CWs and specific operational IT failure types.

IT Failure Type (dependent) / **IT Processes with IT-CWs**	***Confidentiality*-Type IT Failures**		***Integrity*-Type IT Failures**		***Availability*-Type IT Failures**	
	Coeff. (*t*-stat)	Sensitivity: Δ prob.	Coeff. (*t*-stat)	Sensitivity: Δ prob.	Coeff. (*t*-stat)	Sensitivity: Δ prob.
AI2 (Acquire & Maintain Application Software)	-2.7770* (-1.71)	-14.84%	**1.8831*** (2.89)**	**34.94%**	-0.6796 (-0.68)	-2.06%
AI6 (Manage Changes)	0.1391 (0.09)	1.96%	-0.9760 (-1.63)	-23.23%	**1.7855*** (3.12)**	**16.71%**
AI7 (Install & Accredit Solutions & Changes)	-1.4572*** (-2.48)	-11.76%	**1.3457*** (2.66)**	**28.12%**	0.3444 (0.71)	1.65%
DS2 (Manage Third Party Services)	**2.7479*** (3.71)**	**58.83%**	-1.7267*** (-3.62)	-36.43%	-0.4636 (-0.66)	-1.54%
DS3 (Manage Performance & Capacity)	-	-	-0.0460 (-0.06)	-1.15%	**2.1593** (1.98)**	**23.57%**
DS4 (Ensure Continuous Service)	-	-	-2.1274*** (-2.51)	-41.33%	**3.6195*** (4.91)**	**58.16%**
DS5 (Ensure Systems Security)	**2.6495*** (5.19)**	**56.94%**	-2.0938*** (-3.45)	-40.97%	0.9642 (1.19)	6.19%
DS7 (Educate & Train Users)	-1.0575 (-1.40)	-9.80%	**1.4452* (1.66)**	**29.58%**	-	-
DS10 (Manage Problems)	-0.0613 (-0.07)	-0.81%	-0.4488 (-0.45)	-11.15%	0.5173 (0.31)	2.69%
DS11 (Manage Data)	**1.4127*** (2.73)**	**27.90%**	-0.0272 (-0.07)	-0.68%	-	-
DS12 (Manage the Physical Environment)	0.2713 (0.22)	3.99%	-	-	**3.8436*** (2.70)**	**63.25%**
Constant	-1.6576*** (-3.83)	-	0.1323 (0.27)	-	-3.1120*** (-3.90)	-
Number of observations	212		212		212	
Pseudo-R^2	0.4626		0.3852		0.2959	
Wald χ^2-statistic	43.68***		77.60***		77.77***	
ROC area	0.9095		0.8859		0.8351	
Baseline Proportion(1)	40.57%		44.81%		14.62%	
Sensitivity: Proportion(1|1)	95.35%		85.26%		64.52%	
Specificity: Proportion(0|0)	78.57%		79.49%		90.06%	
Overall proportion correctly specified	85.38%		82.08%		86.32%	

***, **, and * denote statistical significance at 1%, 5%, and 10% levels, respectively.
Missing coefficients are for IT processes not found to contribute to a particular IT failure type.

Table 2: Logistic Regressions

Severity of IT-CWs as Remediation Difficulty

To test Hypothesis 2, which states that more detrimental (Availability and Integrity) IT failures are associated with more severe IT-CWs, we need to measure severity of IT-CWs. This is a challenge with our

[2] Sensitivity is computed as change in the estimated probability as each dichotomous variable switches from zero to one while holding other independent variables at their median values.

data. Accounting research assesses severity of SOX-disclosed CWs based on their effects on the firm, as reflected by accounting measures (e.g., earnings, profitability, earnings quality, and audit fees [Canada et al. 2009; Tseng 2007; Hammersley et al. 2008; Chan et al. 2008; Klamm et al. 2012; Stoel and Muhanna 2011]), financial reporting measures (e.g., number of management forecast errors, financial restatements, and accounting errors [Li et al. 2012; Grant et al. 2008; Klamm and Watson 2009), and market measures (e.g., abnormal returns measured upon event revelation [Tseng 2007]). Accounting studies using these measures rely on ample SOX data on *ex ante* reported CWs and matched samples. In our context, we lack *ex ante* data on firms that may have had CWs but did not experience IT failures.

We opt for a different approach. Instead of inferring the severity from direct (but difficult to measure) effects on the firm, we start with knowledge of which specific IT-CWs are associated with more severe IT failures (Table 2) and then verify that those are IT-CWs more severe in the sense that are more difficult to remediate. In other words, we consider the remediation difficulty of an IT-CW as an indicator of that control's severity. As such, our measure of severity of a particular IT-CW is tied to the IT control's degree of systemic influence on the IT control system as a whole. The idea is that those IT-CWs that are more closely interdependent with other IT-CWs (i.e., if they fail, they may do so hand in hand with other IT controls) are weaknesses in those IT controls are more difficult to remediate. This parallels the way accounting research associates greater remediation difficulty with entity-level CWs because of their systemic scope (Hammersley et al. 2012) and the resources they require to improve the competency of people and ISs comprising the internal control system.

Unfortunately, since the literature does not identify which exact IT controls are so-called entity-level controls, we use *normative* measures of remediation difficulty as an alternative. The measures are: (1) the number of IT controls associated with a type of IT failure and (2) these controls' input/output interdependencies with other IT controls. We use these two measures to quantify how systemic the influence of an IT control is. They are operationalized using tools from the Social Network Analysis. In our context, network nodes are IT controls and directional links between the nodes represent input/output relationships between controls. The links are coded as 1 or 0 depending on the presence of the link between any pair of two nodes.[3] Similar approach has been used to identify foundational, high-priority IT controls that firms ought to implement first (Singh 2010; Goldschmidt et al. 2009). The advantage of this approach is that it tells us which IT-CWs are likely to be more difficult to remediate because of their links with "input" IT controls they depend on and/or "output" IT controls that depend on them.

We construct two separate matrices to represent the links between IT controls – one for input and one for output relationship. Such matrices allow us to calculate measures of "centrality" of an IT control in a input/output network of IT controls. Intuitively, centrality represents how a particular IT control is important to the network. For each IT control (or node *k*) we measure centrality using three commonly used metrics of influence from Social Network Analysis (Borgatti and Everett 2006):

- *Degree Centrality*: number of nodes with inflowing and outflowing ties to node *k*.
- *Eigenvector Centrality*: overall influence of node *k* on the rest of the network, where influence is proportional to the weighted sum of the influences of nodes to which node *k* is connected.
- *Betweenness Centrality*: fraction of shortest paths between all pairs of nodes in the network that pass through node *k*.

An IT control that rates higher on these measures would be considered more difficult to remediate.

As explained earlier, theoretical and empirical literature posits that Integrity and Availability types IT failures pose greater damage to a firm than Confidentiality type failures. Therefore, they should be associated with more severe IT-CWs. We therefore expect IT-CWs associated with more consequential (Availability and Integrity) IT failure types to be more difficult to remediate. Using Network Analysis tools, this implies that such IT failures should be linked to more IT-CWs, on average, and that the associated IT-CWs that failed should rate higher on measures of centrality (interdependence).

Following measure (1) of our approach described earlier, we start with the number of IT-CWs per IT

[3] We use unweighted networks in this study. Weighted networks can be used if the degree of dependence between any two nodes has a well-defined weight structure.

failure type. The average per IT failure is 1.561 for the entire sample, 1.3 for Confidentiality failures, and 1.74 for Integrity and Availability failures. Mean difference *t*-tests show Integrity and Availability failures to have significantly more IT-CWs per failure than Confidentiality failures.

Proceeding to the measures of centrality (measure (2)), Table 3 shows the centrality measures of CobIT processes that had statistically significant positive links with IT failures in our logistic regression results (Table 2). In line with our conjecture, IT processes linked to Availability and Integrity failures have overall higher centrality scores than those linked to Confidentiality failures. In fact, only IT processes linked with Availability and Integrity failures have centrality scores that exceed the median scores of the IT processes depicted in Table 3 (second row from the bottom) and of all IT processes in CobIT overall (bottom row); DS5 is the sole exception linked to Confidentiality failures.

Collectively, these results support Hypothesis 2, by showing that more consequential IT failure types are, on average, linked to more severe IT-CWs as measured by their anticipated remediation difficulty.

Operational IT failure type	IT Processes with significant links to IT failures	Degree Centrality		Betweenness Centrality		Eigenvector Centrality*
		In	Out	In	Out	
Confidentiality	**DS2** (Manage Third Party Services)	0.152	0.091	1.126	0.993	0.044
	DS5 (Ensure Systems Security)	0.152	0.182	1.931	1.583	0.060
	DS11 (Manage Data)	0.152	0.061	0.268	0.288	0.025
Integrity	**AI2** (Acquire & Maintain Application Software)	**0.212**	0.182	**2.869**	**1.712**	0.043
	AI7 (Install & Accredit Solutions & Changes)	**0.242**	**0.242**	**10.056**	**5.528**	**0.073**
	DS7 (Educate & Train Users)	0.152	0.061	1.004	0.487	0.026
Availability	**AI6** (Manage Changes)	**0.273**	0.212	**6.095**	**3.845**	**0.059**
	DS3 (Manage Performance & Capacity)	0.091	0.212	1.368	1.315	**0.068**
	DS4 (Ensure Continuous Service)	0.152	**0.242**	**3.006**	**2.158**	**0.076**
	DS12 (Manage the Physical Environment)	0.091	**0.030**	**0.173**	**0.177**	**0.022**
[redacted]						

* This measure works only for undirected networks – its values were computed using one symmetric matrix for both inputs and outputs.

Table 3: Centrality Scores of IT Processes with Control Weaknesses Linked to IT Failures

Discussion

Set out to identify IT-CWs at the root of operational IT failures, we uncover three insightful patterns. First, most broadly, we link IT failures to weaknesses in a relatively small set of IT controls – about 40 out of 350 IT controls in CobIT. Effective design and enforcement of those controls should reduce the likelihood of experiencing IT failures. Since enterprises choose which controls to implement and which not, they leave "holes" in their system of IT controls (ITGI 2007).

Second, more revealing are the subsets of IT-CWs linked to different IT failure types. Availability failures are linked mostly to IT-CWs over (1) managing change in IT applications, (2) managing performance and capacity requirements, and (3) ensuring continuous service by regularly testing recovery plans and re-training IT personnel. Integrity failures are linked mostly to IT-CWs over (1) the acquisition and maintenance of application software, including embedding of automated integrity IT controls, and (2) the installation, testing and quality assurance of IT solutions and changes to them. Confidentiality failures are linked to IT-CWs over (1) managing third-party services, (2) ensuring systems security through enforcement of policies and software updates, (3) managing security problems promptly, before they propagate, and (4) managing data, especially timely closure of user accounts and proper disposal of devices. Ensuring the effectiveness of these subsets of IT-CWs should reduce the likelihood of (re)occurrence of respective IT failures. A third insightful result is that more consequential (Integrity and Availability) IT failure types are linked to more difficult to remediate IT-CWs than Confidentiality failures, as seen from the greater degree of interdependence between the associated IT controls.

In light of these results, our study identifies the "holes" in the IT control system that are most critical in relation to operational IT failures. On the side of practice, the novel results of this study could help focus management attention to the more critical IT controls which an organization ought to design and enforce effectively. The results of this study call for better strategic allocation of IT budget resources to help prevent future operational IT failures. Firms should become proactive in identifying and remediating these critical IT control weaknesses, whether an IT failure event has occurred or not. Firms should ensure that any new IT control is appropriately designed and implemented, by bridging the objectives of the

traditional internal audit and IT audit (Juergens et al., 2006) and by involving internal auditors in the design of IT controls (Bellino and Hunt, 2007).

On the side of research, our study has three notable implications. First, the patterns of linkages between specific IT-CWs and specific IT failure types may be useful for theory development. For example, these patterns may help develop a characterization of the types of IT controls that "qualify" as entity-level controls in order to close a clear gap in extant literature on IT controls. Second, our study highlights theoretical and empirical limits to applying accounting research methods to the study of IT failures, and this may suggest a need to branch to other disciplines for additional guidance and to develop new methods for collecting and analyzing data on IT failures. In particular, the inherent problem of having data only on "positive" (or observed) cases where firms experienced IT failures and had IT-CWs observed only *ex post* after those IT failures occurred (as opposed to *ex ante* reported) precludes the use of matched samples, for example. Third, our study suggests another venue for the study of IT controls in connection with firm performance. Our finding that more consequential IT failures are associated with more difficult to remediate IT-CWs raises the possibility that the consequentiality of IT failures, at least as judged by market investors, is also a function of underlying IT-CWs. In this sense, IT-CWs may play a moderating role on the relationship between operational IT failures and their negative impact on firm performance. This line of inquiry is common in accounting research but has appeared primarily in the context of SOX-reported weaknesses in controls over financial reporting. Lastly, there is also a broad implication relating to accountability for weaknesses in IT controls. Some of the patterns we uncovered suggest that failures to enforce IT controls may rest equally with the business side (i.e., business process owners, head of operations) and the IT side (i.e., CIO, head of development), at least for some IT failure types. On another level, since oversight over IT controls may ultimately be an IT governance function, it seems logical to investigate the link between the existence of IT-CWs and the effectiveness of IT governance in firms experiencing IT failures.

Some limitations of our study should be mentioned. First, the set of IT-CWs linked to IT failures in our sample may be incomplete because the descriptive narratives of IT failures available in public sources are not the product of some systematic, in-depth post-mortem analysis of IT failures. Second, the categories in the Confidentiality/Integrity/Availability triad may not be mutually exclusive or collectively exhaustive. Third, it is not clear whether CobIT (or any one IT control framework) covers every IT control linked to IT failures. Fourth, our data sample may be subject to a selection bias: it covers only IT failures known publicly and that occurred in publicly-traded financial services firms.

In summary, by framing the origins of operational IT failures in terms of weaknesses in IT controls, this study yields novel insights into a subject that has received little attention in the IT literature. We identify empirical regularities that may be useful to advance theory development and practice in the area. We hope that this study, through its conceptual exploration and empirical findings, will jump-start scholarly and industry dialogues and foster follow-up research on operational IT failures and their root causes.

REFERENCES

Ashbaugh-Skaife, H., Collins, D., Kinney, W., and LaFond, R. 2009. "The Effect of SOX Internal Control Deficiencies on Firm Risk and Cost of Equity Capital," *Journal of Accounting Research* (47:1), March, pp. 1-43.

Bellino, C., and Hunt, S. 2007. *Auditing Application Controls*, The Institute of Internal Auditors (IIA), July.

Benaroch, M., Chernobai, A., and Goldstein, J. 2012. "An Internal Control Perspective on the Market Value Consequences of IT Operational Risk Events," *International Journal of Accounting Information Systems* (13:4), December, pp. 357-381.

Beneish, M. D., Billings, M., and Hodder, L. 2008. "Internal Control Weaknesses and Information Uncertainty," *The Accounting Review* (83:3), pp. 665-703.

Bolster, P., Pantalone, C. H., and Trahan, E. A. 2010. "Security Breaches and Firm Value," *Journal of Business Valuation and Economic Loss Analysis* (5:1), April, pp. 1-13.

Borgatti, S. P., and Everett, M. G. 2006. "A Graph-Theoretic Framework for Classifying Centrality

Measures," *Social Networks* (28:4), pp. 466-484.

Boritz, E., and Lim, J.-H. 2007. "Impact of Top Management's IT Knowledge and IT Governance Mechanisms on Financial Performance," in *Proceedings of the International Conference on Information Systems (ICIS)*, Montreal, Quebec, Canada, December 2007.

Campbell, K., Gordon, L., Loeb, M., and Zhou, L. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *Journal of Computer Security* (11:3), March, pp. 431-448.

Canada, J., Kuhn, J. R., and Sutton, S. G. 2009. "The Pervasive Nature of IT Controls: An Examination of Material Weaknesses in IT Controls and Audit Fees," *International Journal of Accounting and Information Management* (17:1), pp. 106-119.

Carr, N. G. 2003. "IT Doesn't Matter," *Harvard Business Review* (81:5), May, pp. 5-12.

Chan, K., Farrell, B., and Lee, P. 2008. "Earnings Management of Firms Reporting Material Internal Control Weaknesses under Section 404 of the Sarbanes-Oxley Act," *Auditing Journal Practice and Theory* (27:2), pp. 61-79.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise Risk Management – Integrated Framework: Executive Summary*, The Committee of Sponsoring Organizations of the Treadway Commission, NY: New York.

Doyle, J. T., Ge, W., and McVay, S. 2007. "Accruals Quality and Internal Control over Financial Reporting," *Accounting Review* (82:5), October, pp. 1141-1170.

Garg, A., Curtis, J., and Halper, H. 2003. "Quantifying the Financial Impact of IT Security Breaches," *Information Management & Computer Security* (11:2), pp. 74-83.

Gatzlaff, K., and McCullough, K. A. 2010. "The Effect of Data Breaches on Shareholder Wealth," *Risk Management & Insurance Review* (13:1), pp. 61-83.

Goldschmidt, T., Dittrich, A., and Malek, M. 2009. "Quantifying Criticality of Dependability-Related IT Organization Processes in CobIT," in *Proceedings of the 15th IEEE Pacific Rim International Symposium on Dependable Computing*, pp. 336-341.

Goldstein, J., Chernobai, A., and Benaroch, M. 2011. "Event Study Analysis of the Economic Impact of IT Operational Risk and Its Subcategories," *Journal of the Association of Information Systems* (12:9), September, pp. 606-631.

Grant, G. H., and Miller, K. C. 2007. "Improving Financial Reporting through Effective IT Controls: Evidence from the SOX 404 Audit," Working Paper, California State University at Pomona.

Grant, G. H, Miller, K. C., and Alali, F. 2008. "The Effect of IT Controls on Financial Reporting," *Managerial Auditing Journal* (23:8), pp. 803-823.

Guldentops, E., Van Grembergen, W., and De Haes, S. 2002. "Control and Governance Maturity Survey: Establishing a Reference Benchmark and a Self-Assessment Tool," *Information Systems Control Journal* (6), pp. 32-35.

Hammersley, J. S., Myers, L. A., and Shakespeare, C. 2008. "Market Reactions to the Disclosure of Internal Control Weaknesses and to the Characteristics of those Weaknesses under Section 302 of the Sarbanes Oxley Act of 2002," *Review of Accounting Studies* (13:1), March, pp. 141-165.

Hammersley, J. S., Myers, L. A., and Zhou, J. 2012. "The Failure to Remediate Previously Disclosed Material Weaknesses in Internal Controls," *Auditing: A Journal of Practice & Theory* (31:2), pp. 73-111.

IT Governance Institute (ITGI). 2007. *COBIT 4.1 Framework*, IT Governance Institute, IL: Rolling Meadows.

Juergens, M., Maberry, D., Ringle, E., and Fisher, J. 2006. *Global technology audit guide: management of IT auditing*, Deloitte & Touche LLP.

Kannan, K., Rees, J., and Sridhar, S. 2007. "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," *International Journal of Electronic Commerce* (12:1), Fall, pp. 69-91.

Kerr, D. S., and Murthy, U. S. 2007. "The Importance of the CobIT Framework IT Processes for Effective Internal Control over the Reliability of Financial Reporting: An International Survey," Presented at *University of Waterloo Symposium on Information Systems Assurance*, October 11-13.

Kim, G., Milne, K., and Phelps, D. 2006. *Prioritizing IT Controls for Effective, Measurable Security*, IT Process Institute, https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/deployment/577-BSI.html.

Klamm, B. K., and Watson, M. W. "SOX 404 Reported Internal Control Weaknesses: A Test of COSO Framework Components and IT," *Journal of Information Systems* (23:2), pp. 1-23.

Klamm, B. K., Kobelsky, K. W., and Watson, W. M. 2012. "Determinants of the Persistence of Internal Control Weaknesses," *Accounting Horizons* (26:2), pp. 307-333.

Ko, M., and 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), pp. 13-22.

Lainhart, J. W. 2000. "CobIT: A Methodology for Managing and Controlling Information and Information Technologies and Risks and Vulnerabilities," *Journal of Information Systems* (14), pp. 21-25.

Li, C., Peters, G., Richardson, V. J., and Watson, M. W. 2012. "The Consequences of Information Technology Control Weaknesses on Management Information Systems: The Case of Sarbanes-Oxley Internal Control Reports," *MIS Quarterly* (36:1), pp. 179-203.

Messier, W. F. Jr., Eilifsen, A., and Austen, L.A. 2004. "Auditor Detected Misstatements and the Effect of Information Technology," *International Journal of Auditing* (8), pp. 223-235.

Parent, M., and Reich, B. H. 2009. "Governing Information Technology Risk," *California Management Review* (51:3), May, pp. 133-152.

Payne, N. 2003. "IT Governance and Audit," *Accountancy* SA, January, p. 35.

Singh, H. 2010. "Selecting IT Control Objectives and Measuring IT Control Capital," in *Proceedings of the 21st Australasian Conference on Information Systems (ACIS)*, Brisbane, Australia, December 1-3.

Stoel, M. and Muhanna, W., "IT Internal Control Weaknesses and Firm Performance: An Organizational Liability Lens," *International Journal of Accounting Information Systems* (12:4), pp. 280-304.

Tseng, C. Y. 2007. *Internal Control, Enterprise Risk Management, and Firm Performance*, PhD Dissertation, Department of Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland.

Webb, P., Pollard, C., and Ridley, G. 2006. "Attempting to Define IT Governance: Wisdom or Folly?" in *Proceedings of the 39th Hawaii International Conference on System Sciences*, Hawaii, pp. 1-10.