JOURNAL OF MANAGEMENT INFORMATION SYSTEMS
2020, VOL. 37, NO. 3, 758–787
https://doi.org/10.1080/07421222.2020.1790190

Routledge
Taylor & Francis Group

Centralized Information Technology Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions

Che-Wei Liu[a], Peng Huang[b], and Henry C. Lucas, Jr.[b]

[a]Kelley School of Business, Indiana University, Bloomington, USA; [b]Robert H. Smith School of Business, University of Maryland, College Park

ABSTRACT

Despite the consensus that information security should become an important consideration in information technology (IT) governance rather than the sole responsibility of the IT department, important IT governance decisions are often made on the basis of fulfilling business needs with a minimal amount of attention paid to their implications for information security. We study how an important IT governance mechanism—the degree of centralized decision making—affects the likelihood of cybersecurity breaches. Examining a sample of 504 U.S. higher-education institutions over a four-year period, we find that a university with centralized IT governance is associated with fewer breaches. Interestingly, the effect of centralized IT governance is contingent on the heterogeneity of a university's computing environment: Universities with more heterogeneous IT infrastructure benefit more from centralized IT decision making. In addition, we find the relationship between centralized governance and cybersecurity breaches is most pronounced in public universities and those with more intensive research activities. Collectively, these findings highlight the tradeoff between granting autonomy and flexibility in the use of information systems and enforcing standardized, organization-wide security protocols.

KEYWORDS

Information security; cybersecurity breach; IT governance; centralized decision making; IT heterogeneity; IT centralization

Introduction

Information security has become a top priority for managers in both public and private sectors. With cybersecurity breaches causing significant disruptions in business operations, huge financial losses, and other long-term, intangible damage, information security management (ISM) has drawn much attention from IS researchers [6-8, 69, 70, 82]. Although much progress has been made in the field of ISM, there remain several limits to current understanding.

First, there is a dearth of empirical research that uses archival data to examine this issue, possibly due to the difficulties of obtaining relevant data.[1] As Kotulic and Clark [50, p. 597] point out, "the majority of the relevant literature is based on opinion, anecdotal evidence, or experience." The lack of large sample empirical evidence leads to several implications: for example, there is a minimal amount of evidence-based insight on what types of information technology (IT)-related policies and practices lead to better information security. Furthermore, it is difficult

CONTACT Che-Wei Liu cwliu@iu.edu Kelley School of Business, Indiana University, HH 4115, 1309 E. 10th Street, Bloomington IN, 47405, USA.

Supplemental data for this article can be accessed on the publisher's website.

for corporate executives to evaluate and justify investments in information security without understanding the effectiveness of these investments.

Second, although managers are increasingly cognizant that information security should become an important consideration in IT governance rather than the responsibility of the IT department alone [65, 72], research on ISM has rarely examined the impact of IT governance on information security. As a result, important governance policies, such as those regarding IT decision-making rights, are often made exclusively on the basis of fulfilling business objectives such as achieving flexibility, agility, or efficiency [98], and information security rarely enters the calculus in the formulation of such policies. This attitude is a surprise, considering that organizations bear significant costs, and in some cases suffer catastrophic consequences in the wake of a cybersecurity breach. For example, the Target data breach in 2013 affected 70 million customers, resulted in $67 million settlement payouts [76], and cost its CIO and eventually its CEO their jobs [11].

We aim to address these gaps in the literature by empirically examining the relationship between a particularly important mechanism in IT governance—the degree of centralization in IT decision rights—and the likelihood of cybersecurity breaches in the context of higher education. The relationship between centralized IT governance and information security has been the subject of intense debate in recent years. While some cybersecurity experts argue in favor of a decentralized solution and maintain that there is no one-size-fits-all approach in the cybersecurity domain [67], surveys of CIOs and chief IT security officers point to the culture of decentralization as one of the major barriers to information security [19]. Therefore, we ask the following research questions: *Does centralized IT decision making lead to better or worse information security? In addition, under what conditions is the relationship most salient?*

To answer these questions, we develop research hypotheses and evaluate them by examining a sample of 504 U.S. higher education institutions over a four-year period. We choose higher education as the context of the empirical exercises for a number of reasons: First, higher education represents a significant fraction of cybersecurity breaches. According to Huq [42], the education industry accounts for 16.8% of data breaches during the period 2005-2015, which is second only to the healthcare industry (26.9%) in the total number of breaches. Second, the higher education institutions vary in size, ownership structure (i.e., public vs. private universities), and the priority they place on IT investments (e.g., emphasizing efficiency or flexibility), allowing for the comparison among subgroups and the evaluation of the generalizability of the findings. Lastly, similar to prior empirical research that studies security breaches [53], the focus on a single sector results in a sample consisting of relatively homogeneous organizations, and therefore helps rule out potential confounds due to structural differences across many industry segments.

To preview our results, we find that a university with centralized IT decision making is associated with fewer cybersecurity breaches. By our estimate, a one standard deviation increase in IT centralization (or increase the level of IT centralization by 0.16 on a scale between zero and one) is associated with an average reduction in the probability of a cybersecurity breach by 2.6 percentage points. Given a 5.7% sample mean probability of breach, this represents a 45.6% decrease. Interestingly, we find that the effect of centralized IT governance is contingent on the heterogeneity of a university's computing environment: universities with more heterogeneous IT infrastructure benefit more from centralized IT governance. We show that these findings are robust to various endogeneity concerns. Our results also suggest that the effect of centralized IT governance on cybersecurity is most

pronounced in public universities and those with extensive research activities. Overall, these findings suggest that information security should become a crucial consideration in IT governance and provide several insights for mitigating security risks.

Related literature

Information security management

The management of information security has drawn significant research interests in the IS field. One stream of this literature focuses on information security planning in an organization. For example, Straub and Welke [82] identify four phases in a model of security risk planning and characterize information security management as comprised of a number of sequential activities: deterrence, prevention, detection, and remedies. Cerullo and Cerullo [22] argue that a business continuity plan should be considered part of the overall IT security plan, and identify major causes for unavailability in critical business systems.

The majority of studies on ISM focus on the tools and processes involved in the implementation of security countermeasures. For example, Cavusoglu et al. [21] investigate the conditions under which an intrusion detection system (IDS) offers value and demonstrate that improperly configured IDSs damage firms in a way that attracts more hacking. Ransbotham and Mitra [69] focus on the managerial process of control for technical solutions, resources, and tools, and propose a model which classifies security compromises as following either a deliberate or an opportunistic path. Some studies have also investigated practices related to software vulnerability disclosure and patching. For example, Arora et al. [6] find that software vulnerability disclosure accelerates software vendors' patch releases by nearly two and a half times, and open-source software vendors release patches more quickly than closed source software vendors. Cavusoglu et al. [20] adopt a game-theoretic model to study vendors' patch management and show that social loss is minimized when patch release and update cycles are synchronized. August and Tunca [7] explore the optimal patch restriction policy and show that if the patching costs are relatively low, it is optimal to provide patches to all users including software pirates. Ransbotham et al. [70] suggest that market-based disclosure of vulnerabilities restricts the diffusion of vulnerability exploitations, reduces the risk of exploitation, and decreases the volume of exploitation attempts.

A number of studies also examined the issues related to security policy auditing and compliance. For example, drawing on the theory of planned behavior, Bulgurcu et al. [18] investigate how the benefit of compliance, the cost of compliance and the cost of non-compliance affect users' intention to comply with information security policy. D'Arcy et al. [25] show that users' awareness of security countermeasures such as security policies and training directly affect users' perception of the severity of sanctions associated with information system misuse, leading to reduced misuse intention.

Finally, with cybersecurity breaches at organizations such as Target, Heartland Payment, and Sony inflicting damages on a large number of consumers [31, 41, 56], some researchers started investigating the strategies and policies that can be employed to reduce cybersecurity breaches. For instance, Kwon and Johnson [52] show that regulatory compliances can significantly reduce breach occurrences for operationally immature organizations in the healthcare industry, but the same does not apply to operationally

mature organizations. Moreover, Kwon and Johnson [53] investigate proactive and reactive strategies on data breaches in the healthcare field and find that proactive security investment is associated with fewer security failures and positive externalities. Sen and Borle [74] show that stricter laws on data breach notifications can benefit consumers by reducing data breaches. A few studies have also investigated remedial actions after customers' data have been compromised. For example, Goode et al. [31] find that compensation can be an effective tool to improve customers' perception of service quality and continuance intention, and Gwebu et al. [34] show that firms' reputation is important to protect firms' value amid a security breach incident.

IT governance

IT governance is the specification of decision rights and accountability, which is intended to encourage desired outcomes from an organization's investment in IT [adapted from 92]. Weill and Ross [91] identify five major decision domains that fall under the purview of IT governance, including *IT principles, IT architecture, IT infrastructure, business application needs*, and *prioritization and investment*, and highlight *decision making structure, alignment processes*, and *formal communications* as the three major governance mechanisms. Sambamurthy and Zmud [73] argue that the choice of IT governance mode is subject to the influences of multiple contingency forces, which often amplify, dampen, or override one another. Alreemy et al. [2] have defined a set of critical success factors that are important in the implementation of IT governance through a comprehensive review of well-known standards, best practices, and frameworks of IT governance. Studies have also discovered a range of structural, procedural and relational practices that are used to govern information artifacts [84].

Recent studies have placed significant attention on identifying the antecedents of effective IT governance, such as the roles of IT steering committees and IT-related communication policies [40], senior management involvement in IT [28], or the presence of relational culture and attitudinal commitment [23]. A number of studies have also empirically examined the relationship between IT governance and organization performance. For example, using data of matched CIOs and CEOs surveys, Wu et al. [97] show that strategic alignment mediates the effectiveness of IT governance on organizational performance. In addition, Bradley et al. [15] find that the quality of IT governance has a positive impact on risk management and the contribution of IT to hospital performance using survey data gathered from CIOs of U.S. hospitals. Finally, some suggest that there is a significant interplay between organizational IT architecture and IT governance structure in shaping IT alignment [88].

Theoretical background and hypotheses

IT governance and information security management

There has been increasing awareness of the importance of information security among researchers and practitioners. Many argue that managing information security risks can no longer be a concern delegated to the IT department alone, and must be considered an integral component of IT governance [65, 72]. For example, Ferguson et al. [28] argue that one of the central functionalities of IT governance is to facilitate risk assessments and to identify fraud and data breaches. Indeed, some researchers introduce the notion of Information Security Governance

(ISG) as an essential element of enterprise governance, defined as "the leadership, organizational structures, and processes involved in the protection of informational assets" [45, p. 127], and call for bringing information security to the attention of corporate boards and CEOs [94]. In addition, a governance approach to information security is said to help better manage risks by communicating more effectively within an enterprise and with external parties such as regulators [62]. Building on this line of literature, we argue that information security constitutes a key element in IT governance that pervades the major governance decision areas. As an example, in Table 1, we list some typical information security considerations involved in the IT governance decision areas as defined in Weill and Ross [91]. We present a detailed discussion of how centralized IT decision making—one of the most fundamental IT governance mechanisms highlighted in prior literature [91]—may affect information security, and develop our research hypotheses in the next subsection.

Hypotheses

One of the commonly used measures of information security performance is the incidents of cybersecurity breaches [53]. Consistent with prior literature, we define a cybersecurity breach as "an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so" [1, p. 22], and propose hypotheses regarding the relationship between IT governance decisions and cybersecurity breaches.

Centralized IT governance and cybersecurity breaches

An enduring theme of the research in IT governance is whether various decision rights regarding IT in an organization, such as those involving IT application, infrastructure, or project implementation, should be centralized [16, 73]. Prior research suggests that there are significant advantages and downsides associated with both centralized and decentralized decision making. For example, Xue et al. [98] argue that delegating the authority for IT decisions to business units may reap the benefits of quality and timeliness of decision making. This is because the business units are best positioned to make swift and informed decisions in response to their idiosyncratic local needs, changing environment and emerging opportunities [3, 64]. Conversely, a decentralized IT governance may also raise the issues of control because of agency problems; the objectives of a business unit and the organization are not always perfectly aligned [37, 43]. As a result, IT governance modes differ significantly across firms; in general, those that emphasize efficient operations are more likely to adopt a centralized approach to IT governance, while those that focus on rapid growth and innovation are more likely to espouse a decentralized approach [91]. Tiwana and Kim [87] suggest that firms exhibit more strategic agility when local units possess the decision rights for applications while a central IT group makes decisions on IT infrastructure. Ultimately, the choice of IT governance mode depends on the tradeoffs between the costs and benefits of different assignments of decision rights.

We argue that when it comes to information security, centralized IT decision making will lead to lower cybersecurity risks.

First, placing the decision-making authority in a centralized unit ensures *uniform control* and facilitates better strategic planning in information security, as the central unit can establish organization-wide security standards and data access policies by virtue of its vantage point of the whole organization's IT architecture [17]. In contrast, under

Table 1. Information Technology (IT) Governance decision areas and examples of information security considerations

	Decision Areas				
	IT Principles	IT Architecture	IT Infrastructure	Business Application Needs	Prioritization and Investment
Information Security Considerations	Data access policies Security protocols Business continuity and disaster recovery	Security architecture Centralized or distributed data storage	Identity management Anti-virus software Intrusion detection systems	Secure transactions Protect customer data Regulatory compliance	In-house or outsource information security Choice between open source vs. proprietary solutions

a decentralized IT governance mode where academic units are left to make most of their IT-related decisions, the units are likely to be concerned primarily with securing their own systems, resulting in fragmented information security policies and inconsistent standards. As King [49, p. 338] argues, centralized decision making "allows management to control adherence to organizational standards in system design and quality." Furthermore, the *alignment* between IS strategies and business needs is repeatedly ranked as one of the most critical issues for business leaders [83]. The inclusion of senior executives in a centralized governing body helps alleviate agency problems and ensures that the organization's business needs in information security are communicated effectively, and a shared consensus is reached between the central IT and business units during the process of strategic planning [28]. Finally, centralized IT governance also helps remove ambiguities in the *accountability* of decision-makers by explicitly assigning duties and defining responsibilities. Such formal control ensures that the parties involved are aware of their responsibilities and are held accountable in the event of a security failure [28].

Second, a centralized decision structure facilitates more effective *assessment* and *audit* of the compliance of security protocols, because the centralized unit makes it easier to integrate assessment procedures into its organization-wide standard routines and enforce universal compliance [58]. A centralized approach is also beneficial to the reporting and review of security incidents as it facilities *information sharing* across subunits, allowing one subunit to benefit from the lessons learned by another. The literature on information security has found that information sharing results in reduced IT spending and an increased level of security [30, 32]. In addition, a concerted effort by a central IT unit raises the level of *awareness* and *coordination* across the campus about information security issues, leading to more effective security information gathering, diagnosis, and dissemination. For example, once areas of security vulnerability are identified, a central IT governing body can quickly send out alerts and deploy countermeasures throughout the organization.

Finally, the management of information security requires highly specialized technical skills, as well as a holistic understanding of the university's IT architecture as most security breaches today arrive via a network and spread quickly throughout a campus. Under such conditions, a central IT office, by virtue of *specialization* and *economies of scale* [49], is more likely to possess the requisite knowledge and expertise. For example, a centralized IT office can afford to have a critical mass of personnel devoted to information security and a budget for the procurement of expensive security software, firewalls, and sophisticated intrusion detection tools. It may also have stronger bargaining power with external security software and service vendors, and achieve greater efficiency by avoiding duplication in resources, effort, and expertise [90], leading to better security performance. Based on the aforementioned discussion, we hypothesize:

Hypothesis 1 (H1): Universities with a higher degree of centralized IT governance will have fewer cybersecurity breaches.

Moderating role of IT heterogeneity

The relative advantage of centralized IT decision making may also depend on the computing environment, such as the heterogeneity of an organization's IT infrastructure. Technologically heterogeneous systems may lead to ambiguity and uncertainty regarding system development and use [59] and, therefore, causing difficulties in system integration and interoperability.

Technological heterogeneity may be determined by a host of factors, such as the diversity of IT platforms and applications, and the variety of technology vendors.

We argue that with more heterogeneous computing infrastructure, the benefits of centralized IT governance on strengthening information security are amplified. This is because, in the presence of more complex heterogeneous information systems, *specialization* and *economies of scale* play a more critical role in the defense against cybersecurity intrusions. With high IT heterogeneity, a business unit is unlikely to afford a highly skilled IT security staff that is well versed in intrusion prevention, detection, and remedies across a variety of platforms and applications [46, 71, 85]. By contrast, a centralized IT office is more likely to acquire such specialized skills because it can use resources more efficiently and avoid duplication of effort. Furthermore, the major advantages of a decentralized approach—*autonomy* and *flexibility*—are reduced in the presence of a heterogeneous IT environment. Under such conditions, the decentralized department IT staff, due to its narrow focus on its own IT systems, has a limited understanding of how the various platforms and applications are interconnected and how security risks are interdependent, leading to a reduced capacity to respond to security threats.

In addition, as the computing environment becomes more heterogeneous, the requirement for *interoperability* and *compatibility* increases when different IT subsystems need to comply with a set of standard security protocols, and centralized IT governance is better able to meet these requirements. It is well known that under a decentralized IT governance, system integration is difficult, and standardization faces greater challenges [14, 26]. For example, when a university has multiple heterogeneous enterprise application systems for teaching, research, and human resource management, centralized identity and access management (IAM) with single sign-on not only meets control requirements but also makes life easier for the end-user [68]. By comparison, a decentralized IAM results in multiple, fragmented identities for the same end-user, creating difficulty in using systems and more vulnerability for security breaches. Therefore, we hypothesize:

Hypothesis 2 (H2): The effect of centralized IT governance on reducing cybersecurity breaches is greater for a university with a heterogeneous IT environment than for one with a homogeneous IT environment.

Data and methods

Data

We assembled a longitudinal data set of cybersecurity breaches that have occurred in the higher education sector, as well as the institutional characteristics, IT-related investments, and IT practices of a sample of 504 U.S. higher education institutions during a four-year period (2011- 2014). Our data set consists of three major components, gathered from separate data sources. In addition to these three databases, we also use data obtained from *the Internet Crime Complaint Center (IC3)* of the Federal Bureau of Investigation (FBI). We provide details of these three major data components in this section.

Cybersecurity breaches

As cybersecurity breaches increasingly pose a threat to corporations, government agencies, and entities in the public sector, a number of organizations started data collection programs

on security breaches that aim to increase the awareness and reduce the risk for businesses and consumers.[2] We collected data on cybersecurity breaches from two such databases that provide open access to the public: The Identity Theft Resource Center (ITRC), and the Privacy Rights Clearinghouse (PRC). These two databases are chosen because they provide the most comprehensive information about security breaches, and have been frequently used in prior studies to examine topics related to cybersecurity breaches [24, 47, 53]. For the purpose of this research, we collected all the security breaches that involve U.S. higher educational institutions. We used the union of the breach incidences from the two independent sources to compile one comprehensive set of breach events during the time period of our study.

IT investments, governance, and security policies

The second source of our data is the Educause Core Data Service (CDS), from which we obtain the measures of IT investments, IT governance, and related information security practices and policies. Educause is a nonprofit association dedicated to advancing higher education by shaping strategic IT decisions through the use of information technology. Educause has over 1,800 colleges and universities as its members, who complete an annual survey on IT staffing, finance, and services. The annual CDS survey is organized into a set of *required modules* that collect basic, core IT information and *optional modules* that collect more details on specific IT domains such as IT personnel, educational IT use, research computing, and information security policies. The participating institutions use CDS data for communicating the value of IT, benchmarking IT budgets and staffing, and comparing IT department structure and service delivery with peer universities.

University characteristics

We obtain various characteristics of the higher education institutions from the Integrated Postsecondary Education Data System (IPEDS), which conducts a system of interrelated surveys for the U.S. National Center for Education Statistics (NCES) to collect data from all primary providers of postsecondary education. The annual IPEDS surveys are mandatory for institutions that participate in any federal student financial programs and more than 7,500 institutions complete IPEDS surveys each year. IPEDS collects data in key areas such as admission and enrollment, student financial aid, degrees and certificates conferred, and institutional human and fiscal resources, among others. The data is widely used by educational research organizations, such as the *College Board, Peterson's*, and *U.S. News & World Report* to compile their publications.

Empirical models

We specify that for a university i, the expected number of cybersecurity breaches it experiences in year t is the product of two factors, assuming that security breaches are observable and fully detected (we further relax the full detection assumption in the Supplemental Online Appendix):

$$E[N_{it}(breach)] = M_{it}(attack) * q_{it}(breach|attack) \quad (1)$$

where N_{it} is the number of security breaches that university i had during year t, M_{it} is the number of the cybersecurity attacks that university i encountered during year t, and q_{it} is

the conditional probability of a cybersecurity breach when the university is subject to an attack. M_{it} is likely to be affected by a host of variables $\mathbf{X_{it}}$ that make the university a high-value target for the hackers, such as the size of the institution or the number of data centers. q_{it} is likely a function of a set of variables $\mathbf{Z_{it}}$ that determine the university's ability to secure its digital assets against cybersecurity attacks, such as its IT security policies, its intrusion detection efforts, and its employment of managed security service providers. Assuming that the elements in $\mathbf{X_{it}}$ and $\mathbf{Z_{it}}$ multiplicatively shape M_{it} and q_{it}, we have

$$E[N_{it}(breach)] = e^{\alpha+\beta_1\mathbf{X_{it}}} * e^{\gamma+\beta_2\mathbf{Z_{it}}}$$

Or in log form,

$$lnE[N_{it}] = \beta_0 + \beta_1\mathbf{X_{it}} + \beta_2\mathbf{Z_{it}} \tag{2}$$

where $\beta_0 = \alpha + \gamma$. Equation 2 can be estimated by a number of regression models, such as the Poisson model or linear regression models. In our sample, however, it is extremely rare for a university to suffer more than one cybersecurity breach during any given year.[3] Therefore, the dependent variable, $lnE[N_{it}]$, is essentially binary. As a result, we replace the dependent variable with a binary response to estimate the following model:

$$E[p_{it}(breach)] = f(\beta_0 + \beta_1\mathbf{X_{it}} + \beta_2\mathbf{Z_{it}}) \tag{3}$$

where p_{it} is the probability of observing a security breach. A natural estimation model that is often used for binary responses is the logistic regression model, where the log-odds ratio is a linear function of the predictors. Logistic regressions relax the assumption that the error terms need to be normally distributed, and address issues such as heteroscedastic errors and the out-of-the-range probability predictions produced by linear models [33, p. 663].

A second approach of estimating equation 3 is the linear probability model (LPM), which represents a linear approximation to the nonlinear models. LPM is known to have several limitations; for example, it may result in predictions of probabilities that are not bounded by the range of zero and one, and the error term is heteroskedastic by definition. However, LPM is more amenable to the controlling for unobserved heterogeneities by using panel data methods (i.e., through the use of fixed effects), and has well-developed methods to address endogeneity issues. In addition, prior research has shown that LPM generates reasonable estimates within the region of support of the data with appropriate robust standard error corrections [4, pp. 102-107; 60]. Therefore, we use LPM as our baseline estimation model and use logistic regression as a secondary estimation method.

Sample and variables

The sample of our empirical investigation is defined as follows. We started with the set of universities surveyed by IPEDS, and matched IPEDS and Educause CDS data by university name using automated name matching. We then manually examined the unmatched names to rule out the possibility of different naming conventions used in the two systems. The process resulted in 1,069 universities in both IPEDS and Educause CDS databases. We further excluded observations for which important variables of interest (such as information security policies) are missing due to incomplete reporting. In addition, according to

IPEDS, a university falls into one of the following categories: 1) Degree-granting, graduate with no undergraduate degrees; 2) Degree-granting, primarily baccalaureate or above; 3) Degree-granting, not primarily baccalaureate or above; 4) Degree-granting, associate's and certificates; 5) Non-degree-granting, above the baccalaureate; 6) Non-degree-granting, sub-baccalaureate; 7) Not reported or not applicable. Because the Educause CDS survey primarily targets universities in the second category, we limit our sample to a relatively homogeneous set of universities that are degree-granting, primarily baccalaureate or above. This results in a sample of 1,278 observations for 504 universities over a 4-year period, representing an unbalanced panel. To allow for a causal interpretation and rule out reverse causality, all the independent variables are lagged for one year, meaning that we use IT governance and other institutional characteristics in year *(t-1)* to predict cybersecurity breach in year *t*.[4] As 2011 marks the first availability of Educause CDS data, we collect data for a 4-year period from 2011 to 2014 for all the independent variables, and use data from 2012-2015 for the dependent variable of cybersecurity breaches at the universities.

We provide details on the variables we use in the regressions in the following. As a summary, Table 2 presents the definition of all the variables included in this study.

Dependent variable

Following prior literature [5, 53], the dependent variable, Cybersecurity Breach, is defined as a binary indicator that represents whether a university encountered a cybersecurity breach in a given year. We collect the security breach data from both ITRC and PRC databases for all incidents in the higher education sector, and use the union of the two data sets to define our dependent variable by matching the security breach list to our sample universities. *Security Breach* is set to 1 if a university encountered at least one cybersecurity breach event in a year, and to 0 otherwise. We present the number of observations, as well as the distribution of cybersecurity breaches by year in Table 3. Overall, we observe 73 breaches among the 1,278 observations in our sample during the period of 2012-2015, representing 5.7% of the sample.

Independent variables

IT centralization. We construct the measure of the degree of IT centralization using data from the Educause CDS database. The Educause CDS survey provides information on the organizational units that are responsible for a series of IT functions and services. For each IT function or service, the respondent answers if it is provided by (i) primarily central IT; (ii) shared between central IT and other admin or academic unit(s); (iii) primarily other admin or academic unit(s); (iv) primarily system or district office; (v) primarily outsourced; and (vi) not applicable or no organizational unit responsible. Consistent with our theoretical arguments, the IT Centralization measure is constructed based on the whole range of IT functions and services provided by a university rather than the specific domain of IT security. Because there are slight differences in the IT functions and services included in the CDS survey over the four-year period of our study, we calculate the IT centralization variable using only the IT functions that were consistently included in the survey over the sample period; these IT functions are considered the most mission-critical ones, including "IT policy," "Project management/Business process/Systems analysis," "Institutional research," "IT support services - Help desk," "Classroom and learning space support," "Library," "Research technology

Table 2. Variable descriptions

Variable	Description	Source
Dependent variable		
Security Breach	Whether a university encounters a cybersecurity breach in a given year or not.	ITRC and PRC
Independent variables		
IT Centralization	The degree of IT centralization.	Educause CDS
IT Heterogeneity	The average of Blau's Indexes of operating systems and server systems used in the data centers.	Educause CDS
Variables that influence cybersecurity attacks (X)		
Students	The number of students in a university.	IPEDS
Data Centers	The number of data centers a university manages.	Educause CDS
Carnegie Classification	Carnegie Classification 2010	IPEDS
Research Grants	The sum of federal, state and local research grants.	IPEDS
Locale Codes	Locale codes identify the geographic status of a university on an urban continuum ranging from city size, suburb size, town size, to rural.	IPEDS
State Cybercrimes	The number of complaints of Internet crime/population (per 10,000 residents) of each state.	IC3
Variables that influence the probability of cybersecurity breach (Z)		
Outsourced Security	Whether a university outsources IT Security or not.	Educause CDS
Scan Policy	Whether a university conducts proactive scans for its critical systems and institutionally owned or leased computers or not.	Educause CDS
Patch Policy	Whether a university requires its critical systems and institutionally owned or leased computers to be expeditiously patched or updated or not.	Educause CDS
Multi-institutional Collaboration	Whether an institution participates in public/private information sharing activities such as the U.S. FBI InfraGard program or not.	Educause CDS
IT Funding	The dollar amount of central IT funding during the fiscal year, normalized by the number of students.	Educause CDS
Instrumental Variables for IT centralization		
Average Distance	The average physical distance between the focal university and other universities in the same multi-campus university system.	IPEDS
Private Sector CIO	Whether CIO's prior job is in a private sector or not.	Educause CDS

Notes: ITRC, Identity Theft Resource Center; PRC, Privacy Rights Clearinghouse; Educause CDS, Educause Core Data Service; IPEDS, Integrated Postsecondary Education Data System; IC3, Internet Crime Complaint database.

Table 3. Number of cybersecurity breaches by year

	No breach	Breach	Total
2012	292	25	317
	92.11%	7.89%	100.00%
2013	356	20	376
	94.68%	5.32%	100.00%
2014	329	18	347
	94.81%	5.19%	100.00%
2015	228	10	238
	95.80%	4.20%	100.00%
Total	1205	73	1278
	94.29%	5.71%	100.00%

services," "Data center," and "Network infrastructure and services." For each university-year observation, we then calculated the percentage of IT functions that the central IT office or system IT office was responsible and use this percentage as our measure of *IT centralization*.

IT heterogeneity. Prior research has emphasized that system integration and the exchange of data are particularly difficult when an organization has a multitude of heterogeneous and autonomous information systems [35]. We capture the heterogeneity of a university's computing environment by the types of operating systems and the hardware systems used in its data centers, which are obtained from the Educause CDS database. Therefore, this variable reflects IT heterogeneity at the university level. For operating systems, the survey respondent indicates whether operating systems (1) Mainframes, (2) Windows, (3) Unix, (4) Linux, or (5) other operating systems are used in each data center that the university operates. For hardware systems, the survey respondent indicates if any of the following systems were deployed in each data center: (1) Apple servers, (2) Cisco servers, (3) Dell servers, (4) Fujitsu servers, (5) Hitachi servers, (6) HP servers, (7) IBM servers, (8) Sun/Oracle servers, or (9) other servers. We employ a commonly used measure of heterogeneity, the Blau's index [13], to calculate the heterogeneity of operating systems and hardware systems in the data centers, and average the two as our measure of IT heterogeneity. The variable is calculated as:

$$IT\ Heterogeneity = \frac{OS\ Heterogeneity + HW\ Heterogeneity}{2} = \frac{\left(1-\sum_{i=1}^{R_{os}} p_i^2\right)+\left(1-\sum_{j=1}^{R_{hw}} p_j^2\right)}{2}$$

where p represents the percentage of data centers that deploy operating system i or hardware system j, and R represents the total number of operating systems or hardware systems. A higher level of Blau's index implies a higher level of heterogeneity.

Variables that influence cybersecurity attacks (X)

Universities vary in their attractiveness as a target of cybersecurity attacks, which depends on a host of institutional attributes. We control for a multitude of institutional characteristics that may influence the likelihood of cybersecurity attacks.

First, larger universities, such as those having a greater number of students, are likely to store a larger amount of sensitive data records such as student financial information and social security numbers. The wealth of sensitive information they keep, as well as their high visibility, makes these universities highly valued targets for intruders. To account for the size of an institution, we include in our regressions the total number of students

enrolled in the university (*Students*), which is retrieved from the IPEDS database. Prior research on information security has used similar measures such as the number of full-time employees to control for organization size [61]. We use the log form of *Students* in the regressions as its distribution is highly skewed. We have also experimented with adding other controls for the university size such as the size of the faculty or staff, the number of schools within the university, the number of programs offered, and they do not significantly change our findings. To avoid potential collinearity issues, we exclude these alternative measures of size from the models.

Second, data centers play a critical role in the storage, management, and dissemination of data, as well as the execution of business transactions in a university, making them a primary target for cybersecurity intrusions. A larger number of data centers operated by a university increases the risk exposure of the university. Therefore, we include a control variable obtained from Educause—the number of *Data Centers* operated by a university—in the regressions. Our inclusion of this variable is consistent with earlier work that used the amount of IT equipment as a proxy for available IT resources [53].

Third, the research and development (R&D) activities carried out by a university's faculty and researchers make it a particularly attractive target for cybersecurity attacks, because these activities usually generate valuable intellectual properties that are at risk of being stolen and misappropriated. We control for the input of the R&D activities through the amount of *Research Grants* a university obtains [75]. The amount of Research Grants is defined as the sum of federal, state, and local research grants that the university receives in a given year. We use the log form of *Research Grants* in the regressions as its distribution is highly skewed.

Fourth, prior research shows that organization type may influence exposure to information security risks [5, 53]. Therefore, we added the *Carnegie Classification* of a university as a control variable. The Carnegie Classification of Institutions of Higher Education is a framework for classifying colleges and universities in the United States and is often used to identify groups of roughly comparable institutions.

Finally, prior research suggests that the pattern of cybersecurity attacks displays significant spatial variations [47, 51]. To tease out the potential influences of geography, we:

(1) Used the *Locale Codes* of a university as a control for the geographic region. The value of this variable ranges from city, suburb, town, to rural area.
(2) We constructed a variable that represents the frequency of cybercrimes at the state level from the *Internet Crime Complaint* (IC3) database from the FBI. We collected the number of reported cybercrimes from each state and year during our sample period and normalize the number by the state population. The variable *State Cybercrime* is defined as the number of cybercrimes per 10,000 residents.

Variables that influence the conditional probability of cybersecurity breach (Z)

Outsourced security. Enterprise information systems are constantly subject to ever more sophisticated cybersecurity attacks, and it becomes increasingly difficult and costly for an organization to protect its digital assets against cybersecurity intrusions. As a result, some organizations choose to employ external vendors to manage their information systems security and defend against intruders. The outsourcing of information security might benefit from economies of scale and access to highly specialized labor [54], which are difficult to

obtain if security is managed in-house. Therefore, in our regression models, we control for whether a university outsourced its security to a third-party vendor. The Educause CDS survey includes a question that asks the respondents whether IT security is primarily the responsibility of outsourced vendors. We created the binary indicator variable, *outsourced security*, which is set to 1 if a university outsources its IT security and to 0 otherwise.

Intrusion detection and prevention policies. An important decision with respect to cybersecurity is whether or not a university addresses security problems proactively or reactively [53]. A proactive policy, for example, may involve using systems to scan networks, to detect and fix vulnerabilities before an outside intruder can exploit them [21], or require computers to be regularly and expeditiously patched or updated [6]. We collect data on a series of intrusion detection and prevention activities conducted by the universities in our sample from the Educause CDS database. These policies are broadly classified into two groups:

(1) whether a university conducted proactive scans to detect known security exposures of the university network for its critical systems and institutionally owned or leased computers (*Scan Policy*).
(2) Whether a university requires its critical systems and institutionally owned or leased computers to be expeditiously patched or updated (*Patch Policy*).

Multi-institutional collaboration. To improve information security compliance and data protection, a number of multi-institutional programs or confederations have been established to provide coordination among higher education institutions [66, 99]. [5] The Educause CDS database reports the participation of member universities in these multi-institutional collaborations. Sharing information on breaches allows universities to increase their awareness of security risks and benefit from the lessons learned from other universities. This variable is set to 1 if a university participates in any public/private collaboration programs, and to 0 otherwise.

IT funding. A large part of a university's IT capability, including its capability of detecting and preventing cyber intrusions, is determined by universities' investments in its IT personnel and infrastructure [53]. Therefore, we control for *IT Funding* in our setting, which is the dollar amount of the total funding the central IT department receives. We normalize this variable by dividing IT Funding by the number of students at a university. We also experimented with an alternative measure, the size of the IT staff, and all findings remain similar.

Summary statistics and correlations

In Table 4a we present the summary statistics of the main variables used in the data analyses.[6] On average, the central IT office is responsible for 61% of IT functions and services. The universities in our sample have a moderately heterogeneous computing environment in their data centers, with an average Blau's Index of 0.60. The average number of students is 7,631. The majority of the universities patch critical systems and institutional-owned computers (70%), but only about a third (39%) conduct a proactive scan of critical systems and institutional-owned computers. Universities in our sample on average have 3.95 data centers, and the mean IT funding per student is about $1,610 a year.

Table 4a. Descriptive statistics

	Mean	SD	Min	Max
Security Breach	0.06	0.23	0.00	1.00
IT Centralization	0.61	0.16	0.00	1.00
IT Heterogeneity	0.60	0.16	0.00	0.81
Outsourced Security	0.02	0.15	0.00	1.00
Log (Average Distance)	1.96	2.62	0.00	8.33
Private Sector CIO	0.08	0.27	0.00	1.00
# Data Centers	3.95	7.45	0.00	98.00
Log (# Students)	8.94	1.08	6.36	11.22
IT Funding per Student ($1,000)	1.61	2.41	0.00	31.32
Log (Research Grants)	7.92	8.77	0.00	21.00
State Cybercrimes (per 10,000 residents)	7.29	1.85	4.24	37.48
Multi-institutional Collaboration	0.38	0.49	0.00	1.00
Scan Policy	0.39	0.49	0.00	1.00
Patch Policy	0.70	0.46	0.00	1.00

Notes: IT, information technology. Number of observations: 1,278. Number of universities: 504.

The correlations among the variables are presented in Table 4b. We observe a negative correlation between IT centralization and cybersecurity breaches. In addition, universities with a more complex computing environment appear to be associated with a higher likelihood of a cybersecurity breach. We also find a moderately positive correlation between cybersecurity breaches with the number of students. However, one should interpret these bivariate correlations with caution because they do not control for the effect of other covariates.

Results

Baseline estimations

We follow Tiwana [86] to use a step-wise hierarchical regression model to test the hypotheses. We start estimating the relationship between centralized IT decision making and cybersecurity breaches by employing linear probability models as specified in Equation (3), where *IT Centralization* is included as part of the set of variables in **Z**. To test the moderating role of *IT Heterogeneity*, we then add the *IT Heterogeneity* variable and its interaction with *IT Centralization* into the model. In all the regressions, we use robust standard errors clustered by the universities. Particularly, we present the results from a pooled OLS estimation of the linear probability model (LPM) in columns 1 (the main effect of IT centralization) and 2 (with the moderating effect of IT heterogeneity) of Table 5, while controlling for the set of institutional characteristics and a set of year fixed effects.[7] With a panel data set, we also estimate the fixed effects (FE) panel data LPM. By using the fixed-effects model, we eliminate the effects of all time-invariant university heterogeneities and use only within-university variations for statistical inferences. We present the results of the FE models in columns 3 (the main effect) and 4 (with the moderating effect). To test the robustness of our findings, especially with regard to the model assumptions underlying the LPM estimations such as the distribution of the error term, we test two alternative, nonlinear model specifications and present these results. Specifically, in columns 5 and 6, we present the results from a binary response model using a logistic link function that controls for the unobserved heterogeneity through random effects [95]. We do not use the conditional logit (also

Table 4b. Correlation table

		1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Security Breach	1.00													
2	IT Centralization	-0.16*	1.00												
3	Outsourced Security	0.01	-0.11*	1.00											
4	IT Heterogeneity	0.09*	-0.16*	-0.02	1.00										
5	Log (Average Distance)	0.09*	-0.18*	0.01	0.20*	1.00									
6	Private Sector CIO	0.01	-0.05	0.05	0.04	-0.00	1.00								
7	# Data Centers	0.08*	-0.26*	-0.03	0.15*	0.10*	0.01	1.00							
8	Log (# Students)	0.20*	-0.39*	-0.03	0.40*	0.48*	0.06*	0.31*	1.00						
9	IT Funding per Student ($1,000)	-0.01	0.04	-0.03	0.05	-0.09*	-0.05	0.02	-0.19*	1.00					
10	Log (Grants)	0.12*	-0.23*	-0.06*	0.29*	0.68*	0.04	0.20*	0.64*	-0.09*	1.00				
11	State Cybercrimes (per 10,000 residents)	0.03	-0.03	0.04	0.09*	0.02	-0.02	-0.02	0.06*	0.01	0.00	1.00			
12	Multi-institutional Collaboration	0.09*	-0.17*	-0.04	0.24*	0.24*	0.03	0.16*	0.48*	0.06*	0.30*	0.02	1.00		
13	Scan Policy	0.03	-0.02	0.03	0.00	0.13*	0.03	-0.02	0.08*	0.06*	0.10*	0.01	-0.01	1.00	
14	Patch Policy	0.02	0.05	-0.03	-0.06*	0.03	-0.05	0.03	-0.06*	0.01	-0.00	0.07*	-0.09*	0.27*	1.00

Notes: IT, information technology; CIO, . For brevity, we suppress the categorical control variables such as Carnegie classification, and locale.
Number of observations: 1,278. Number of universities: 504. * $p < .05$.

Table 5. Cybersecurity breach: Main models

	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	OLS		Fixed Effects		Random-effects Logit		Penalized Likelihood Logit	
IT Centralization	-0.146**	-0.145**	-0.161^{+}	-0.175^{+}	-2.439**	-1.924*	-2.208**	-1.693*
	(0.052)	(0.052)	(0.094)	(0.094)	(0.843)	(0.915)	(0.781)	(0.829)
IT Heterogeneity	-0.039	-0.013	-0.024	0.027	-0.360	-0.552	-1.117	-1.395
	(0.035)	(0.037)	(0.127)	(0.129)	(1.116)	(1.029)	(1.235)	(1.188)
IT Centr. X IT Hetero.		-0.750**		-1.037*		-10.644*		-10.989^{+}
		(0.259)		(0.481)		(5.281)		(5.685)
Constant	-0.096	-0.121	0.789	0.779	-10.609**	-11.235**	-7.498**	-8.209**
	(0.132)	(0.132)	(1.713)	(1.709)	(2.051)	(2.146)	(2.877)	(2.945)
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	1278	1278	1278	1278	1278	1278	1278	1278
R^2	0.076	0.081	0.021	0.027				
Log likelihood					-242.263	-240.762	-207.069	-207.081
Prob > Chi^2					0.000	0.000	0.017	0.011

Notes: All regressions include the control variables: Outsourced Security; # Data Centers; Log(# Students); IT Funding per Student; Log(Research Grants); State Cybercrimes; and Multi-institutional Collaboration. We also include a set of categorical variables as controls: Carnegie Classification, Locale Code, and Intrusion Detection and Prevention policies. Both IT Centralization and IT Heterogeneity are centered.

Robust standard errors clustered by universities are in parentheses. $^{+}$ $p < .1$, * $p < .05$, ** $p < .01$.

known as the fixed-effects logit) models because the conditional logit model only uses observations of universities that switched status (i.e., universities that suffered security breaches in some years but not others) in the estimation [9, p. 211]. Therefore, the use of such models would result in dropping the majority of the observations from our sample, because for a large number of universities the dependent variable does not vary over the years (i.e. they never suffered a cybersecurity breach during the sample period). Finally, since the cybersecurity breaches in our sample are relatively rare, a conventional logit model might not be adequate because it may suffer from small-sample bias and sharply underestimate the probability of rare events [48]. The penalized likelihood method is a commonly used approach to reduce such bias by using maximum likelihood estimations [29, 36]. Therefore, we use penalized maximum likelihood in accordance with logistic regression (or Penalized Likelihood Logit model) to address the issues associated with rare events and show the results in columns 7 and 8.

We find strong support for H1, which predicts that universities with a centralized IT governance will have fewer cybersecurity breaches than those with a decentralized IT governance. Particularly, the results from the main effect models across the different specifications, presented in columns 1, 3, 5, and 7, consistently show that IT centralization reduces the probability of suffering a cybersecurity breach. The coefficient estimated from the FE model, for example, implies that a one standard deviation increase in IT centralization (or increase the level of IT centralization by 0.16 on a scale between zero and one) is associated with a reduction in the probability of a cybersecurity breach by 0.161*0.16 = 2.6%. Given the mean cybersecurity breach probability of 5.7%, this represents a 45.6% reduction in the breach likelihood.

Next, we turn to the evaluation of the moderating effect of IT heterogeneity on the relationship between centralized IT governance and cybersecurity breaches. We follow prior literature to mean-center the variables in the interaction term [57, 78] to allow for a more intuitive interpretation.[8] We find strong support for H2, and the negative coefficients of the interaction term, *(IT centralization) X (IT heterogeneity)*, in columns 2, 4, 6, and 8 consistently

show that when a university has a more heterogeneous computing environment, the benefit of having centralized IT governance in reducing cybersecurity breaches is greater. For example, the marginal effect calculations based on column 4 (the FE model) suggest that when IT heterogeneity is at the 1st quartile of the sample (IT heterogeneity = -0.054), the effect of IT centralization on the probability of cybersecurity breach is -0.175+(-1.037)*-0.054 = -0.119. This means a one standard deviation increase of IT centralization (0.16) is associated with a reduction in the probability of a cybersecurity breach by 1.9%, accounting for 33.3% of the mean breach probability of 5.7%. In contrast, when the IT heterogeneity is at the 3rd quartile of the sample (IT heterogeneity = 0.107), the marginal effect of IT centralization is -0.175 +(-1.037)*0.107 = -0.286. This means a one standard deviation increase of IT centralization is associated with a reduction in the probability of a cybersecurity breach by 4.6%, accounting for 80.7% of the mean breach probability of 5.7%.

Robustness checks

One of the identification challenges in the context of our study is the endogeneity of the degree of IT centralization. Although our use of fixed-effects panel data models helps control for all time-invariant, unobserved university-level heterogeneities, and we explicitly control for many other university characteristics, there may still be some time-varying unobservables that are correlated with both IT governance mode and the probability of cybersecurity breaches. To address this concern, we turn to instrumental variables methods to correct for the potential bias. Two instrumental variables are identified:

(1) *Average Distance*, which is defined as the average distance between a focal university and other universities in the same multi-campus university system, and
(2) *Private Sector CIO*, a binary indicator of whether the university CIO's immediate prior job is in a private sector (a detailed description of the instrumental variables can be found in the Supplemental Online Appendix).

We first conduct a two-stage least square (2SLS) analysis with fixed effects to address the endogeneity associated with the main effect of *IT centralization*, and present the results in columns 1 and 2 of Table 6. In the first stage, as we expected, both IVs, *Average Distance* and *Private Sector CIO*, are positively associated with centralized IT governance ($p<0.05$). The second stage of the 2SLS regression confirms that our finding with regard to H1 is robust to the endogeneity of *IT centralization*, as its coefficient remains negative and significant ($p < 0.05$). The F-statistic of the excluded instruments in the first stage has a value of 37.79, which is greater than the conventional threshold value of 10 [79], and indicates that our instruments are not weak. This is further confirmed by the Kleibergen-Paap rk Wald F statistic (with a value of 37.79), which is greater than the Stock-Yogo critical value [12, 81] at 10% maximal IV size (19.93). In addition, the Hansen J statistic has a value of 0.98 and cannot reject the null ($p = 0.32$) that the overidentification restrictions are valid.

We next turn to a 2SLS model in which we instrument for both the main effect of *IT centralization* and its interaction with *IT Heterogeneity*. To address the endogeneity of the interaction term *IT Centralization X IT Heterogeneity*, we use the interactions of *IT Heterogeneity* and the two IVs – *Average Distance X IT Heterogeneity* and *Private Sector CIO X IT Heterogeneity* – as additional instruments. In other words, we have two endogenous

Table 6. 2SLS estimation

	(1)	(2)	(3)	(4)	(5)
	Main effect		Moderating effect		
	First Stage	Second Stage	First Stage	First Stage	Second Stage
Dependent Variable	IT Centr.	Security Breach	IT Centr.	IT Centr. X IT Hetero.	Security Breach
Log (Average Distance)	0.042**		0.014	0.011**	
	(0.006)		(0.016)	(0.003)	
Private Sector CIO	0.052*		0.010	0.029	
	(0.023)		(0.075)	(0.041)	
Log (Average Distance) x IT Hetero.			0.042^{+}	-0.020**	
			(0.022)	(0.005)	
Private Sector CIO x IT Hetero.			0.074	-0.038	
			(0.118)	(0.063)	
IT Heterogeneity	0.116*	0.352^{+}	0.045	0.053**	0.364*
	(0.052)	(0.188)	(0.054)	(0.018)	(0.182)
IT Centralization		-2.267*			-1.713^{+}
		(1.154)			(0.990)
IT Centr. X IT Hetero.					-4.145^{+}
					(2.452)
N	1170	1170	1170	1170	1170†
Hansen J	0.983 (p = 0.321)			1.364 (p = 0.506)	
Kleibergen-Paap rk Wald F statistic	37.79 (p = 0.00)			10.58 (p = 0.00)	
Stock-Yogo critical value, 10% max IV size	19.93			7.56	

Notes: All regressions include the control variables: Outsourced Security; # Data Centers; Log(# Students); IT Funding per Student; Log(Research Grants); State Cybercrimes; and Multi-institutional Collaboration. We also include a set of categorical variables as controls: Carnegie Classification, Locale Code, and Intrusion Detection and Prevention policies. Both IT Centralization and IT Heterogeneity are centered.

Robust standard errors clustered by universities are in parentheses. $^{+}$ $p < .1$. * $p < .05$. ** $p < .01$. †108 observations dropped due to singletons.

variables and four instruments in this exercise. The results of this 2SLS model are presented in columns 3-5 of Table 6. We find that H2, which states a moderating effect of *IT Heterogeneity* on the relationship between *IT centralization* and cybersecurity breaches, is also robust to the endogeneity of *IT Centralization*, as suggested by the negative and significant coefficient of *IT Centralization X IT Heterogeneity*. Here, again, we find that our instrumental variables do not suffer from weak identification, as suggested by the F-statistic of excluded instruments (19.11 and 12.93, respectively) in the first stage, as well as the Kleibergen-Paap rk Wald F statistic (10.58). In addition, the Hansen J statistic indicates that overidentification restrictions are valid ($J = 1.36$, $p = 0.51$). Overall, the instrumental variables regressions increase our confidence that the findings are not due to estimation bias associated with the endogeneity of *IT Centralization*.

Beyond endogeneity concerns, we further explored the robustness of the findings through a series of tests. First, we employed an alternative estimation strategy using hazard models, which are often employed for medical data analyses [44] and are gaining popularity in IS research [39, 53]. Survival analyses usually model the underlying and unobserved hazard rate as the dependent variable and assume the covariates multiplicatively shift the baseline hazard function. They do not depend on the normality assumption imposed in some other models and provide an approach to address the incomplete observation of survival times when censoring occurs [38]. For example, applying a Cox proportional hazard model—a semiparametric specification that makes no assumption with regard to the shape of baseline hazard over time—to our context, we have

$$h_i(t|\mathbf{X_{it}}, \mathbf{Z_{it}}) = h_0(t) * exp(\beta_0 + \beta_1 \mathbf{X_{it}} + \beta_2 \mathbf{Z_{it}}) \quad (4)$$

where $h_i(t|\mathbf{X_{it}}, \mathbf{Z_{it}})$ is the conditional instantaneous hazard rate of cybersecurity breach for university i at time t; $h_0(t)$ is the baseline hazard function that depends solely on time, and the second component on the right-hand side characterizes how the hazard function changes as a function of covariates; $\boldsymbol{X}$ and $\boldsymbol{Z}$ are the same variables used in the main model; and β can be interpreted as the impact of variables of interest on the hazard rate associated with security breaches. The survival time is measured by years in our baseline model. In addition, we use a specification that accommodates multiple failure (breach) events, allowing a university with a security breach event to be subject to breach hazard again in subsequent periods.

We investigate the robustness of H1 and H2 using survival models as specified in Equation (4).

First, we test two functional forms that are most commonly employed in survival analyses: a semiparametric specification in the form of a Cox proportional hazard model and a parametric specification where the probability density function follows an exponential distribution [80]. The results are reported in columns 1-4 of Table 7. We find that H1 and H2 are consistently supported across all the model specifications, although the interpretations of the marginal effects are different from an LPM approach due to the nonlinear nature of these models. For example, the calculations based on the results in column 1 suggest that when comparing a situation where IT centralization is 1 (completely centralized) to a situation where IT centralization is 0 (completely decentralized), the *hazard ratio* (or the ratio of the two *hazard rates*) is 0.136 (=exp(-1.997)), or a reduction in the instantaneous *hazard rate* by 86.4% when IT centralization changes from 0 to 1.

Second, we have taken a number of measures to address some of the limitations of our baseline regressions, including issues related to partial observability of the security breaches, the omission of the severity of a breach event, and potential learning effect from the security breaches. The results of these robustness tests are presented in the Supplemental Online Appendix.

Table 7. Cybersecurity breach: Survival models

	(1)	(2)	(3)	(4)
	Survival Model (Cox)		Survival Model (Exponential)	
IT Centralization	-1.997**	-1.521*	-1.917**	-1.453*
	(0.678)	(0.736)	(0.681)	(0.736)
IT Heterogeneity	-0.979	-1.225	-0.905	-1.142
	(1.121)	(1.050)	(1.127)	(1.049)
IT Centr. X IT Hetero.		-9.044^{+}		-9.273*
		(4.707)		(4.623)
Constant			-7.056**	-7.673**
			(2.325)	(2.422)
Year fixed effects	Yes	Yes	Yes	Yes
N	1278	1278	1278	1278
Log pseudolikelihood	-374.022	-372.761	-187.769	-186.389
Prob > Chi^2	0.000	0.000	0.000	0.000

Notes: All regressions include the control variables: Outsourced Security; # Data Centers; Log(# Students); IT Funding per Student; Log(Research Grants); State Cybercrimes; and Multi-institutional Collaboration. We also include a set of categorical variables as controls: Carnegie Classification, Locale Code, and Intrusion Detection and Prevention policies. Both IT Centralization and IT Heterogeneity are centered.

Robust standard errors clustered by universities are in parentheses. $^{+}$ $p < .1$. * $p < .05$. ** $p < .01$.

Subsample analyses

We note that our sample consists of a variety of universities of different ownership structures as well as organizational objectives. This provides an excellent context for testing the contrasts between subgroups, and for inferring the potential generalizability of the findings. For example, research universities, in addition to providing higher education, also conduct basic and applied research, as well as provide services to the larger community. As a result, they usually have a pro-innovation culture and a set of organizational routines that encourage academic freedom and a high degree of autonomy in comparison to teaching universities. Such culture and routines place a greater emphasis on flexibility rather than efficiency in the implementation and use of IT systems, and therefore often result in more decentralized IT governance and a more complex IT environment.

We conduct two split sample analyses to examine the differential effects of IT centralization across different types of universities.

First, we compare universities with a heavy research orientation (which include Carnegie Classifications of *research university–extensive* and *research university–intensive*) with those that focus primarily on teaching (other Carnegie Classes). Consistent with our expectation, we find that research universities on average have a lower level of IT Centralization (55.6%) than that of teaching universities (64.7%), and have a more heterogeneous IT environment (0.66) than teaching universities (0.57). In columns 1 and 2 of Table 8, we show the contrast between the subsamples using the fixed effects LPM model.[9] We find that research universities benefit significantly from *IT Centralization* in reducing their chances of cybersecurity breaches, but the effect is not present for teaching universities. This result is consistent with our argument that organizations with a more heterogeneous IT environment benefit more from centralized governance.

Second, unlike some other industries, the higher education sector consists of large numbers of both public and private institutions. Comparing the two groups, we find that private universities not only have a higher level of IT Centralization (64.9%) than that of

Table 8. Subsample analyses

	(1)	(2)	(3)	(4)
	Fixed Effects LPM			
Sample	Teaching University	Research University	Private University	Public University
IT Centralization	-0.016	-0.372*	-0.059	-0.249^{+}
	(0.096)	(0.179)	(0.116)	(0.147)
IT Heterogeneity	0.043	0.067	-0.047	0.031
	(0.107)	(0.354)	(0.123)	(0.267)
Constant	-0.427	6.054	0.082	0.974
	(1.415)	(5.064)	(1.627)	(3.623)
Year fixed effects	Yes	Yes	Yes	Yes
N	813	465	666	612
R^2	0.020	0.081	0.027	0.026

Notes: All regressions include the control variables: Outsourced Security; # Data Centers; Log(# Students); IT Funding per Student; Log(Research Grants); State Cybercrimes; and Multi-institutional Collaboration. We also include a set of categorical variables as controls: Locale Code, and Intrusion Detection and Prevention policies. Column (3) and (4) also control for Carnegie Classification variable. Both IT Centralization and IT Heterogeneity are centered.

Robust standard errors clustered by universities are in parentheses. $^{+}$ $p < .1$. * $p < .05$. ** $p < .01$.

public universities (57.5%) but also have a lower degree of IT heterogeneity (0.56) than public universities (0.65), probably because many private universities have a highly specialized focus. We conduct a subsample analysis and present the contrast in columns 3 and 4 of Table 8. Interestingly, we find a strong effect of *IT Centralization* in reducing cybersecurity breaches for public universities, but not for private universities. Overall, the results suggest that the effect of IT centralization is most salient for organizations with less centralized governance and a more heterogeneous IT environment.

Conclusions

This study examines the implications of the mode of IT decision making on information security management. We developed hypotheses regarding how centralized IT decision making impacts information security and test them using a sample of 504 universities over a four-year period. Our theoretical development and empirical analyses yield two important findings.

First, we show that centralized IT governance in a university is associated with fewer cybersecurity breaches. We attribute the effect to a number of underlying mechanisms; for example, centralized IT governance is conducive to the establishment of uniform control and organization-wide security policies, better strategic alignment, and well-defined accountability. In addition, centralized IT governance facilitates universal compliance with security protocols, results in better security information sharing, raises the level of awareness of security issues, and enhances coordination between business units.

Second, we find that the effect of centralized governance on information security is stronger when a university has a more heterogeneous IT environment with different computer operating systems and hardware from a multitude of vendors. We argue that this is due to specialization and economies of scale associated with centralization. Under a more heterogeneous computing environment, it is doubly difficult for a department-level IT staff to understand how the various IT subsystems interoperate with one another, and how security risks are interdependent, resulting in a reduced ability to respond to cybersecurity issues appropriately. A centralized IT unit, by advantages of resource pooling and a better understanding of the overall IT architecture, is more capable of managing security risks under a sophisticated IT environment.

Our research makes an important contribution to the literature on information security management. We focus on information security implications of IT governance decisions and policies, a responsibility that usually resides with top executives and board of directors, instead of the daily activities of the IT department such as software patching [7, 20] or intrusion detection and prevention [21, 25]. Consistent with recent call for bringing the issue of cybersecurity to the attention of board of directors [65, 72], the results of our study suggest that information security should enter the calculus when management makes IT governance decisions, and it needs to be considered alongside other factors such as flexibility [27], agility [93], and efficiency [10]. This process will invariably introduce subtle tradeoffs in information systems planning and sometimes lead to conflict and delicate compromises, such as sacrificing the flexibility of information systems for the benefits of enforcing standardized security protocols. Our research provides empirical justifications for making such tradeoffs. Another notable contribution of our study is that in managing information security, the heterogeneity of an organization's

computing environment needs to be considered alongside other organizational factors, because it may interact with IT governance decisions in complex ways and influence the performance of ISM.

We also provide several insights for information security practices in the higher education sector. In a university setting, the implementation and use of IT systems often place a strong emphasis on individual autonomy [16] and flexible solutions that cater to idiosyncratic department needs [98], resulting in a fragmented, heterogeneous IT infrastructure with minimum standards and low level of compliance of security protocols, and the situation is particularly alarming in public, research universities. Therefore, it is important for IT steering committees in such universities to realize that a centralized IT governance approach can help establish uniform security standards and protocols throughout the campus and enforce universal user compliance. In addition, centralized governance is more efficient in system integration, information sharing, and coordination among various departments and, therefore, helps with a concerted effort to combat cyberattacks. The delicate balance between business needs and security considerations may result in a hybrid approach that combines centralized infrastructure governance (including security) and decentralized application governance, as proposed by Tiwana and Kim [87].

Like much of the earlier research in information security management, our study has a number of limitations. First, due to data limitations, the sample of this study represents a relatively short panel during the period of 2011 to 2015. This is because several important independent variables used in our analyses are not available in years subsequent to 2015 due to changes in Educause survey questions. We call for future research to investigate the research questions using more recent datasets. Second, our focus on cybersecurity breaches in a single industry, the higher education sector, implies that caution needs to be exercised when extrapolating our results to other contexts. Nevertheless, the higher education sector represents a significant fraction of the U.S. economy and therefore is important in its own right. According to the National Center for Education Statistics [77], the total revenues of degree-granting postsecondary institutions are $604.6 billion, accounting for 3.5% of GDP in 2014 [96]. In 2013, postsecondary education in the United States employed 3.8 million workers in total, representing 2.4% of the 155 million workers in the labor force [89]. In addition, higher education institutions invest heavily in information technology. On average, the education sector spends 6.2% of its revenue on IT, a level surpassing all industries except for the financial services and government sectors [63]. Although the generalizability of the findings to other industry sectors needs to be validated by future research, our subsample analyses do point to the conditions under which our findings are most likely to hold, for example, in organizations that have an entrenched culture of decentralized decision making and those with heterogeneous IT infrastructures. It is our conjecture that a similar effect of IT centralization will be found in industries that share some of these characteristics, such as the healthcare industry. It is exactly the combination of these conditions that make an organization vulnerable to cyberattacks in the first place [19]. In these days of escalating attempts to breach information systems everywhere, it is imperative that senior management and CIOs consider the impact of IT governance decisions on their organizations' cybersecurity outcomes.

Notes

1. There are a number of notable exceptions. For example, see Kwon and Johnson [53].
2. For a detailed discussion of the sources of security breach data, see Adebayo [1].

3. In our sample of 1,278 observations, only one has reported two security breaches in a year.
4. For example, a university that suffers from a security breach may invest heavily in security countermeasures after the event in the same year. The use of contemporaneous predictors will lead to the incorrect inference that more investment in security countermeasures causes more breaches, due to reverse causality.
5. These programs include: Higher Education Information Security Council (HEISC); REN-ISAC (Research and Education Network Information Sharing and Analysis Center); Public/private information sharing activities such as the U.S. FBI InfraGard program; National Security Higher Education Board; EDUCAUSE Security Discussion List; EDUCAUSE Policy Discussion List; EDUCAUSE Identity Management Discussion List; State or regional group; Internet2.
6. There are a few universities reported an unusually small number of students, low IT Funding, or low number of data centers. We identified 23 observations (with 18 universities) as possible outliers, and all the results still hold when we exclude these outliers.
7. We calculated the variance inflations (VIFs) to test the multicollinearity. The average VIF is 1.57, and the maximum variance inflation factor value is 5.74, which is smaller than the usual threshold of 10.
8. In addition, we perform a test using the residual centering approach [55] and find our results to be robust.
9. Other models such as logistic models and survival models show similar results.

References

1. Adebayo, A.O. A foundation for breach data analysis. *Journal of Information Engineering and Applications*, *2*, 4 (2012), 17–23.
2. Alreemy, Z.; Chang, V.; Walters, R.; and Wills, G. Critical success factors (CSFs) for information technology governance (ITG). *International Journal of Information Management*, *36*, 6 (2016), 907–916.
3. Anand, K.S.; and Mendelson, H. Information and organization for horizontal multimarket coordination. *Management Science*, *43*, 12 (1997), 1609-1627.
4. Angrist, J.D.; and Pischke, J.-S. *Mostly Harmless Econometrics: An Empiricist's Companion*. Princeton, NJ: Princeton University Press, 2008.
5. Angst, C.M.; Block, E.S.; D'Arcy, J.; and Kelley, K. When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly*, *41*, 3 (2017), 893–916.
6. Arora, A.; Krishnan, R.; Telang, R.; and Yang, Y. An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. *Information Systems Research*, *21*, 1 (2010), 115–132.
7. August, T.; and Tunca, T.I. Let the pirates patch? An economic analysis of software security patch restrictions. *Information Systems Research*, *19*, 1 (2008), 48–70.
8. August, T.; and Tunca, T.I. Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science*, *57*, 5 (2011), 934–959.
9. Baltagi, B. *Econometric Analysis of Panel Data*. John Wiley & Sons, New York, 2008.
10. Banker, R.D.; Kauffman, R.J.; and Morey, R.C. Measuring gains in operational efficiency from information technology: A study of the positran deployment at Hardee's Inc. *Journal of Management Information Systems*, *7*, 2 (1990), 29–54.
11. Basu, E. Target CEO fired - Can you be fired if your company is hacked?, *Forbes*, 15 June, 2014.
12. Baum, C.F.; Schaffer, M.E.; and Stillman, S. Enhanced routines for instrumental variables/GMM estimation and testing. *Stata Journal*, *7*, 4 (2007), 465–506.
13. Blau, P.M. *Inequality and Heterogeneity: A Primitive Theory of Social Structure*. Free Press, New York, 1977.

14. Braa, J.; Hanseth, O.; Heywood, A.; Mohammed, W.; and Shaw, V. Developing health information systems in developing countries: The flexible standards strategy. *MIS Quarterly*, *31*, 2 (2007), 381–402.
15. Bradley, R.V.; Byrd, T.A.; Pridmore, J.L.; Thrasher, E.; Pratt, R.M.; and Mbarika, V.W. An empirical examination of antecedents and consequences of IT governance in US hospitals. *Journal of Information Technology*, *27*, 2 (2012), 156–177.
16. Brown, C.V. Examining the emergence of hybrid IS governance solutions: Evidence from a single case site. *Information Systems Research*, *8*, 1 (1997), 69–94.
17. Brown, C.V.; and Magill, S.L. Reconceptualizing the context-design issue for the information systems function. *Organization Science*, *9*, 2 (1998), 176–194.
18. Bulgurcu, B.; Cavusoglu, H.; and Benbasat, I. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*, 3 (2010), 523–548.
19. Caruso, J.B. I*nformation Technology Security: Governance, Strategy, and Practice in Higher Education*. Educause Center for Applied Research, EDUCAUSE, 2003. https://library.educause.edu/resources/2003/10/information-technology-security-governance-strategy-and-practice-in-higher-education
20. Cavusoglu, H.; Cavusoglu, H.; and Zhang, J. Security patch management: Share the burden or share the damage? *Management Science*, *54*, 4 (2008), 657–670.
21. Cavusoglu, H.; Mishra, B.; and Raghunathan, S. The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, *16*, 1 (2005), 28–46.
22. Cerullo, V.; and Cerullo, M.J. Business continuity planning: A comprehensive approach. *Information Systems Management*, *21*, 3 (2004), 70–78.
23. Chong, J.L.; and Tan, F.B. IT governance in collaborative networks: A socio-technical perspective. *Pacific Asia Journal of the Association for Information Systems*, *4*, 2 (2012).
24. Collins, J.D.; Sainato, V.A.; and Khey, D.N. Organizational data breaches 2005-2010: Applying SCP to the healthcare and education sectors. *International Journal of Cyber Criminology*, *5*, 1 (2011), 794–810.
25. D'Arcy, J.; Hovav, A.; and Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*, 1 (2009), 79–98.
26. DeSanctis, G.; and Jackson, B.M. Coordination of information technology management: Team based structures and computer based communication systems. *Journal of Management Information Systems*, *10*, 4 (1994), 85–110.
27. Duncan, N.B. Capturing flexibility of information technology infrastructure: A study of resource characteristics and their measure. *Journal of Management Information Systems*, *12*, 2 (1995), 37–57.
28. Ferguson, C.; Green, P.; Vaswani, R.; and Wu, G.H. Determinants of effective information technology governance. *International Journal of Auditing*, *17*, 1 (2013), 75–99.
29. Firth, D. Bias reduction of maximum likelihood estimates. *Biometrika*, *80*, 1 (1993), 27–38.
30. Gal-Or, E.; and Ghose, A. The economic incentives for sharing security information. *Information Systems Research*, *16*, 2 (2005), 186–208.
31. Goode, S.; Hoehle, H.; Venkatesh, V.; and Brown, S.A. User compensation as a data breach recovery action: An investigation of the Sony Playstation network breach. *MIS Quarterly*, *41*, 3 (2017), 703–727.
32. Gordon, L.A.; Loeb, M.P.; and Lucyshyn, W. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, *22*, 6 (2003), 461–485.
33. Greene, W.H. *Econometric analysis*. Prentice Hall, Upper Saddle River, NJ, 2003.
34. Gwebu, K.L.; Wang, J.; and Wang, L. The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*, 2 (2018), 683–714.

35. Hasselbring, W. Information system integration. *Communications of the ACM*, *43*, 6 (2000), 32–38.
36. Heinze, G.; and Schemper, M. A solution to the problem of separation in logistic regression. *Statistics in Medicine*, *21*, 16 (2002), 2409–2419.
37. Holmstrom, B.; and Milgrom, P. Multitask principal-agent analyses: Incentive contracts, asset ownership, and job design. *Journal of Law, Economics, & Organization*, *7*, SP (1991), 24–52.
38. Hosmer, D.W.; Lemeshow, S.; and May, S. *Applied Survival Analysis: Regression Modeling of Time to Event Data*. Wiley, 2008.
39. Huang, P.; Ceccagnoli, M.; Forman, C.; and Wu, D.J. Appropriability mechanisms and the platform partnership decision: Evidence from enterprise software. *Management Science*, *59*, 1 (2013), 102–121.
40. Huang, R.; Zmud, R.W.; and Price, R.L. Influencing the effectiveness of IT governance practices through steering committees and communication policies. *European Journal of Information Systems*, *19*, 3 (2010), 288–302.
41. Hui, K.-L.; Ke, P.F.; Yao, Y.; and Yue, W.T. Bilateral liability-based contracts in information security outsourcing. *Information Systems Research*, *30*, 2 (2019), 411–429.
42. Huq, N. *Follow the data: Analyzing breaches by industry*. Trend Micro Analysis of Privacy Rights Clearinghouse, 2015. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data
43. Jensen, M.C.; and Meckling, W.H. Specific and general knowledge and organizational structure. In L. Werin and H. Wijkander (eds.), *Contract Economics*. Oxford: Blackwell, 1992, pp. 251–274.
44. Johnson, N.L. *Survival Models and Data Analysis*. John Wiley & Sons, New York, 1999.
45. Johnston, A.C.; and Hale, R. Improved security through information security governance. *Communications of the ACM*, *52*, 1 (2009), 126–129.
46. Kankanhalli, A.; Teo, H.-H.; Tan, B.C.; and Wei, K.-K. An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*, 2 (2003), 139–154.
47. Khey, D.N.; and Sainato, V.A. Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal*, *26*, 4 (2013), 367–382.
48. King, G.; and Zeng, L. Logistic regression in rare events data. *Political Analysis*, *9*, 2 (2001), 137–163.
49. King, J.L. Centralized Versus Decentralized Computing: Organizational Considerations and Management Options. *ACM Computing Surveys (CSUR)*, *15*, 4 (1983), 319–349.
50. Kotulic, A.G.; and Clark, J.G. Why there aren't more information security research studies. *Information & Management*, *41*, 5 (2004), 597–607.
51. Kshetri, N. Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, *11*, 4 (2005), 541–562.
52. Kwon, J.; and Johnson, M.E. Health-care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems*, *30*, 2 (2013), 41–66.
53. Kwon, J.; and Johnson, M.E. Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, *38*, 2 (2014), 451–472.
54. Lacity, M.C.; Khan, S.A.; and Willcocks, L.P. A review of the IT outsourcing literature: Insights for practice. *The Journal of Strategic Information Systems*, *18*, 3 (2009), 130–146.
55. Lance, C.E. Residual centering, exploratory and confirmatory moderator analysis, and decomposition of effects in path models containing interactions. *Applied Psychological Measurement*, *12*, 2 (1988), 163–175.
56. Lee, C.H.; Geng, X.; and Raghunathan, S. Mandatory standards and organizational information security. *Information Systems Research*, *27*, 1 (2016), 70–86.
57. Liu, C.Z.; Au, Y.A.; and Choi, H.S. Effects of freemium strategy in the mobile app market: An empirical study of google play. *Journal of Management Information Systems*, *31*, 3 (2014), 326–354.
58. Lorange, P. *Corporate Planning: An Executive Viewpoint*. Englewood Cliffs, NJ: Prentice-Hall, 1980.

59. McKeen, J.D.; Guimaraes, T.; and Wetherbe, J.C. The relationship between user participation and user satisfaction: an investigation of four contingency factors. *MIS Quarterly*, *18*, 4 (1994), 427–451.
60. Miller, A.R.; and Tucker, C. Privacy protection and technology diffusion: The case of electronic medical records. *Management Science*, *55*, 7 (2009), 1077–1093.
61. Miller, A.R.; and Tucker, C.E. Encryption and the loss of patient data. *Journal of Policy Analysis and Management*, *30*, 3 (2011), 534–556.
62. Moulton, R. Applying information security governance. *Computers and Security*, *22*, 7 (2003), 580.
63. Nash, K.S. Information Technology Budgets: Which Industry Spends the Most?, *CIO*, 2007. https://www.cio.com/article/2437731/information-technology-budgets–which-industry-spends-the-most-.html
64. Nault, B.R. Information technology and organization design: Locating decisions and information. *Management Science*, *44*, 10 (1998), 1321–1335.
65. Nolan, R.; and McFarlan, F.W. Information technology and the board of directors. *Harvard Business Review*, 83, 10 (2005), 96.
66. Patton, M. Battling data breaches. *Community College Journal*, *86*, 1 (2015), 20.
67. Pomerleau, M. Does a centralized approach help or hurt DOD cybersecurity?, Defense Systems, 2015. https://defensesystems.com/articles/2015/11/05/dod-cybersecurity-open-architecture-summit.aspx
68. Pulkkinen, M.; Naumenko, A.; and Luostarinen, K. Managing information security in a business network of machinery maintenance services business – Enterprise architecture as a coordination tool. *Journal of Systems and Software*, *80*, 10 (2007), 1607-1620.
69. Ransbotham, S.; and Mitra, S. Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research*, *20*, 1 (2009), 121–139.
70. Ransbotham, S.; Mitra, S.; and Ramsey, J. Are Markets for vulnerabilities effective? *MIS Quarterly*, *36*, 1 (2012), 43–64.
71. Raymond, L. Organizational context and information systems success: A contingency approach. *Journal of Management Information Systems*, *6*, 4 (1990), 5–20.
72. Rothrock, R.A.; Kaplan, J.; and Van Der Oord, F. The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*, 2 (2018), 12–15.
73. Sambamurthy, V.; and Zmud, R.W. Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly*, *23*, 2 (1999), 261–290.
74. Sen, R.; and Borle, S. Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*, 2 (2015), 314–341.
75. Shackelford, S.J. Protecting intellectual property and privacy in the digital age: The use of national cybersecurity strategies to mitigate cyber risk. *Chapman Law Review*, *19* (2016), 445.
76. Sidel, R. Target to settle claims over data breach. *The Wall Street Journal*, 18 August, 2015.
77. Snyder, T.D.; de Brey, C.; and Dillow, S.A. Digest of Education Statistics 2015. National Center for Education Statistics, Institute of Education Sciences, U.S. Department of Education Washington, DC, 2016.
78. Srivastava, S.C.; and Teo, T.S. Contract performance in offshore systems development: Role of control mechanisms. *Journal of Management Information Systems*, *29*, 1 (2012), 115–158.
79. Staiger, D.; and Stock, J.H. Instrumental variables regression with weak instruments. *Econometrica*, *65*, 3 (1997), 557.
80. Stanley, C.; Molyneux, E.; and Mukaka, M. Comparison of performance of exponential, Cox proportional hazards, weibull and frailty survival models for analysis of small sample size data. *Journal of Medical Statistics and Informatics*, *4*, 1 (2016).
81. Stock, J.H.; and Yogo, M. Testing for weak instruments in linear IV regression. In D.W.K. Andrews and J.H. Stock (eds.), *Ch. 5 Identification and Inference for Econometric Models: Essays in Honor of Thomas* J. *Rothenberg*. Cambridge University Press, New York, 2005.
82. Straub, D.W.; and Welke, R.J. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, *22*, 4 (1998), 441–469.

83. Tallon, P.P. A Process-oriented perspective on the alignment of information technology and business strategy. *Journal of Management Information Systems*, *24*, 3 (2007), 227–268.
84. Tallon, P.P.; Ramirez, R.V.; and Short, J.E. The information artifact in IT governance: toward a theory of information governance. *Journal of Management Information Systems*, *30*, 3 (2013), 141–178.
85. Thong, J.Y.; Yap, C.-S.; and Raman, K. Top management support, external expertise and information systems implementation in small businesses. *Information Systems Research*, *7*, 2 (1996), 248–267.
86. Tiwana, A. Systems development ambidexterity: Explaining the complementary and substitutive roles of formal and informal controls. *Journal of Management Information Systems*, *27*, 2 (2010), 87–126.
87. Tiwana, A.; and Kim, S.K. Discriminating IT governance. *Information Systems Research*, *26*, 4 (2015), 656–674.
88. Tiwana, A.; and Konsynski, B. Complementarities between organizational IT architecture and governance structure. *Information Systems Research*, *21*, 2 (2010), 288–304.
89. U.S. Bureau of Labor Statistics. Employment status of the civilian noninstitutional population, 1947 to date 2017. https://www.bls.gov/cps/cpsaat01.pdf (accessed March 17, 2018).
90. Warkentin, M.; and Johnston, A.C. IT security governance and centralized security controls. In M. Warkentin and R. Vaughn (eds.), *Enterprise Information Assurance and System Security: Managerial and Technical Issues*, Idea Group Publishing, Hershey, PA, 2006, pp. 16–24.
91. Weill, P.; and Ross, J. A matrixed approach to designing IT governance. *MIT Sloan Management Review*, *46*, 2 (2005), 26.
92. Weill, P.; and Ross, J.W. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Harvard Business Press, Boston, 2004.
93. Weill, P.; Subramani, M.; and Broadbent, M. Building IT infrastructure for strategic agility. *MIT Sloan Management Review*, *44*, 1 (2002), 57.
94. Wilkin, C.L. A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems*, *24*, 2 (2010), 107.
95. Wooldridge, J.M. *Econometric Analysis of Cross Section and Panel Data*. The MIT Press, Boston, 2002.
96. World Bank. World Bank GDP 1960-2016 2018. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD (accessed March 17, 2018).
97. Wu, S.P.-J.; Straub, D.W.; and Liang, T.-P. How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. *MIS Quarterly*, *39*, 2 (2015), 497–518.
98. Xue, L.; Ray, G.; and Gu, B. Environmental uncertainty and IT infrastructure governance: A curvilinear relationship. *Information Systems Research*, *22*, 2 (2011), 389–399.
99. Yerby, J.; and Floyd, K. Faculty and staff information security awareness and behaviors. *Journal of The Colloquium for Information System Security Education*, *6*, 1 (2018), pp. 23–23.

About the Authors

Che-Wei Liu (cwliu@iu.edu; corresponding author) is an Assistant Professor of Information Systems at the Kelley School of Business, Indiana University. He received his Ph.D. at the Robert H. Smith School of Business, University of Maryland. His research interests include business analytics, mobile health, and business value of IT. Specifically, his research addresses the impact of digital technologies on users' behaviors in mobile health, IT labor market, and stock market. His work has been accepted for publication in *Information Systems Research* and *Journal of Economic Behavior & Organization*.

Peng Huang (huang@umd.edu) is an Associate Professor of Information Systems at the Robert H. Smith School of Business, University of Maryland. He holds a Ph.D. from the College of

Management, Georgia Institute of Technology. His research interests include platform ecosystems, knowledge-sharing virtual communities, and as technology entrepreneurship. His recent work has appeared in such journals as *Management Science, Information Systems Research, MIS Quarterly, Journal of Marketing*, and *MIT Sloan Management Review*. He received the Sandra Slaughter Early Career Award from the Information Systems Society, the Kauffman Dissertation Fellowship from the Ewing Marion Kauffman Foundation, the Ashford Watson Stalnaker Memorial Prize at Georgia Tech, and multiple Best Conference Paper Awards at the International Conference on Information Systems.

Henry C. Lucas, Jr. (hlucas@rhsmith.umd.edu) is the Robert H. Smith Professor Emeritus of Information Systems at the Robert H. Smith School of Business, University of Maryland. He received his Ph.D. from the Sloan School of Management, M.I.T. Dr. Lucas is the author of 20 books and nearly 100 articles in professional periodicals on the impact of information technology (IT), the value of investments in technology, implementation of IT, decision-making for technology, and IT and corporate strategy. His most recent research concerns technology-enabled transformations and disruptions. Dr. Lucas has served on the faculties of Stanford and NYU and has taught at INSEAD in France and NTU in Singapore on sabbaticals.