Journal of Forensic and Investigative Accounting
Volume 11: Issue 3, July–December 2019

Predicting Reported Cybersecurity Breaches Using Financial Measures

Nishani Edirisinghe Vincent
*John Trussel**

I. Introduction

> *"In recent months, cybersecurity has become a top concern to American companies, regulators, and law enforcement agencies. This is in part because of the mounting evidence that the constant threat of cyber-attack is real, lasting, and cannot be ignored. There is no doubt that the SEC must play a role in this area. What is less clear is what that role should be…However, the increased pervasiveness and seriousness of the cybersecurity threat raises questions about whether more should be done to ensure the proper functioning of the capital markets and the protection of investors."* (SEC Commissioner Luis A. Aguilar, March 26, 2014)

An ISACA (2015) survey reports a forty-eight percent increase of cybersecurity breaches from 2013 to 2014. Further, in a recent survey (ISACA, 2018), fifty percent of survey respondents report that their enterprise experienced more security attacks in 2017 compared to the previous year. Due to the increasing threat, cybersecurity has become an important issue among executive managers, boards of directors, and regulators. Cybersecurity risk can stem from management decisions that impact any area of the firm. Management decisions that change the firm's environment can directly and indirectly affect a firm's IT environment, which consists of IT systems, IT architecture, infrastructure, IT processes, and human resources. Therefore, firms can experience a cybersecurity breach as a result of information technology (IT) and other enterprise risks in other areas.

For example, the incident at Equifax in 2017 that impacted 146 million U.S. citizens resulted from not communicating and running a patch on an application in a timely manner (Bernard and Cowley, 2017). Since extant IT/Information Systems (IS) literature shows that management decisions on IT directly or indirectly affect a firm's performance and, therefore, are reflected in the financial statements (Bharadwaj, 2000; Santhanam and Hartono, 2003; Chae et al., 2014), financial statements may also provide some insights into a firm's IT environment by indicating whether a firm has the necessary resources to invest in technology to minimize risks and optimize IT opportunities in subsequent years. Therefore, we suggest that financial measures can be used to predict a firm's potential IT risk exposure and likelihood of experiencing a cybersecurity breach.

Given the dire consequences of a materialized IT risk exposure through a cybersecurity incident, various stakeholders demand information about a firm's IT risks. Hence, the Securities Exchange Commission (SEC) is currently concerned about the adequacy of the financial statement disclosures. Since reported cybersecurity breaches have negative effects on a firm's performance through loss of reputation, loss of customers, and increased remediation costs, the SEC has recognized management's responsibility to various stakeholders in disclosing such information in their annual and quarterly reports. The SEC held a roundtable discussion in March 2014, to specifically discuss cybersecurity and its effects on financial statement disclosures. In February 2018, the SEC released interpretive guidance on cybersecurity disclosure requirements stating that firms should consider the impact of IT in their internal control assessment and risk factor disclosures. Cybersecurity is only one component of IT risk; hence, the SEC is not only concerned specifically about cybersecurity disclosures, but also about IT risk disclosures in general. Further, the SEC realizes that cybersecurity disclosures are a balancing act and therefore advises firms to maintain transparency, but not at the cost of disclosing too much information that helps hackers penetrate existing systems.

Campbell et al. (2014) address the SEC's concern whether firm disclosures are boilerplate and find that risk factor disclosures are firm specific and useful to the investors. Li et al. (2018) further investigate cybersecurity risk disclosures pre- and post-SEC guidance in 2011 and find that the presence and length of risk factor disclosures in the pre-guidance

*The authors are, respectively, assistant professor and professor at University of Tennessee at Chattanooga.

period are related to future reported cybersecurity incidents. However, they do not find this association in the post-guidance period. They interpret these results to indicate that firms are disclosing more information even though there is no material cybersecurity risk. However, they also do not find an association between firm specific cybersecurity disclosures and future cybersecurity incidents. If stakeholders cannot make inferences about cybersecurity risk based on risk factor disclosures even though they are firm specific, can financial statement information be used to make inferences about management decisions on IT and hence infer the likelihood of cybersecurity risks?

Since financial statements convey useful information about a firm's current financial position, changes to the financial position, and performance, these statements should also provide insights into management decisions that impact the firm in the long-term. Consequently, financial statements can also provide information about management decisions on IT and the complexity of the firm's IT environment. Higgs et al. (2017) propose a propensity score to predict the probability of a cybersecurity breach. Therefore, we use a similar approach and explore 1) whether financial measures are associated with future cybersecurity breach and 2) whether financial measures can be used to develop a predictive model that can be used to make inferences about the likelihood of a cybersecurity breach.[1] [See Figure 1, pg. 518]

In this paper, we posit that the likelihood of a cybersecurity breach is a function of management decisions about a firm's business strategy and IT use. Thus, we develop a model to predict reported cybersecurity breaches using financial measures that reflect a firm's strategic choices and IT use. Figure 1 summarizes the rationale for model development using financial measures. These relationships will be further discussed in the model development section. Given the proliferation of IT in business operations, strategic decisions directly and indirectly influence a firm's use of technology. Consequently, as the firm becomes more dependent on technology, the number of IT components will increase causing the firm's IT environment to become more complex. If the firm experiences a change in the IT environment as a result of strategic decisions, these changes would be reflected indirectly through the events reported in the financial statements. Therefore, we use complexity theory to identify financial measures that indicate a change to the composition of the firm's IT components/environment.

The more complex the IT environment the more likely the firm will have unobserved sources of IT threats. These unobserved IT threats can be used by various cyber criminals to gain access to a firm's information system. As in the Equifax example noted above, when the number of applications maintained by a firm increases (i.e., complexity of the IT environment increases), as a result of growth for example, the likelihood of overlooking a significant patch release is higher. This may be due to a lack of IT staff to oversee all applications, an overwhelming number of patch releases per application, an increase in undocumented applications maintained by users, etc. Consequently, hackers can use known vulnerabilities in unprotected applications to gain unauthorized access to a firm's information system. Vincent et al. (2017) find that there is a gap in a firm's IT risk exposure and the maturity of IT risk management practices. This finding implies that firms do not keep abreast with IT risk management as the complexity of the firm's IT environment increases. Therefore, a firm with a more complex IT environment will have higher cybersecurity risk, and higher risk exposure will lead to a higher likelihood of having a cybersecurity breach.

Based on existing research and complexity theory, we suggest growth, acquisitions, restructuring, leverage, concentration of segment revenues, size, and operating profits reflect the strategic choices of a firm, hence the complexity of a firm's IT environment. Based on these measures we develop a model to predict reported cybersecurity breaches. Figure 2 summarizes the operationalization of our theoretical model and the expected associations. We will fully develop this model and these relationships in the remainder of the paper. [See Figure 2, pg. 519]

We obtain financial measures for firms with reported cybersecurity breaches and a sample of firms with no reported cybersecurity breaches. We find that growth, concentration of segment revenues, size, and operating profit are positively associated with reported cybersecurity breaches. The sector to which a firm belongs also plays a significant role with relatively more reported breaches in the telecommunications and information technology sectors than other sectors. However, a firm's restructuring charges and relative amount of debt are not associated with of the likelihood of reported cybersecurity breach. Mergers and acquisitions are significantly and negatively associated with reported cybersecurity breaches. Further, the predictive model based on financial measures correctly categorizes up to eighty-eight percent of firms as either having a reported cybersecurity breach or not.

[1] Risk assessment considers two aspects (i.e., the impact and the likelihood). Throughout this paper, we refer to the likelihood of occurrence when we mention cybersecurity risks. Since firms will have some controls implemented, we make the distinction between risk and risk exposure. Risk exposure is the firm's exposure after controls are implemented.

The proposed model and findings contribute to the management and IT governance literature and the profession. The results contribute to the IT governance and management literature by identifying financial measures that reflect the complexity of the IT environment. Researchers can use the proposed financial measures as a proxy for the complexity of the IT environment in extending our understanding of IT governance in firms. Further, we contribute to the complexity theory literature by applying complexity theory to identify financial measures that reflect IT environment complexity.

Our contribution to the profession is twofold. First, we contribute to the ongoing discussions on disclosures on cybersecurity and other IT risks. In interpretive guidance (SEC, 2011), the SEC clarifies that technology risk disclosures should be specific to the firm. However, disclosing technology related risks may have unanticipated dire consequences. Therefore, managers should balance the technology risk disclosures in a manner that does not increase the opportunities for cyberattacks and reduce competitive advantage, while maintaining transparency for investors. The Division of Corporation Finance staff within the SEC continues to highlight the importance of this issue and to discuss whether additional disclosures should be imposed on firms on cybersecurity risks (SEC, 2011; 2018). However, the findings of this paper suggest that existing disclosures and financial statements provide adequate information to make preliminary inferences about the firm's cybersecurity risk exposure.

Second, we develop a predictive model. Outside stakeholders, such as investors, can use the model to make initial predictions about a given firm. Given the increase and the inevitability of cybersecurity incidents, the risk model can help insurance firms, analysts, forensic investigators, valuators and other stakeholders assess the cybersecurity risk of the firm.

The subsequent sections are as follows. Section II provides a literature review, defines the complexity of the IT environment and cybersecurity risk exposure, and develops the predictive model. Section III describes the data and the research design. Section IV provides empirical testing. Discussion and conclusions are provided in Section V.

II. Literature Review And Model Development

Since risk of cybersecurity is a function of the firm's IT environment (as indicated in Figure 1), we use complexity theory to identify the instances that cause complexity within the IT function. Therefore, in this section, we discuss relevant literature on cybersecurity risk, complexity theory and financial measures that would reflect IT environment complexity.

Cybersecurity Risk

The International Telecommunication Union (ITU) defines cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization, and user's assets" (ITU-T X.1205).[2] Consequently, cybersecurity risk is not one specific risk but a combination of risks which differ based on technology, firm's culture, processes, actors, etc. Further, cybersecurity risk can be seen as a component of information security risk, which in turn is a component of IT risk. Extant literature explores the optimum level of investment to manage different types of information security threats (Huang et al., 2008), various frameworks for information security risk management (Webb et al., 2014), and board involvement in setting information security strategy (McFadzean et al., 2007), to name a few. Li et al. (2018) find that post-SEC guidance in 2011, cybersecurity risk disclosures are not associated with future reported cybersecurity incidents. If firms are disclosing too much information, as Li et al. suggest, their findings question the value relevance of the cybersecurity disclosure. This finding also poses an intriguing question whether there is an indirect way to make inferences about the IT environment using financial measures.

Complexity Theory and IT Environment Complexity

Complexity theory suggests that various components within a large system use feedback loops to gain experience and organize themselves to bring order to the system over time (Thompson, 1967). A firm can be viewed as a complex system with many different components such as structures, departments, and people groups. Hence, a complex IT environment, defined as a "set of interdependent parts, which together make up a whole that is interdependent within some larger environment" (Thompson, 1967 p. 6), can be seen as a product of a diversity of footprints, tools, and workforce (Baldwin,

[2] Definition retrieved from https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

2015).[3] According to Chief Information Officers (CIO), the complexity of the IT environment increases as a result of impractical/imprudent demands from the business, leftover systems from mergers, acquisitions, and internal reorganizations, multiple systems, undocumented knowledge of the technology in place, multiple systems conducting the same function, illogical architectures etc. (Baldwin, 2015).

Anderson (1999) suggests that firm complexity can be measured along three dimensions: 1) vertical complexity—the number of levels in an organizational hierarchy, 2) horizontal complexity—the number of job titles or departments across the firm, and 3) spatial complexity—the number of geographical locations. Therefore, these dimensions can be used to identify the firm's IT environment complexity. Vertical complexity can arise as a firm grows. Growth and size influence firms to have structured organizational hierarchy for better control. For example, to facilitate increased sales, firms may hire more employees, use technology to expedite production, leading to an increased need for supervision, separation of duties etc.[4] Horizontal and spatial complexity may increase when firms engage in mergers and acquisitions. Another firm event that can cause complexity is restructuring which reorganizes firm components. When firm's components are rearranged, the firm induces complexity by changing when, where, what, and how each component communicates with each other. The rearranged components now have to learn to interact differently with new neighboring components which increases the complexity. Further, restructuring may induce vertical and horizontal complexity by changing the number of departments, organizational hierarchy, and job titles. Firms may engage in vertical or horizontal integration which could result in increasing the number of segments. Further, as the number of segments (brand names/product lines) increases, horizontal and spatial complexity will increase through increasing job titles, departments, and/or locations.

According to complexity theory, complex system components learn overtime and evolve to a point that will benefit the firm (Warfield, 1999). However, for these components to learn, evolve, and maintain a self-organized state, firms have to inject energy into the system. In the context of IT, for a firm to attain equilibrium, IT needs more funding (energy) to address integration of systems so that new components added to the system can communicate and be incorporated into the existing IT architecture and infrastructure. Warfield (1999) suggests that every activity has a corresponding set of limits which determines the feasible extent of that activity. Consequently, one aspect of the firm that will induce such a limitation on IT funding would be leverage. Since the firm's ability to borrow and the level of debt may affect firm's investment decisions on upgrades, system integration, sophisticated IT equipment etc., leverage can influence a firm's IT environment complexity. Moreover, operating profits can also be considered as a source of energy. As a firm makes profits, a portion of the profit is retained and injected back into the firm to increase future performance. Consequently, a firm's operating profits enable more investments in IT systems, upgrades, staff, etc., increasing the complexity.

The extant literature in project management has established the association between complexity and risk. Qazi et al. (2016) demonstrate the importance of considering complexity as a factor when identifying risks associated with projects. Further, Taylor et al. (2012) develop a model of complexity and risk and suggest that complexity of the project is an important consideration in evaluating and responding to risks. Taylor et al. (2012) and Shenhar (2001) attribute high scores on complexity of customization/configurations, data conversions, application interface, external project/process dependencies, and span of impact likely to be associated with uncertainty.[5] Given the established association between complexity and risk, next we explain why financial measures would reflect IT environment complexity and identify financial measures that reflect this complexity.

IT and Financial Measures

Extant literature on IT and firm performance finds that IT positively affects firm performance and that the association is conditional on environmental and technical factors.[6] Thus, the firm and IT environments impact firm performance. Kobelsky et al. (2008) explore the determinants of a firm's IT budget and find that organizational factors (operating profit, leverage

[3] The International Foundation for Information Technology defines an IT environment as "a controlled and often repeatable configuration or set of configurations that are perceived to act as a contained, bordered or surrounding operational context and that allow one or more entities such as resources or systems to perform one or more controlled functions or activities (IF4IT 2009)".
[4] We further explain how growth, mergers and acquisition, restructuring, leverage and segments may explain IT environment complexity when developing the proxies for IT complexity in Section III.
[5] The link between IT complexity and cybersecurity incidents (risk) is depicted in Figure 1.
[6] See Lim, Dehning, Richardson, and Smith (2011, 154) for a detail list of studies exploring the association between IT and firm performance.

and growth), environmental factors (concentration, uncertainty, and diversification), and technological factors (industry strategic IT role, and high and low-tech industry) influence IT budget levels and in turn influence future firm performance.

Since the relationship between IT and firm performance is somewhat complex, the impact of IT decisions may not be reflected in the current year performance. For example, development of a new application may decrease profits as a result of the requirement to expense research and development costs but may have a positive influence in productivity of the future years. Lim et al. (2011) argue that the definition and measurement of IT investment (i.e., IT strategy, IT capability, or IT spending) and firm performance (market measures vs. accounting measures) may influence the strength of the relationship between IT investment and firm financial performance, and they find the relationship to be stronger for process level accounting measures than for market measures. This finding suggests that accounting measures reflect firms' IT decisions.[7] Higgs et al. (2017) used a breach propensity score including firm performance measures. However, they have not provided a rationale as to the inclusion of the variables. Therefore, we develop a formal model using complexity theory to identify financial measures that reflect IT environment complexity.[8]

III. Research Design and Sample Selection

Based on extant literature and complexity theory, we posit that certain financial measures reflecting IT environment complexity are associated with the likelihood of cybersecurity breach. Our measure for the likelihood of cybersecurity breach is whether the firm has a reported cybersecurity breach or not in the subsequent year. Based on complexity theory, we identify seven financial measures (growth, acquisitions, restructuring, leverage, concentration of segment revenues, size and operating profits) that reflect vertical, horizontal, spatial and energy that influence complexity of the IT environment.[9] We discuss these predictor variables, as well as the data selection process in this section.

Growth

Sales growth in firms such as Walmart and Target cause these firms to spend more on IT to provide support for the increased demand for online shopping (Wahba, 2016, 2017). Growth not only impacts primary activities in a value chain, such as inbound, outbound logistics, sales, marketing, and operations, but also impacts support functions, such as human resources and infrastructure. Consequently, a growing firm will need better systems for tracking primary activities as well as support activities. An increase in customer base requires better systems to track sales orders, shipments, billing, and cash collections. Additionally, a firm's growth will lead to more hiring, consequently, create a need for better record keeping, coordination, communication, performance evaluation, and monitoring. Consequently, firms will have to consider systems implementation and integration, increase hardware and software utilization, and increase internet enabled network capacity.

However, growth also imposes constraints on the firm's resources. Since, the firm has to decide between various investments, Kobelsky et al. (2008) find that growth is negatively associated with IT budget levels. They argue that IT managers may have difficulty justifying IT investments when growth creates other investment opportunities. Consequently, managers may be pressured to present IT investment opportunities that will support growth rather than investments necessary for IT control. With more IT investments to support growth, firms will increase IT environment complexity. Further, when the IT environment complexity increases without adequate IT controls, cybersecurity risk exposure will increase as a result of the demand placed on solutions, staff, and infrastructure. Therefore, we anticipate that a firm's growth will be positively associated with reported cybersecurity breach. Year over year growth in total sales is used as a proxy for the firm's growth. Sales growth (GROWTH) is calculated as (total sales $_{i,t-1}$ - total sales $_{i, t-2}$)/total sales $_{i, t-2,}$ where t indicates the current year for firm i.

Mergers and Acquisitions

Firms engage in mergers and acquisitions for various strategic reasons, such as to increase market share, pool resources, create synergies, and control supply chain through vertical integration. However, mergers and acquisitions can also increase IT environment complexity (Siwicki, 2017). Buck-Lew et al. (1992) explain how IT environment is interrelated with many

[7] The findings from the extant literature is summarized in the links between business strategy, to IT complexity and firm performance as depicted in Figure 1.

[8] For parsimony we exclude governance variables and focus only on financial measures here.

[9] Since we are developing a predictive model, all proxy measures considered are lagged variables. We explore whether the previous year's growth, mergers and acquisitions, restructuring, leverage, segments, size, and operating profits will predict cybersecurity risk exposure for the current year.

aspects of the business and demonstrate that the importance of IT (IT infrastructure, people, and the quality of information) fit affects the success of the merger/acquisition. For instance, two financial institutions that merge will have two different information systems. Once the firms have merged, management must decide whether to enforce one system on the other, to implement a new system altogether, or to maintain two different systems, while developing interfaces for information sharing between the merged firms.

Chang et al. (2014) demonstrate the importance of information systems integration for successful mergers and acquisitions. In spite of the decision, mergers and acquisitions introduce complexity to the firm's IT environment by introducing new (or perhaps outdated) technology, infrastructure, hardware, software, and expertise. For example, after Delta acquired Comair in 1999, Comair's crew management system crashed, costing the parent company approximately twenty million dollars, damaging the airline's reputation and prompting an investigation by the Department of Transportation (Overby, 2005).

Even after performing due diligence in mergers and acquisitions, firms may still face challenges when trying to integrate, maintain, upgrade, and support legacy or new systems due to a lack of expertise and skills in the acquired technology. The substantial investment in IT after mergers and acquisitions to acquire new skills and technology may increase the firm's IT environment complexity. When the firm's IT environment becomes more complex, the ability to keep abreast with system, network, and infrastructure support, maintenance, change management, and upgrades can become challenging. Consequently, firms may be slow to implement IT risk management practices, and IT threats may go undetected. Therefore, we suggest that firms that experience mergers and acquisitions will have a more complex IT environment and, therefore, a higher likelihood of a cybersecurity breach. We use the amount invested in mergers and acquisitions$_{(t-1)}$ scaled by total assets$_{(t-1)}$ to measure mergers and acquisitions (ACQUISITIONS).

Restructuring

Corporate restructuring is "the process by which firms renegotiate or rewrite the financial contracts—both written and unwritten—that they have entered into with their stakeholders, including creditors, shareholders, employees, suppliers and customers" (Gilson, 2010, p. xv). Firms may engage in restructuring as a preemptive measure or as a last resort and may involve reducing a firm's debt, improving financial performance, exploiting new opportunities, improving market valuations, cutting operating expenses, acquiring assets, or changing the firm's equity ownership structure (Gilson, 2010).

Outsourcing the IT function is a method of restructuring that changes the IT environment. Gewald et al. (2006) find that managers are more willing to outsource business processes that they perceive to be risky. Florin et al. (2005) mention that some IT outsourcing strategies have preceded costly restructuring efforts and find that the market reacts negatively to restructuring charges after an IT outsourcing announcement. They also find that the long-term effect of IT outsourcing decisions on market value is dependent on the degree of organizational restructuring. Even though a decision to outsource IT can reduce the complexity of the IT function, the market's negative reaction to subsequent restructuring charges raises the question whether the complexity of the IT environment was actually reduced or whether it was transformed to an unobservable complexity.

Firms may engage in restructuring with the objective to lower operating costs, increase automation, improve financial performance, and exploit new opportunities. These restructuring attempts today involve the use of IT which increases the firm's dependence on IT. Dopson and Stewart (1993) conclude that firms invest in IT as the means to restructure. Mulligan and Gordon (2003) describe that the need for improved communication across services, better document flows, and better sharing of information about customers creates a need for continuous restructuring in the financial services industry. Consequently, more firms are increasing IT investments to facilitate restructuring and increase information flow throughout the firm by implementing new technology/system, integrating systems/networks with new interfaces, expanding the infrastructure to allow for increased demand on IT, and increasing access to information systems for better information sharing, which in turn increases IT environment complexity. With increased information sharing, system access points, integration etc., the firm will be more vulnerable to cyber risks after restructuring activities. Consequently, we conjecture that a firm engaging in restructuring activities will have a higher likelihood of cybersecurity breach. Restructuring is measured using the reported restructuring costs$_{(t-1)}$ scaled by total sales$_{(t-1)}$ (RESTRUCTURING).[10]

Leverage

[10] Since firms do not consistently report restructuring chargers with regard to IT, we use total restructuring charges reported in the annual reports.

Kobelsky et al. (2008) investigate various firm-level factors that directly influence the firm's IT budget level. Their findings suggest that the level of debt in the firm has a direct impact on the firm's IT budget. They argue that debt constrains management's ability to invest in other areas such as IT; hence, debt is negatively associated with IT budget amounts. Consequently, when the firm's internally generated funds are allocated towards debt obligations, management has less discretion and ability to allocate funds towards IT expenditures. Therefore, lack of funds for IT may force the firm to shirk on upgrading existing systems, hiring and maintaining IT staff, and implementing new processes and technology for IT risk management. Inability to provide and maintain adequate IT services due to a lack of funds increases the complexity of the IT environment by delaying upgrades on existing systems to a version with more advanced preventive, detective, and monitoring controls, shirking on proper change management procedures due to lack of staff, and overworking IT staff. Consequently, having to monitor legacy systems, not having control over system changes, and overworked staff will increase the IT environment complexity, and hence, cybersecurity risk exposure for the firm. Therefore, we postulate that leverage is positively associated with a likelihood of cybersecurity breach. We employ the commonly used debt ratio to indicate a firm's leverage. The debt ratio (LEVERAGE) is calculated by dividing total liabilities$_{(t-1)}$ by total assets$_{(t-1)}$.

Concentration of Segment Revenues

An operating segment is "a component of an entity that engages in business activities from which it may earn revenues and incur expenses; whose operating results are regularly reviewed by the entity's chief operating decision maker to make decisions about resources to be allocated to the segment and assess its performance; and for which discrete financial information is available (FAS, 131; PwC, 2008)". As the number of operating segments increases a firm's operating environment becomes more complex as a result of the increased need to gather and share information about each segment among the business units (Mihailovic et al., 2010). Therefore, IT systems need to be integrated in order to provide adequate information to management at varying detail. One major challenge IT departments face today is dealing with systems that grow organically. As a firm's operations increase, firms add components to the existing system without taking the time or spending the money to redesign their IT architecture, infrastructure, and systems (Gruman, 2007). Further, Liu et al. (2008) find diversification (different business segments) is positively associated with IT investment, indicating a need to increase IT spending when different segments are added to the firm. Increased investment (either on new systems or new components) increases complexity of the IT environment. We use concentration of segment revenues, rather than number of segments, to measure the complexity of the IT environment surrounding a firm's segments. We develop an index of the concentration of segment revenues (CONCENTRATION) by summing the square of sales of each segment to total segment sales (Trussel and Greenlee, 2004). Concentration of segment revenues better captures the relative size of each segment. Suppose that there are two firms that each has two segments with a combined revenue of $100 million. The two segments in firm A have the same revenues, fifty million dollars each. In firm B, one segment has revenues of ninety million dollars and the other has ten million dollars. If we used the number of segments to measure IT complexity, then the two firms would have equal complexity with two segments each. However, firm B is likely to have a less complex IT environment, given the relatively small size of the second segment. Firm A's concentration index is 0.50, while firm B's concentration index is 0.82.[11] The index would be 1.0 if there was only one segment and would approach zero with several segments. Therefore, we anticipate that concentration of segment revenues (i.e., the revenue concentration index) is negatively associated with the firm's risk exposure.

Firm Size

Firm size is another major factor that determines the level of IT use in a firm. Chandran and Rasiah (2013) find that firm size is related to technology capability and firm performance. Since larger firms have a greater need for IT assets and have more resources to invest in IT assets such as hardware, software, and infrastructure, larger firms will have a more complex IT environment than smaller firms. Firm size will also have an impact on the amount of data collected, stored, and distributed as a result of having a larger customer base, more human resources, more communication channels etc. Due to higher IT asset utilization, increased number of access points to a system, and multiple sources used for data collection, the firm's IT environment complexity will increase which in turn will increase the cybersecurity risk exposure. Further, in recent years, many security breach incidents have been targeted towards large firms such as Target, JP Morgen Chase, Equifax, and Marriot. Therefore, we posit that the size of the firm is positively related to the firm's cybersecurity risk exposure. We measure SIZE as the natural log of total sales$_{(t-1)}$.

[11] See formula in Table 1. Firm A = $(50/100)^2 + (50/100)^2 = 0.50$. Firm B = $(90/100)^2 + (10/100)^2 = 0.82$.

Operating Profit

Rather that debt financing, firms may also use internally generated funds as a means of financing. Operating profit is a good indicator of the amount of internally generated funds. Further, when a firm has internally generated funds, management has the ability to make discretionary investments in technology. Kobelsky et al. (2008) find that operating profits are positively associated with IT budget levels. Extending this finding, we suggest that when a firm has operating profits, the firm's management has the ability to invest in technology. These investments will increase the complexity of the IT environment by adding more IT assets. An increase in IT assets will in turn lead to increased IT risk exposure because the firm will have more IT assets that need safeguarding, which will in turn increase cybersecurity risks. Therefore, we theorize that operating profits are positively associated with the firm's cybersecurity risk exposure. We measure PROFIT as net operating income$_{(t-1)}$ to total sales$_{(t-1)}$.

Sector—Control Variable

IT risk might vary based on the sector membership of the firm. For example, a firm in the financial services sector is more likely experience a breach than a firm in the materials sector. Therefore, we include sector as a control variable in our model. The predictor variables are summarized in panel A of Table 1. [See Table 1, pg. 520]

Sample Selection

We searched the privacy rights clearinghouse database using the firm name to identify Fortune 500 firms that have reported a security breach from 2005 to 2015.[12] From the search we also obtained the date of the reported breach. Using the breach date, we identified the fiscal year of the breach. Data for growth, acquisitions, restructuring, leverage, concentration of segment revenues, size and operating profits were obtained from Compustat for all firms listed on the Fortune 500 for the years 2005–2015 (breached and non-breached firms). We merged the files for all of the years to create a cross-sectional longitudinal (panel) data set. The firms in the Fortune 500 vary slightly from year to year; thus, there are more than 500 firms that made the list throughout the eleven-year sample period.

Panel B of Table 1 displays the final sample of firms by sector and status (breach or not). The consumer discretionary sector has the highest number of firms that experienced data breaches, while the telecommunications sector has the highest percentage of firms in the sample with reported data breaches. In fact, the telecom sector had nearly three times the rate of reported data breaches as the next highest sector, the information technology sector, and over four times the rate of all firms in the sample. The varying rate of data breaches among the sectors supports our use of sector as a control in our model.

IV. Results

The Univariate Profile of Cybersecurity Risk

Table 2, Panel A displays the descriptive statistics for all of the indicators of complexity of the IT environment from Table 1 segregated by status (data breach or not). Also displayed are the results of the t-tests on the differences of the means of each indicator by status. The results suggest a (univariate) financial profile of a firm at risk of data breach. At the five percent significance level, firms with IT breaches have fewer acquisitions, have higher concentrations of segment revenues (CONCENTRATION), are larger (SIZE) and have higher profit margins (PROFIT). There are no significant differences in growth, restructuring charges or the relative amount of debt between the two groups of firms at the univariate level.

Panel B of Table 2 includes the Pearson correlation coefficients for the independent variables. Although some of the coefficients are statistically significant, the magnitude of their correlations does not give rise to concerns about multicollinearity for the regression model. [See Table 2, pg. 521]

The Multivariate Model of IT Risk

Our hypothesis is that the financial measures (summarized in Table 1) are associated with the likelihood of a reported cybersecurity breach. We use logistic regression and adjust the panel data for autocorrelation by assuming that repeated

[12] Privacy rights clearinghouse provides a database of data breaches publicized since 2005. The link to the website is as follows https://www.privacyrights.org/data-breaches

measurements have a first-order autoregressive relationship.[13] The correlation between any two elements is equal to rho for adjacent elements, rho-squared for elements that are separated by a third, and so on.[14]

The underlying latent dependent variable is the firm's cybersecurity risk exposure, which is the probability of experiencing a data breach for firm *i*. This probability is related to the observed variable, $Status_i$, through the relation:

$Status_i$ = 1, if the firm reported a data breach, and
$Status_i$ = 0, otherwise.

Logistic regression using all the proxies for IT environment complexity predicts the probability of cybersecurity risk exposure for the k^{th} status for firm *i* as $P(Status_{ik})$ and is calculated as:

$$P(Status_{ik}) = \frac{1}{1+e^{-Z}} \quad (1)$$

where:

$Z_i = \beta 0 + \beta 1\ GROWTH_{t-1} + \beta 2\ ACQUISITIONS_{t-1} + \beta 3\ RESTRUCTURING_{t-1} + \beta 4\ LEVERAGE_{t-1} - \beta 5\ CONCENTRATION_{t-1} + \beta 6\ SIZE_{t-1} + \beta 7\ PROFIT_{t-1} + \beta 8\ SECTOR$

The estimation sample consisting of half the data set (used to develop the model) is randomly selected from the original sample. The other half of the data set (the holdout sample) is used to test the model. The results of the logistic regression model are shown in Table 3. Overall, the corrected quasi-likelihood under independence model criterion (QIC) value of 803.9 indicates the model fits the data well. As hypothesized, three indicators, GROWTH, SIZE, and PROFIT, are positively associated with cybersecurity risk and are statistically significant at less than the 0.05 level. CONCENTRATION also has a significant positive association with cybersecurity risk, which contradicts our hypothesized direction. ACQUISITIONS are marginally significant ($p<0.10$) and negatively associated with cybersecurity risks. RESTRUCTURING and LEVERAGE are not statistically significant in the model. Thus, controlling for the other indicators and as expected, firms experiencing a data breach have significantly higher growth rates, more segment concentration, higher revenues and larger profit margins than their counterparts that had no IT breaches. Also, firms that have IT breaches have marginally fewer acquisitions. However, a firm's level of debt financing and restructuring costs do not significantly contribute to the regression model. [See Table 3, pg. 522]

Predicting Data Breaches

Logistic regression is used to test the predictive ability of the model. The observed logistic regression equation (from Table 3, time subscripts not shown) for entity *i* at time *t* is:

$P(i,t) = 1/(1+e^{-Zi})$

where:

Z_i = -7.181 + 0.262 GROWTH – 3.045 ACQUISITIONS - 0.287 RESTRUCTURING - 0.721 LEVERAGE + 1.383 CONCENTRATION + 0.587 SIZE + 0.282 PROFIT – 3.372 Energy Sector – 3.481 Materials Sector - 1.264 Industrials Sector – 1.352 Consumer Discretionary Sector - 1.352 Consumer Staples Sector - 1.431 Healthcare Sector – 4.736 Financials Sector – 0.895 Info Tech Sector - 0.946 Telecom Sector – 2.000 Utilities Sector

The predicted dependent variable, the probability of a data breach for firm *i*, is computed using the actual indicators for each firm in the sample. The resulting probabilities are used to classify firms as at risk of data breach or not. Jones (1987) suggests two ways of adjusting the cutoff probability for classifying as at risk or not at risk of data breach. First, the prior probability of data breach is incorporated, and second, the expected cost of misclassification is included. We apply a similar methodology used by Trussel and Patrick (2009 and 2013).

When using logit, the proportion of at-risk firms in the sample must be the same as the proportion in the population to account for the prior probability of a data breach. If the proportion is not the same, then the constant must be adjusted

[13] Since the dependent variable is categorical (a firm had a breach during the sample period or not) logistic regression is an appropriate analysis.
[14] Making other assumptions about the relationship do not change the tenor of the results.

(Maddala 1991).[15] Since the proportion of at risk firms in the population of all firms is unknown, we assume that the proportion of firms in the sample that had a data breach is an unbiased estimator of the proportion in the population of all firms. Since four percent of the firm-years in the sample had a data breach, the prior probability of a data breach is assumed to be 0.04.

The ratios of the cost of Type I errors (incorrectly classifying firms with data breaches as not having data breaches—a false positive) to Type II errors (incorrectly classifying firms that had no data breaches as firms that had data breaches—a false negative) also must be determined. The particular cost function is difficult to ascertain and will depend on the user of the information. In most applications, the cost of a Type I error is much greater than a Type II error. For example, a creditor may want to minimize loan losses (and thus Type I error) by not lending to a firm that will have a data breach; however, he or she will suffer an opportunity cost (Type II error) by not lending to a firm that will not have a data breach if credit is granted to another borrower at a lower rate. Thus, we incorporate several relative cost ratios (and cutoff probabilities) into our analysis. Specifically, we include the relative costs of Type I to Type II errors of 1:1, 10:1, 20:1, 25:1, 30:1, 50:1, and 100:1 (Beneish, 1999; Trussel, 2002).

The results of using the logit model to classify firms as having a data breach or not are included in Panel A of Table 4 for the estimation sample. The cutoff probabilities are chosen to minimize the expected costs of misclassification. Following Beneish (1999), the expected costs of misclassification (ECM) is computed as:

$$ECM = P(DB)P_I C_I + [1 - P(DB)]P_{II} C_{II},$$

where:

P(DB) is the prior probability of a reported data breach, P_I and P_{II} are the conditional probabilities of Type I and Type II errors, respectively, and C_I and C_{II} are the costs of Type I and Type II errors, respectively. Consequently, firms with probabilities (predicted using equation 1) greater than the cutoff probability are predicted to have a reported data breach.

Table 4 also shows the resulting Type I error rate (false positives), the Type II error rate (false negatives), the overall error rate (either misclassification) and the overall correct rate (one minus the overall error rate). The results from the estimation sample indicate that the model can correctly classify firms with reported data breaches between thirty percent (at a 100:1 relative cost ratio) and eighty-eight percent (at a 1:1 relative cost ratio). This is the overall correct percentage based on applying the model for each ratio of the cost of Type I to Type II error. [See Table 4, pg. 523]

The validity of the model is tested on a holdout sample data using the same cutoff probabilities from the estimation sample (see Table 4 Panel B). In the holdout sample, twenty-nine percent (at a 100:1 relative cost ratio) to ninety-six percent (at a 1:1 relative cost ratio) of the firms are correctly classified. The wide range of results is due to the change in relative cost ratios. The model is shown to be quite cost-effective even in light of this wide range.

To test the usefulness of the model, we compare these results to a naïve strategy. This strategy classifies all firms as having a reported data breach (no data breach) when the ratio of relative costs is greater than (less than or equal to) the prior probability of a data breach. This switch in strategy between classifying all firms as having no data breaches to classifying all of them as having data breaches occurs at a relative cost ratio of 25:1 (i.e., 1 / 0.04, the prior probability of a data breach). If all firms are classified as having data breaches (not having data breaches), then the naïve strategy makes no Type I (Type II) errors. In this case, P_I (P_{II}) is zero, and P_{II} (P_I) is one. The expected cost of misclassification for the naïve strategy of classifying all firms as not having data breaches (having data breaches) reduces to $0.96C_{II}$ ($0.04C_I$).

We also report the relative costs or the ratio of the ECM for our model to the ECM for the naïve strategy in Table 4. Relative cost below one is an indication of a cost-effective model. For the estimation sample, our model has a lower ECM than the naïve strategy across all ranges of costs of Type I and Type II errors, except for a 1:1 ratio in the estimation sample. It is unlikely that a user will have a relative cost ratio of 1:1, as previously discussed. For the holdout sample, our model has a consistently lower ECM than the naïve strategy at all ranges of the cost ratios. These results provide evidence that the cybersecurity risk model is extremely cost-effective in relation to a naïve strategy for nearly all of the ranges of the costs of Type I and Type II errors.

[15] This is a problem when a paired sample method is used, which is not the case here.

Applying the Prediction Model

We use one firm from the healthcare sector to illustrate the model. From the results of the logistic regression, cybersecurity risk exposure is the probability of the data breach for firm *i* at time *t*, *P(i,t)*:

$$P(i,t) = \frac{1}{1+e^{-zi}} \qquad (1)$$

where:

Z_i = -7.181 + 0.262 GROWTH – 3.045 ACQUISITIONS - 0.287 RESTRUCTURING - 0.721 LEVERAGE + 1.383 CONCENTRATION + 0.587 SIZE + 0.282 PROFIT – 3.372 Energy Sector – 3.481 Materials Sector - 1.264 Industrials Sector – 1.352 Consumer Discretionary Sector - 1.352 Consumer Staples Sector - 1.431 Healthcare Sector – 4.736 Financials Sector – 0.895 Info Tech Sector - 0.946 Telecomm Sector – 2.000 Utilities Sector

Using the values for the firm in the healthcare sector (in parentheses) to substitute the actual variables obtains:

Z_i = -7.181 + 0.262 (-0.032) – 3.045 (0.039) - 0.287 (0.035) - 0.721 (0.505) + 1.383 (0.287) + 0.587 (8.510) + 0.282 (0.14) - 1.431 (Healthcare Sector)
Z_i = -3.684
$P = 1 / (1+e^{-3.684})$
P = 0.024.

Compare P = 0.024 to the cutoff probabilities in Panel A of Table 4. The actual cybersecurity risk (0.024) is less than the cutoff at all levels of the ratio of Type I to Type II errors, except for the 100:1 level which accurately indicates that the firm will not have a data breach. In this case, the model correctly predicted the status of this firm, unless the user's relative cost ratio is 100:1.

Robustness Tests

We test the assumption of prior probability used in the model for robustness. The prior probability of a data breach in developing the prediction model was assumed to be four percent, since four percent of the firms in the initial sample had data breaches. The sensitivity of the model to other specifications of the prior probability of a data breach is evaluated by using prior probabilities of 0.02 and 0.08. These prior probabilities were chosen to represent half and twice the probability found in the sample and are likely to be the lower and upper bounds of the actual prior probability. The changes do not alter the results significantly (results not shown).

V. Conclusions

Cybersecurity is a top concern of senior management, boards of directors, and regulators. Cybersecurity risks can stem from various sources, hence, managing cybersecurity risks involves taking a holistic view of the firm's IT environment. A firm's IT environment and its complexity play a major role in implementing and following adequate and efficient risk management practices throughout the firm. In this paper, we develop a model to explore whether reported financial performance measures can help stakeholders make inferences about the complexity of the firm's IT environment and predict cybersecurity risk exposure. Based on complexity theory we identified seven factors, namely growth, mergers and acquisitions, restructuring, leverage, concentration of segment revenues, size and operating profits, that may add to the complexity of the firm's IT environment. Based on prior research in project management that finds an association between complexity and risk, we posit that these seven factors are associated with cybersecurity risk exposure. We measure cybersecurity risk exposure based on whether a firm has reported an IT related breach or not. We find that firms that had reported a cybersecurity breach have significantly higher growth rates, have higher concentration of segment revenues, are larger and more profitable with marginally fewer acquisitions than their counterparts that did not report a breach. The sector to which a firm belongs also plays a significant role with relatively more breaches in the telecommunications and information technology sectors than other sectors. Using these performance measures, we correctly predict up to eighty-eight percent of firms as either having a cybersecurity breach or not.

However, there are some limitations. Given the extent of data collection, we have limited our analysis to Fortune 500 firms. Therefore, our model only represents relatively large firms. The current dependent variable is a dichotomous variable. Future research could extend the dependent variable to a multinomial variable to provide more meaningful categorization of risk exposure levels. Further, the model developed here is parsimonious therefore, can be extended to include other financial

measures that provide insight into the complexity of the IT environment. Future research could explore the validity and predictability of the model by varying the lagged terms. We also did not find the expected direction for the associations for concentration of segment revenues and mergers and acquisitions. One possible explanation is that type of segment and acquisition (related versus unrelated) may have a different effect on cybersecurity risk exposure. Future research could examine the impact of engaging in related versus unrelated segments and vertical versus horizontal mergers on cybersecurity risk exposure.

Our model and findings contribute to the extant literature and the profession. The results contribute to IT governance and management literature by identifying proxies to measure IT environment complexity. Further, we contribute to the complexity theory literature by applying the theory to identify financial measures that reflect complexity. Our contribution to the profession is twofold. First, we provide a predictive model that insurance firms, analysts, and other stakeholders could use to predict a firm's cybersecurity risk exposure. Second, we contribute to the ongoing discussions on disclosures on cybersecurity and IT risks. Our model provides preliminary evidence that current financial performance measures provide some insights into the firm's cybersecurity risk exposure.

References

Anderson, P. 1999. Complexity theory and organization science. *Organization Science,* 10(3): 216–232.

Baldwin, H. 2015. How to reduce IT complexity and increase agility. *Computerworld,* Aug 5, 2015. Retrieved from https://www.computerworld.com/article/2954527/it-management/how-to-reduce-it-complexity-and-increase-agility.html

Beneish, M. 1999. The detection of earnings manipulation. *Financial Analysts Journal,* September/October (55): 24–41.

Bernard, T. and S. Cowley. 2017. Equifax breach caused by lone employee's error, former C.E.O. Says. *The New York Times.* October 3, 2017. Retrieved from https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html

Buck-Lew, M., C. Wardle., and N. Pliskin. 1992. Accounting for information technology in corporate acquisitions. *Information & Management,* 22: 363–369.

Bharadwaj, A. S. 2000. A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly,* 24(1): 169–196.

Campbell, J., H. Chen., D. Dhaliwal., H. Lu., and L. Steele. 2014. The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies,* 19: 396–455.

Chae, H., C. Koh., and V. Prybutok. 2014. Information technology capability and firm performance: Contradictory findings and their possible causes. *MIS Quarterly,* 30(1): 305–326.

Chandran, V., and Rasiah, R. 2013. Firm size, technological capability, exports and economic performance: The case of electronics industry in Malaysia. *Journal of Business Economics and Management,* 14(4): 741–757.

Chang, S., I. Chang., and T. Wang. 2014. Information systems integration after merger and acquisition. *Industrial Management and Data Systems,* 114(1): 37–52.

Dopson, S. and R. Stewart. 1993. Information technology, organizational restructuring and the future of middle management. *New Technology Work and Employment,* 8(1): 10–20.

Florin, J., M. Bradford., and D. Pagach. 2005. Information technology outsourcing and organizational restructuring: An explanation of their effects on firm value. *Journal of High Technology Management Research,* 16: 241–253.

Gewald, H., K. Wüllenweber, and T. Weitzel. 2006. The influence of perceived risks on banking managers' intention to outsource business processes: A study of the German banking and finance industry. *Journal of Electronic Commerce Research,* 7(2): 78–95.

Gilson, C. 2010. Creating value through corporate restructuring: Case studies in bankruptcies, buyouts and breakups. John Wiley and Sons, Inc. Hoboken: New Jersey.

Gruman, G. 2007. Strategies for dealing with IT complexity. *CIO,* November 26, 2007. Retrieved from https://www.cio.com/article/2437606/it-organization/strategies-for-dealing-with-it-complexity.html

Higgs, J., R. Pinsker., T. Smith., and G. Young. The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems,* 30(3): 79–98.

Huang, C., Q. Hu., and R. Behara. 2008. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics,* 114(2): 793–804.

International Foundation for Information Technology (IF4IT). 2009. Retrieved from https://www.if4it.com/SYNTHESIZED/FRAMEWORKS/ENVIRONMENT/environment_framework.html#CONCLUSIONTS

ISACA. 2015. State of cybersecurity: Implications for 2015 an ISACA and RSA conference survey. Retrieved from http://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2015.aspx. 1-22

ISACA. 2018. State of cybersecurity 2018: Part 1: Workforce development. Retrieved from http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2018-part-1_res_eng_0418.PDF

Jones, F. 1987. Current techniques in bankruptcy prediction. *Journal of Accounting Literature,* 6: 131–164.

Kobelsky, K., V. Richardson., R. Smith., and R. Zmud. 2008. Determinants and consequences of firm information technology budgets. *The Accounting Review,* 83(4): 957–995.

Li, C., G. Peters., V. Richardson., and M. Watson. 2012. The consequences of information technology control weaknesses on management information systems: The case of Sarbanes-Oxley internal control reports. *MIS Quarterly,* 36(1): 179–203.

Li. H., W. No., T. Wang. 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems,* 30: 40–55.

Liu, Y., and T. Ravichandran. 2008. A comprehensive investigation on the relationship between information technology investments and firm diversification. *Information Technology and Management,* 9(3): 169–180.

Lim, J., B. Dehning., V. Richardson., and R. Smith. 2011. A meta-analysis of the effects of IT investment on firm performance. *Journal of Information Systems,* 25(2): 145–169.

Maddala, G. S. 1991. Perspective on the use of limited-dependent and qualitative variables models in accounting research. *The Accounting Review,* 66(4): 788–807.

McFadzean, E., J. Ezingeard., and D. Birchall. 2007. Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review,* 31(5), 622–660.

Mihailovic, I., D. Ranõelovic., and D. Stojanovic. 2010. Accounting information as resource for business decisioning. 20th Biennial International Congress Tourism and Hospitality Industry, 1067–1074.

Mulligan, P., and S. Gordon. 2003. Restructuring in financial services: A transaction cost perspective. *E-Service Journal,* 3(1): 77–98.

Overby, S. 2005. Comair's Christmas Disaster: Bound to Fail. CIO. May 1, 2005. Retrieved from https://www.cio.com/article/2438920/risk-management/comair-s-christmas-disaster--bound-to-fail.html?page=2

PricewaterhouseCoopers (PwC). 2008. A practical guide to segment reporting. Retrieved from https://www.pwc.com/gx/en/ifrs-reporting/pdf/segment-reporting.pdf

Qazi, A., J. Quigley., A. Dickson., K. Kirytopoulos. 2016. Project complexity and risk management (ProCRiM): Towards modelling project complexity driven risk paths in construction projects. *International Journal of Project Management,* 34(7): 1183–1198.

Santhanam, R., and Hartono, E. 2003. Issues in linking information technology capabilities to firm performance. *MIS Quarterly,* 27(1): 125–153.

Securities Exchange Commission (SEC). 2011. CF Disclosure Guidance: Topic No. 2 Cybersecurity. Retrieved from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Securities Exchange Commission (SEC). 2018. Commission statement and guidance on public company cybersecurity disclosures. Retrieved from https://www.sec.gov/rules/interp/2018/33-10459.pdf

Shenhar, A. 2001. One Size does not Fit All Projects: Exploring Classical Contingency Domains. *Management Science,* 47(3): 394–414.

Siwicki, B. 2017. Why healthcare mergers, acquisitions can uncover new cybersecurity risks. *Healthcare IT News,* October 20, 2017. Retrieved from http://www.healthcareitnews.com/news/why-healthcare-mergers-acquisitions-can-uncover-new-cybersecurity-risks

Taylor, H., E. Artman., and J. Woelfer. 2012. Information technology project risk management: bridging the gap between research and practice. *Journal of Information Technology,* 27(1): 17–34.

Thompson, D. 1967. Organizations in Action. McGraw-Hill, New York.

Trussel, J. M. 2002. Revisiting the prediction of financial vulnerability. *Nonprofit Management and Leadership*, 13: 17–31.

Trussel, J., and J. Greenlee. 2004. A Financial Risk Rating System for Nonprofit Organizations. *Research in Governmental and Nonprofit Accounting*, 11: 105–127

Trussel, J., and P. Patrick. 2009. A predictive model of fiscal distress in local governments. *Journal of Public Budgeting Accounting and Financial Management*, 21(4): 578–616.

Trussel, J. and P. Patrick. 2013. The symptoms and consequences of fiscal distress in municipalities: An investigation of reductions in public services. *Accounting and the Public Interest*, 13(December): 151–171.

Vincent, N., J. Higgs, and R. Pinsker. 2017. Board and management-level factors affecting the maturity of IT risk management practices. (Working paper, University of Tennessee Chattanooga).

Vincent, N., and R. Pinsker. 2017. IT risk management: A relational perspective based on strategy implementation. (Working paper, University of Tennessee Chattanooga).

Warfield, J. 1999. Twenty laws of complexity: science applicable in organizations. *Systems Research and Behavioral Science*, 16(1): 3–40.

Wahba, P. 2016. Target lays out multi-billion-dollar e-commerce plan. *Fortune*, March 2, 2016. Retrieved from http://fortune.com/2016/03/02/target-ecommerce-2/

Wahba, P. 2017. Walmart's massive tech investments drive another quarter of big sales gains. *Fortune*, August 17, 2017. Retrieved from http://fortune.com/2017/08/17/walmart-results-2q-tech-investment/

Webb, J., A. Ahmad, S. Maynard., and G. Shanks. 2014. A situation awareness model for information security risk management. *Computers & Security*, 44: 1–15.

Yoon, C. 2011. Measuring enterprise IT capability: A total IT capability perspective. *Knowledge-Based Systems*, 24: 113–118.

Figure 1: Model Rationale

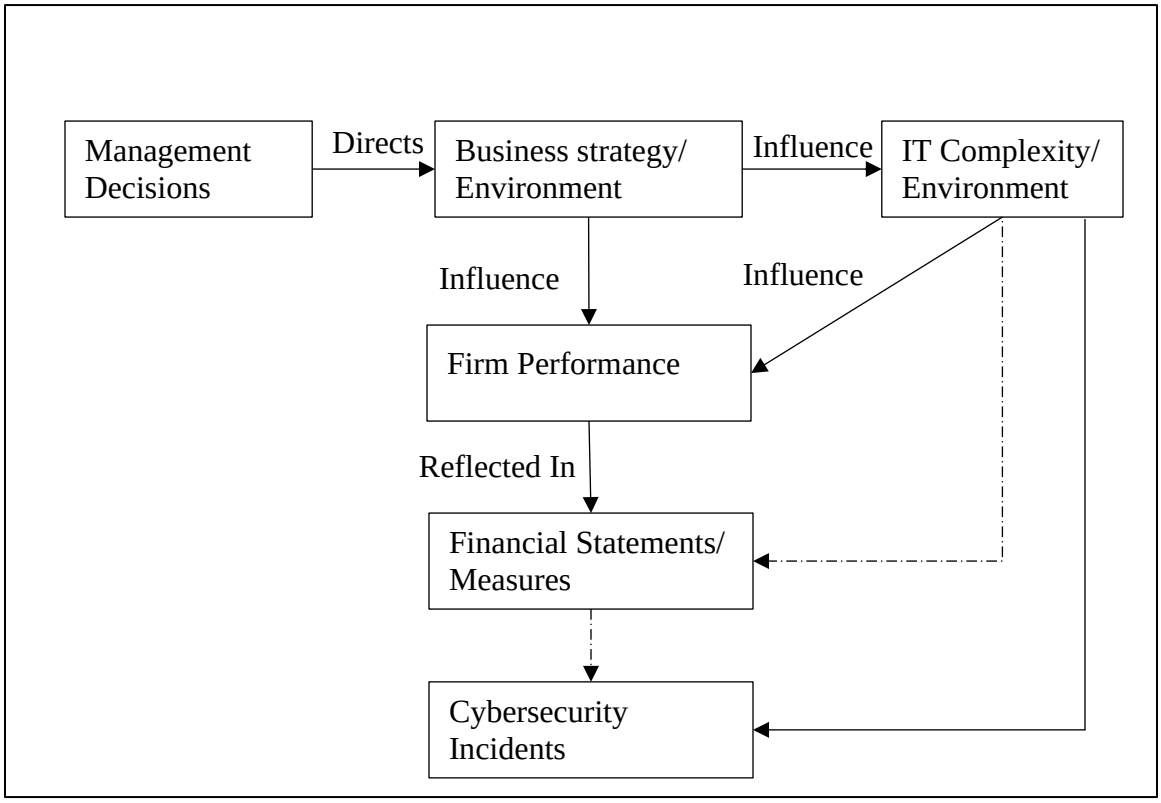

Figure 2: Operationalizing the Theoretical Model

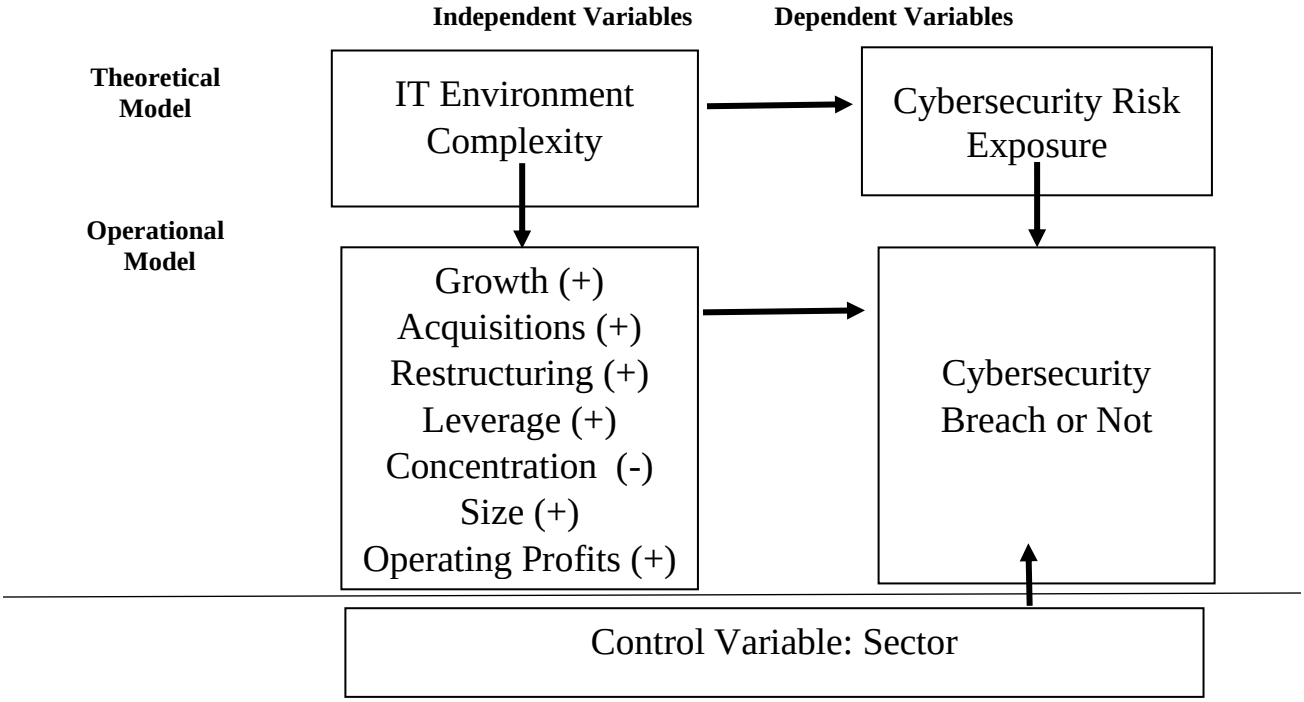

Table 1: Summary of the Predictor Variables and the Sample

Panel A: Variables

Variable*	Measure (Lagged)	Hypothesized Sign
GROWTH	$\frac{Sales_{t-1} - Sales_{t-2}}{Sales_{t-2}}$	+
ACQUISITIONS	$\frac{Mergers\ \&\ Acquisitions_{t-1}}{Total\ Assets_{t-1}}$	+
RESTRUCTURING	$\frac{Restructuring\ Charges_{t-1}}{Sales_{t-1}}$	+
LEVERAGE	$\frac{Total\ Liabilities_{t-1}}{Total\ Assets_{t-1}}$	+
CONCENTRATION	$\Sigma\left[\left(\frac{Segment\ Sales_{i,t-1}}{Sales_{t-1}}\right)^2\right]$	-
SIZE	$\ln(Sales_{t-1})$	+
PROFIT	$\frac{Operating\ Profit_{t-1}}{Sales_{t-1}}$	+

*All variables are measured in the year prior to the year of breach. We also control for Sector, including Energy, Materials, Industrials, Consumer Discretionary, Consumer Staples, Healthcare, Financials, Information Technology, Telecommunications, Utilities and Other.

Panel B: Sample by Sector

Sector	No Breach	Breach*	Total	% Breach
Energy	439	4	443	0.9%
Materials	306	1	307	0.3%
Industrials	714	35	749	4.7%
Consumer Discretionary	895	58	953	6.1%
Consumer Staples	382	17	399	4.3%
Healthcare	563	30	593	5.1%
Financials	732	4	736	0.5%
Info Tech	703	50	753	6.6%
Telecomm	48	11	59	18.6%
Utilities	319	4	323	1.2%
Other	253	7	260	2.7%
Total	5,354	221	5,575	4.0%

*A breach firm is one identified as such by the privacy rights clearinghouse, which provides a database of data breaches publicized from 2005 to 2015.

Table 2: Descriptive Statistics

Panel A: Univariate Tests

Variable	Breach	Mean	Std. Dev.	t	Sig.
GROWTH	No	0.081	0.693	-1.107	0.269
	Yes	0.099	0.204		
ACQUISITIONS	No	0.041	0.157	2.425	0.015*
	Yes	0.016	0.045		
RESTRUCTURING	No	0.005	0.067	0.945	0.345
	Yes	0.002	0.051		
LEVERAGE	No	0.611	0.223	0.441	0.661
	Yes	0.604	0.221		
CONCENTRATION	No	0.471	0.358	-4.632	<0.001**
	Yes	0.558	0.267		
SIZE	No	8.97	1.253	-9.325	<0.001**
	Yes	9.909	1.468		
PROFIT	No	0.193	1.831	-3.559	<0.001**
	Yes	0.719	5.778		

**Significant at the 0.05 level (two-tailed)
*Significant at the 0.10 level (two-tailed)

Panel B: Correlation Coefficients

Variable	GROWTH	ACQUISITIONS	RESTRUCTURING	LEVERAGE	CONCENTRATION	SIZE
ACQUISITIONS	0.033*					
RESTRUCTURING	-0.006	-0.002				
LEVERAGE	-0.042**	-0.014	0.021			
CONCENTRATION	0.026	0.003	-0.013	0.109**		
SIZE	-0.076**	-0.104**	-0.079**	0.253**	0.032*	
PROFIT	-0.009	0.015	-0.498**	-0.020	-0.01	0.084**

**Significant at the 0.01 level (two-tailed)
*Significant at the 0.05 level (two-tailed)

Table 3: Logistic Regression Security Breach Model

Variable	B	Std. Error	Wald Chi-Square	Sig.
Constant	-7.181	0.859	69.912	<0.001***
GROWTH	0.262	0.114	5.281	0.022**
ACQUISITIONS	-3.045	1.647	3.416	0.065*
RESTRUCTURING	-0.287	6.972	0.002	0.967
LEVERAGE	-0.721	0.609	1.403	0.236
CONCENTRATION	1.383	0.348	15.786	<0.001
SIZE	0.587	0.104	32.062	<0.001***
PROFIT	0.282	0.128	4.811	0.028**
Energy Sector	-3.372	0.796	17.934	<0.001***
Materials Sector	-3.481	1.129	9.502	0.002***
Industrials Sector	-1.264	0.508	6.200	0.013**
Consumer Discretionary Sector	-1.352	0.460	8.628	0.003***
Consumer Staples Sector	-2.118	0.586	13.051	<0.001***
Healthcare Sector	-1.431	0.558	6.581	0.010**
Financials Sector	-4.736	1.178	16.151	<0.001***
Info Tech Sector	-0.895	0.517	2.997	0.083*
Telecomm Sector	-0.946	0.801	1.395	0.238
Utilities Sector	-2.000	0.675	8.773	0.003***

***Significant at the 0.01 level (one-tailed)
**Significant at the 0.05 level (one-tailed)
*Significant at the 0.10 level (one-tailed)

Table 4: The Predictive Ability of the Security Breach Model

Panel A: Probability of Data Breach - Estimation Sample

	Cost of Type I to Type II Error						
Initial Sample	1:1	10:1	20:1	25:1	30:1	50:1	100:1
Cutoff	0.530	0.120	0.110	0.040	0.040	0.030	0.010
Type I Error	0.983	0.635	0.617	0.183	0.183	0.130	0.043
Type II Error	0.080	0.142	0.151	0.405	0.405	0.493	0.721
Overall Error	0.118	0.162	0.171	0.395	0.395	0.477	0.693
ECM Model	0.117	0.396	0.651	0.575	0.613	0.740	0.870
ECM Naïve	0.041	0.410	0.820	0.959	0.959	0.959	0.959
Relative Costs	2.858	0.966	0.794	0.600	0.639	0.772	0.907
Overall Correct	0.882	0.838	0.829	0.605	0.605	0.523	0.307

Panel B: Probability of Data Breach - Holdout Sample

	Cost of Type I to Type II Error						
Initial Sample	1:1	10:1	20:1	25:1	30:1	50:1	100:1
Cutoff	0.530	0.120	0.110	0.040	0.040	0.030	0.010
Type I Error	0.990	0.582	0.561	0.194	0.194	0.143	0.031
Type II Error	0.000	0.075	0.091	0.378	0.378	0.470	0.740
Overall Error	0.040	0.096	0.110	0.371	0.371	0.457	0.712
ECM Model	0.041	0.311	0.547	0.561	0.601	0.743	0.836
ECM Naïve	0.041	0.410	0.820	0.959	0.959	0.959	0.959
Relative Costs	1.000	0.758	0.667	0.585	0.627	0.775	0.871
Overall Correct	0.960	0.904	0.890	0.629	0.629	0.543	0.288

Note: Firms with probabilities greater than the cutoff are predicted to have a data breach. the expected costs of misclassification (ECM Model) are computed as $ECM = P(DB)P_IC_I + [1 - P(DB)]P_{II}C_{II}$, where P(DB) is the prior probability of a reported data breach, P_I and P_{II} are the conditional probabilities of Type I and Type II errors, respectively, and C_I and C_{II} are the costs of Type I and Type II errors, respectively.