The Role of Ethical Climate on employee's Perceived security risk assessment

Extended Abstract

Randi Jiang
Louisiana Tech University
502 W Texas Ave, Ruston, LA
rji003@latech.edu

Jaeung Lee
Louisiana Tech University
502 W Texas Ave, Ruston, LA
jakelee@latech.edu

Tom Stafford
Louisiana Tech University
502 W Texas Ave, Ruston, LA
Stafford@latech.edu

Selwyn Ellis
Louisiana Tech University
502 W Texas Ave, Ruston, LA
ellis@latech.edu

Keywords

Fraud Triangle, Ethical Climate, Perceived Risk Assessment, Internal Data Breach

The Role of Ethical Climate on employee's Perceived security risk assessment

Introduction

Cybersecurity is a concept that has only recently become a part of mainstream awareness in terms of corporate governance (Lanz 2014). But, a key reason for its recent awareness is that in the last decade there have been multiple companies across a number of business sectors unintentionally leaking customer information into cyberspace. The risk of cybersecurity breaches (and the harm that these breaches pose) is one of increasing significance for many companies and is therefore an area for heightened board focus (Gregory and Pollack 2002), and some studies demonstrate the value of a robust interaction between internal audit functions and information security skillset (Stafford 2017; Steinbart et al. 2013).

On July 29, 2017, a prominent security breach occurred at the credit bureau Equifax. According to a CNN report (O'Brien 2017), this breach is estimated to have affected over 143 million users and involved sensitive personal information including but not limited to social security numbers, dates of birth, personal and business addresses, driver's license numbers and credit card information. Androitis et al. (2017) reports that there was an internal notification of a possible threat months before the actual data breach, indicating poor cybersecurity procedures were in place at Equifax. The history of large-scale cybersecurity breaches is not limited to the Equifax case; Yahoo (2013-2014), eBay (2014), Target (2013), and JP Morgan Chase (2014) have all suffered security breaches within last 5 years and the impact of these events have negatively impacted these companies.

In the process of understand how and why an organization may have internal data breaches, we seek to apply the precepts of the Bright ICT Initiative (Lee 2015), in an effort to support critical principals and minimize user issues associated with cybersecurity. The Bright ICT Protocol calls for governance structure, we believe that moderating effect of governance from companies will allow organization to have the chance to reduce information leakage, design traceable anonymity, and heighten the sense of strong internal controls within a company.

In this research, we specifically focus on following research questions: 1) Will any elements of the Fraud Triangle affect employee's perceptions of risk assessment? 2) Will ethical climates within an organization decrease the possibility of an internal data breach? This research will contribute to the literature on information security in the context of minimizing internal security threats. Our focus will be on the insider whom given the right opportunity, attitude, and pressure may still be deterred from committing a data breach because of a strong ethical climate within the organization. To our knowledge, our research is the first study that investigates impact of fraud triangle factors on information security risk assessment and the role of ethical climate that can be a potential factor to minimize the internal security threat.

American states define security breach as the "unauthorized acquisition of access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector." (Anandarajan et al. 2013) We understand a data breach is a fraudulent act. Our model attempts to alert organizations on how to reduce the possibility of an internal data breach. Common data breaches include identify theft and there has been prior research to see if disclosure laws help the security (Romanosky et al. 2011). The disclosure of a security results in the loss of a $2.1 of a firm's market valuation (Cavusoglu et al.

2004). This will benefit development of institutional policies.

The rest of this paper is organized as follows: we present a review of the "the fraud triangle" and contrast it with ethical climate theory and risk assessment concepts to develop a 3 positive approach to enforcing cybersecurity practices in the firm. Next, we develop research hypotheses and provide a research model. We conclude this abstract with an overview of our research plan.

Related Works / Hypothesis Development

In our research, we take the fraud triangle (Dorminey et al. 2012) from the accounting literature and apply this as a foundation of our theoretical model, which implies but does not formalize interrelationships between three fraud risk categories called opportunity, rationalization and pressure. The fraud triangle is a dominant framework in auditing and forensic accounting and it has become entrenched in the formal ethical standards of professional associations around the globe (Murphy and Free 2015).

We define the three perceived elements of the fraud triangle to be opportunity, rationalization, and pressure. Opportunity is defined as engaging in fraudulent activity arise when employees perceive a control weakness is present and that the ability to commit a fraudulent act without detection is high while the likelihood of being caught is remote (Dorminey et al. 2012). We propose that such opportunities for the commission of fraudulent acts are likely to manifest themselves when employee's sense that they might be safely able to use their credentials to circumvent internal Information Technology (IT) security controls for purposes of committing a harmful data breach. We understand rationalization to be when individuals who commit fraud desire to do so without incurring negative self-perceptions, so they will typically seek to rationalize their fraudulent actions to themselves (Dorminey et al. 2012). We propose the rationalization variable to describe how employees attempt to self-justify their actions to circumvent internal IS security controls. We present pressure in our research as personal financial stress (Conger et al. 1999); employees under financial strain can trend to seek to circumvent internal security controls for personal gain. The "external pressure" part of the fraud triangle in the model is construed as work-related stress (Cavanaugh et al. 2000). Employees who face unreasonable work deadlines or are given a large amount of responsibilities with unmanageable expectations are considered under work related stress. This type of stress may cause employees to overcome safe internal controls in order to perform their duties.

In addition to the operationalization of the fraud triangle variables to explain employee's inclination to engage in breaches, we also assume that company instrumental climate can influence employee decision making in the organization, and will subsequently be used to assess how employees gauge their personal risk if they chose to circumvent internal controls to commit fraud (Murphy and Free 2015). Ethical climate theory is important to our research model because firms under external audit must provide evidence of their adherence to ethical principles and guidelines. The Sarbanes-Oxley Act, for example, requires firms to adopt ethical codes of conduct to prevent businesses from problematic events. Ethical climate theory is a based on ethical philosophies and the related sociological precepts of peer reference groups. Culture, in that context, is defined as rules, codes, rewards, leadership, rituals, and stories that shape behaviors (Treviño et al. 1998). An "ethical work climate," then, is defined as the prevailing perceptions of typical organizational practices and procedures that have positive ethical valence (Murphy and Free 2015; Victor and Cullen 1988). Every organization has a unique work climate that describes how employees carry out its practices and procedures. Thus, we consider rules and ethics as ethical climate of company. Such organizational culture will influence attitudes and ethical behavior.

A properly secured working environment in an organization requires employees to contribute to assessment of risks (Baskerville et al. 2015). In our model, we suggest that 4 perceived employee risk assessment will be the perceived likelihood of sensitive data being breached and that the associated perceptions of severity of data breach are indicated by the degree of losses/damages caused by employees in the following year of operations (Lee et al. 2017).

We propose there are any of the three key elements of the fraud triangle are present in a given situation, that there will be a high-risk assessment of an internal IT security data breach for an organization. However, we believe that if a strong ethical climate emphasizing rules or ethics exists in the firm, that it will moderate this relationship and negatively impact the relationship between the elements of the fraud triangle and an organization's risk assessment. Thus, we present the following hypotheses and Figure 1 below shows our conceptual model of this research.

H1 (+): An employee's perceived opportunity to the Information system is positively associated with an employee's risk assessment of a data breach.

H2 (+): An employee's perceived level of honesty (Rationalization) is positively associated with an employees' risk assessment of data breach.

H3 (+): An employee's perceived pressure is positively associated with employees' risk assessment of data breach.

H4a (-): A rules based climate in an organization negatively moderates the relationship between an employee's perceived opportunity and perceived employee's risk assessment of a data breach.

H4b (-): A rules based climate in an organization negatively moderates the relationship between an employee's rationalization (level of honesty) and perceived employee's risk assessment of a data breach.

H4c (-): A rules based climate in an organization negatively moderates the relationship between the employee's perceived pressure and perceived employee's risk assessment of a data breach.

H5a (-): An ethics based climate in an organization negatively moderates the relationship between an employee's perceived opportunity and perceived employee's risk assessment of a data breach.

H5b (-): An ethics based climate in an organization negatively moderates the relationship between an employee's rationalization (Level of honesty) and perceived employee's risk assessment of a data breach.

H5c (-): An ethics based climate in an organization negatively moderates the relationship between an employee's perceived pressure and perceived employee's risk assessment of a data breach.

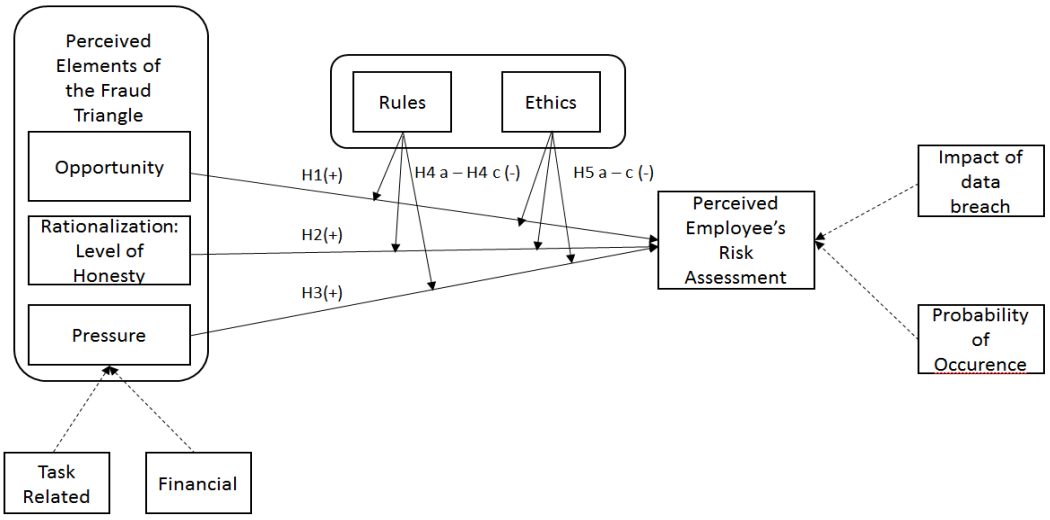

Figure 1. Research Model

Conclusion

In this abstract, we provided research model that is developed by literature review about fraud triangle, ethical climate and risk assessment to answer our two research questions presented earlier. We assumed by investigating our research model, not only we could understand the impact of fraud triangle factors on risk assessment of potential data breach, but also could capture the importance role of ethical climate of organization to minimize internal threat. We are planning to collect survey data from employees working in multiple companies. Based on collected data, we will perform the empirical analysis. We hope the result will be beneficial to contribute to the literature on information security in the context of minimizing internal security threat and can implement to develop better security policy. This paper is still in early stages which we plan to complete based on comments from Bright ICT Submit.

References

Anandarajan, M., D'Ovidio, R., and Jenkins, A. 2013. "Safeguarding Consumers against Identity-Related Fraud: Examining Data Breach Notification Legislation through the Lens of Routine Activities Theory," International Data Privacy Law (3:1), pp. 51(A1-A9).

Andriotis, A., Rapoport, M., and Rexrode, C. 2017. "Lawmakers Slam Equifax Ex-Ceo over Hack." Wallstreet Journal. retrieved from https://www.wsj.com/articles/lawmakersslam- equifax-ex-ceo-over-hack-1507051747

Baskerville, R. L., Kaul, M., and Storey, V. C. 2015. "Genres of Inquiry in Design-Science Research: Justification and Evaluation of Knowledge Production," MISQ (39:3) pp.541-564.

Cavanaugh, M. A., Boswell, W. R., Roehling, M. V., and Boudreau, J. W. 2000. "An Empirical Examination of Self-Reported Work Stress among Us Managers," Journal of applied psychology (85:1), pp. 65-74.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), pp.70-104.

Conger, R. D., Conger, K. J., Matthews, L. S., and Elder, G. H. 1999. "Pathways of Economic Influence on Adolescent Adjustment," American journal of community psychology (27:4), pp. 519-541.

Dorminey, J., Fleming, A. S., Kranacher, M.-J., and Riley Jr, R. A. 2012. "The Evolution of Fraud Theory," Issues in Accounting Education (27:2), pp. 555-579.

Gregory, H., and Pollack, J. 2002. "Corporate Social Responsibility," Global Counsel), pp. 41-55.

Joshi, A. W., and Arnold, S. J. 1997. "The Impact of Buyer Dependence on Buyer Opportunism in Buyer–Supplier Relationships: The Moderating Role of Relational Norms," Psychology & Marketing (14:8), pp. 823-845.

Lanz, J. 2014. "Cybersecurity Governance: The Role of the Audit Committee and the Cpa," The CPA Journal (84:11), p. 6.

Lee, J., Wang, J., de Guzman. M., Korni. K., Gupta. M., Rao. H.R., 2017. "Risk Data Breaches in Financial Institutions: A Routine Activity Perspective," Dewald Roode Workshop on IS Security Research IFIP, Tampa, Florida.

Lee, J. K. 2015. "Research Framework for Ais Grand Vision of the Bright Ict Initiative," MISQ (39:2), pp 3-12.

Martin, K. D., and Cullen, J. B. 2006. "Continuities and Extensions of Ethical Climate Theory: A Meta-Analytic Review," Journal of Business Ethics (69:2), pp. 175-194.

Melancon, J. P., Noble, S. M., and Noble, C. H. 2011. "Managing Rewards to Enhance Relational Worth," Journal of the Academy of Marketing Science (39:3), pp. 341-362.

Murphy, P. R., and Free, C. 2015. "Broadening the Fraud Triangle: Instrumental Climate and Fraud," Behavioral Research in Accounting (28:1), pp. 41-56.

O'Brien, S. A. 2017. "Giant Equifax Data Breach: 143 Million People Could Be Affected."

Romanosky, S., Telang, R., and Acquisti, A. 2011. Do data breach disclosure laws reduce identity theft? Journal of Policy Analysis and Management, 30(2), pp. 256-286.

Rothwell, G. R., and Baldwin, J. N. 2007. "Ethical Climate Theory, Whistle-Blowing, and the Code of Silence in Police Agencies in the State of Georgia," Journal of Business Ethics (70:4), pp. 341-361.

Saridakis, G. 2013. "Shop Crime and Deterrence: Evidence on Shoplifting among Young People in the Youth Lifestyle Survey (Yls)," Review of Law & Economics (9:2), pp. 197-237.

Slovic, P., Fischhoff, B., and Lichtenstein, S. 1980. "Facts and Fears: Understanding Perceived Risk," Societal risk assessment: How safe is safe enough (4), pp. 181-214.

Stafford, T., Graham, G., Poston, R., Jiang, R., and Lyons, R. 2017. "Role of Accounting and Professional Associations in It Security Auditing." Working paper

Steinbart, P. J., Raschke, R. L., Gal, G., and Dilla, W. N. 2013. "Information Security Professionals' Perceptions About the Relationship between the Information Security and Internal Audit Functions," Journal of Information Systems (27:2), pp. 65-86.

Treviño, L. K., Butterfield, K. D., and McCabe, D. L. 1998. "The Ethical Context in Organizations: Influences on Employee Attitudes and Behaviors," Business Ethics Quarterly (8:3), pp. 447-476.

Victor, B., and Cullen, J. B. 1988. "The Organizational Bases of Ethical Work Climates," Administrative science quarterly, pp. 101-125.

Wang, J., Gupta, M., and Rao, H. R. 2015. "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," MISQ (39:1), pp 91-112.