# Network Effects and Data Breaches: Investigating the Impact of Information Sharing and the Cyber Black Market

*Research-in-Progress*

**Michele Maasberg**
The University of Texas at San Antonio
1 UTSA Circle, San Antonio, TX 78249
michele.maasberg@utsa.edu

**Charles Zhechao Liu**
The University of Texas at San Antonio
1 UTSA Circle, San Antonio, TX 78249
charles.liu@utsa.edu

## Abstract

*This paper was motivated by the growing data breach activities confronting organizations. Building on the literature on information sharing and network effects, we attempt to empirically examine how the number of security breaches may change as a result of two opposing network effects in the data breach battlefield, namely, the positive network effects driven by industry-wide information sharing efforts, and the negative network effects driven by the supply and demand changes in the underground cybercrime ecosystem, and whether a feedback loop can be formed so that the information sharing efforts can influence the costs and availability of malicious tools and suppress their demand. As one of the first studies to empirically examine the dynamics in the cybercrime economy, our research will provide important policy guidance to improve collaborative mechanisms to enhance industry wide information security, and illuminate a new way to monitor and curtail the flow of cyber-criminal activities.*

**Keywords:** Data breach, security, underground cyber black market, network effects, information sharing.

## Introduction

Nowadays, on top of the harsh and turbulent business environments, firms are increasingly confronted with the challenge of protecting their information systems from data breaches, which have increased considerably within the past decade (Frei 2014). A data breach is a security incident in which the disclosure or potential exposure of data occurs, most often through external hacking (Verizon 2015). These attacks have been directed at a wide variety of organizations, and the majority of the attacks appear to be driven primarily by financial motives (Liu et al. 2011). According to a recent study conducted by Ponemon Institute, the probability of a data breach is largely based on the number of customer records a company maintains and varies across industries. Specifically, U.S. public sector organizations and consumer-intensive industries are far more likely to suffer a data breach than energy and industrial companies are. (Ponemon Institute, 2014).

Due to the vast amount of customer data that need to be transmitted and stored in the business process, retailers are particularly vulnerable to data breach-related attacks (Mandiant 2015). For example, the reported frequency of point of sale (POS) intrusions, one of the most common security breach classification patterns, is highest in accomodation/food services and retail industries. The primary target in data breaches is organizational data or individual's personally identifiable information (i.e., name, social security number, credit or debit card number) (Ponemon Institute 2014). Despite the growing awareness and efforts from retailers to fight this cybercrime, hackers continue to find unique ways to steal sensitive and valuable data from the retailers' information systems and sell these data on the black

market. Verizon (2015) forecast that the average loss for a breach of 1,000 records is between $52,000 and $87,000. The enormous profits derived from this highly sensitive personal information has stimulated the demand for such breached data, which in turn drives the proliferation of malicious hacking tools in the underground hacker markets.

The persons that perpetrate these data breach-related crimes are typically professional cyber criminals who prepare their attacks based on known demands from the underground markets or are hired to commit the cybercrime (Mandiant 2015). The connections among recent data breach incidents are gaining attention as more and more of the attacks and mechanisms for the attacks are repeatedly employed by the same group of suspects (Ablon et al. 2014). For example, the Russian cyber criminals that attacked Staples, Inc. in November of 2014 appear to be the same Russian cyber criminals that attached Michael's, Target, Neiman Marcus, and P.F. Chang's (Krebs 2014; Privacy Rights Clearinghouse 2015a, 2015b). The Home Depot breach in September of 2014 appeared to contain a new variant of the malicious software BlackPOS found at Target in December of 2013 (Krebs 2014). Card information from customers at Home Depot then also showed up on the same underground cybercrime site Rescator[dot]cc that sold millions of cards from Target (Krebs 2014).

As more data breaches occur, the types of underground cybercrime sites, or black markets that sell spyware, malware, viruses, or even hacking services, are growing in size and complexity (Ablon et al. 2014). Known sites exist in a small city in south central Russia consisting of a few dozen individuals as well as in China, where underground activity by advanced persistent threat (APT) groups doubled between 2012 and 2013 (Paganini 2014). A large portion of cybercrime transactions can also be traced to an Eastern European underground market that has been virtually undetected for about 15 years (Bennett 2015). This shadow economy is now surpassing a half trillion dollars in annual revenue and experiencing exponential growth (Bennett 2015). As this underground market achieves economy of scale, the prices of various forms of malicious infiltration are fluctuating rapidly, either because the vulnerabilities that these malicious tools targeted have been patched, or because newer or more effective hacking tools have been invented to circumvent current protective technologies. For example, prices for products in the Russian underground have decreased significantly for garden variety tools and services in the majority of cases in the last three years, with the cost of exploit kits decreasing to almost $0 and Crypter and Traffic products volume prices declining by 75% (Paganini 2014). On the other hand, boutique products and services, new malware designs, stolen-to-order, or those unconventional tools requiring specialized knowledge and skill to craft are commanding higher and higher prices (Ablon et al. 2014; Paganini 2014).

Efforts to counteract such malicious forces have gone beyond enhancing security protection of the systems. Policy makers and researchers have proposed industry wide efforts to break the information barrier among all affected parties to avoid repeated perpetration of same groups of cybercriminals using similar malicious tools. Among these efforts, of particular interest is the formation of information sharing alliances within different industries (Liu et al. 2013) to share characteristics and patterns of the hacking activities and unidentified vulnerabilities by victim organizations. In many of these industries, an Information Sharing and Analysis Center (ISAC) has been established to coordinate sharing, analysis, detection and alerts of cybersecurity incidents, threats, and vulnerabilities (McCarthy et al. 2014). The founding of the ISACs in various industries has provided a new mechanism that complements the existing technological solutions to curb the increasing cybercrime, and has offered a unique opportunity for researchers to examine the effectiveness of such a new system. More specifically, unlike physical security infrastructure that works independently of the other organizations' security technologies (and have no spillover effect on the overall security of the industry), the mechanisms underlying theses ISACs has the potential to create positive network externalities by reducing the probability of being repeatedly exploited by the same malicious tools, hence minimizing the vulnerabilities and the associated loss of the participating organizations.

In addition to reducing the number of breaches, the effectiveness of the information sharing mechanisms is likely to have a significant influence on availability of various malicious tools their and prices in the underground market. As more malicious code and its variants are revealed and shared and security vulnerabilities become known and fixed, the effectiveness of the malware will be dramatically reduced, increasing the difficulty and the amount of efforts involved to develop new tools that are capable of penetrating the organizations' much enhanced security infrastructure. Ideally, such a change in market

dynamics may slow down the demand and supply for breached records, and potentially suppressing the growth of the underground breached data market and the number of future breach attempts.

In light of these connections between the collaborative industry efforts to foster security-related information sharing and the evolution of the underground breached data market, in this study we attempt to examine how the extent of the information sharing by organizations such as ISACs can reduce the number of breaches in industries plagued with data-related cybercrime, and consequently, the malicious tools availability and prices in the underground market. Departing from the extant literature that primarily focuses on investigating the causes and consequences of security breaches, or studying procedural control issues in mitigating the risk of a breach, this study takes a unique economics perspective to empirically examine the dynamics on both sides of the cybersecurity battlefield. On the one hand, we seek to estimate how the growth of the ISAC networks and the increasing extent of information sharing can reduce the scope and magnitude of security breaches in the U.S. retail industry. On the other hand, we also attempt to examine how such efforts influence the cost and availability of malicious data breach tools and services available in the black market, and its impact on the evolution of the growing underground cybercrime ecosystem that consists of hackers, brokers, mediators (Agrawal et al. 2013), and breached data exploiters. The rest of this paper is organized as follows. First, we review the literature on information sharing and network effects which form the theoretical basis of our study, and derive a conceptual model that integrates the eight hypotheses we proposed. Next, we discuss our empirical plan to evaluate the hypotheses. Finally, we conclude with our expected contribution and plan for future work.

## Theoretical Background and Hypotheses

Previous studies in the IS literature have examined the phenomenon of breaches from a variety of angles such as innovation diffusion (Bagchi and Udo 2003), ethical (Culnan and Williams 2009; Lowry et al. 2014), administrative/policy (Bulgurcu et al. 2010; D'Arcy and Greene 2014; Shaw 2009; Siponen et al. 2014; Vance et al. 2015), behavioral (Crossler et al. 2013; Luo et al. 2013; Posey et al. 2013; Vishwanath et al. 2011), technical (Mookerjee et al. 2011; Yue and Çakanyıldırım 2010), and risk analysis (Chen et al. 2011; Straub and Welke 1998). In the empirical literature, the majority of the studies focus on examining the causes of security breaches (i.e., governance and compliance) and the consequences of the disclosure of data breaches (i.e. stock market responses) through event study or archival data analysis. Many of these studies have found that there is a general negative stock market response to vulnerabilities (Campbell et al. 2003; Das et al. 2012; Garg et al. 2003), but the extent of such a negative impact depends on the victim organization's short or long term reactions (Gordon et al. 2011; Kannan et al. 2007). Others have found evidence of a positive relationship between market disclosures and firm value due to timely discovery and elimination of potential security vulnerabilities (Gordon et al. 2010). A common theme of the extant literature is that security breaches are treated as unrelated occurrences and are therefore analyzed independently at the organization level. Given the evidence discussed in the introduction, we contend that the majority of the cybercrime activities are carried out by closely related groups of hackers and many of the tools these cyber criminals used can be traced to the same origins. Hence a more systematic approach should be adopted in measuring the effectiveness of our anti-cybercrime efforts. Specifically, in our study, we depart from the extant literature by focusing on two unique characteristics of the data breach battle: information sharing and network effects which we briefly discussed below.

### *Information Sharing and Network Effects*

The literature on information sharing originates from the micro economics theory on incentive mechanisms and has been recently applied to the context of information security (Campbell et al. 2003; Cavusoglu et al. 2004; Gal-Or and Ghose 2005; Gordon and Loeb 2002; Liu et al. 2013). The primary premise in these studies is that organizations often withhold or delay release of security breach-related information due to concerns about the potential negative impact on the tangible (i.e. stock prices, sales, etc.) and intangible (i.e., reputation, customer loyalty, etc.) assets of their organizations, even though such a sharing could lead to a mutual beneficial outcome for both individual organizations and the entire industry in the long run (Gal-Or and Ghose, 2005). By taking advantage of such private incentives, hackers can repeatedly use the same tools to exploit similar vulnerabilities in other peer organizations, which in turn results in the wide proliferation of these malicious tools, lower costs of attacks, and increasing financial loss on victim firms.

Realizing such an inefficiency in fighting cybercrime, over the last couple of decades, the U.S. federal government has encouraged the establishment of security based information sharing organizations (SB/ISOs) such as ISACs, Computer Emergency Response Teams (CERT), InfraGard (partnership between the FBI and the private sector), and the U.S. Secret Service Electronic Crimes Task Forces and Working Groups (ECTF) (Gal-Or and Ghose 2005; Gordon et al. 2003; Hausken 2007). Establishment of ISACs was encouraged in May 1998 under Presidential Decision Directive (PDD) 63 in order to protect critical infrastructure of the United States. On May 14, 2014, the Retail Industry Leaders Association launched an independent organization known as the Retail Cyber Intelligence Sharing Center (R-CISC), which operates the Retail Information Sharing and Analysis Center (Retail-ISAC) (Lennon 2014). The Retail-ISAC allows the retail industry to share cyber intelligence on incidents, threats, vulnerabilities, and security controls (Retail Leader Industry Association 2015). R-CISC was formed through input of more than 50 U.S. retailers, including American Eagle Outfitters, Gap, J.C. Penney Company, Lowe's Companies, Nike, Safeway, Target Corporation, VF Corporation and Walgreens (Lennon 2014).

The establishment of the security-related information sharing agencies is likely to have a profound impact on our efforts to safeguard organizations and individuals against cybercrime, especially for the retail industry whose routine business processes rely heavily on the integrity of customer and organizational data. As shown in the prior studies that analyze the consequences of establishing the aforementioned organizations (Gal-Or and Ghose 2005; Gordon et al. 2003), information sharing activities may leverage the power of the network to create positive externalities, also known as network effects (Katz and Shapiro 1986), which arise when the welfare of the individual member in the network depends on the consumption or contribution of other members in the network, and hence the value of the network increases exponentially with the number of members joining the network (Shapiro and Varian 1999).

In the context of security information sharing, the accuracy and timeliness of threat detection, analysis, and alerts depend critically on the amount of information collected and extrapolated. Often times, a small trait in the hacking activities allows experts to uncover the details of the entire criminal process, and the probability of such an outcome is positively associated with the amount of the information reported, the timing of the report, and the number of sources. In this regard, the retail industry is more likely to see the presence of such a positive network effect due to the similarity in their business transactions, as many retailers adopt similar IT infrastructure and/or data storage and transmission technologies. This similarity certainly entices persistent attacks from cyber criminals who have successfully compromised other retailers' similar systems, but at the same time also results in higher return of information sharing, if implemented and executed successfully. Therefore, if network effects brought by these information sharing networks do arise, then over time, we should see a significant reduction in the number of successful breaches, and possibly a decline in the total number of attacks, as more effective detection mechanisms will not only increase the difficulty level required to develop malicious tools, but also deter the attempts of the hackers. In the literature on network effects, the strength of network effects is usually measured by the size of the network installed base (Brynjolfsson and Kemerer 1996; Keith et al. 2013). In this study, the installed base is measured by the number of member organizations participating in an information sharing network. Since a larger information sharing network size not only increases the likelihood of capturing the patterns and tools used by hackers, but also maximize the benefits of sharing these information (more members can be alerted), we propose that:

**Hypothesis 1a:** *The installed base of a security breach-related information sharing alliance within an industry has a negative impact on the total number of industry wide security breaches.*

While large information sharing network size contributes to the likelihood of capturing and disseminating critical security-related information, the effectiveness of information sharing also depends on the extent of sharing within the network, which is measured by total the number of security vulnerability and alerts announced and distributed within the information sharing network. As more security vulnerabilities are identified and distributed, more members can be protected. Specifically, we propose that:

**Hypothesis 1b:** *The extent of the security breach-related information sharing activities within an industry has a negative impact on the total number of industry wide security breaches*.

## *Supply and Demand in the Cyber Black Market*

A typical cyber black market includes a hierarchy of participants that consists of market administrators, suppliers, vendors, intermediaries, and buyers for products and services[1] involved in digitally based crime (Ablon et al. 2014). Two major types of players are suppliers, who often have the dual masks of both technical experts and tool sellers, and buyers who may be individuals, criminal organizations, or commercial vendors. These markets emerged in the early to mid-2000s with an initial focus on credit card data and expanded to also target credentials for eCommerce and social media sites. The ubiquity of the Internet, along with easy access to different types of social media sites, forums, and chat channels where goods can be bought and sold, has resulted in a rapid increase in the number of individuals participating in these marketplaces. Some of these organizations contain 70,000-80,000 individuals and bring in hundreds of millions of dollars (Ablon et al. 2014).

Surprisingly (or maybe not surprisingly), the cyber black market also follows the economic law of supply and demand. The price of a particular tool or service depends primarily on two factors, the number of similar tools available in the market (and the prices of their competitors), and the effectiveness of the tool. Following earlier discussion, if the information sharing mechanisms can successfully prevent exploits by the commonly used malicious tools, then a direct consequence will be a reduction in the attractiveness of these vicious tools, and consequently their prices. If we use the security breaches as a proxy for the effectiveness of the malicious hacking tools, if follows that:

**Hypothesis 2a:** *The total number of security breaches is positively associated with the price of the existing malicious hacking tools or services.*

As current hacking tools are increasingly identified by the information sharing efforts and the associated vulnerabilities are patched, hackers will have to spend more time and efforts to develop new and more effective malicious tools that can bypass the much enhanced detective and preventive systems, which dramatically increases the cost of development. Therefore, as the number of security breaches (or the effectiveness of the tools) decreases, we should expect the hackers to charge a much higher price for their newly developed malicious tools. To illustrate this relationship, we predict that:

**Hypothesis 2b:** *The total number of security breaches is negatively associated with price of the newly released malicious hacking tools.*

At the same time, as these criminals quickly realize that their products only have a very short life span and customers will quickly turn to newer tools due to lower reusability of the existing tools, they will be forced develop and release new tools at a much higher frequency, so as to remain competitive in the market. Consequently, we propose that:

**Hypothesis 2c:** *The total number of security breaches is negatively associated with the frequency of the release of the new malicious hacking tools.*

## *Negative Network Effects in the Cyber Black Market*

As discussed earlier, network effects generally create positive externalities and benefit all network participants. However, negative network effects may arise when excessive use of the network impose significant usage-related cost that has to be shared by its members (Asvanund et al. 2004). Examples include congestion on the highway, energy service interruption due to unbalanced workload, or slow Internet connection due to limited bandwidth and large number of users. In these examples, the value of the membership decreases dramatically as more members join the network. In the context of the cyber black market, driven by the large financial return from selling the breached data, cyber criminals will go after every possible tool they can find in the black market to attempt data breaches. Any reduction in price is more likely to stimulate this mania, and accordingly, more repeated use of the same or a variant of the same tools. In this case, if the information sharing mechanisms are working effectively, such an increase

[1] Examples of goods and services include initial access tools (i.e., zero day vulnerabilities, exploits), payload parts and features (i.e., crypters), payloads (i.e., botnets), enabling services (i.e., spam and phishing services), full services (i.e., hackers for hire, botnets for rent), enabling and operations support products (i.e., infrastructure, cryptanalytic services), digital assets (i.e, credit card information, account information, email login/password, PII), and digital asset commerce and digital laundering (i.e., mule services and counterfeit goods).

in malicious tools usage may only facilitate easier detection of the malicious attempts, as the information regarding the tool becomes part of the ISAC's information sharing inventory.

To a large extent, the abuse of the malicious tools may lead to an effect similar to negative network effects caused by congestion. When the cyber black market is flooded with cheap but relatively ineffective or quickly obsolete tools, it will have two opposing consequences. On one hand it will lead to more attacks of the organization's information systems. On the other hand, these attacks may result in much lower success rates, hence fewer successful breaches. Therefore, as hacking tools proliferate in the black market, the effectiveness of the information sharing efforts will be enhanced and we expect to see that:

**Hypothesis 3a:** *The size of the installed base of the cyber black market positively moderates the relationship between the information sharing efforts and the total number of industry-wide security breaches.*

Moreover, even though in the short run the price reduction may drive more usage of the malicious tools, in the long run such a price-driven demand will diminish due to lower likelihood of penetration using these short-lived tools, and greater chance of being caught. If the above conjecture holds, then the growth of the cyber black market will fall into a negative feedback loop as predicted in the network effects theory (Shapiro and Varian 1999). A similar situation often arises in a market where the demand is driven by cheap but low quality products, and vendors have to constantly reduce product quality in order to remain competitive. Ultimately the market collapses due to unhealthy dynamics. In this study, we define short run as a period of one month or less, as the underground cybercrime market is highly volatile and it only takes a few weeks for the market to pick up any shock in supply and demand (Paganini 2014). Accordingly, long run is defined as a period over three months, as this is generally the period of time needed for an information sharing network to track down the origin of the hacking tools and issue warnings or countermeasures for them (Liu et al. 2011). Based on these discussions, we theorize that:

**Hypothesis 3b:** *The decrease in the prices of the malicious hacking tool will lead to an increase in the installed base of the cyber black market in the short term.*

**Hypothesis 3c:** *The decrease in the prices of the malicious hacking tool will lead to a decrease in the installed base of the cyber black market in the long term.*

## *Organizational Factors*

In addition to the information sharing mechanisms, organizational factors also play an equally important role in curbing cybercrime and complement the efforts by organizations such as ISACs. It is imperative that each organization invest in both technical and behavioral protective measures to minimize the chances of exploits. These include but are not limited to a strong security posture (i.e., security policy, including provisions recommended for retail industry secured remote access, secured access to PCI environment, application whitelisting on critical assets, managed privileged accounts, strong passwords, restricted access to internet, antivirus, POS software applications up to date, firewall installed), presence of Chief Information Security Officer (CISO/CSO) position, presence of important plans (incident response, disaster recovery, business continuity), management support (Harris 2013; Mandiant 2015; Ponemon Institute 2014). These organizational factors will serve as control variables for the level of security protection when we measure the relationship between the information sharing efforts and the number of breaches.

## *Research Model*

As stated earlier, the entities examined in the hypotheses presented above are inter-connected and a change in one of these entities or hypothesized relationships may have a series of transitive consequences on other associated entities and relationships. In order to provide a holistic view of their connections, we present an integrated research model that bridges these eight hypotheses in Figure 1.

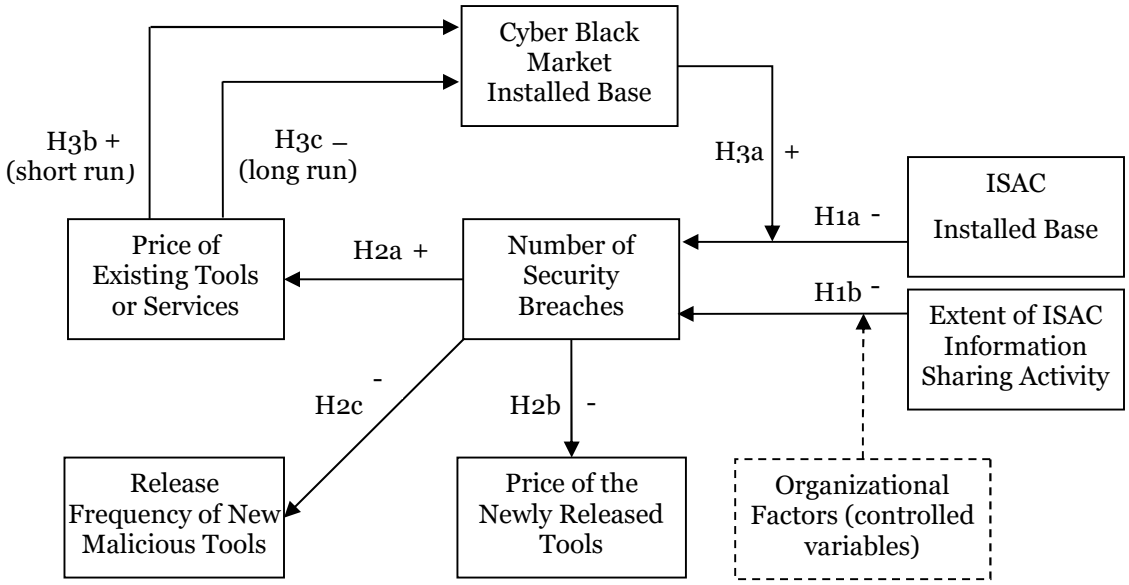


**Figure 1. Proposed Theoretical Model**

## Data and Plan for Empirical Analysis

In the security literature, due to the difficulty to obtain breach-related data and hacker's information, most studies have focused on examining the relationship between the organizations preventive actions (i.e. through surveys or organization reports) and their outcomes (i.e. using the publicly announced number of breaches). Very few studies have attempted to investigate the dynamics in the underground cybercrime market. This study attempts to fill this gap by applying an economics lens to both the bright and dark sides of data breach battlefield. To test our hypotheses, we will compile a longitudinal data set that consists of monthly measures of the variables presented in our research model. We have started our data collection efforts in the retail industry and will expand our efforts into the financial service sector (Liu et al. 2013) and other industries, provided that equivalent data are available.

In Hypothesis 1a, the installed base of the information sharing alliance will be measured by the number of members that participate in an information sharing alliance such as the Retail-ISAC which was recently formed in 2014[2]. We will also collect data on the monthly membership size of the National Retail Federation (NRF, which plans to ultimately integrate its platform with R-CISC) (Higgins 2014).

In Hypothesis 1b, the level of the information sharing activities can be measured by the number of threat announcements, threat and vulnerability alerts, and security warnings that an information sharing alliance such as NRF publish in a given month. NRF also publishes annual reports that date back to 2009 and began running a threat alert system since early June 2014 (Higgins 2014).

For the number of breaches variable, we plan to collect the number security breaches reported and distributed by NRF on monthly basis, and complement this dataset using security breach data published by the Privacy Rights Clearinghouse data source as well as other data sources including U.S. state Attorney General security breach data, DataBreaches.net, DataLossDB (Open Security Foundation 2015), PHIprivacy.net, and media analysis through LexisNexis.

The variables involved in H2a through H2c and H3a present the greatest challenge of this study. We have identified several underground black market sites for our data collection efforts. Data on the number of malicious tools and services and theirs prices will be scraped from these websites using a software agent. As expected, data on the actual users of these malicious tools (the installed base variable) are impossible

[2] http://www.r-cisc.org/

to find. However, we will be able to obtain web traffic data (the number of visitors to a given website) on cyber black market sits through some web traffic monitor sites (i.e., Alexa traffic ranks), which will be used as a proxy for installed base in the black market.

Methodologically, Structural equation modeling (SEM) will be used to empirically estimate the model as SEM is the best option for a non-traditional variance model. Since our model involves a chain of relationships that form a closed loop, SEM will allow us to measure the hypothesized relationships between variables without isolating the effects of associated variables. When estimating the model, lagged values of the outcome variables will be used as many of these relationships takes months or even quarters to be realized.

In a preliminary analysis, we found that the data we have collected so far are consistent with our H1a and Gal-Or and Ghose (2005) finding that information sharing may result in prevention of future breaches. By analyzing 917 data breaches occurred between 2013 and 2014 obtained from Privacy Rights Clearinghouse data source (Privacy Rights Clearinghouse 2015c), we found that the number of retail breaches appeared to decrease in 2014 as compared to 2013, possibly associated with the instantiation of Retail-ISAC as well as institution of threat alert system from NRF. Our data collection effort will continue after our ICIS paper submission and is expected to last for six months, which will be right in time for us to present the results at ICIS in December 2015.

## Expected Contribution and Future Work

This paper was motivated by the growing data breach-related cybercrime activities confronting organizations and collaborative industry efforts to respond to these security challenges. Building on the extant literature on information sharing and network effects, we attempt to apply a unique economic lens to industries plagued with data breach-driven security attacks. In particular, we are interested in exploring how the number of security breaches may change as a result of two opposing network effects in the data breach battlefield, namely, the positive network effects driven by industry-wide information sharing efforts, and the negative network effects driven by the supply and demand changes in the underground cybercrime ecosystem, and whether a feedback loop can be formed in the underground cybercrime economy so that the information sharing efforts can influence the costs and availability of malicious tools in this market and suppress the demand for these tools. To the best of our knowledge, our paper is one of the first academic studies to focus on the underground cyber black market and empirically examine the effectiveness of information sharing in the security domain. The results of our study will provide important support and guidance for policy makers and industry leaders in improving collaborative inter-organizational mechanisms to enhance industry wide information security, and illuminate a new way to monitor and curtail the flow of cyber-criminal activities.

## Acknowledgements

Michele Maasberg was a Kudla Fellow at the University of Texas at San Antonio while working on this paper. She thanks the Fellowship program for its support during the 2013-2015 academic year.

## References

Ablon, L., Libicki, M. C., and Golay, A. A. 2014. *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Santa Monica, CA: RAND Corporation.

Agrawal, M., Hariharan, G., Rao, H. R., and Kishore, R. 2013. "Competition In Mediation Services: Modeling the Role of Expertise, Satisfaction, and Switching Costs," *Journal of Organizational Computing and Electronic Commerce* (23:3), pp. 169–199 (doi: 10.1080/10919392.2013.807711).

Asvanund, A., Clay, K., Krishnan, R., and Smith, M. D. 2004. "An Empirical Analysis of Network Externalities in Peer-to-Peer Music-Sharing Networks," *Information Systems Research* (15:2), pp. 155–174 (doi: 10.1287/isre.1040.0020).

Bagchi, K., and Udo, G. 2003. "An analysis of the growth of computer and Internet security breaches," *Communications of the Association for Information Systems* (12:1), p. 46.

Bennett, C. 2015. "Feds search for ways to impede 'cyber bazaar,'" *The Hill*, March 15 (available at http://thehill.com/policy/cybersecurity/235726-feds-search-for-ways-to-impede-cyber-bazaar; retrieved March 25, 2015).

Brynjolfsson, E., and Kemerer, C. F. 1996. "Network externalities in microcomputer software: An econometric analysis of the spreadsheet market," *Management Science* (42:12), pp. 1627–1647.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly* (34:3), pp. 523–548.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. 2003. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," *Journal of Computer Security* (11:3), pp. 431–448.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "A model for evaluating IT security investments," *Communications of the ACM* (47:7), pp. 87–92.

Chen, P.-Y., Kataria, G., and Krishnan, R. 2011. "Correlated failures, diversification, and information security risk management," *MIS Quarterly* (35:2), pp. 397–422.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future directions for behavioral information security research," *Computers & Security* (32), pp. 90–101 (doi: 10.1016/j.cose.2012.09.010).

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* (33:4), pp. 673–687.

D'Arcy, J., and Greene, G. 2014. "Security culture and the employment relationship as drivers of employees' security compliance," *Information Management & Computer Security* (22:5), pp. 474–489 (doi: 10.1108/IMCS-08-2013-0057).

Das, S., Mukhopadhyay, A., and Anand, M. 2012. "Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics," *Journal of Information Privacy & Security* (8:4), p. 27.

Frei, S. 2014. "Analyst Brief - Why Your Data Breach is My Problem," Austin, TX: NSS Labs, pp. 1–14.

Gal-Or, E., and Ghose, A. 2005. "The economic incentives for sharing security information," *Information Systems Research* (16:2), pp. 186–208 (doi: 10.1287/isre.1050.0053).

Garg, A., Curtis, J., and Halper, H. 2003. "Quantifying the financial impact of IT security breaches," *Information Management & Computer Security* (11:2), pp. 74–83 (doi: 10.1108/09685220310468646).

Gordon, L. A., and Loeb, M. P. 2002. "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)* (5:4), pp. 438–457.

Gordon, L. A., Loeb, M. P., and Lucyshyn, W. 2003. "Sharing information on computer systems security: An economic analysis," *Journal of Accounting and Public Policy* (22:6), pp. 461–485 (doi: 10.1016/j.jaccpubpol.2003.09.001).

Gordon, L. A., Loeb, M. P., and Sohail, T. 2010. "Market value of voluntary disclosures concerning information security," *MIS quarterly* (34:3), pp. 567–594.

Gordon, L. A., Loeb, M. P., and Zhou, L. 2011. "The impact of information security breaches: Has there been a downward shift in costs?" *Journal of Computer Security* (19:1), pp. 33–56.

Harris, S. 2013. *CISSP All in One Exam Guide* (6th ed.), New York: McGraw Hill Companies.

Hausken, K. 2007. "Information sharing among firms and cyber-attacks," *Journal of Accounting and Public Policy* (26:6), pp. 639–688 (doi: 10.1016/j.jaccpubpol.2007.10.001).

Higgins, K. J. 2014. "Retailers Now Actively Sharing Cyberthreat Intelligence," *InformationWeek DARKReading*, October 30 (available at http://www.darkreading.com/attacks-breaches/retailers-now-actively-sharing-cyberthreat-intelligence/d/d-id/1317086; retrieved April 20, 2015).

Kannan, K., Rees, J., and Sridhar, S. 2007. "Market Reactions to Information Security Breach Announcements: An Empirical Analysis," *International Journal of Electronic Commerce* (12:1), pp. 69–91 (doi: 10.2753/JEC1086-4415120103).

Katz, M. L., and Shapiro, C. 1986. "Technology adoption in the presence of network externalities," *The journal of political economy*, pp. 822–841.

Keith, M. J., Babb, J., Lowry, P. B., Furner, C., and Abdullat, A. 2013. "The Roles of privacy assurance, network effects, and information cascades in the adoption of and willingness to pay for location-based services with mobile applications," in *Proceedings of the Dewald Roode Workshop in Information Systems Security 2011*, Blacksburg, VA, September (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2287446).

Krebs, B. 2014. "Home Depot Hit By Same Malware as Target," *KrebsonSecurity In-depth security news and investigation*, September (available at http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/; retrieved March 24, 2015).

Lennon, M. 2014. "Retailers Share Cyber Attack Data Through New Retail-ISAC," *SecurityWeek*, May 15 (available at http://www.securityweek.com/retailers-share-cyber-threat-intelligence-through-new-retail-isac; retrieved March 23, 2015).

Liu, C., Zafar, H., and Au, Y. A. 2013. "Rethinking FS-ISAC: An IT Security Information Sharing Model for the Financial Services Sector," (available at http://digitalcommons.kennesaw.edu/facpubs/3148/).

Liu, D., Ji, Y., and Mookerjee, V. 2011. "Knowledge sharing and investment decisions in information security," *Decision Support Systems* (52:1), pp. 95–107 (doi: 10.1016/j.dss.2011.05.007).

Lowry, P. B., Posey, C., Roberts, T. L., and Bennett, R. J. 2014. "Is Your Banker Leaking Your Personal Information? The Roles of Ethics and Individual-Level Cultural Characteristics in Predicting Organizational Computer Abuse," *Journal of Business Ethics* (121:3), pp. 385–401 (doi: 10.1007/s10551-013-1705-3).

Luo, X. (Robert), Zhang, W., Burd, S., and Seazzu, A. 2013. "Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration," *Computers & Security* (38), pp. 28–38 (doi: 10.1016/j.cose.2012.12.003).

Mandiant. 2015. "M-Trends 2015: A View From the Front Lines," No. RPT.MTRENDS.EN-US.022415, pp. 1–24 (available at https://www2.fireeye.com/WEB-2015RPTM-Trends.html).

McCarthy, C., Harnett, K., and Hatipoglu, C. 2014. "Assessment of the Information Sharing and Analysis Center Model," No. DOT HS 812 076, Washington, DC: National Highway Traffic Safety Administration.

Mookerjee, V., Mookerjee, R., Bensoussan, A., and Yue, W. T. 2011. "When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination," *Information Systems Research* (22:3), pp. 606–623 (doi: 10.1287/isre.1100.0341).

Open Security Foundation. 2015. "About OSF Data Loss,"

Paganini, P. 2014. "Pricing Policies in the Cyber Criminal Underground," *InfoSec Institute* (available at http://resources.infosecinstitute.com/pricing-policies-cyber-criminal-underground/; retrieved March 30, 2015).

Ponemon Institute. 2014. "2014 Cost of Data Breach Study: United States," No. SEL03017-USEN-01, Traverse City, MI: Ponemon Institute LLC, pp. 1–25 (available at http://databreachinsurancequote.com/wp-content/uploads/2014/11/2014-Cost-of-a-DB-Study.pdf).

Posey, C., Roberts, T., Lowry, P. B., Bennett, B., and Courtney, J. 2013. "Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors," *Mis Quarterly* (37:4), pp. 1189–1210.

Privacy Rights Clearinghouse. 2015a. "Staples, Inc.," *Staples, Inc.* (available at https://www.privacyrights.org/data-breach-asc?title=staples; retrieved March 23, 2015).

Privacy Rights Clearinghouse. 2015b. "The Home Depot," *Privacy Rights Clearinghouse* (available at https://www.privacyrights.org/data-breach-asc?title=home+depot; retrieved March 24, 2015).

Privacy Rights Clearinghouse. 2015c. "Chronology of Data Breaches: Security Breaches 2005-Present," *Privacy Rights Clearinghouse* (available at https://www.privacyrights.org/data-breach; retrieved April 8, 2015).

Retail Leader Industry Association. 2015. "R-CISC Retail Cyber Intelligence Sharing Center," (available at http://www.rila.org/rcisc/home/Pages/default.aspx; retrieved March 23, 2015).

Shapiro, C., and Varian, H. R. 1999. *Information Rules A Strategic Guide to the Network Economy*, Boston: Harvard Business Review Press.

Shaw, A. 2009. "Data breach: from notification to prevention using PCI DSS," *Colum. JL & Soc. Probs.* (43), p. 517.

Siponen, M., Adam Mahmood, M., and Pahnila, S. 2014. "Employees' adherence to information security policies: An exploratory field study," *Information & Management* (51:2), pp. 217–224 (doi: 10.1016/j.im.2013.08.006).

Straub, D. W., and Welke, R. W. 1998. "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, pp. 441–469.

Vance, A., Lowry, P. B., and Eggett, D. L. 2015. "Increasing Accountability Through User-Interface Design Artifacts: A New Approach to Addressing the Problem of Access-Policy Violations," *MIS Quarterly, Forthcoming* (available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2549000).

Verizon. 2015. "2015 Data Breach Investigations Report," No. WP16368, Verizon.

Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. 2011. "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Systems* (51:3), pp. 576–586 (doi: 10.1016/j.dss.2011.03.002).

Yue, W. T., and Çakanyıldırım, M. 2010. "A cost-based analysis of intrusion detection system configuration under active or passive response," *Decision Support Systems* (50:1), pp. 21–31 (doi: 10.1016/j.dss.2010.06.001).