NETWORKS OF CYBERCRIME PREVENTION

A PROCESS STUDY OF THE CREDIT CARD

Research in Progress

Dahabiyeh, Laila, Warwick Business School, University of Warwick, Coventry, UK,
phd13ld@mail.wbs.ac.uk

Abstract

This research-in-progress paper reports on a project that seeks to develop a new process perspective on incentive mechanisms in cybercrime prevention networks. Adopting such a view is of great importance given the continuous innovations in cybercrime that makes fighting it a constant endeavour, involving actors from multiple networks. To this end, we zoom in on specific prevention encounters occurring throughout the process of producing prevention measures, to identify incentive mechanisms needed to bring heterogeneous actors together in cybercrime prevention networks. Our longitudinal case study of credit card fraud and how it has developed over time resulted in identifying eleven prevention encounters that are critical in the fraud prevention lifecycle. Upon completion of this research, we anticipate to contribute to current literature on security networks in three ways. First, offer a new understanding on incentive mechanisms that accounts for the role of contextual conditions in shaping these incentives. Second, add diversity to research methods used to study incentives by adopting a qualitative case study approach. Third, we shed more light on the role of technology in building incentive mechanisms in cybercrime prevention networks.

Keywords: cybercrime, IS security, networks, incentives, credit card, credit card fraud, prevention encounters, extra-organizational settings

1 Introduction

Cybercrime comes with significant cost. It is estimated that the global economic cost of cybercrime can reach up to $400 billion (McAfee, 2014). This makes the phenomenon a serious problem (Chung et al., 2006), not least since there is little sign that the fight against cybercrime beats the emergence of new types of crime (Hunton, 2009).

Besides its economic challenges, the threat of cybercrime rises from its networked nature. Today's interconnected business environment increases organizations' vulnerability to security attacks (Dhillon and Backhouse, 2001, Straub and Welke, 1998) as security is no longer confined by organizational boundaries but transcends them to be dependent on all those operating on the same network (Anderson and Moore, 2006, Zhao et al., 2013). As an example, the well-known Target security breach was not caused by insufficient security controls from the retailer's side, but rather from a deficiency in one of its contractor security system.

The origins of security threats are thus manifold (Mookerjee et al., 2011, Smith et al., 2007); as organizations seek to fix one loophole another emerges. This makes security attacks exceed a single organi-

zation's capability of fighting them (Gupta and Zhdanov, 2012, Kunreuther and Heal, 2003, Smith et al., 2007). Hence, IS security is no longer only a matter of organizational processes (Bulgurcu et al., 2010, Posey et al., 2013, Puhakainen and Siponen, 2010, Siponen, 2000, Straub, 1990), but is also expanded to include extra-organizational settings (Straub et al., 2008, Whittington, 2006) that recognize the open systems organizations operate in (Katz and Kahn, 1966, Kast and Rosenzwe, 1972). Studying organizations from a "population of organizations" perspective therefore might be more insightful and offer new knowledge in comparison to a "single organization" view (Aldrich, 1971) .We focus on extra-organizational settings and use this concept to refer to the wider context that exists outside organizational boundaries where organizations get involved in information and resource sharing in order to better secure their systems. Therefore, we envisage security efforts rising from multiple actors who come together (converge) and form networks, and define networks of cybercrime prevention as *collective efforts pursued by distributed actors operating on the same network, whether directly or indirectly, to develop or adopt different measures to maintain the security of their network.*

Adopting this network perspective on cybercrime prevention brings forward a focal question of the incentives necessary to ensure enrollment and active involvement of the network various actors. IS security literature identifies different incentives schemes used to align actors' interests in security networks, those range from rewards and subsidies to liability and cost sharing (Cavusoglu et al., 2008, Liu et al., 2014, Gal-Or and Ghose, 2005, Hui et al., 2012). Despite offering valuable knowledge, this literature tends to study incentives through static models (Cezar et al., 2014, August and Tunca, 2011). As security threats (Hunton, 2009) and actors' interests evolve over time (Kaplan and Henderson, 2005), incentive mechanisms are expected to change to adjust to such transformations (August and Tunca, 2011). A process view on incentives is therefore expected to provide richer understanding on incentive mechanisms needed to prevent cybercrime. This is of great importance given the diversity of actors required to fight the plethora of cybercrime emerging every day.

This research-in-progress seeks to answer the question of *what are the incentive mechanisms for converging heterogeneous actors to develop and adopt prevention measures to fight cybercrime?* To address this question, we are conducting a case study of credit card fraud as it has developed over the past fifty years. This historical coverage enables us to observe and trace changes in incentives coinciding with different prevention measures, and examine how contextual conditions shape incentive structures. We focus on specific prevention encounters between actors that shake an established pattern of how cybercrime is prevented. These encounters are identified and explored using a qualitative, historical case (Mason et al., 1997). The data was collected from multiple sources: trade publications, journal articles, books, industry reports, and legal and government documents.

This research seeks to offer a number of contributions. First, we develop a new process perspective on incentive mechanisms in cybercrime prevention networks. Second, we enrich the literature that examines incentives through analytical models based on rational choice by offering an empirical qualitative study on incentives. Further, our historical research approach provides diversity needed in IS security research (Siponen, 2005). Third, we shed more light on technology as a crucial player in cybercrime prevention networks that has been understudied, and examine its role in building needed incentive mechanisms.

The paper proceeds with an overview of incentives for collective effort in cybercrime prevention, followed by our framing of incentive mechanisms in cybercrime prevention networks. We then describe our research design and method, and end with preliminary findings and conclusion.

2 Incentives for Collective effort in Cybercrime Prevention

The spread of security breaches across organizations from different sectors shifted security efforts to emphasize the importance of collaboration to halt the progression of the phenomenon (Gal-Or and Ghose, 2005, Gupta and Zhdanov, 2012). Collective effort to prevent cybercrime is evident in the

emergence of various security networks[1] that aim to harness the effort of various actors to build a secure environment. Such networks include; Information Sharing and Analysis Center, such as Financial Services Information Sharing and Analysis Center, and Vulnerability Disclosure Networks, as Computer Emergency Response Team and iDefense.

There are different motives for actors to contribute[2] to collective effort towards security. *Cost savings* is a dominant incentive in cybercrime prevention networks. Security is expensive; the complexity of technological solutions, the need for professional security staff, along with external pressure to meet certain security requirements (such as Payment Card Industry Standards), make security exceed allocated budget (Hui et al., 2012). To alleviate part of this high costs, organizations participate in security networks where they save costs either directly through passing security functions to specialized service providers, taking advantage of their economies of scale (Schechter and Smith, 2003, Cezar et al., 2010). Or indirectly by receiving information that makes their security investment more targeted (Gal-Or and Ghose, 2005). For instance, information regarding a particular vulnerability in software X (e.g. firewall, intrusion detection system) may cause an organization to reconsider its security investment and shift to another more secure product, eliminating by this unnecessary costs. Having access to security breach incidents enables the application of quick prevention measures that protect organizations from falling into the same security trap and costs associated with that. Organizations are increasingly looking at security networks as a way to substitute high investment in security and reduce overall costs (Gordon et al., 2003, Hausken, 2007).

Increasing demands is another incentive for participating in security networks. Operating in today's competitive business environment, organizations seek to be more alert to actions competitors take and the different strategies to maintain or increase their market share; security networks offer such an opportunity. Sharing information about security status opens a window for organizations to increase their sales due to demand spillover (Gal-Or and Ghose, 2005; Cezar et al. 2010). A technical flaw in one company's product may shift demand to competitor's product increasing by this its profits. Organizations that believe security networks can increase demands on their products are more inclined to get involved in these networks.

Organizations security actions have a major impact on their reputation and market value (Yayla and Hu, 2011, Cavusoglu et al., 2007). By participating in security networks where organizations collaborate and share best security practices, organizations *signal* their commitment to security, and emphasize their responsibility towards their stakeholders (Gal-Or and Ghose, 2005), relieving by this customers anxiety regarding the security of their personal information and maintaining their trust. In addition, joining such collective effort indicates that security threats once identified, rapid corrective actions will follow, decreasing the value of the threat and making organizations less attractive to attackers (Ransbotham et al., 2012, Schechter and Smith, 2003, Gupta and Zhdanov, 2012, Kannan and Telang, 2005). Organizations thus benefit from the different signals they send when becoming part of security networks, which give them incentives not only to join these networks but also to be active members as well. For instance, software vendors' fear of the impact discovered vulnerabilities in their products might have on the quality perceived of their overall services gives them more inclination to supply their clients with corrective patches in a timely manner (Arora et al., 2010).

[1] In this paper, security networks and cybercrime prevention networks are used interchangeably.

[2] Contributing to collective effort include both participating in security networks and active involvement to attain security in these networks.

Liability for security breaches is a recognized approach to drive genuine security efforts in security networks (August and Tunca, 2011; Liu et al., 2014), and a reason why some organizations decide to join these networks (Zhao et al., 2013). Liability policies, which are often incorporated in service level agreements and membership rules, put more pressure on the responsible party by increasing the cost of security in case of failure to meet specified conditions, stimulating better security behaviour. At the same time, liability can be seen by some as an opportunity to transfer security risks to other actors giving them further motivations to participate in security networks. Besides benefits from accumulated knowledge and expertise, organizations outsource their security functions to move liability burden from themselves to the outsourcer (Rowe, 2007).

3 A Process View on Incentive Mechanisms in Cybercrime Prevention Networks

Current literature shows that if collective effort to prevent cybercrime is to survive, it is the incentives that bring actors together that have to be ensured. Despite the valuable knowledge this literature gives on incentives to explain why actors decide to contribute to collective effort, we argue that our knowledge of incentives is derived from a limited and static view on collective effort to prevent cybercrime, which confine the phenomenon to pre-existing security networks, such as CERT and FS-ISAC, and examine relationships between actors through predefined set of variables (Mohr, 1982), for instance the impact of security costs on incentives to share security information, or vulnerabilities' severity on speed of releasing patches, which may deviate when confronting real-life situations (Cowen, 1998).

Little is known therefore about the *process* of collective effort to prevent cybercrime, that is, how actors come together to prevent cybercrime by developing and adopting prevention measures over time, and the underlying incentive mechanisms. This is very crucial given the fact that security is a moving target (Mookerjee et al., 2011) where no single prevention measure is sufficient to prevent a certain cybercrime, such as credit card fraud, from occurring. Collective effort for cybercrime prevention is thus a *continuous process* that involves heterogeneous actors (Choo, 2011) with diverse interests that change over time (Kaplan and Henderson 2005). Without the ability to explain how and why actors continuously converge to prevent cybercrime, our knowledge of incentive mechanisms is incomplete (Schelling, 1998). In addition, despite showing the importance of multiple agents in IS security, we note that existing literature tends to shy away from studying technology as a crucial player in preventing cybercrime. The socio-organizational aspect of IS security cannot be undermined, nonetheless how technology is interwoven in it is also important (Dhillon and Backhouse, 2001, Ransbotham and Mitra, 2009).

Knowledge of processes and events taking place while preventing cybercrime is thus crucial to explain how and why actors come together to build a secure environment (Ransbotham et al.2012), and how consequences of certain actions direct future prevention efforts (Zhao et al., 2013; Mookerjee et al. 2011).We will obtain this knowledge by zooming on in specific prevention encounters (Newman and Robey, 1992) that reflect actions taken by heterogeneous actors to develop and adopt prevention measures that shake an established pattern. By this, we focus on critical events that had significant impact on how cybercrime is prevented, and the dynamisms associated with the prevention processes, allowing us to better capture the complexity of the phenomenon (David, 2003). Through following these prevention encounters over time, we acknowledge the dynamic nature of both cybercrime (Mookerjee et al., 2011) and incentive mechanisms (August and Tunca, 2011, Cavusoglu et al., 2008). The former by considering a collective of prevention measures rather than a single one and the latter by examining different contextual conditions where incentives are enacted.

Prevention encounters represent 'windows of opportunity' (Tyre and Orlikowski, 1994) for rethinking current security practices and how cybercrime is prevented. By this, they challenge an established process (Isabella, 1990), and force actors to re-evaluate the effectiveness of existing prevention meas-

ures and negotiate possible future directions (Bettenhausen and Murnighan, 1985). Such interruptions in cybercrime prevention do not come out of thin air; rather they rise from certain events that trigger changes in prevention measures. We refer to these events as prevention encounters triggers, and use the concept to denote to changes in prevention measures due to elements of technology, laws, social pressure, and/or economics (Lessig, 1999). First, the continuous advancements in information technology make it crucial in ensuring information security and confidentiality. This is seen not only through technologies specifically developed to meet this purpose such as cryptography, but also in technologies developed in another domain but find themselves new applications in IS security field (Levinthal, 1998). Second, laws are associated with regulatory bodies' responsibility towards the public perceived in regulations they enact to protect and maximize the social welfare of a society (Blind, 2012). In doing this, laws can change organizations' institutional environment and market mechanisms (Haveman et al., 2001), which in turn impact organizations' current and future security plans. For instance, by mandating public announcement of security breach incidents, security breach notification laws attempt to put more pressure on organizations to implement better security controls (Winn, 2009). Third, social pressure stems from organizations' moral and social responsibility towards their stakeholders (Culnan and Williams, 2009). It entails the voice of external groups who are affected by organization's actions and exert pressure towards more security. Those groups manifest themselves in various forms such as, general public or society groups that advocate consumers' privacy rights (Benston, 1982), or industry groups who seek to draw attention to the severity of a particular phenomenon (Huber, 1991) and the threat it poses on their social and economic fitness (Oliver, 1991). Lastly, economics of information security refer to the cost-benefit trade-off that influence investments level in IS security (Gordon and Loeb, 2002).

4 Research Methods

To develop a process view on incentive mechanisms in cybercrime prevention networks, we chose to use a case study approach. Specifically, we will use a historical case study as longitudinal data enrich process oriented research (Markus and Robey, 1988). Moreover, history is deemed an essential element for understanding present situations and drawing future strategies (Kaplan and Orlikowski, 2013). Longitudinal data reveals "movements from continuity to change and vice versa" (Pettigrew, 1990, p.272) which is consistent with our notion of prevention encounters as critical change opportunities for prevention measures. Our case study approach can be best described as a structured and focused one with emphasis on process-tracing (George and Bennett, 2005). That is, it is structured and guided by our question of identifying incentive mechanisms in cybercrime prevention networks, and focused in terms that from the voluminous data available on the selected case, we only zoom in on the prevention encounters aspect of the phenomenon. As prevention encounters are often associated with different prevention measures, subcases of our general case (Ragin, 1992) can be derived (each prevention encounter is considered a subcase) enabling us to conduct both within and cross-case analysis (Eisenhardt, 1989) to gain deeper understanding of each prevention encounter and identify patterns across them that can explain how actors are induced to contribute to cybercrime prevention.

The case of credit card fraud is selected to generate a process view on incentive mechanisms in cybercrime prevention networks due to a number of reasons. First, the heterogeneity of actors involved in the credit card industry (technology, banks, regulatory agencies, merchants, and customers) and the complexity of their relationships (Lablebici, 2012), make the case 'prevention encounters rich' where through these encounters actors try to motivate the production of prevention measures. Second, statistics show that cybercrime is aimed more toward achieving financial gains, and financial sector is among the top sectors exposed to cybercrime incidents (Choo, 2011, Symantec, 2009). Third, the number of credit card usage in offline and online transactions is in continuous growth (Capgemini and RBS, 2013), making credit cards an indispensable technology in our daily lives. Fourth, credit cards are considered the technology that ignited electronic value exchange (Naar and Stein, 1975), by under-

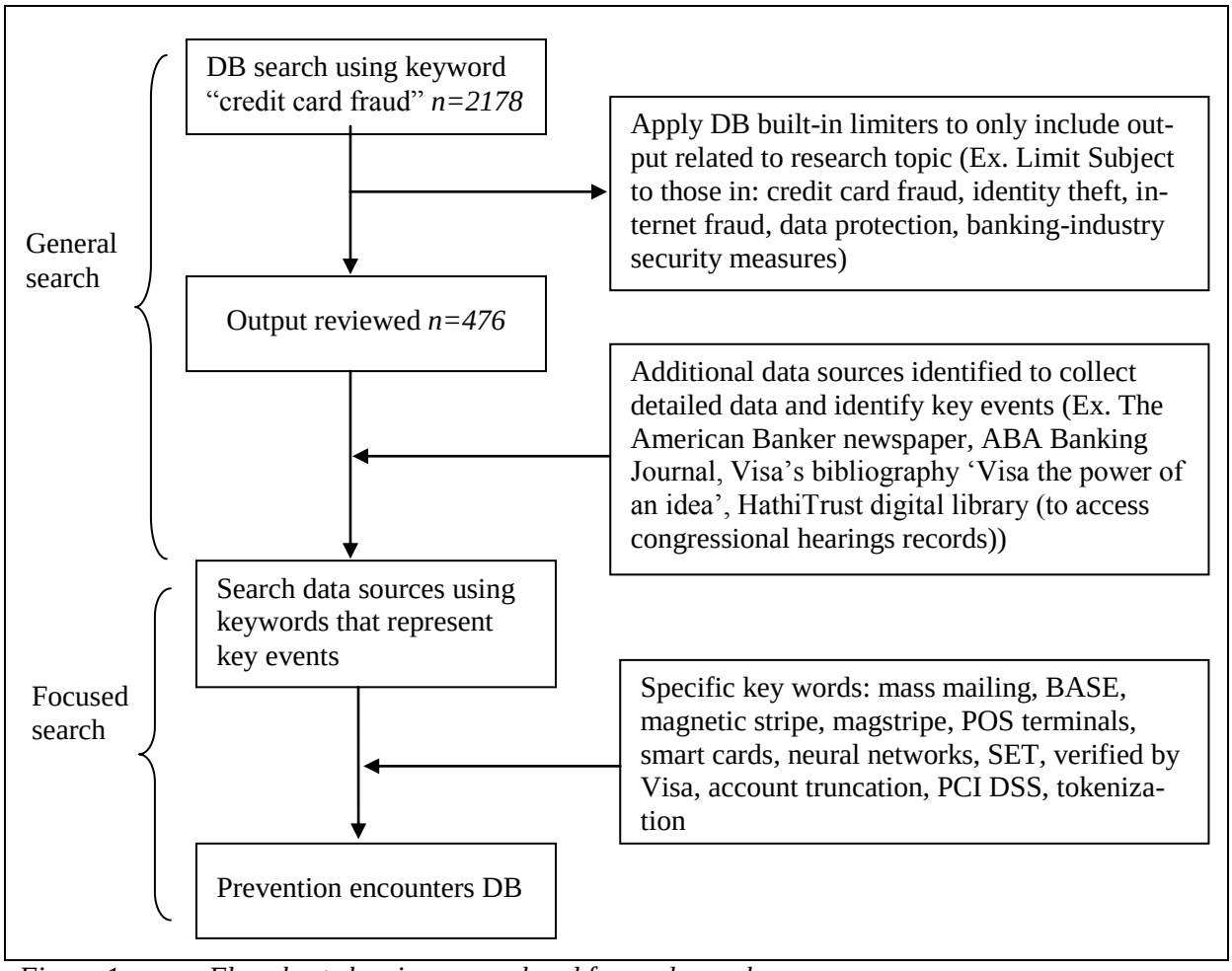

Figure 1. Flowchart showing general and focused search processes.

standing its case we can draw further implications on incentive mechanisms necessary to face security threats rising from continuous innovations in digital payments.
Credit card industry is hence the focus of our research where we will specifically examine the case of *Visa* credit card to explore the different prevention encounters the company was involved in to build and maintain secure credit card transactions.

4.1 Data Collection and Analysis

Data was collected from multiple sources: trade journals, industry reports, books, journal articles, and legal and government documents. This allowed us to structure events in credit card fraud in a timeline and observe how they influence subsequent events (Langley, 1999).

Data collection went through two main steps: general and focused search (see Figure 1). General search, using a broad keyword (credit card fraud), aimed to identify key events (those that encapsulate prevention encounters) using prevention encounters triggers, and build a timeline of these events. Through general search we also identified major data sources to be used in our focused search. The American Banker Journal and ABA Banking Journal were identified the top data sources that are often cited in research targeting credit card industry. The company's biography "Visa the Power of an Idea" as well as its founder's biography "Birth of the Chaordic Age" were also among the highly cited books. Though these last two sources might be biased to favour the company's side, our main purpose was identifying key events and time of their occurrences, and those were further corroborated by data

Steps	Tasks	Outputs
1. General database search	a. Search Business Source Premier using keywords as "credit card fraud". b. Output screening through database built-in filtration criteria, and title and abstract review.	Database of case materials
2. Identifying key events	a. Use prevention encounters triggers to identify key events in the case materials. b. Extract prevention encounters from key events. c. Identify major data sources.	a. Chronology of key events. b. List of major data sources.
3. Focused database search	a. Search database using specific keywords as "POS terminals", "magnetic stripe", "smart card". b. Use identified data sources in collecting further data.	a. Data that enrich our understanding of prevention encounters. b. Prevention encounters database
4. Coding process	a. First cycle coding that summarizes prevention encounters into descriptive codes. b. Second cycle coding to identify patterns and categories within descriptive codes.	a. A list of descriptive codes. b. A list of pattern codes.
5. Identifying incentive mechanisms	a. Analyze patterns to elicit incentive mechanisms. b. Identify incentive mechanisms in cybercrime prevention networks.	Incentive mechanisms for collective action in cybercrime prevention

Table 1. Data collection and analysis process.

collected from other sources. "Electronic Value Exchange: Origins of the Visa Electronic Payment System" was a valuable source with rich data on Visa's use of technology to prevent fraud with useful insights on the associated encounters.

In focused search we sought to collect detailed data on prevention encounters, and the underlying incentives around the development and adoption of various prevention measures. So far, we have identified 11 prevention encounters that are considered critical in preventing credit card fraud. As the analysis process continues, gaps may be identified that require further data collection which might add to our prevention encounters database.

Coding prevention encounters will go through two cycles of coding (Miles et al., 2014). The first cycle of coding involves open coding to generate general descriptive codes regarding prevention encounters, which will then be used to discover patterns and categories within these codes (second cycle) to identify incentive mechanisms for collective action in preventing cybercrime, how they adjust to their context, and whether they differ across prevention encounters.

Table 1 summarizes the data collection and analysis process.

5 Preliminary Findings and Conclusion

Our preliminary analysis shows that cybercrime prevention is a *continuous process of negotiation and conflict resolution*, where incentive mechanisms are essentially about mobilizing and recruiting actors to one's side to win the negotiation. Further, the interdependencies in this process create a *chain of incentives* where recruiting one actor is necessary to recruit another. As we formalize our analysis, we expect to identify and classify incentive mechanisms necessary in cybercrime prevention networks; this can have important implications for policy makers on what strategies to pursue under which condition when fighting this phenomenon.

This research argues that adopting a process view in preventing cybercrime is very crucial given the fact that cybercrime is increasing in intensity and evolving in nature (Hunton, 2009), making the mul-

tiplicity of prevention measures and the heterogeneity of actors involved a natural consequence. By tracing prevention encounters over time, we will be able to reveal the process by which actors converge to prevent cybercrime and the incentive mechanisms necessary for their convergence. In addition, our networks perspective aim to stress the importance of distributed agency in IS security and encourage future research to go beyond studying security within organizational context and consider extra-organizational settings to enrich our understanding of the various aspects affecting this phenomenon. Lastly, we hope that our concept of prevention encounters, which views cybercrime prevention as a result of disruptive processes, create interests among researchers and serve as a building block for future IS security research.

References

Aldrich, H. (1971), "ORGANIZATIONAL BOUNDARIES AND INTER-ORGANIZATIONAL CONFLICT", *Human Relations*, 24 (4), 279-293.

Anderson, R. and Moore, T. (2006), "The economics of information security", *Science*, 314 (5799), 610-613.

August, T. and Tunca, T. I. (2011), "Who should be responsible for software security? A comparative analysis of liability policies in network environments", *Management Science*, 57 (5), 934-959.

Benston, G. J. (1982), "ACCOUNTING AND CORPORATE ACCOUNTABILITY", *Accounting Organizations and Society*, 7 (2), 87-105.

Bettenhausen, K. and Murnighan, J. K. (1985), "THE EMERGENCE OF NORMS IN COMPETITIVE DECISION-MAKING GROUPS", *Administrative Science Quarterly*, 30 (3), 350-372.

Blind, K. (2012), "The influence of regulations on innovation: A quantitative assessment for OECD countries", *Research Policy*, 41 (2), 391-400.

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), 523-548.

Capgemini and RBS (2013), "World Payments Report 2013", Capgemini and Royal Bank of Scotland.

Cavusoglu, H., Cavusoglu, H. and Raghunathan, S. (2007), "Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge", *Ieee Transactions on Software Engineering*, 33 (3), 171-185.

Cavusoglu, H., Cavusoglu, H. and Zhang, J. (2008), "Security patch management: Share the burden or share the damage?", *Management Science*, 54 (4), 657-670.

Cezar, A., Cavusoglu, H. and Raghunathan, S. (2010), "Competition, speculative risks, and IT security outsourcing", *Economics of Information Security and Privacy*, Springer, pp. 301-320.

Cezar, A., Cavusoglu, H. and Raghunathan, S. (2014), "Outsourcing Information Security: Contracting Issues and Security Implications", *Management Science*, 60 (3), 638-657.

Choo, K.-K. R. (2011), "The cyber threat landscape: Challenges and future research directions", *Computers & Security*, 30 (8), 719-731.

Chung, W. Y., Chen, H. C., Chang, W. P. and Chou, S. C. (2006), "Fighting cybercrime: a review and the Taiwan experience", *Decision Support Systems*, 41 (3), 669-682.

Cowen, T. (1998), "Do economists use social mechanisms to explain?", in Hedstrom, P. and Swedberg, R. (Eds.) *Social Mechanisms: An Analytical Approach to Social Theory*, Cambridge University Press, pp. pp. 125-146.

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), 673-687.

David, J. S. (2003), "Discussion of Information transfer among internet firms: The case of hacker attacks", *Journal of Information Systems*, 17 (2), 83-86.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, 11 (2), 127-153.

Eisenhardt, K. M. (1989), "BUILDING THEORIES FROM CASE-STUDY RESEARCH", *Academy of Management Review*, 14 (4), 532-550.

Gal-Or, E. and Ghose, A. (2005), "The economic incentives for sharing security information", *Information Systems Research*, 16 (2), 186-208.

George, A. L. and Bennett, A. (2005), *Case studies and theory development in the social sciences*, Mit Press.

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), 461-485.

Gupta, A. and Zhdanov, D. (2012), "GROWTH AND SUSTAINABILITY OF MANAGED SECURITY SERVICES NETWORKS: AN ECONOMIC PERSPECTIVE", *Mis Quarterly*, 36 (4), 1109-1130.

Hausken, K. (2007), "Information sharing among firms and cyber attacks", *Journal of Accounting and Public Policy*, 26 (6), 639-688.

Haveman, H. A., Russo, M. V. and Meyer, A. D. (2001), "Organizational environments in flux: The impact of regulatory punctuations on organizational domains, CEO succession, and performance", *Organization Science*, 12 (3), 253-273.

Huber, G. P. (1991), "ORGANIZATIONAL LEARNING: THE CONTRIBUTING PROCESSES AND THE LITERATURES", *Organization Science*, 2 (1), 88-115.

Hunton, P. (2009), "The growing phenomenon of crime and the internet: A cybercrime execution and analysis model", *Computer Law & Security Review*, 25 (6), 528-535.

Isabella, L. A. (1990), "EVOLVING INTERPRETATIONS AS A CHANGE UNFOLDS - HOW MANAGERS CONSTRUE KEY ORGANIZATIONAL EVENTS", *Academy of Management Journal*, 33 (1), 7-41.

Kannan, K. and Telang, R. (2005), "Market for software vulnerabilities? Think again", *Management Science*, 51 (5), 726-740.

Kaplan, S. and Henderson, R. (2005), "Inertia and incentives: Bridging organizational economics and organizational theory", *Organization Science*, 16 (5), 509-521.

Kaplan, S. and Orlikowski, W. J. (2013), "Temporal Work in Strategy Making", *Organization Science*, 24 (4), 965-995.

Kast, F. E. and Rosenzwe, J. E. (1972), "GENERAL SYSTEMS THEORY - APPLICATIONS FOR ORGANIZATION AND MANAGEMENT", *Academy of Management Journal*, 15 (4), 447-465.

Katz, D. and Kahn, R. L. (1966), *The Social Psychology of Organizations*, John Wiley & Sons, New York, London.

Kunreuther, H. and Heal, G. (2003), "Interdependent security", *Journal of Risk and Uncertainty*, 26 (2), 231-249.

Lablebici, H. (2012), "THE EVOLUTION OF ALTERNATIVE BUSINESS MODELS AND THE LEGITIMIZATION OF UNIVERSAL CREDIT CARD INDUSTRY: EXPLORING THE CONTESTED TERRAIN WHERE HISTORY AND STRATEGY MEET ", in Kahl, S. J., Silverman, B. S. and Cusumano, M. A. (Eds.) *History and strategy*, Bingley, U.K, Emerald e-book.

Langley, A. (1999), "Strategies for theorizing from process data", *Academy of Management Review*, 24 (4), 691-710.

Lessig, L. (1999), *Code and Other Laws of Cyberspace*, Basic Books, New York.

Levinthal, D. A. (1998), "The slow pace of rapid technological change: gradualism and punctuation in technological change", *Industrial and corporate change*, 7 (2), 217-247.

Markus, M. L. and Robey, D. (1988), "INFORMATION TECHNOLOGY AND ORGANIZATIONAL-CHANGE - CAUSAL-STRUCTURE IN THEORY AND RESEARCH", *Management Science*, 34 (5), 583-598.

Mason, R. O., McKenney, J. L. and Copeland, D. G. (1997), "Developing an historical tradition in MIS research", *MIS Quarterly*, 21 (3), 257-278.

McAfee (2014), "Net Losses:Estimating the Global Cost of Cybercrime ", Center for Strategic and International Studies.

Miles, M. B., Huberman, A. M. and Saldaña, J. (2014), *Qualitative data analysis: A methods sourcebook*, SAGE Publications, Incorporated, Los Angeles; London.

Mohr, L. (1982), "Approaches to Explanation: Variance Theory and Process Theory", *Explaining Organizational Behaviour*, Jossey- Bass Publishers, San Francisco ; London.

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), 606-623.

Naar, A. S. and Stein, S. B. (1975), "EFTS: the computer revolution in electronic banking", *Rutgers J. Computers & L.*, 5, 429-486.

Newman, M. and Robey, D. (1992), "A SOCIAL-PROCESS MODEL OF USER-ANALYST RELATIONSHIPS", *Mis Quarterly*, 16 (2), 249-266.

Oliver, C. (1991), "STRATEGIC RESPONSES TO INSTITUTIONAL PROCESSES", *Academy of Management Review*, 16 (1), 145-179.

Pettigrew, A. M. (1990), "LONGITUDINAL FIELD RESEARCH ON CHANGE: THEORY AND PRACTICE", *Organization Science*, 1 (3), 267-292.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J. and Courtney, J. F. (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), 1189-1210.

Puhakainen, P. and Siponen, M. (2010), "Improving employees' compliance through information systems security training: an action research study", *Mis Quarterly*, 34 (4), 757-778.

Ragin, C. C. (1992), ""Casing" and the process of social inquiry", in Ragin, C. C. and Becker, H. S. (Eds.) *What is a Case? Exploring the Foundations of Social Inquiry*, Cambridge University Press, Cambridge, pp. 217-226.

Ransbotham, S. and Mitra, S. (2009), "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise", *Information Systems Research*, 20 (1), 121-139.

Ransbotham, S., Mitra, S. and Ramsey, J. (2012), "ARE MARKETS FOR VULNERABILITIES EFFECTIVE?", *Mis Quarterly*, 36 (1), 43-64.

Rowe, B. R. (2007), "Will Outsourcing IT Security Lead to a Higher Social Level of Security?", *The Workshop of the Economics on Information Security (WEIS)* Pittsburgh, Pennsylvania.

Schechter, S. E. and Smith, M. D. (2003), "How much security is enough to stop a thief?", in *Financial Cryptography*, pp. 122-137.

Schelling, T. C. (1998), "Social mechanisms and social dynamics", in Hedstrom, P. and Swedberg, R. (Eds.) *Social Mechanisms: An Analytical Approach to Social Theory*, Cambridge University Press, pp. pp. 32-44.

Siponen, M. T. (2000), "A conceptual foundation for organizational information security awareness", *Information Management & Computer Security*, 8 (1), 31-41.

Siponen, M. T. (2005), "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods", *Information and organization*, 15 (4), 339-375.

Smith, G. E., Watson, K. J., Baker, W. H. and Pokorski, J. A., II (2007), "A critical balance: collaboration and security in the IT-enabled supply chain", *International Journal of Production Research*, 45 (11), 2595-2613.

Straub, D. W. (1990), "Effective IS Security: An Empirical Study", *Information Systems Research*, 1 (3), 255-276.

Straub, D. W., Goodman, S. and Baskerville, R. L. (2008), "Framing the Information Security Process in Modern Society", in Straub, D. W., Goodman, S. and Baskerville, R. L. (Eds.) *Information security : policy, processes, and practices*, M.E. Sharpe, Armonk, N.Y, pp. pp. 5 - 12.

Straub, D. W. and Welke, R. J. (1998), "Coping with systems risk: Security planning models for management decision making", *Mis Quarterly*, 22 (4), 441-469.

Symantec (2009), "Symantec Global Internet Security Threat Report: Trends for 2008", Symantec.

Tyre, M. J. and Orlikowski, W. J. (1994), "WINDOWS OF OPPORTUNITY - TEMPORAL PATTERNS OF TECHNOLOGICAL ADAPTATION IN ORGANIZATIONS", *Organization Science*, 5 (1), 98-118.

Whittington, R. (2006), "Completing the practice turn in strategy research", *Organization Studies*, 27 (5), 613-634.

Winn, J. K. (2009), "Are Better Security Breach Notification Laws Possible", *Berkeley Tech. LJ*, Vol. 24, p. 1133.

Yayla, A. A. and Hu, Q. (2011), "The impact of information security events on the stock value of firms: the effect of contingency factors", *Journal of Information Technology*, 26 (1), 60-77.

Zhao, X., Xue, L. and Whinston, A. B. (2013), "Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements", *Journal of Management Information Systems*, 30 (1), 123-152.