IS Security Networks in Credit Card Fraud Prevention

Laila Ali Dahabiyeh

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

Warwick Business School, University of Warwick

January 2017

Table of Contents

List of Tables

List of Figures

Acknowledgement

“Praise be to Allah, who has guided us to this, never could we have found guidance had it not been for the guidance of Allah” (The Qur’an, 7: 43).

I wish to convey special acknowledgement to a number of people to whom I am indebted for their help and support during my PhD journey. Special appreciation goes to my supervisors, Ola Henfridsson and Panos Constantinides. I have always enjoyed discussing my ideas with you. Your comments, questions and suggestions encouraged me to think differently and delve into areas I would not have considered on my own. From you I have learned how to become a better researcher.

My sincere thanks to my ISM group whose feedback has contributed in improving this work. Thanks to all scholars who have presented their work during different ISM seminars, listening and talking to them helped me clarify my ideas and put me on track when in doubt. Loving thanks to all my friends; Bo, thank you for your words of encouragement; Philip I really enjoyed working with you. Gongtai and Rezwan our brief encounters were always enjoyable. Wish you all the best in your PhD. My friend Malik, thank you for your efforts to cheer me up when I was down and giving me the opportunity to discuss my research with you.

To my lovely family, words cannot express enough how grateful I am to all your support. Your unconditional love, prayers, and trust kept me motivated. Mum, dad I hope I make you proud. To my adorable sister Lina, it was stressful having both of us doing our PhDs at the same time but I know it would have been a very difficult journey if you were not there by my side each step along the way.

Finally, I would like to thank my financial sponsor The University of Jordan for supporting my study.

Declaration

This thesis is submitted to the University of Warwick in support of my application for the degree of Doctor of Philosophy in Information Systems Management. It has been composed by myself and has not been submitted in any previous application for any degree at any other university. All the work presented here, including the data and analysis, was carried out by the author.

Abstract

In our increasingly connected world, maintaining the security of information systems is challenging. Today's interconnected business environment calls for a change in how IS security is achieved to include thinking about the entire networks of relationships involved in preventing threats rather than just focusing on individual organizational security processes. Despite acknowledging the role of distributed and heterogeneous actors in achieving a secure environment, there is a lack of knowledge of how these actors actually prevent security threats. Moreover, the heterogeneity of actors involved gives rise to the issue of incentives needed to align their interests to ensure successful collective security efforts.

This PhD thesis addresses these issues by zooming in on security networks, defined as collective efforts pursued by distributed actors to develop and adopt prevention measures to achieve security, to explain how these networks prevent security threats and identify the incentive mechanisms for converging the network's heterogeneous actors. I challenge equilibrium and linearity assumptions identified in the current literature and argue for the need to adopt different theoretical and methodological approaches to uncover the dynamics in these networks. Through a historical case study of credit card fraud and how its prevention measures evolved over the last 55 years, I develop a process model of prevention encounters in security networks. The model depicts the dynamic and interactive nature of the prevention process and shows how the three proposed prevention mechanisms, namely, proposing solutions, resolving dissonance, and paving the way, interact to achieve prevention. The thesis further proposes three new forms of incentive mechanisms (transformative, preparatory, and captive) that are crucial for the survival of collective security efforts and show how they interact with the three prevention mechanisms.

By this, this research complements the current security networks literature by offering a process model that explains how security networks achieve prevention. In addition, the interplay between the three incentive mechanisms reveals that incentives are not only ready-made structures or one-time event as depicted in the current literature but that they should also be seen as a socially dynamic process.

Keywords: security networks, IS security, prevention encounters, prevention mechanisms, incentive mechanisms, credit card, process model

1 INTRODUCTION

"If you are not a data breach victim, you are not paying attention"[1]

Maintaining the security of information systems (IS) is a critical activity. Security threats disrupt the continuity of business operations and negatively affect organizations' reputation and market value (Cavusoglu *et al.*, 2004). Attaining security has become more complex given today's interconnected business environment. In such an environment organizations are more susceptible to security attacks (Dhillon & Backhouse, 2000; Straub & Welke, 1998) because the origins of security threats are 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 organization's capability of fighting them (Gupta & Zhdanov, 2012; Kunreuther & Heal, 2003; Smith *et al.*, 2007).

IS security is thus no longer confined by organizational boundaries but transcends them to be dependent on all those operating on the same network (Anderson & Moore, 2006; Zhao *et al.*, 2013), where security is expanded to include extra-organizational settings (Straub *et al.*, 2008; Whittington, 2006) and not only organizational ones (See (Bulgurcu *et al.*, 2010; Posey *et al.*, 2013; Puhakainen & Siponen, 2010; Siponen, 2000; Straub, 1990)). Extra-organizational settings refer to the wider context that exists outside organizational boundaries where organizations get involved in information and resource sharing to better secure their systems.

Therefore, security efforts are envisaged to be rising from heterogeneous and distributed actors who come together (converge) and form networks which this research will refer to by *security networks*. Security networks are defined as *collective efforts pursued by distributed actors to develop and adopt prevention measures to achieve security.*

[1] Larry Ponemon in Pagleiry (2014). Half of the American adults hacked this year. Available from http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/. Accessed 25/3/2015

1.1 Motivation for the Study

Security attacks have become pervasive. News stories seldom devoid of any security breach incidents. Even organizations with vast resources (e.g. Sony, Target, Neiman Marcus, Adobe) are vulnerable. This indicates that they *by themselves* cannot face the continuous rise in security threats and collective security efforts are needed.

Nonetheless, on the one hand, the security perspective that receives wide attention in IS security literature is one that examines security within organizational settings. In this perspective, issues like IS security policies, security strategies, risk management, employees compliance with security policies become the focus for research. On the other hand, security research that acknowledges the distributed and collective nature of security focuses on cause-effect relationships. Therefore, little is known about how actors in collective security efforts actually collaborate to prevent threats. That is, we lack knowledge of the processes by which security networks develop and adopt prevention measures to achieve security.

Another critical issue stems from the heterogeneity of actors involved and their interests. Since collective effort is needed, it becomes important to understand the incentives required to align actors' interests and motivate them to contribute to security networks. While IS security literature that accounts for its distributed nature identifies different and valuable incentive schemes used to encourage actors to become part in these collective efforts, which range from rewards and subsidies to increasing profits and cost savings (Cavusoglu *et al.*, 2008; Gal-Or & Ghose, 2005; Hui *et al.*, 2012; Liu *et al.*, 2014), incentives are mainly studied through static models (August & Tunca, 2011; Cezar *et al.*, 2014). However, security threats (Hunton, 2009) and actors' interests evolve over time (Kaplan & Henderson, 2005), and incentives are expected to change to adjust to such transformations (August & Tunca, 2011). A need for a dynamic model that accounts for the changes in security efforts and the underlying incentive mechanisms therefore emerges (Cavusoglu *et al.*, 2008; Cezar *et al.*, 2014). In addition, the current knowledge in incentives is mainly drawn from analytical models based on rational choice. Financial incentives are therefore seen to be the primary driver for collective security efforts. Unifying the incentives required under one type nonetheless does not acknowledge the heterogeneity of actors and their interests that would make one kind of incentives not enough to converge actors in security networks. Moreover, the paucity of empirical data drove researchers to call for more empirical studies that can better identify incentives in real-life contexts (Arora *et al.*, 2008; Gal-Or & Ghose, 2005; Gordon *et al.*, 2003; Kannan & Telang, 2005; Ransbotham *et al.*, 2012)

This research addresses these needs by offering a process model on security networks. The model facilitates a deeper understanding of the process by which actors converge to prevent security threats and attain security, and show the incentive mechanisms in play. This is of great importance because although maintaining a secure environment is a shared goal across actors, they do not necessarily work towards achieving it. Identifying when and how actors successfully converge in security networks promise to offer valuable implications for organizations and policymakers when formulating security strategies.

1.2 Research Objectives

In the digital age, security threats are on the rise. Innovations in committing criminal activities are likely to be one step ahead of those seeking to prevent it. As achieving security hinges on heterogeneous actors, this research aims to offer a process model on security networks and identify incentive mechanisms needed to maintain the collective efforts. It also seeks to shed light on the neglected but important role of technology in security networks and uncover the socio-technical interactions in these networks.

Accordingly, the research has the following objectives:

- Understand the process by which prevention measures are developed and adopted over time.
- Identify actors, their interests, and how the latter are aligned to ensure convergence.
- Identify the role of technology in security networks.

In meeting these objectives the research seeks to answer the following questions:

1. *What is the process by which security networks achieve prevention?*

2. *What are the incentive mechanisms for converging heterogeneous actors to develop and adopt prevention measures to better secure their systems?*

1.3 Thesis Outline

This thesis is structured as follows. Chapter two provides a review of the literature in IS security that embraces the notion of extra-organizational settings and the heterogeneity of actors needed to achieve security. Fundamental issues and key assumptions are discussed along with how they limit our knowledge about security networks and incentive mechanisms. The chapter thus advocates the need for a new theoretical perspective to address current limitations. Chapter three presents a process perspective on security networks that should address identified limitations. It introduces and discusses the concept of prevention encounters that is used to develop a process understanding of security networks. The chapter further synthesizes three forms of incentives for converging actors in collective security efforts that go beyond ones currently identified in the literature. Chapter four details the research methods and design, it discusses the historical case study approach adopted as well as data collection and analysis processes. Research findings start with a narrative of the case study in chapter five. Chapter six is dedicated to case analysis. It presents a process model on security networks along with the incentive mechanisms for converging actors in collective security efforts. It by this answers the research questions. Chapter seven is a discussion of the research findings relating them to the relevant literature. Implications for theory and practice, limitations, and opportunities for future research are discussed in chapter eight.

2 PERSPECTIVES ON SECURITY NETWORKS

2.1 Introduction

The aim of this chapter is to review the current approaches in security networks. It first starts by acknowledging the mainstream literature in IS security that focuses on security within organizational processes. I show that within the objectives of my research this literature offers limited value. Accordingly, I move to discuss in details the stream of literature that acknowledges the distributed nature of IS security, its underlying assumptions, and explain how these affect our knowledge about security networks and incentives in these networks. Given the current focus on variance theory the chapter argues for a need for a different theoretical lens to acknowledge the dynamic and complex nature of IS security.

2.2 Security within Organizational Settings

Organizations' defence lines against security threats have evolved over time to keep pace with the rapid changing environment. The movement from closed silo systems to open interconnected ones was associated with a parallel movement in prevention measures from a mere focus on technical controls to admitting the importance of the social aspect in protecting organizations against security threats.

Security within organizational settings focuses on creating a secure environment through developing security policies (Goel & Chengalur-Smith, 2010; Png & Wang, 2009), and ensuring employees compliance with them through security awareness, training and education programs (Boss *et al.*, 2015; Bulgurcu *et al.*, 2010; D'Arcy *et al.*, 2009; Johnston & Warkentin, 2010). Of importance in this stream as well is investing in IS security. Spending on information security needs to be justified and therefore research on risk assessment (Salmela, 2008; Sun *et al.*, 2006) and the value of prevention measures (Cavusoglu *et al.*, 2005; Cavusoglu *et al.*, 2009; Kumar *et al.*, 2008) becomes crucial.

This perspective provides valuable knowledge on how organizations can build stronger security. Nonetheless, the interconnected business environment makes security not only a matter of organizational processes. Organizations might have a strong security system but become vulnerable to security attacks because of a deficiency in one of their partners' system. An example is the infamous Target security breach that compromised nearly 40 million credit and debit cards. The breach was not caused by low security measures from Target's side but rather insufficient security procedures in one of its contractors. Accordingly, achieving security requires collaboration between different actors that reside outside organizational boundaries. As the central concern in this stream of security literature is organizational processes, it is not surprising to find that it offers limited insights on such collective security efforts, which is the main focus of this research. Therefore, I will move next to discuss in more details the literature on IS security that acknowledges its distributed nature.

2.3 Current Approaches on Security Networks

The outstanding innovations in digital technologies are fiercely challenging any left organizational boundaries. Information can now be accessed via multiple paths, adding to an already complex task of protecting information asset. Organizations are realizing that security is distributed across actors outside their boundaries, and so there is a need to collaborate with others to be better protected against security threats (Gal-Or & Ghose, 2005; Gupta & Zhdanov, 2012).

Preventing security threats and maintaining a secure environment therefore are perceived as a result of distributed agency that cuts across organizations and industries. Collective security efforts are evident in the emergence of various security networks that aim to harness the efforts of heterogeneous actors to build a secure environment. Such networks include; information sharing and analysis alliances, such as Financial Services Information Sharing and Analysis Center, vulnerability disclosure networks, as Computer Emergency Response Team and iDefense, and IS security outsourcing.

In what follows, I provide an overview of how collective security efforts are currently theorized, mainly around streams of IS security outsourcing, information sharing alliances, and vulnerability disclosure networks, and how their underlying assumptions influence our understanding of the phenomenon.

2.3.1 IS Security Outsourcing

This form of collective security efforts is manifested in outsourcing relationships between organizations and their managed security service providers (MSSPs). The constant growth in MSSP market which ranges between 18%-21% annually (Ferrara *et al.*, 2013) indicates consensus on the value of delegating security functions to other actors.

Security is a challenging and costly task. The increasing complexity in security requirements in terms of compliance to security standards and government regulations, and the dynamic IT environment with the multiplicity of software applications and operating systems put more pressure on resources needed to achieve security organizations may not necessarily afford (Gupta & Zhdanov, 2012). Outsourcing security functions hence become an attractive move (Lee *et al.*, 2013). MSSPs offer valuable expertise and resources needed to confront new waves of security threats as well as the bewildering number of technological solutions. Their security solutions are various and include network monitoring, intrusion protection, managed firewall services, and vulnerability scanning. Coordinating security responsibilities between the organization and its MSSP is crucial for the success of the collective efforts (Lee *et al.*, 2013). Unfortunately, outsourcing relationships suffer from principle-agent problem because it is hard to verify the efforts of each actor. Ensuring collective efforts gets even more challenging when going beyond this bilateral relationship to consider the impact MSSP's multiple clients have on overall security. MSSP clients share the same security infrastructure, this indicates the larger the MSSP client base, the higher the security risk since a security breach in one client's system can spill over to the others as well, affecting outsourcing decisions (Hui *et al.*, 2012; Zhao *et al.*, 2013). Nevertheless, having multiple clients build to MSSP's expertise and help in preventing security attacks through knowledge accumulation and distribution (Lee *et al.*, 2013). MSSP learns from security threats occurring in one client and utilizes this knowledge to better protect all other clients.

Since security is distributed across organizations and MSSPs, designing effective service level agreements is critical to prevent security attacks and maintain collective efforts. Cezar et al. (2014) show outsourcing contracts that adopt a dual strategy of rewarding MSSP when revealing a breach and imposing penalties if it was responsible for it ensures maximum benefits from security outsourcing. While these researchers focused on bilateral contracts, Lee et al. (2013) recognize organizations' security responsibility as well as MSSPs' and propose a new multilateral contract that organizes the payment structure to include all MSSP's clients not only the one that suffers from a security breach. Their new contract design acknowledges the negative or positive effect one organization's security efforts can have on other organizations in the networks and seek to restructure refunds or penalties accordingly.

2.3.2 Information Sharing Alliances

Another manifestation of security networks is information sharing alliances. Information sharing alliances were established upon the U.S. federal government's initiatives to help secure the private sector's critical infrastructure against the constant and severe threats of cybercrime (Gordon *et al.*, 2003). Sharing security information such as, breaches, detection and prevention methods is presumed to encourage a proactive approach towards security since it can prevent other organizations from falling into the same attack (Gordon *et al.*, 2003; Hausken, 2007) as well as deter future attacks as sharing will increase attacker's risk of being caught (Schechter & Smith, 2003). Collaborative behaviour in sharing alliances is also enhanced because of interdependent security (Kunreuther & Heal, 2003) among organizations. In this context, organizations realize that security threats in any of them can easily transcend to the rest. Therefore, collaboration and contributing to information sharing will leave each organization in a better position (Hausken, 2007).

Members in sharing alliances shape one another especially with regards to decisions about security investments and level of sharing. The relationship between those two can either have a complementary or a substitute effect. Complementary effect of sharing rises in highly competitive environment. Gal-Or and Ghose (2005) show that an organization decision to increase its information sharing or security investment will cause its competitors to adopt similar decisions in an attempt to protect their market share. Substitute effect of sharing benefits organizations, especially those with limited resources, as sharing compensates for part of investments needed in security solutions (Gordon *et al.*, 2003; Hausken, 2007). However, due to free-riding behaviour, decentralization of information security decisions engenders insufficient investments in prevention measures with each organization relying on investments made by others (Gordon *et al.*, 2003). If organizations can gain knowledge of security threats, how to detect them and what prevention measure is best to adopt with relatively no costs, they will lack incentives to invest in new and innovative methods.

Free-riding behaviour is a common problem in information sharing alliances, and if it proliferates the collective efforts will dissolve. Several organizations involved in security breaches incidents that hit the news (ex. Heartland Payment Systems, TJX, JP Morgan Chase, HSBC) were actually members in Financial Services Information Sharing and Analysis Center. The lack of incentives for members to cooperate and share their security information and act opportunistically instead is seen the cause for information sharing alliances ineffectiveness (Liu *et al.*, 2014). Given its importance in maintaining the collective efforts, scholars call for researches that examine strategies for diminishing free-riding behaviour and increasing information sharing (Gal-Or & Ghose, 2005; Gordon *et al.*, 2003; Liu *et al.*, 2014).

2.3.3 Vulnerability Disclosure Networks

Many security breaches are caused by software vulnerabilities (Cavusoglu *et al.*, 2007). In vulnerability disclosure networks ensuring information security is distributed across actors involved in the vulnerability disclosure process. Those range from originators who discover the vulnerability to technology vendors who have to patch the software flaws.

Multiple mechanisms exist for disclosing vulnerabilities with each having a different impact on affected actors. In *full vendor disclosure*, the vulnerability is only reported to vendors who then develop a patch to correct the flaw. Since the vulnerability is exclusively disseminated to vendors, the latter retained the full control over fixing it and lacked incentives for a prompt response. Therefore, vulnerabilities were not patched or patched after long delays (Cavusoglu *et al.*, 2007). Vendors' passive engagement increased risks of security breaches and another mechanism for disclosing vulnerabilities that ensure their commitment was developed. In *immediate public disclosure,* the public becomes aware of the vulnerability as soon as it is discovered. This disclosure mechanism aims to exert more pressure on vendors to release a patch while at the same time giving software users the opportunity to take provisional corrective actions till the patch is released. This mechanism nevertheless has its own caveat. Instantly disclosing the vulnerability to the public enlightens hackers who can promptly exploit the vulnerability causing more damage. It can also hurt vendors who are genuinely committed to security by not giving them sufficient time to correct the flaw. *Hybrid disclosure* emerged to align actors' interests by giving vendors a grace period for releasing a patch after which the vulnerability is disclosed to the public. A recent disclosure mechanism is *pre-notifications disclosure* where a third party (infomediary) provides financial rewards to discoverers for vulnerabilities reported to it. The infomediary then disseminates this information to its clients who use it to adopt precautionary measures until a patch is released. This mechanism is presumed to deter hackers from finding and exploiting vulnerabilities (Kannan & Telang, 2005; Ransbotham *et al.*, 2012).

The multiplicity of actors involved, the diversity of their interests, and the presence of multiple disclosure mechanisms make vulnerability disclosure a complex process. It is in organizations' interest, for instance, to receive vulnerability information as soon as it is discovered in order to take prompt intermediate corrective actions till a patch is released. This nonetheless can have negative consequences on organizations that have not yet developed an intermediary solution, and on vendors who become less incentivized because vulnerability information already went public and organizations are temporarily protected, therefore they stall patch development process (Arora *et al.*, 2008; Cavusoglu *et al.*, 2007). Such complexities and entanglements in relationships make the locus of action shifts during vulnerability disclosure process from one actor to another, and so actors collectively contribute to securing their network. These actions shape subsequent actions; the grace period determined by coordinators for example or the presence of infomediaries influence vendor's patch release time, which can further influence other vendors' patch release decisions (Kannan & Telang, 2005; Li & Rao, 2007). Determining the conditions under which each mechanism is the best course of action plays a significant role in achieving security and motivating actors' engagement in security efforts.

2.4 Assumptions in Current Approaches

In their investigation of the relationships among actors to understand how their decisions affect security and obtain knowledge on best strategies to follow, researchers depend mostly on game theory and rational choice models, where actors' relationships are examined through predefined set of variables (Mohr, 1982), such as the relationship between information sharing and security investments (Gal-Or & Ghose, 2005; Gordon *et al.*, 2003; Hausken, 2007; Zhao *et al.*, 2013), and vulnerability disclosure and speed of releasing patches (Arora *et al.*, 2010; Cavusoglu *et al.*, 2007; Ransbotham *et al.*, 2012). Explanation is thus based on variance theories and discovering associations between variables. In here, actors are perceived to *react* to specific exogenous factors (e.g. vulnerability disclosure time, outsourcing contract design), which are then used to determine the best approach that results in the desired action and derive incentives consequently. For example, software vendors' reaction to different vulnerability disclosure mechanisms, whether it is immediately after discovery, after a determined period of time, or no public disclosure at all, is explored to determine which mechanism yield better security outcome. The current security networks literature therefore focuses on investigating causal effects rather than identifying causal processes behind explored associations. Since the aim of such variable-oriented research is to discover general laws that would allow generalization, certain assumptions follow (Abbott, 2001; Mohr, 1982). Little or no attention is given to the process aspect of security networks. That is, we lack a thorough understanding of events unfolding and interactions between actors in security networks. This is of paramount importance because security in a networked environment is *interdependent* and reliant on every actor's actions (Kunreuther & Heal, 2003). This interdependence makes security networks a complex phenomenon where explanation requires observing processes occurring over time rather than focusing on variables and their effects (Brady *et al.*, 2010).

In addition, the emphasis on causal effects tends to shy away from acknowledging the role of context in explaining collective security efforts. That is, it is not clear *when* actors actually converge to prevent security threats. In the current literature, it is recognized that actors converge to reach equilibrium, however the broader context of why actors are not in equilibrium from the start, and therefore why they need to combine their efforts is unknown. Exogenous shocks are the main cause for disequilibrium but what are these shocks, what causes them and how they disrupt the equilibrium remains unclear. Therefore, the contextual conditions behind the formation of and interactions in security networks receive scant attention. This can be due to the way security networks are theorized. The presence of these networks along with their constituent actors is already assumed. In vulnerability disclosure networks, for example, the discoverer, the coordinator, the organization, and the software vendor comprise the network before the research begins, so what becomes of interest is not to explain how and why these actors come together but rather to identify the best mechanism for disclosing the vulnerability in a way that maximizes security. Context is crucial for explanatory research not only because it can give new insights into the formation and the prevention processes of security networks but also because it helps in drawing boundaries for the proposed theoretical explanation and facilitates transposing the theory to other situations.

Assuming a univocal meaning of variables and that time, context and other variables have no impact on meaning is a common assumption in research focusing on causal effects (Abbott, 2001; Maxwell, 2004). The current security networks literature thus does not give a role to actors' beliefs and perceptions in collective security efforts or how meanings shape such collective efforts. For example, we do not know how outsourcing contracts or software patches are interpreted by the interacting parties and the role these interpretations have on outsourcing decisions and patch release and installation time. The social aspect of IS security is well-recognized (Dhillon & Backhouse, 2001) and prevention technologies can have multiple interpretations (Orlikowski & Gash, 1994). Translating these interpretations into variables is difficult (Maxwell, 2004) and understanding their implications on security networks' prevention processes requires moving beyond examining associations between variables to delving more in depth to uncover the causal chain of events occurring while achieving security. This would require a change in the theoretical and methodological approaches used to investigate the phenomenon (Meyer *et al.*, 2005).

2.5 Incentives in Current Security Networks Literature

The current literature on security networks stresses that if collective security efforts are to survive, it is the incentives that bring actors together that have to be ensured. Incentives intervene with actors' behaviour and drive it towards the required output (Gneezy *et al.*, 2011), their main goal is thus to *influence behaviour*. They are extrinsic in nature and act as an exogenous stimulus to alter actors' future actions and mobilize movements around the desired act.

The current literature on security networks identifies different incentives that motivate actors to contribute to collective efforts towards security. *Cost savings* is a dominant incentive in security 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 these high costs, organizations participate in security networks. Cost savings can be attained directly through passing security functions to specialized service providers who offer security services to large customer base, allowing organizations to achieve security at less cost due to provider's economies of scale (Cezar *et al.*, 2010; Schechter & Smith, 2003). Or indirectly by receiving information that makes an organization's security investment more targeted (Gal-Or & 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 investments in security and reduce overall costs (Gordon *et al.,* 2003; Hausken, 2007).

Increasing market demand is another incentive for participating in security networks. Operating in today's competitive business environment, organizations seek to be more alert to actions taken by their competitors and different ways they can 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 (Cezar *et al.,* 2010; Gal-Or & Ghose, 2005). A technical flaw in one company's product may shift demand to a 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 significant impact on their reputation and market value (Cavusoglu *et al.*, 2007; Yayla & Hu, 2011). 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 & Ghose, 2005), relieving by this customers anxiety regarding the security of their personal information and maintaining their trust. Also, joining such collective efforts indicates that security threats once identified, rapid corrective actions will follow, decreasing the value of the threat and making organizations less attractive to attackers (Gupta & Zhdanov, 2012; Kannan & Telang, 2005; Ransbotham *et al.*, 2012; Schechter & Smith, 2003). 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 what impact discovered vulnerabilities in their products might have on the perceived quality of their overall services, gives them more motivation to supply their clients with corrective patches in a timely manner (Arora *et al.*, 2010).

Liability for security breaches is a recognized approach to drive genuine security efforts in security networks (August & 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 members by making the organization that caused a certain security breach take full responsibility and swallow associated costs, 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. As an example, besides benefits from accumulated knowledge and expertise, organizations outsource their security functions to move liability burden from themselves to the outsourcer (Rowe, 2007).

The rational self-interested actor is a common assumption in models used in security networks literature, where each actor seeks to maximize his or her own utility. This can be seen from the type of incentives identified that are inclined towards financial gains. Dependence on rational choice models makes it difficult to detect other forms of incentives and possible changes in them over time as the theory presumes actors' motives remain stable, and that every actor will behave rationally. It is not surprising therefore to find discrepancies between the theory and the observed phenomenon (Green & Shapiro, 1994). Moreover, the literature does not recognize that IS security has a social aspect as well, and therefore it does not pay attention to the role of language and discourse in motivating desired security behaviour.

Incentives for collective action are not solely driven by utility maximization and rational economic actors who seek to pursue their own objectives through means of alternatives evaluation and selection. Competing views such as ones that perceive actors as part of a political system with conflicting goals can offer different insights on incentives for influencing actors' behaviour (Eisenhardt & Zbaracki, 1992) and allow better explanation of incentives mechanisms behind collective efforts in preventing security threats and achieving security since it will cater for the heterogeneity of actors that seems to be neglected in the current research on security networks.

2.6 Summary

This chapter provided an overview of collective security efforts in IS literature. It revealed how our understanding of the three main manifestations of security networks; IS security outsourcing, information sharing alliances, and vulnerability disclosure networks, is seen through the lens of variance and static models. The chapter further illustrated incentives defined in this literature and showed how the literature offers a limited view on incentives because they are derived from analytical model based on rational choice where incentives also tend to remain static over time. In the context of security however, the environment is always in flux. Interests change, and innovative security threats continually emerge where new prevention measures to thwart those arise subsequently. Within these conditions, there is a need to adopt a different approach in investigating the phenomenon that focuses on processes and disequilibria rather than variables and equilibria. I move to explain this in the next chapter.

3 TOWARDS A PROCESS VIEW ON SECURITY NETWORKS

3.1 Introduction

In the previous chapter, I argued that to acknowledge the dynamic and complex nature of IS security and the required incentives we need to adopt a different theoretical perspective. A process lens promises more useful insights on security networks. In this chapter, I present and discuss concepts that are used to help me meet the research objectives and develop the process model. First, I introduce and discuss the concept of prevention encounters, which I use to examine security networks. I then introduce three new forms of incentives that I have synthesized from the literature on collective action. These incentives complement ones currently identified in security networks literature. In later chapters, I explain their role in the data analysis and how these incentives come into play in the process of developing and adopting prevention measures (i.e. how they are incorporated in the process model).

3.2 Prevention Encounters in Security Networks

The complexity of security networks requires moving beyond the current focus on examining causal effects to identifying causal mechanisms that are better equipped to offer a robust explanation of the phenomenon. The interdependent nature of security networks brings forth the importance of the reciprocal relationships amongst actors and the impact their interactions have on subsequent decisions and the overall security of the network. In such a complex situation, it is not enough to provide a description of the succession of events to explain how security networks prevent threats and achieve security. Rather, complexity calls for an explanation that is based on complex causality (Hesketh & Fleetwood, 2006) that surpasses narrating preceding events to considering the entire interacting elements of context, mechanisms, actors, and structure. To appreciate the complexity of security networks and to capture causal mechanisms in collective security efforts, I have departed from the current focus on variance theories and adopted process theory to study security networks. Process theory is an appropriate lens for capturing contextual details and mechanisms necessary for gaining the 'how' of events (Markus & Robey, 1988).

Since security networks are dynamic the question that arises is where one can start studying this phenomenon. This is challenging especially as the uncertainty surrounding security efforts results in changes in these networks to adapt to new forms of threats (Mookerjee *et al.*, 2011). The starting point in the analysis, this study argues, is these change opportunities. This is because it is during these periods actors' convergence to achieve better security is best manifested, and incentives for collective efforts can be identified. These convergence points are referred to by *prevention encounters* (Newman & Robey, 1992), which denote actions taken by heterogeneous actors to develop and adopt prevention measures that shake an established pattern. Prevention encounters represent critical events that have a significant impact on how security is attained. They are seen as 'windows of opportunity' (Tyre & Orlikowski, 1994) for rethinking current security practices. By this, they challenge an established process (Isabella, 1990), and force actors to re-evaluate the effectiveness of existing prevention measures and negotiate possible future directions (Bettenhausen & Murnighan, 1985). Reaching agreement or equilibrium becomes a *continuous process* between actors to restore relative stability rather than an end state (Tieben, 2012), and one traced by observing how actors interact to respond to events that disrupt their status quo. Security networks are hence not preconceived but rather emerge throughout these processes. By zooming in on the chain of events occurring while preventing a certain threat, prevention encounters shift the focus from a static snapshot view to a dynamic moving pictures one.

Interruptions in security practices do not come out of thin air; they rather arise from certain events that trigger changes in prevention measures. Organizational change literature shows that organizations undergo periods of upheavals that restructure their environment (Meyer *et al.*, 1990). The causes of such discontinuities vary from social pressure to government regulations and technological advancements which constitute *prevention encounters triggers*. *Social pressure* reflects organizations' moral and social responsibility towards their stakeholders (Culnan & Williams, 2009). It relates to discrepancies between an organization's goals and its actual practices that drive attention and contempt for not only the organization but its industry as well (Chandler, 2014; Hoffman & Ocasio, 2001). Social pressure can be externally as well as internally driven. It can rise from the public's outcry about a certain issue that consequently encourage the involvement of other actors such as regulators. Or it can arise internally from the industry's members themselves who recognizing the negative impact their practices have on their image decide to react and take self-examination and corrective actions to restore public's trust and preserve their image (Hoffman & Ocasio, 2001). As all issues can be seen important and calls for a change (Hilgartner & Bosk, 1988), the capability of social pressure to act as a prevention encounter trigger lies in its ability to threaten the industry's image and status in the business world (Hoffman & Ocasio, 2001).

Laws and regulations are another cause of discontinuous change. Through enacting laws, legislative and regulatory agencies can disrupt organizations' environment, requiring them to restructure their processes and activities in order to cope with the new conditions. The infamous Enron scandal questioned organizations' accounting practices and resulted in the passage of Sarbanes-Oxley Act of 2002. The act which introduced stricter financial governance procedures held organization's board of directors responsible for the accuracy of financial statements, created criminal penalties for misconduct, mandated the independence of auditors along with other requirements was considered one of U.S. greatest reforms in business practices. Regulations can further trigger profound shifts in organizational relationships and business strategies (Meyer *et al.*, 1990). Dobbin and Dowd (2000) illustrate how railroad companies changed their business model from one that relied on cooperative relationships to one that is based on mergers and acquisitions upon the enactment of antitrust laws that rendered the cooperative model illegal. In a similar vein, Security Breach Notification Law mandates organizations to publicly announce security breach incidents. Enacting this law attempted to change organizations' security behaviour and put more pressure on them to implement better security controls (Winn, 2009). Government regulations therefore change organizations' institutional environment and market mechanisms (Haveman *et al.*, 2001) which in turn impact organizations' current and future security plans.

Finally, *technology* plays a key role in triggering change and restructuring organizations' industry. Meyer et al.'s (1990) research of change in the health care industry shows how advances in outpatient surgery and diagnostic and treatment technologies were perceived as competence-destroying innovations since they allowed non-medical organizations to enter medical services market. Technology in this sense eroded barriers to market entry and facilitated mobility within and across industries. In triggering change in a given industry, technology needs not be developed to serve the needs of that industry. Rather, technologies can be developed in one industry but find themselves new applications in another where they can challenge existing practices (Levinthal, 1998). An example is the Internet which was originally developed by the U.S. government to provide communications between academic and military networks but then became the backbone for commercial services introducing new forms of business models. Technology, as a prevention encounter trigger, then promises a fundamental change in how security is achieved through either advancement in technologies specifically developed to meet this purpose (security) such as cryptography, biometrics, intrusion detection systems, and firewalls; or technologies developed for other purposes but can be used for security solutions.

Besides its role in offering a different view on security networks, the concept of prevention encounters will facilitate realizing the overlooked role of technology in these networks. The seminal paper by Dhillon and Backhouse (2001) called for moving beyond the technical focus in IS security research to investigate the socio-organizational aspect of the phenomenon. At the same time, technology also matters (DeSanctis & Poole, 1994; Markus & Silver, 2008). Focusing on the interaction between the social and the technical is crucial as technology shapes social interactions between actors while those interactions themselves can change its structure. Technology is at the heart of prevention encounters since the latter is concerned with prevention measures, which often come in the form of different technologies, and interactions surrounding them. Prevention encounters therefore acknowledge the socio-political aspect of technology and the consequences this have on the network's prevention efforts.

3.3 Forms of Incentives in Collective Action Research

A major challenge in any collaborative or collective efforts is motivating actors to contribute to the end goal. Research in collective action literature offers a great opportunity to synthesize different forms of incentives that go beyond the emphasis on economic actors and monetary incentives prominent in the current security networks literature. Through reading this literature, I have synthesized three forms of incentives; transformative, preparatory, and captive, with each aiming at a different target to stimulate actions.

3.3.1 Transformative Incentives

The first form of incentives targets actors' *beliefs*. Through interacting with their surrounding environment, actors utilize their cognitive capabilities to interpret events, construct meaning and take the appropriate course of action (Kanfer, 1990; Kaplan, 2008). Actors therefore hold certain beliefs about a certain phenomenon (Kim & Bearman, 1997). Those beliefs are of paramount interest as they are the driving force and consulting agency for actor's actions. Incentives therefore cannot be separated from beliefs (Kaplan & Henderson, 2005). From here, attempts to make others do what one wants have to seek *beliefs alignment.* To attain this, significant efforts have to be exerted to change actors' current framing (Benford & Snow, 2000; Kim & Bearman, 1997) of a particular situation from one against the desired behaviour to one supporting it. Transformative incentives therefore seek to induce actors by transforming their beliefs to be aligned with the end goal. Hence, it is the differences in opinions and beliefs that stir this form of incentives (Che & Kartik, 2009).

The literature on social movements represents one of the best manifestations of transformative incentives. This literature shows how movement's goals are conceptualized play a vital role in reshaping perceptions about the phenomenon of interest and forming the new belief. Framing the movement cause in a way that expands its impact by applying "vocabularies of motive" (Benford, 1993) increases the chances of disrupting actors current beliefs and replacing them with new supportive ones. Transformative incentives are ideological in nature and aims for change (Clark & Wilson, 1961).

The primary tactic used to transform beliefs is rhetoric (Kamenica, 2012). As an art of persuasion, rhetoric is an indispensable element in any cognitive manipulation attempt (Suddaby & Greenwood, 2005). It comprises continuous negotiations where through careful selection of words diplomatic actors (Mills, 1940) seek to displace targeted audience goals with those of theirs (Clark & Wilson, 1961; Latour, 1987). A challenging process as it is, belief transformation might face resistance that can hinder the recruitment of others to support the end goal. The targeted audience is not passive and will fight attempts to change its longstanding beliefs. Different rhetorical devices (or types) are thus needed to react to this opposition and make a persuasive argument to justify the desired reshape. Hirschman (1991) distinguishes three types of rhetorical arguments: perversity, futility, and jeopardy. Perversity argument stresses the contradictory effect the action in consideration will have in case it was pursued. That is, if the desired action is supposed to improve the current situation, it will in fact backfire and produce unintended negative consequences. Futility argument claims the current situation is deeply institutionalized that any attempt to change it will be in vain or would only result in scratching the surface, leaving main structures unchanged. Promises given for a brighter future will hence be shattered when facing reality. The jeopardy argument argues the desired action is associated with high costs and threatens previous valuable accomplishments. So it is not that the action by itself is not desirable but rather its consequences that make it unwelcomed when taking contextual conditions into consideration.

Actors draw on these rhetorical arguments to change how others perceive their cause, displace their original beliefs, and mobilize them towards the end goal. In a way, they exert much effort to reframe the issue at hand to make others see it through their lens (Barrett *et al.*, 2013). Social phenomenon is nonetheless open to multiple interpretations, and these same rhetorical arguments can be used by the opposite party to undermine the need for the action in question. To persuade the audience, recruiters have to rely on a repertoire of vocabularies (Benford, 1993; Hartelius & Browning, 2008) that can cut across the three rhetorical arguments. In his study of the activities of social movement organizations involved in nuclear disarmament, Benford (1993) found that activists increased participation in the collective action by framing their goal around vocabularies of severity and personal efficacy. Contrary to the belief that nuclear weapons are developed to protect the nation from external threat and ensure peace, nuclear weapons constitute the major threat to life on earth, and unless action is taken to stop further development, doomsday is very near (perversity). To respond to futility claims rose by actors who believed their efforts are useless and doubted the collective action ability to do anything to change the status quo, movement leaders had to develop a new vocabulary of motive, personal efficacy, which they promoted through fliers and newsletters that helped in mitigating pessimism and gaining support.

Rhetoric is heavily used by leaders in their transformative efforts (Hartelius & Browning, 2008) where the act of leadership by itself is crucial to alter beliefs (Clark & Wilson, 1961; Panke, 2013). Those in leadership positions will take it upon themselves to shape the identity of their purpose and mobilize actors by invoking common interests (Dosh, 2009). Political entrepreneurs (Broz, 1999) constitute a powerful resource for mobilizing actors. They possess valuable knowledge regarding the various interests of targeted actors (Hartelius & Browning, 2008) which enable them to better tune their recruitment strategies to influence others and transform their beliefs (Kim & Bearman, 1997; Panke, 2013).

Transformative incentives therefore rely on using rhetoric to influence actors' behaviour and alter their beliefs about the phenomenon of interest. Although changing beliefs can be associated with other tools, such as monetary and non-monetary incentives, this research claims that rhetoric represents the *main* tool applied in this form of incentives that distinguish it from the other forms.

3.3.2 Preparatory Incentives

The second form of incentives used to change behaviour and mobilize actors is preparatory incentives. This form of incentives acts as an activating agent that triggers or enables other incentives. It mediates between context and end goal to manipulate the former to attain the latter (Brickson, 2000). Preparatory incentives therefore assume that actors already have incentives to perform the desired goal. However, some actions need to take place to either boost such incentives or eliminate a few roadblocks that are in the way. Providing progress feedback reports, for instance, evoke intrinsic incentives such as a sense of mastery and competence that can optimize employees' performance (Kanfer, 1990). Similarly, to increase organizational outcomes in demographically diverse settings and encourage cooperation, Brickson (2000) shows that certain identity orientation had to be provoked to improve diversity dynamics. By restructuring organizational and task structure (e.g. organizations based on network structure and team-based tasks), organizations can provide the proper context for evoking the desired identity orientation that in turn improves performance.

Policymakers are increasingly acknowledging the effectiveness of market-based incentives (e.g. supply, demand, competition) over traditional incentive approaches that rely on command-and-control (Heine, 2013; Verma *et al.*, 1999). Different laws and regulations have been enacted to activate such market-based incentives. Being a well-known incentive mechanism for improving quality and lowering prices, legislators direct their efforts to enable and improve competition. The passage of the Hatch-Waxman Act, for example, created a competitive environment in the pharmaceutical industry by hastening the time generic drugs can enter the market. The act granted generic drug manufacturers the right to challenge existing drug patents instead of the usual practice of waiting till the patent gets expired (Hemphill & Lemley, 2011).

To encourage innovation and knowledge advancement, governments enact property rights laws to grant innovators legal protection against free-riders, creating a safe environment for them to reap the benefits of the innovation by exploiting it in manufacturing and selling products or through license agreements. Promoting innovation will be hard to achieve without a proper mechanism to secure it. Innovators seek to utilize their innovation and recoup costs associated with it, and when the business environment cannot provide them that, they find investment in innovative activities a risky decision (Sichelman, 2010). In a similar vein, product market diversification allows organizations to encourage employee firm-specific investment behaviour by expanding the scope of the applicability of their resources across multiple businesses, increasing the expected payoff from such investments (Wang & Barney, 2006). A preparatory stage is therefore sometimes needed to mobilize actors and facilitate the realization of their interests.

By acknowledging different kinds of incentives that have already proved to mobilize actors around the desired action, preparatory incentives come as an answer to the prerequisites required to activate and boost such incentives (Lindenberg & Foss, 2011). Property rights laws, for example, do not *directly* touch upon actors' interests; they do not directly offer a particular financial reward but rather provide contextual conditions that enable actors to realize their interests, all under the broader aim of attaining the chosen goal. Creating a favourable business environment through the provisioning of proper infrastructure (Bachtler & Raines, 1997) is very crucial as insecure environment, whether it is legal, political, or social, increases risk, creates uncertainty and fails in influencing actors' behaviour (Alfranca & Huffman, 2003; Glaessner & Mas, 1995).

Preparatory incentives therefore aim to manipulate actors' *environment* to match their interests (Heine, 2013). It can be seen as a strategic manoeuvre to influence behaviour without direct intervention, one that shapes the context while giving actors the freedom to choose their future direction accordingly (Marengo & Pasquali, 2012).

3.3.3 Captive Incentives

Another effective mechanism for influencing behaviour is placing the desired action to be in *actors' interests'* path. For actors, performing the desired action becomes a means to an end; they may not necessarily be interested in the action per se but rather the benefits it brings that match their interests (Schneider, 2002). They become captives as realizing their interests cannot be attained without performing the action (Callon, 1986; Latour, 1987; Verma *et al.*, 1999).

Collaborative relationships within and across organizations have become a standard feature in today's business environment. This created interdependencies as one actor’s actions can greatly influence those of others. Organizations that focus on unit specialization but at the same time want to reap more benefits from integration across units reside to manage this interdependence by tying employees’ benefits not only to the performance of their unit but also that of other units as well (Kretschmer & Puranam, 2008). Actors become part of an interlocking network (Kim & Bearman, 1997) where incentives are embedded in others’ interests in addition to one’s own interest (Beersma *et al.*, 2003; Brickson, 2000).

Captive incentives are used to solve the free-riding problem when mobilizing actors. In information security literature, organizations that operate on one network tend to invest in protecting themselves from external threats but not ones originating from the network, relying on others investment to prevent the latter. This behaviour puts the network at risk as it can lead to minimal protection (Kunreuther & Heal, 2003). To discourage this behaviour and motivate security investment, fines (subsidies) are bound to the party responsible for the breach (invest in security). As it is in actor’s best interest to shift the liability for security breaches to others, investing in security becomes the channel that allows them to realize this interest (Liu *et al.*, 2014; Zhao *et al.*, 2013).

By granting or denying access to private rewards actors can be steered towards the end goal. Von Hippel and von Krogh (2003) show that firms are not willing to invest in open source software unless they can receive something in return. Only those who have propriety products that are compatible with the free software will be induced to support open source software. Such investment will increase the diffusion of the software and thus demand for the firm’s products. Open source software becomes a source of a new revenue stream. Naturally firms have the choice of capturing this opportunity or not. What matters in captive incentives is that a firm cannot realize benefits from open source software without devoting some resources to support it. A crucial point to mention here is that the private benefits actors can have from the new desired action have to outweigh any costs associated with cooperating in order to justify the change in behaviour (Bradford & Ben-Shahar, 2012). Mobilizing actors is a process that competes for resources and without a proper justification for the required shift or if no interests are at stake, inducing actors’ cooperation is questionable (Panke, 2013).

Captive incentives are generally based on exchange relationships (Schneider, 2002), like ones found in business contracts where organizations offer employees some benefits in exchange for their time and effort in meeting organization's objectives, and in insurance plans. Titmuss (1970) found that insured blood plan (or family credit plan) is an effective strategy for inducing blood donation. According to this plan, donors donate blood now to cover their future blood needs without the burden of finding replacement donors. So as long as one donates blood, he is guaranteed free access to it when in need.

So the focal point in captive incentives is to tie incentives that represent actors' *direct interests* - regardless of their nature whether monetary or non-monetary – with the new desired behaviour. It is crucial that actors can relate the latter with the former in order to ensure the desired behaviour will be seen as something of *value* which increases the effectiveness of the incentive (Verma *et al.*, 1999).

In summary, captive incentives must bind actors' interests with the desired action in a way that makes it difficult to achieve one without the other, in other words, they become jointly produced (Broz, 1999) and must be valuable enough in order to simulate behaviour and justify reallocation in resources from other competing actions (Bradford & Ben-Shahar, 2012).

Table 3-1 provides a summary of the three forms of incentives.

So where do incentives defined in the current security networks literature (cost saving, increase demand, signalling, liability shift) stand within these forms. These can be classified under captive incentives. Security networks allow actors to reap these benefits which they could not have done so without being involved in these networks. Organizations would not have access to security breach information (to realize cost savings and increase in demand benefits) if they were not a member of the network. Likewise, liability shift rules leave organizations no choice but to improve their security to avoid being the weakest link and the one to bear the costs following security breaches. Signalling differs from the other incentives because it offers non-monetary benefits in terms of organizations' image and reputation. In signalling, security networks are used as channels to communicate organizations'

Table 3-1 *Summary of incentives forms*

Form of Incentives	**Definition**	**Target**	**Focus on**	**Tools applied**
Transformative	Any attempt to influence behaviour through changing actors beliefs to become aligned with the desired action	Beliefs	What *I* want	Rhetoric
Preparatory	Any attempt to influence behaviour through manipulating the context to activate other incentives and enable actors to realize their interests	Environment	What *you* want	Regulations, policies, institutional restructuring
Captive	Any attempt to influence behaviour through tying actor's interests with the desired action so that attaining one cannot be reached without the other	Actor's interest	What *we* want	Varies according to actors' interests (e.g. access to resources, financial rewards…)

security efforts and make them more visible internally and externally (Meyer, 1979). In times where security breaches have become pervasive, participating in security networks proofs organizations' commitment to security and helps them retain positive image among stakeholders.

The fact that incentives identified in security networks literature fell in captive incentives form do not come as a surprise given the literature focus on economic models and rational choice theory as discussed before.

3.4 Summary

Observers of IS security can quickly note the field's constant movements that make disequilibrium moments prevail. The upheavals the field undergo calls for moving away from equilibrium-centric studies to disequilibrium-focused ones. This chapter illustrated steps taken towards this move. It explained the theoretical lenses I am using to develop a process model on security networks. A process lens promises more useful insights on how security networks face and prevent security threats, and how past events influence future security paths. It furthermore helps to go beyond the current focus on rationality and economic incentives, and delve more in depth on other forms of incentives for converging actors to collectively achieve security.

This proposed shift in the theoretical lens ought to be followed by a change in the methodological approach used. It has been argued that capturing dynamism and change requires moving away from quantitative approaches and adopting qualitative ones instead (Tieben, 2012). It has been further argued that historical research is more equipped to capture disequilibrium moments over time (Meyer *et al.*, 2005) and retain the case complexity (Abbott, 2001). Having process theoretical lens in focus and applying a longitudinal sensitive method will unfold prevention encounters taking place while preventing security threats and help me answer the research questions of how security networks achieve prevention and the incentive mechanisms needed to converge actors during the process.

The next chapter examines the research method and details the role the developed concepts (prevention encounters and the three forms of incentives) had in the data collection and analysis process.

4 RESEARCH METHODS

4.1 Introduction

The previous chapter argued that the research objectives are best met by following qualitative research methods. In this chapter, I discuss in details of the qualitative research approach used in this study. I start with the philosophical position supporting the research followed by the rationale for choosing a case study approach. I then show the importance of having a historical perspective and the value adopting such a perspective had on the research. Afterwards, I detail the steps followed in designing the case study, starting with identifying the research objectives, how to select the case, the protocol used in data collection, and ending with data analysis strategies.

4.2 Philosophical Stance

Research in information systems field is informed by three main philosophical positions; positivism, interpretivism and critical realism (Mingers, 2004; Mingers *et al.*, 2013; Wynn & Williams, 2012). This research is based on critical realism position.

Critical realism (CR) bridges between positivism and interpretivism, it adopts a positivist ontology and an interpretivist epistemology. CR acknowledges the social construction of a given phenomenon and the role of actors' interpretations in explaining it while at the same time not neglecting the existence of independent structures that enable or constrains actors' actions (Wynn & Williams, 2012). Therefore, to explain a phenomenon in CR is to give a detailed description of the processes and events taking place and how they are influenced by contextual conditions.

CR views reality as an open system that cannot be reduced to a controlled environment. Interactions between entities and their inherited mechanisms, and the new mechanisms that can emerge from such interactions, make it rare to have an identical set of mechanisms that always result in the same outcome (Wynn & Williams, 2012). The goal of CR hence is not prediction but *explaining* how events come about under certain contextual conditions. Nonetheless, this does not mean that there are no general regularities in the world. Lawson (1998) shows that causal mechanisms may endure across events resulting in similar patterns, he refers to this partial regularity as demi-regularity or demi-reg.

A major aspect in CR is stratified reality into three domains. The real domain contains entities with their inherent causal powers (mechanisms). In the actual domain, these powers are enacted and generate events. The subsets of events that are experienced by humans whether through perception or measurement constitute the empirical domain. Accordingly, a key argument in CR is that we cannot reduce all events to ones we observe, and mechanisms to actual events. Mechanisms may be exercised but never actualized because of countervailing effects of other causal mechanisms. Since reality is an open system, it is the interaction between mechanisms that generates the presence or absence of events (Mingers *et al*., 2013, p.796).

CR promises to shed new light on research in IS field, it shifts the attention from data collection and analysis to real problems encountered and causes behind them (Mingers *et al*., 2013). Therefore, despite the fact that there are multiple manifestations of security networks in IS security literature, there is little understanding of how these networks prevent security threats. Through adopting critical realism this research seeks to uncover the underlying mechanisms of how security networks achieve prevention. And as a second step identify the incentive mechanisms behind bringing actors in these networks together, and how these mechanisms produce their outcome. From a critical realist perspective, entities such as social structures and technological artefacts are sources of emerging powers (causal mechanisms) that exert causal influence. These causal mechanisms generate the events that occur during prevention processes. Explaining the phenomenon becomes a matter of identifying these mechanisms and properties of the entities that

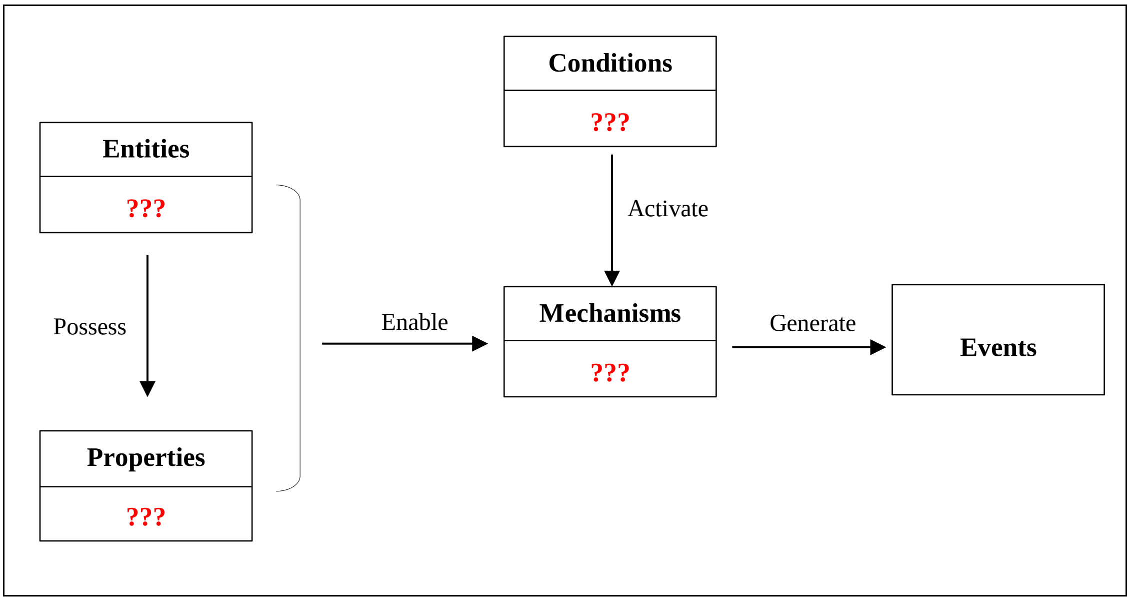


Figure 4-1 *The structure of causal explanation (after Sayer, 1992)*

possess them. That is identifying what it is *about* these entities that give them their power (Sayer, 1992).

Explanation of a phenomenon according to critical realism thus involves identifying entities, their properties, mechanisms responsible for producing observed events, and conditions that activate these mechanisms. This structure of causal explanation is represented in Figure 4-1.

4.3 Case Study Approach

Adopting the appropriate research design is a critical step in any research and one that is often guided by the research questions and objectives. Chapter 3 showed the lack of knowledge of how security networks prevent threats, how and when actors converge and the incentives for convergence. In order to produce this knowledge, an extensive description of security threat prevention processes is needed, deeming case study an appropriate research approach (Yin, 2014). Case studies are known for their ability to give in-depth understanding of the examined phenomenon and therefore it is no wonder they become a popular approach for developing new theories (Eisenhardt & Graebner, 2007). Moreover, researchers interested in identifying causal mechanisms turn into case studies as the method for their investigation (Gerring, 2007).

This research case study approach can be best described as structured and focused one (George & Bennett, 2005). The case study is *structured* because the research objectives are sought to be addressed in each of the cases (or sub-cases) under investigation, while it is *focused* since it has a theoretical focus that zooms in on a particular aspect of the phenomenon (prevention encounters and incentives) rather than another. Having a clear focus is crucial to avoid falling into the trap of voluminous data (Eisenhardt, 1989). This is of particular importance given the research historical perspective which is discussed next.

4.3.1 Historical Perspective

Interest in historical perspective in information systems field has been promoted since the 1990s (Land, 2010; Mason *et al.*, 1997a; Mason *et al.*, 1997b; McKenney *et al.*, 1997; Mitev & De Vaujany, 2012). This move towards historical studies is strongly evident in the publication of a special issue in Journal of the Association for Information Systems in 2012 and two special issues in Journal of Information Technology in 2013 dedicated to IS history.

Historical studies examine events occurring over time, how they happened and why, and search for patterns in order to gain insights into what actions to undertake while facing change opportunities (McDonald in Kantrow, 1986). They can offer unexpected insights into current phenomenon challenging existing theories (Mitev & De Vaujany, 2012), and by this provoke new questions and generate new knowledge (O'Sullivan & Graham, 2010). For example, Jakobs' (2013) historical approach to find out why X.400 email standard failed defied the two popular explanations and proposed more detailed and plausible reasons behind the standard failure. Jakobs argued that the popularity of the Internet cannot be a valid reason for the failure of X.400; the Internet standardization process faced many complexities that made it not so much superior to any other standardization process. Further, the X.400 standard was largely supported and adopted in Europe in comparison to the small scale diffusion of the Internet in the U.S. - back then. Similarly, installed base hostility is unlikely to be the primary reason for X.400 failure since the latter was developed to allow interoperability between already installed-based individual email systems, and was designed to operate over X.25, the most widespread packet switching network. Instead, his historical analysis revealed that X.400 demise cannot be limited to one reason but rather a collection of multiple ones (ex. national monopoly, unfortunate timing) which all contributed to its end.

The present is a product of past actions, events, and decisions that all interact with each other to produce it (Bonner, 2013). Through historical data, we can explain the past, draw inferences for understanding contemporary and future phenomena (Porra *et al.*, 2014) and make informed decisions (Mitev & De Vaujany, 2012). History is thus a valuable source of knowledge for acting intelligently with the future (Marwick, 2001; Tosh, 2008). "It is only through a sense of history that communities establish their identity, orientate themselves, understand their relationship to the past and to other communities and societies. Without history *(knowledge* of the past), we, and our communities, would be utterly adrift on an endless and featureless sea of time." (Marwick, 2001, p.32, emphasis in orginial).

History is a study of change (Porra *et al.*, 2014). Its longitudinal coverage gives it the power to appreciate the complexity of social phenomena, confront current wisdom held about them (Land, 2010), and reveal "movements from continuity to change and vice versa" (Pettigrew, 1990, p.272). By adopting a historical approach on how security networks achieve prevention, I will be better equipped to capture prevention encounters (as they represent periods of change), explain the prevention process, and identify incentive mechanisms to converge actors while facing security threats. In addition, as I explain when discussing case selection/building step, the historical perspective enabled me to develop sub-cases of my general case and so conduct within- and cross-case analysis, which increased the reliability of the research findings and the efficacy of the proposed mechanisms relative to alternative explanation (Wynn and Williams, 2012). Without this rich historical data, it would have been difficult to structure the data around multiple sub-cases.

4.4 Case Study Design Process

Case studies are not story-telling; they should be based on profound foundations to reflect their status as a methodological tool for conducting research. Researchers therefore should carefully design their case study to ensure the reliability of their findings. In designing my theory-oriented case study I drew from George and Bennett (2005) and Eisenhardt's (1989) work to identify the required steps in the case study design process (see Table 4-1).

4.4.1 Identify Research Objectives and Problem

Specifying the purpose of the research is inevitable step in any research design approach (Gerring, 2007). Knowing what the research is expected to achieve and the problem to be solved not only guide subsequent steps in the design process but also helps researchers regain control lest they went off track while conducting their research. This first step gives the research focus. It shows what one wants from the data, and helps in delineating the scope of the study.

Of importance is determining whether the research seeks to test hypotheses or generate a new theory. Each will have its implications on how the extant literature is used in formulating the research questions. Theory testing research adopts a deductive approach that searches the literature to specify variables of interests and construct relationships between them in terms of hypotheses to be tested by the empirical data. Theory building research, on the other hand, focuses mainly on theory emerging from the data and follows inductive reasoning. The literature here is visited to obtain knowledge about the researched area, identify the problem, and possibly develop tentative constructs that shape what the research is about without constraining it in a predetermined direction (Eisenhardt, 1989).

The purpose of this research is theory building. As explained in Chapter 3, the study seeks to offer a process model on how security networks prevent security threats, as well as the incentive mechanisms for ensuring collective security efforts.

Table 4-1 *Case study design process (adopted from George and Bennett (2005) and Eisenhardt (1989))*

Steps	**Activities**
Identify research objectives and problem	RO1. Understand the process by which prevention measures are developed and adopted over time. RO2. Identify actors, their interests, and how the latter are aligned to ensure convergence. RO3. Identify the role of technology in security networks. Problem: 1. Identify the process by which security networks achieve prevention. 2. Identify incentive mechanisms for converging actors in security networks.
Select/build the case	General case of credit card fraud with embedded cases of prevention encounters created through casing process.
Collect the data	Two step process: general and focused search 1. Search Database. 2. Identify key events. 3. Identify major data sources. 4. Locate data sources. 5. Create a timeline of key events. 6. Identify prevention encounters.
Analyse the data	1. Finalize key events timeline. 2. Code the data a. Open coding b. Pattern coding 3. Present the data a. Narrative b. Visual mapping c. Temporal bracketing 4. Within case analysis 5. Cross-case analysis
Enfold literature	Relate findings with existing literature, both conflicting and similar

Accordingly, I defined three research objectives that guided my empirical work and allowed me to answer the research questions:

RO1: understand the process by which prevention measures are developed and adopted over time.

RO2: identify actors, their interests, and how the latter are aligned to ensure convergence.

RO3: identify the role of technology in security networks.

4.4.2 Select/Build the Case

Selecting the appropriate case is a challenging step especially with the lack of consensus on what a case is (Gerring, 2004; Ragin & Becker, 1992), or in Yin's (2014) term what the research unit of analysis is.

The case selected should reflect the research problem and objectives since cases are selected based on their relevance not merely because they are interesting (Eisenhardt, 1989; George & Bennett, 2005). Given the focus on examining security networks, the chosen case should reflect the notion of networks; it should provide the opportunity for studying interactions between heterogeneous actors. In other words, the case ought to be prevention encounters rich. If prevention encounters are not observable in the proposed case, considering an alternative one would seem inevitable to be able to answer the research question.

Taking these issues into consideration, the case of credit card fraud was selected to examine and generate a process model on how security networks achieve prevention. Specifically, three reasons derived the selection of this case. First is theoretical relevance. 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', which is the heart of this research. Second is practical significance. Statistics show that the financial sector is among the top sectors exposed to security threats (Choo, 2011; Symantec, 2009). The total credit card fraud losses in the U.S. was approximately $7.5 billion in 2015 and this is expected to increase (Statista, 2016). Furthermore, the number of credit card usage in offline and online transactions is in continuous growth (Capgemini & RBS, 2013) making credit cards an indispensable technology in our daily lives. Third is future implication. Credit cards are considered the technology that ignited electronic value exchange (Naar & Stein, 1975), by understanding its case we can draw further implications on collective security efforts and incentive mechanisms necessary to face security threats arising from continuous innovations in digital payments.

I should mention that I focused on credit card fraud taking place in the U.S. This is because the U.S. is ranked the top in countries responsible for card fraud losses. For instance, in 2012 the U.S. accounted for 47.3% of the worldwide card fraud losses (PCM, 2015). A second reason is the richness of data sources available for preventing credit card fraud in the U.S.

Credit card fraud represents the general case which then went through *casing* process (Ragin, 1992) to generate *embedded* cases within the general one (Yin, 2014). Those embedded cases (or sub-cases) are exemplified by the research construct 'prevention encounters', with each prevention encounter signifying an embedded case. This theorizing of the research case enables both within-case and cross-case analysis improving the reliability of the generated theory (Eisenhardt, 1989). Cases therefore are not merely selected but also inductively built or constructed by the researcher. They become flexible and manipulable to allow a particular focus that guides empirical work while at the same time be shaped by both theory and empirical evidence (Wieviorka, 1992). An important aspect of casing then is delineating the case so that one will be able to locate them within the voluminous research data (Yin, 2014; Ragin, 1992). When confronting a piece of information, we need to be able to judge whether it falls within the scope of the research or not, if it is part of the case or external to it, i.e. we need a mechanism that specifies how to cut the general case into embedded cases. In investigating the case of credit card fraud, I am interested in collective efforts pursued to prevent the phenomenon; specifically, I am interested in prevention encounters, so my case or unit of analysis is prevention encounters. But since this is a construct developed by the researcher, a mechanism had to be established to specify how cases around that construct are built; that is we need to know the exclusion and inclusion criteria that set the boundaries of the sub-case.

One way to draw the case boundaries is available literature, which has already been visited during the first step when identifying the research problem and objectives. While reviewing the literature, researchers might develop conceptual frameworks with constructs of interest. These frameworks are of great value since the same case can be seen from different angles and theoretical lens. Frameworks remind researchers with the purpose of their research and accordingly what the study should be a 'case of'. Though having predefined constructs may sound contradicting given the emphasis on theory generation, initial constructs or frameworks helps in designing a well-defined focused research. They serve as building blocks for determining what the case is and is not about (Miles *et al.*, 2014). The aim is thus narrowing down what constitute a case leaving analysis and relationships between these constructs (along with others identified while analyzing the data) to a later stage (Andersen & Kragh, 2010; Eisenhardt, 1989).

Accordingly, to identify the prevention encounters and their boundaries I relied on my conceptualizing of the construct. Prevention encounters represent actions taken by heterogeneous actors to develop and adopt prevention measures that shake an established pattern. They are triggered as a response to certain events that constitute a turning key point in security practices. According to this conceptualization, casing from credit card fraud is done according to the following three main criteria:

1. Actors' actions have to be related to developing and adopting prevention measures.
2. Actions have to be initiated by prevention encounters triggers (social pressure, regulations, and technology).
3. Actions are only seen as prevention encounters if they shake an established security practice.

The above protocol was used in the casing process and resulted in creating eight prevention encounters.

4.4.3 Collect the Data

After selecting the case and developing the protocol for identifying prevention encounters, the next step is collecting the data. I should note here that the design of this research, especially with regards to how the case study is conceptualized, was an iterative process. That is, throughout data collection and initial analysis, it became apparent that actors' convergence was most observable in interactions within the context of developing new prevention measures. This helped me to better conceptualize the concept of prevention encounters.

The search for relevant data was guided by the three criteria for determining prevention encounters enabling consistency in data collection across the different sub-cases (Corbin & Strauss, 1990) as well as comparability between them (George & Bennett, 2005). This means that I was selective on the kind of data to use in the research, which is a normal approach especially in historical studies given their voluminous amount of data (Porra *et al.*, 2006). Moreover, as actors involved in preventing credit card fraud are numerous, the data collection was focused on Visa's efforts in preventing fraud which naturally involved identifying other actors who also have a role in fighting fraud.

Data collection went through two main steps: general and focused search.

4.4.3.1 General Search

The first step in collecting the data was doing a general search in order to:

1. Obtain general knowledge of credit card fraud.
2. Identify key events taking place while preventing fraud. Where key events were recognized by comparing them with the concept of prevention encounters. Thus, key events should encapsulate prevention encounters.
3. Extract prevention encounters from key events.
4. Identify major data sources to be used in focused searched to collect more specific data.

To meet these objectives I searched Business Source Premier Database using a broad keyword, credit card fraud, and narrowed the search results using the database built-in limiters. Table 4-2 gives details for the steps followed when doing the general search. The 476 final materials were then analyzed. I used Excel spreadsheet to report the data that seemed relevant to the research in terms of being possible candidates for prevention encounters. The sheet (hereafter data collection sheet) was organized based on the reference and date of the event, with a description of each event.

Initial analysis of data collection sheet showed that actors interacted in the context of developing and adopting prevention measures. Therefore, a new spreadsheet

Table 4-2 *General search steps*

DB search options	**Input**	**Output**
keyword	credit card fraud (in AB abstract)	
Search options	a. Find all my search terms	
Expanders	a. Apply related words b. Also search within the full text of the articles	
Limiters: published date	Jan/1950 - Dec/2013[1]	
Search results		2178
Limit to:		
Subject: Thesaurus Term	credit card fraud, fraud, commercial crimes, identity theft, internet fraud, computer crimes, consumer fraud, data protection, smart cards, data security, commercial credit fraud, phishing, banking industry-security measures	1575
Subject	prevention, security measures, false personation, corrupt practices, computer network resources, safety measures, laws and legislation, criminal law, fraud investigation, crime prevention, biometric identification, law enforcement, case studies, privacy	476

[1] I extended the data collection period for the last prevention encounter to be till the end of 2014 to increase the richness of the data.

(prevention encounters sheet) was created. This sheet was organized according to prevention measures used to prevent fraud, with a description of interactions between actors that accompanied the development and adoption of these prevention measures. Prevention encounters sheet then helped me in drawing a timeline of key events (Figure 4-2). The timeline served as a methodological tool (Mason *et al.*, 1997a) that facilitated data organization and guided the further collection of data.

The initial analysis also identified major data sources to be used in the focused search. Those constituted the references of many of the materials returned by the data search, and sources that were frequently cited by scholars studying the credit card industry. Identified major data sources are:

1. The American Banker – daily newspaper
2. ABA Banking Journal – monthly journal
3. Visa the Power of an Idea – the company's biography
4. Birth of the Chaordic Age – Visa's founder biography

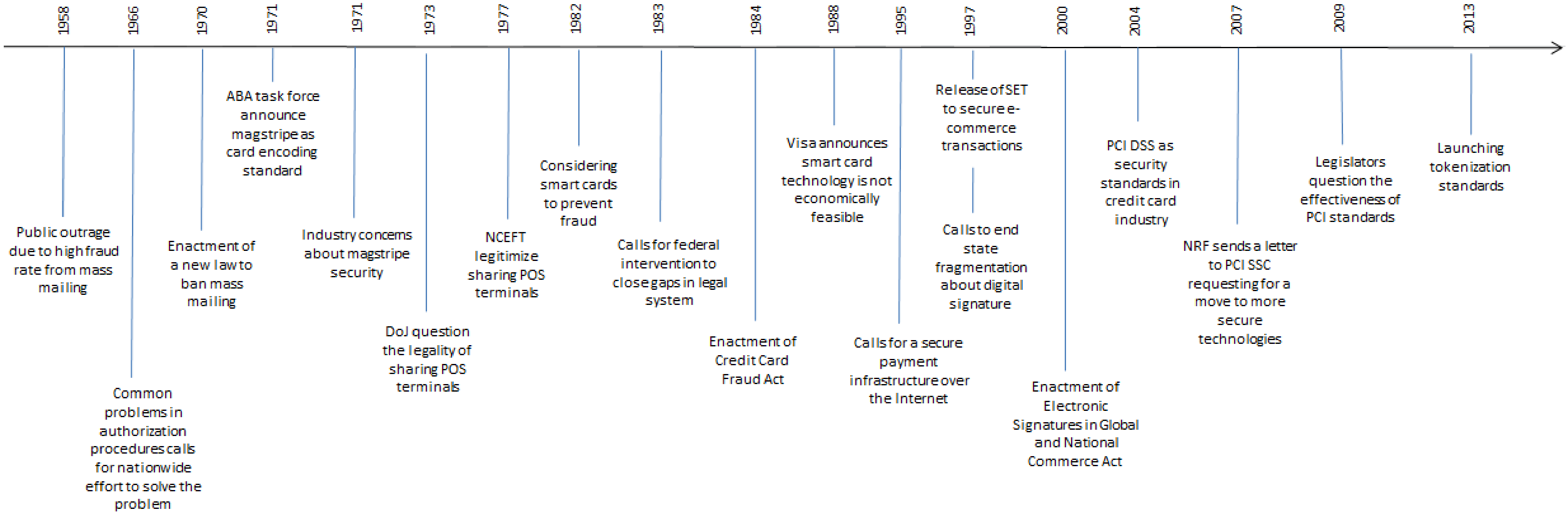

1958
Public outrage due to high fraud rate from mass mailing
1966
Common problems in authorization procedures calls for nationwide effort to solve the problem
1970
Enactment of a new law to ban mass mailing
1971
ABA task force announce magstripe as card encoding standard
1971
Industry concerns about magstripe security
1973
DoJ question the legality of sharing POS terminals
1977
NCEFT legitimize sharing POS terminals
1982
Considering smart cards to prevent fraud
1983
Calls for federal intervention to close gaps in legal system
1984
Enactment of Credit Card Fraud Act
1988
Visa announces smart card technology is not economically feasible
1995
Calls for a secure payment infrastructure over the Internet
1997
Release of SET to secure e-commerce transactions
Calls to end state fragmentation about digital signature
2000
Enactment of Electronic Signatures in Global and National Commerce Act
2004
PCI DSS as security standards in credit card industry
2007
NRF sends a letter to PCI SSC requesting for a move to more secure technologies
2009
Legislators question the effectiveness of PCI standards
2013
Launching tokenization standards

Figure 4-2 *Chronology of key events*

Table 4-3 *Data sources*

Data sources	Description	Main value
Books	• Paying with Plastic: The Digital Revolution in Buying and Borrowing • A Piece of the Action • Electronic Value Exchange: Origins of the Visa Electronic Payment System • Visa the Power of an Idea • Birth of the Chaordic Age	Provide comprehensive historical coverage of credit cards which helped in understanding the context of events taking place and how it affected decisions taken.
Trade journals	• The American Banker • ABA Banking Journal	Provide the ability to follow a certain prevention encounter to examine how it evolved with time.
Press releases/newsletters	Online press releases and newsletters of Visa and NRF	Offer recent and up to date information regarding prevention encounters.
Government documents	Congressional hearings related to certain prevention measure	Provide valuable detailed insights on the heterogeneous actors involved in preventing fraud and perceptions each hold about a certain prevention measure.

Other data sources that are valuable include: “Electronic Value Exchange: Origins of the Visa Electronic Payment System” a book that offers rich data on Visa’s use of technology to prevent fraud with useful insights on associated encounters. Books about the credit card industry: “Paying with Plastic: The Digital Revolution in Buying and Borrowing” and “A Piece of the Action”. Additionally, as the industry is highly regulated and contentious, government documents in terms of congressional hearings provided detailed data on positions held by various actors which helped mitigating data bias (Eisenhardt & Graebner, 2007). I also consulted press releases and newsletters (specifically for Visa and National Retail Federation) which were useful in capturing data about recent prevention encounters. Table 4-3 summarizes the major data sources and the main value derived from each.

In summary, data was collected from these sources: books, trade journals, press releases/newsletter, and government documents. These multiple sources of evidence help in building a stronger and reliable case and writing a coherent story (Yin, 2014). Naturally, every source will tell part of the story that suits its interests, critiquing the evidence is thus necessary (Mason *et al.*, 1997a). For this I used different strategies such as, applying logic, corroborating the event from multiple sources, and assessing the overall coherence of the story (Mason *et al.*, 1997a; Porra *et al.*, 2006). In addition, it is argued that the fact that these sources are publicly available increases the case validity (Porra *et al.*, 2014) and 'keep the researcher honest' (Eisenhardt & Graebner, 2007) as they are openly accessible for scrutiny. Nonetheless, the research data remains limited to what has been publicly announced. Moreover, I should acknowledge that historical knowledge is open to various interpretations where no conclusive meaning of the evidence of the phenomenon can be attained (Marwick, 2001; Porra *et al.*, 2006).

4.4.3.1.1 Locating Data Sources

Once major data sources were identified, the next mission was locating those sources in order to prepare for the second step in data collection; focused search.

Books. Relevant books were purchased online.

Trade journals. I first consulted Warwick Library website to check access to both The American Banker and ABA Banking Journal. Access to the latter was available from 1964 till present offering a comprehensive coverage. I should note however that from 1964 till 1979 the journal was called "Banking". The monthly periodical then changed its name to ABA Banking Journal and it is published under this title since then.

The library has access to The American Banker from 1985 till present. Though this covers a wide time span, The American Banker is a daily newspaper that is dedicated to the banking industry, which indicates the detailed level of information it provides about what is happening in the industry. Also, other data sources (i.e. books) showed that the 1970s was a critical period for the credit card. Thus, I started to search for access to previous records of the newspaper. In doing so, I consulted COPAC Union Catalogue and SUNCAT Union Catalogue, which search a wide range of UK libraries to help researchers locate needed materials. After reviewing search results, University of Essex library was identified as the sole provider of the needed access (access available from 1964 – 1979 in printed form). I contacted the library staff and had the approval for accessing the library's holdings of the newspaper from 1964 till 1979. I planned the field trip and spent a week collecting necessary data. For the period of 1979 - 1985, the same catalogue search identified availability for online access to the newspaper using LexisNexis database.

Press releases and newsletters. Those were accessed through related websites. I focused on press releases and newsletters produced by Visa (www.usa.visa.com) and National Retail Federation (www.nrf.com).

Government documents. Government documents here refer to congressional hearings between legislators and various actors in issues related to credit card security. Books and trade journals often cited congressional hearings, and that is when I became aware that hearings about a certain matter took place. This initial reference was only the start of a thread to draw the complete picture. Gaining full insight was challenging as several hearings occur before the final decision is made. To locate these hearings[1], I referred to the Library of Congress website. The library provides a summary of bills introduced as well as information on where to find full records of the hearings. For this, I used HathiTrust digital library that offers online and free access to a wide coverage of those government documents.

Though the Library of Congress and HathiTrust provide information about hearings, they do not give an indication of the status of the bill. A lot of bills die, i.e. they do not pass the Congress, and no law is enacted accordingly. Tracking bills is important to know whether prevention encounters were successful or not. To achieve this, I consulted GovTrack.us which offers full details on bills history.

4.4.3.2 Focused Search

After identifying key events and locating data sources, I was ready to go through focused search step.

[1] Hearings happen at early stages of legislative policymaking where a bill to enact a new law is introduced and discussed.

Focused search involved using the main data sources to obtain detailed knowledge about each event and the underlying prevention encounter. Here I used specific keywords that reflected the examined prevention encounters. Examples of these keywords are: mass mailing, BASE, magstripe, magnetic stripe, POS terminal, OCR, CVV, smart card, chip and pin, SET, PCI standards, VbyV, tokenization. Keywords also arose when reviewing the resultant material. For example, the search using ‘smart card’ resulted in knowing that Visa called its smart card ‘super smartcard’. This keyword was subsequently used to obtain more information about this technology.

As more data was collected, both data collection and prevention encounters sheets went through several rotations of modifications. This step resulted in updating events timeline to reflect the new data, clarifying the concept of prevention encounters, and identifying eight prevention encounters that are critical in credit card fraud prevention lifecycle.

4.4.4 Analyse the Data

Analysing the data started with the data collection (Corbin & Strauss, 1990) since initial analysis of the materials generated from the general search was needed to conduct the focused search. For instance, I have mentioned before that a chronology of key events was drawn to organize the data and guide focused search. Going through more detailed information in the focused search led to updating and modifying the timeline to correspond more closely with the research construct of prevention encounters.

Data analysis was based on process-tracing methodology (George & Bennett, 2005). Process-tracing is suitable for analysing complex social phenomenon as it recognizes the possible multiple pathways for its occurrence. It thus promotes in-depth investigation to narrow down potential causes. In analysing the data, I sought to trace processes taking place between actors to prevent credit card fraud, including causes and outcomes of actors’ actions as well as how those actions were perceived by different actors. I used Nvivo software to organize all materials and build a database of prevention encounters.

The next step was coding the data. I followed Miles et al. (2014) two coding steps; open and pattern coding. In open coding, I generated codes that describe what I am seeing in the data, whether that was in the form of labels to describe the main idea of a certain amount of text, such as information sharing and privacy concerns, or processes describing actions taking place, such as mobilizing actors and failing to align interests. This resulted in more than 200 descriptive codes. A review of them disclosed some repeated and unrelated concepts. Eventually, I had a list of 192 mutually exclusive descriptive codes.

Unlike open coding, pattern coding is an analytical step. Here, I tried to find regularities, relationships between concepts, and identify patterns. As explicating elements of social structures is central in CR, this step also involved identifying structural entities and their components along with connections among them that enabled them to produce the outcome observed (Wynn &Williams, 2012). I further wrote memos (Glaser & Strauss, 1967) while coding to reflect initial thoughts rising from the data and possible links between codes. In addition, the three forms of incentives synthesized from the literature (transformative, preparatory, and captive) were used while coding the data to provide evidence of their impact on converging actors in security networks. For example, data that represented the use of one or more of the rhetorical arguments was directly coded under the appropriate argument device (perversity, futility, jeopardy). The data was also coded to reflect the vocabulary of motive used to stimulate a particular action (e.g. anti-competitiveness, urgency, shared responsibility) which was then grouped under the subcategory of vocabulary of motives. The category of transformative incentives hence included codes of the three rhetorical devices and the subcategory of vocabularies of motive. I used similar coding strategy for preparatory and captive incentives where I tried to find what aspect of the environment actors was manipulating to drive collective action and how entangled associations between the desired behaviour and actors' interests were created.

As process data is often complex, a combination of strategies was used to help in making sense of it and ease the process of finding relationships. Presentation strategies are: narrative, visual mapping and temporal bracketing (Langley, 1999).

4.4.4.1 Data Presentation Strategies

Data presentation is a significant activity in the analysis process (Miles *et al.*, 2014). The richness of process data poses some challenges on how to best understand them (Langley, 1999). Therefore, I resorted to multiple data presentation strategies to guide me while theorizing from the data.

First, I constructed a thick narrative around key events. I focused on preserving the temporal sequence of these events and therefore decomposed the narrative according to prevention measures that were developed and adopted to prevent fraud over time (i.e. prevention encounters). I also sought to uncover the underlying logic behind actors' actions and discover how those might shape future decisions. The case narrative involved; actions, what triggered them and their outcome in an attempt to explain how security networks achieve prevention and identify incentive mechanisms that come into play to motivate collective efforts to prevent fraud. The narrative purpose was therefore not merely descriptive but also analytical.

The second strategy employed was visual mapping. Visual mapping is a graphical representation of processes, it helps reduce the complexity of the data and make it easier for the researcher to elicit patterns and for the reader to validate the findings (Miles *et al.*, 2014). This strategy goes in line with researches based on process tracing since the later requires being explicit about events taking place and how they link together. Such links are often made visible through graphical representations (Gerring, 2007). Visual maps show the plot in events, and can serve as the foundation for establishing causal analysis because of its emphasis not only on what happened but also how and why (Miles *et al.*, 2014) making it helpful in identifying mechanisms. They also facilitate cross-case comparison to notice similarities and differences between cases (Eisenhardt, 1989). I produced a graphical representation for each of the eight prevention encounters that displayed the sequence of events and how they affect each other (those are presented in the next chapter).

Finally, temporal bracketing is “a way of structuring the description of events” (Langley, 1999, p. 703). In my research, temporal bracketing was associated with the period of each prevention encounter. That is, from the time it was triggered till the time the final decision about the prevention measure was taken. This enabled examination of how decisions to prevent fraud in one period were shaped by decisions made in a previous one.

Table 4-4 summarizes the data collection and analysis process.

Table 4-4 *Data collection and analysis process*

Steps	Tasks	Outputs
1. General database search	a. Search Business Source Premier using keyword "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 understanding of prevention encounters. b. Prevention encounters database
4. Presenting the data	a. Write detailed descriptions of prevention encounters b. Temporal bracketing of prevention encounters c. Draw graphical representations of prevention encounters	a. Thick case narrative b. Temporal structuring of prevention encounters c. Visual maps of prevention encounters
5. 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.
6. Identifying structural entities and contextual triggers	a. Identify structural entities, their components and relationships among them. b. Identify and typify contextual conditions that trigger prevention mechanisms	a. Structural entities and their properties b. Contextual conditions
7. Identifying prevention mechanisms	a. Analyze patterns to elicit prevention mechanisms	Three prevention mechanisms
8. Identifying incentive mechanisms	a. Analyze prevention encounters and map them with synthesized incentive mechanisms (transformative, preparatory, captive) b. Identify incentive mechanisms in security networks	Incentive mechanisms for collective action in preventing security threats

Research Findings

5 THE CASE OF CREDIT CARD FRAUD

5.1 Introduction

This chapter offers a narrative of the research case study. It details Visa's effort, along with others in the credit card industry, to prevent credit card fraud. The narrative is structured around the research concept of prevention encounters, which illustrate heterogeneous actors' efforts to develop and adopt prevention measures over time.

5.2 The Battle against Credit Card Fraud

A turning point in the card payment industry was the year of 1958. Though buying on credit was not an unusual practice before that year with many customers holding Diners Club, the only general purpose credit card at that time, 1958 marked the start of competition in credit card market upon the decision of one of U.S. largest banks, Bank of America (BofA), to issue its own credit card.

5.2.1 Prevention Encounter 1: Credit Card Mass Mailing

Following the success of Diners Club, BofA decided to launch its own credit card (called BankAmericard) in 1958. Unlike other cards that targeted a particular market segment, usually businessmen and high-class customers, BofA targeted middle-class customers seeking to serve a larger customer base. To create this base of cardholders and ensure merchants acceptance of their card, BofA resorted to mass mail BankAmericard to all its customers. The success of the bank's experience alerted other banks to the new lucrative market, where they also resorted to mass mailing to rapidly secure their market share (Weistart, 1972).

With mass mailing becoming the norm to attract customers, the banking industry had been typified by their lack of stringent security practices, placing quick profits over customers' financial safety. The massive fraud rate accompanying mass mailing provoked extreme public anxiety for they were responsible for purchases they have never made, using a card they have not received or requested. The absence of effective security practices for the new innovation adversely affected the banking industry, with regulatory bodies recognizing the phenomenon went out of control and it is time to interfere to control banks' behaviour.

Several bills were introduced in the Congress to either restrict or prohibit credit card mass mailing (for more information on these bills see (Kennedy, 1969)). Wishing no legal intervention in their new business, the banking industry collectively participated in congressional hearings through its Federal Reserve Board (FRB) and American Bankers Association (ABA), stressing that credit cards need no new regulation, and fraud problem has been overestimated. In the defence of their practices, the industry representatives asserted that by changing mailing procedures to check customer credit-worthiness, banks will be able to control fraud and regain stability (Brimmer, 1969). In addition, banks investigations of the public's attitudes towards credit cards concluded that contradictory to the common perception, customers were thrilled not anxious about the cards as receiving one signalled a trust relationship between them and their banks. Another issue was also raised regarding the anticompetitive nature of the new law that refuted legislators' mission of encouraging competition. A ban on mass mailing would put early adopters at a competitive advantage, and erect barriers to entry since other means (such as sending applications) proved to be ineffective (Banking, 1969; Brimmer, 1967).

Despite these efforts, pressure was building up to ban mass mailing or introduce new security practices with the increase in protest letters sent to the Federal Trade Commission (FTC) and the further bills that were introduced in the Congress. With all fingers pointing to banks' reckless behaviour, the latter sought to shift some of the security responsibility to the U.S. Postal system; fraud was mainly caused by mail theft of credit cards, and banks should not be blamed for inappropriate security procedures in the postal system (Banking, 1969). Some bills therefore allowed unsolicited mailing with the condition that cards are sent by registered mail, a solution that was opposed by financial institutions due to its high costs. Other bills proposed sending customers pre-mailers informing them that they will receive a credit card. The bill that received most attention was the one that authorised the FRB to specify requirements that determine who can be targeted by mass mailing, and limited customer liability to only $50 (Unsolicited Credit Cards, 1969). While the FRB and the credit card industry had no objection to the liability argument they rejected the other part of the proposition. First, following FRB examiners' instructions to banks on the importance of improving their mailing screening practices, which has been done, there was no need for the FRB to have this regulatory authority. Second, it was hard to establish a standard for defining customer's credit worthiness in such a diverse industry, and even if this was done it would result in high standards that would make it difficult for middle-income people to get a credit card. The industry further reiterated to the Congress their previous argument regarding the anticompetitive nature of a law that would ban mass mailing. Besides, they argued that the message that would spread upon passing the law is that innovations in the financial industry were not welcomed by the Congress (Brimmer, 1969).

The fact that the bill did not prohibit mass mailing rather placed some restrictions, made it face additional resistance from those calling for a complete banning legislation. To strengthen their arguments, opponents brought legislators' attention to the various negative impact mass mailing had on society, and structured their arguments around four pillars. First, the indiscriminate distribution of credit cards encouraged criminal activities not only through unauthorized usage but also through selling them in underground market to obtain direct cash. Second, credit cards induced customers to spend more, which caused an increase in demand and subsequently increased inflation rate and personal bankruptcies. Third, unsolicited mailing increased credit card diffusion which threatened the economy that has always flourished on thrifts. Finally, customers considered this practice an invasion of their privacy and one that involuntarily involved them in a new financial arrangement they might not seek (Hanley, 1969; Meade, 1969).

These arguments succeeded in gaining the Congress attention, who sought during multiple hearings to validate these claims with witnesses from the financial and retail industry, as well as testimonies from the general public. After nearly three years of negotiations, a new law prohibiting mass mailing was enacted in 1970. Figure 5-1 shows prevention encounters in banning mass mailing.

The passage of the new regulation placed further restrictions on banks, who bore most of the losses from fraudulent transactions with customers liable to only $50. This liability was even activated under stringent conditions. Banks must notify customers of their potential liability, and supply them with a self-addressed stamped notification form to mail their banks in case the card was lost or stolen. Moreover, banks had to prove the card was legitimate, in a sense that it was either requested by the customer or has been used (i.e. prove it was not an unsolicited card), and that any unauthorized use of the card happened before they received the bank notice (Weistart, 1972). Under these conditions, it was very unlikely that banks would go through the trouble of asking customers for this liability share as clearly it was not worth the effort. Moreover, they feared adverse public reaction if they did not absorb the loss. The law thus drove the industry towards adopting better security practices in order to reduce their losses.

With the enactment of this new law, the banking industry's efforts to keep their new business under self-regulation failed. Banning mass mailing law reinforced regulatory agency's power over the banking industry expanding its coverage to include credit cards as well. This had an influence on future security practices actors sought when preventing fraud.

5.2.2 Prevention Encounter 2: Automating Card Transactions

Before its ban, mass mailing allowed BofA to obtain a large customer base for its BankAmericard. This base was nevertheless geographically constrained by federal and state regulations that prohibited banks from branching across states. To achieve its vision of a national recognition of its credit card, in 1966 BofA licensed its BankAmericard program to banks across different states. A security challenge quickly arose; license agreement meant participating banks had to honour cards issued by any licensee (Abouchar, 1969; Stearns, 2011). Failing to provide an effective mechanism for authorizing transactions threatened the achievement of

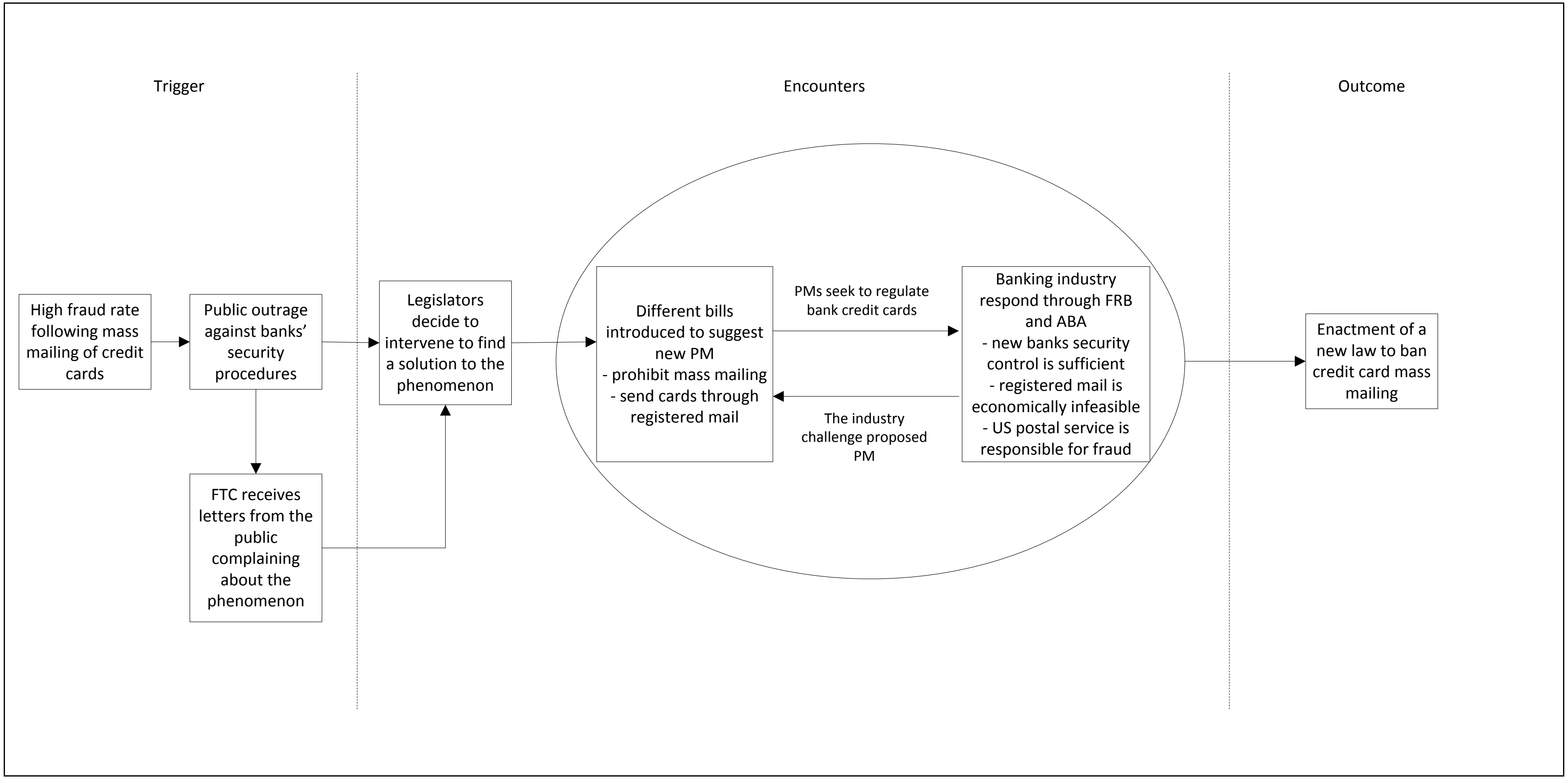

Trigger
Encounters
Outcome
High fraud rate following mass mailing of credit cards
Public outrage against banks' security procedures
FTC receives letters from the public complaining about the phenomenon
Legislators decide to intervene to find a solution to the phenomenon
Different bills introduced to suggest new PM
- prohibit mass mailing
- send cards through registered mail
PMs seek to regulate bank credit cards
The industry challenge proposed PM
Banking industry respond through FRB and ABA
- new banks security control is sufficient
- registered mail is economically infeasible
- US postal service is responsible for fraud
Enactment of a new law to ban credit card mass mailing

Figure 5-1 *Prevention encounters in banning mass mailing*

BofA's vision of a card used anytime anywhere in the U.S. Two alternatives were on the table, either create a centralized database of all licensee cardholders' data, which meant BofA would have full control over banks financial data, an option favoured by neither licensees nor legislators, or maintain the decentralization of cardholders' information and make it acquirers' (merchant's bank) responsibility to direct authorization requests to issuing banks (Stearns, 2011).

Going for the second alternative made the authorization process works as follow (Stearns, 2011; Wiegold, 1971). When a customer presented his credit card for payment, the clerk had first to consult a "hot card" list showing numbers of cancelled credit cards that should not be honoured. Once the card was cleared, the clerk checked the transaction amount; if it was less than the floor limit no authorization was required (from the issuing bank). If otherwise, the clerk called the acquirer authorization center and verbally communicated the card number and transaction amount. The operator on the merchant bank side checked whether the transaction was local (the credit card was issued by the merchant bank) or interchange (card issuer was another bank). If the transaction was local, the operator consulted pre-printed reports that displayed customer account history and credit limit/balance, as well as checking hot card list. If the transaction was authorized, the operator gave the merchant clerk (who waited on the phone during the whole process) an authorization code to write down on the sales draft, acting as evidence that the authorization process has actually taken place. The clerk was also supposed to check customer's signature on the sale draft against that on the card.

If the transaction was an interchange, the acquirer operator telexed or called the issuing bank authorization center and conveyed the transaction details. The operator on the issuer side would perform the same activities mentioned above; communicated the authorization code to the merchant bank authorization center, who then communicated it back to the merchant clerk. Such authorization process took between 5-20 minutes. In cases where the operator could not make a decision on his own (for example the transaction amount exceeded customer credit limit), he had to consult a supervisor who, using the reports, decided the appropriate action.

This authorization mechanism proved its ineffectiveness. In their efforts to satisfy and show respect to their customers, merchants tended to drop hot card list checking from the authorization process (Bartling, 1967; Sutherland, 1981), and sometimes the whole authorization procedure realizing that the massive increase in sales volume made banks too occupied to note replications in authorization codes (Chutkow, 2001). Apparently, security practices for interchange transactions were not carefully thought about, especially with the differences in times zones across states that made them inapplicable as some authorization centers could be simply closed. Licensee rebelled against BofA for its lack of proper security controls that made them lose millions to fraud instead of making profit from the new business.

To tackle the problem, a new self-governing member-owned organization, called National BankAmericard Inc. (NBI)[1] was formed with the responsibilities of facilitating the program's operation and marketing functions nationwide, and developing an interchange system to reduce fraud. The prevalence of authorization problems across banks however made some of them suggest pursuing a joint effort instead of an individual one to collectively plan for a nationwide authorization system. In April 1970, BofA and American Express sent letters to Master Charge, Diners Club, BofA licensees informing them about the joint effort plan and seeking their support (Brooke, 1970b). This attempt did not echo very well. NBI questioned BofA's real intentions as it was specified one of the reasons for forming the new organization was developing an effective authorization system (Hock, 1999). Additionally, Master Charge perceived this action as an attempt to compete with its own authorization system run by Omniswitch Corp. BofA and American Express stressed their plan does not aim to replace or compete with Omniswitch authorization system, but rather complement it by offering early warnings on fraud activities on a national level instead of regional one, and lower communication costs due to shared usage (Brooke, 1970a). These efforts failed to meet their purpose and sentenced BofA and American Express plan to a dead end. The goal of building a single authorization system persisted and soon after a committee of representatives

[1] Renamed to Visa in 1976

from BofA, American Express, NBI, Master Charge and other large card issuers along with major merchants were formed to resolve any conflicts and reach a solution (Hock, 2005).

Fear of creating a monopoly in the card industry that would invite undesirable intervention of regulatory agencies drove NBI to abandon the joint effort and announce a unilateral pursuit to develop its own authorization system (Stearns, 2011; The American Banker, 1971). Though this announcement incited competition between software and hardware vendors, who got the opportunity to submit their proposal to meet an explicit need, failing to meet NBI's specifications pushed the latter to reject the 13 submitted proposals and internally develop the new system called BankAmericard Authorization System Experimental (BASE) (Stearns, 2011; The American Banker, 1972).

BASE went operational on April 1, 1973 exploiting information technology's power, and acting as a central traffic coordinator transforming the authorization process that became as follow. When a customer presented his credit card to a merchant and the amount required authorization, the clerk called his local/acquirer authorization center and relayed the card number and transaction amount, the operator in the authorization center typed this information on a terminal and submitted the inquiry through BASE. Using the first four digits of the card number, BASE determined the issuer and forwarded the authorization request to its authorization center. If the transaction was legitimate, an authorization code was transmitted back to the acquirer center, and the operator then communicated it to the clerk. With BASE, the authorization process that took from 5-20 minutes required less than 60 seconds to be completed (Brooke, 1973a; Chutkow, 2001; Stearns, 2011). Prevention encounters in developing authorization system are depicted in Figure 5-2.

In its first year of operation, BASE saved members more than $30 million in fraud prevention (Chutkow, 2001). Despite this, BASE was mainly a system for automating interchange transactions, replacing telex or telephone communication with a computerized one. Actual authorization procedures depended on whether banks had automated their local authorization processes or not. Further, the process at merchant's side remained inefficient; they had to consult hot card lists which were only getting larger, and call authorization center to complete the transaction. Above all, floor limits still existed which meant most under limit transactions were being processed without authorization (as mentioned previously merchants usually ignored consulting hot card list due to its impracticality and fear of sales loss). To solve this problem, there was a need for a more effective and efficient method for communicating data between merchants and banks (Brooke, 1973a; Stearns, 2011).

5.2.3 Prevention Encounter 3: Automating POS Terminals

Since the early 1970s, the card industry was occupied with developing different technologies to fight fraud. Efforts were directed either towards developing authorization systems (as BASE) or technologies for capturing and transmitting data from merchants' sites to issuing banks (i.e. automating point-of-sale (POS) terminals) (see Figure 5-3). There was an agreement in the card industry that the latter should not require human intervention; the whole authorization process should be automated to eliminate human error and reduce chances of fraud (Stearns, 2011). The encoding technology should also be a viable solution across the industry's various players, i.e. it should be a standardized one to enable cheap and unified terminal implementation and facilitate coordination between different authorization networks. This agreement drove experimentations in machine readable card technologies. To evaluate the various encoding technologies and offer recommendations on which one to become the industry standard ABA formed a card standardization task force (Stearns, 2011; The American Banker, 1970).

From the forty-four proposals submitted to the ABA task force, offering a total of twenty-one distinct encoding technologies including: embossment, magnetic stripe, optical codes, and embossed magnetic, the task force decision came to favour magnetic stripe as the best encoding technology for machine-readable credit card and the one that should be adopted by the credit card industry. The decision was taken according to various criteria. First was proved technology. Magnetic stripe (or magstripe) could not be considered a new technology; it was used in computer systems, and IBM had successfully developed magnetic tape plastic cards prototyped by American Express and American Airlines. Further, the banking industry was

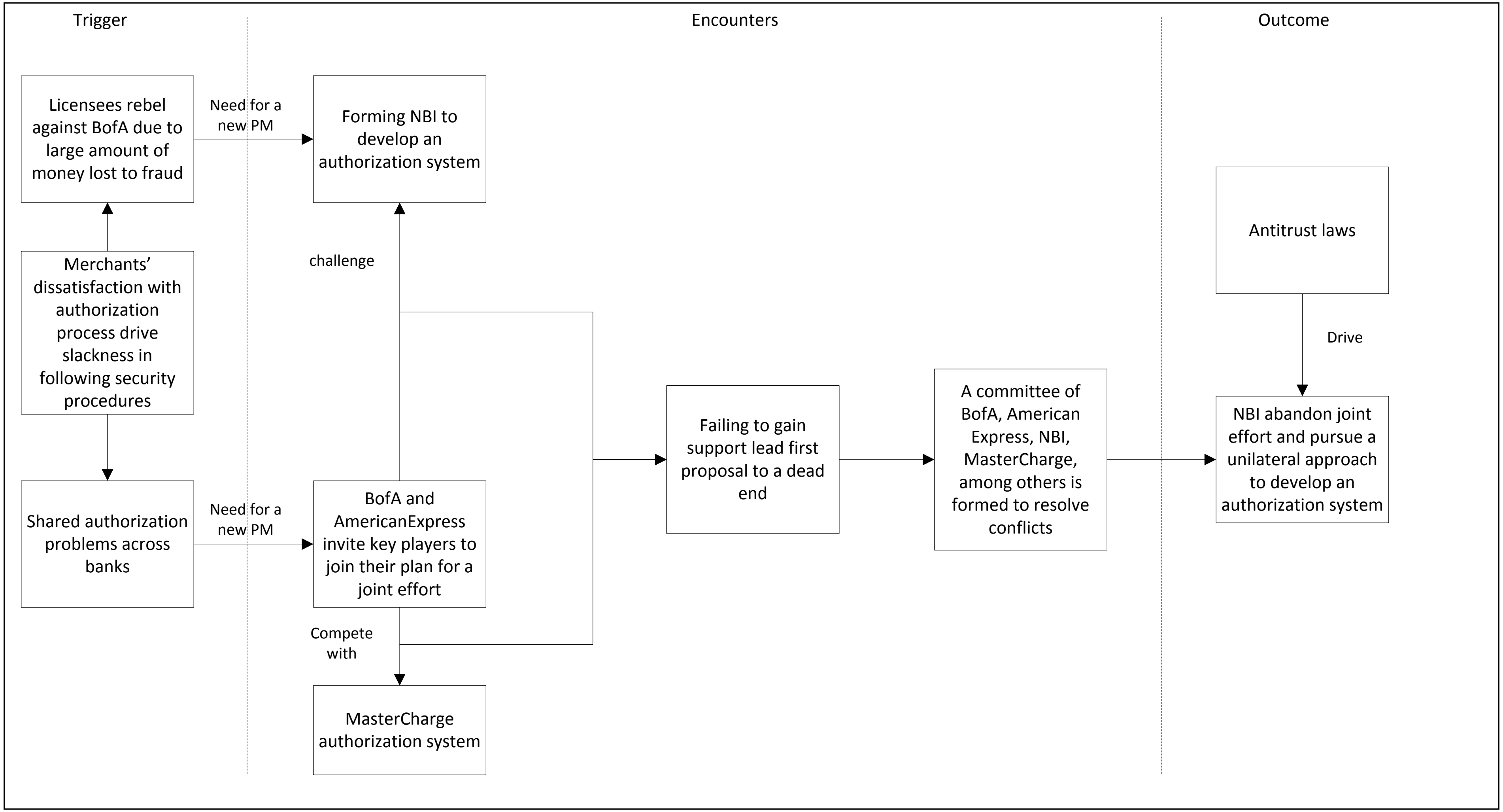

Trigger
Encounters
Outcome
Licensees rebel against BofA due to large amount of money lost to fraud
Need for a new PM
Forming NBI to develop an authorization system
Merchants' dissatisfaction with authorization process drive slackness in following security procedures
challenge
Antitrust laws
Drive
Failing to gain support lead first proposal to a dead end
A committee of BofA, American Express, NBI, MasterCharge, among others is formed to resolve conflicts
NBI abandon joint effort and pursue a unilateral approach to develop an authorization system
Shared authorization problems across banks
Need for a new PM
BofA and AmericanExpress invite key players to join their plan for a joint effort
Compete with
MasterCharge authorization system

Figure 5-2 *Prevention encounters in developing authorization system*

familiar with magnetic technology as it used magnetic ink for processing their checks. Therefore, magnetic technology was well established in the market with capable manufacturers and encoding equipment and terminals that were already available. Second was data capacity. The selected technology had to be scalable in order to meet future needs. Magstripe had the capacity to incorporate multiple recording tracks making it flexible and adaptable. Third was security. While other encoding techniques relied on the embossed character on the card, data in magstripe was invisible making it difficult to alter, thus more secure. Fourth was production volume. The production of plastic cards, applying the magstripe, and finally encoding the data on the stripe could be done at high speed. Fifth was cost. Compared to other technologies, the task force concluded magstripe was the most feasible encoding technology in terms of cost (Banking, 1973; Brooke, 1971b; Bureau, 1971; Stearns, 2011).

ABA task force endorsement of magstripe was contested by multiple actors who invested in other POS systems and encoding technologies, leaving the industry by this in flux. Retailers opted for optical character recognition (OCR) for reading card data, and many were already installing OCR POS terminals. Retailers were accustomed to OCR as they used it to read data on card sales drafts. They supported their technology by confirming that card embossed characters were already printed in an OCR readable format. Banks therefore would not bear any new costs as it would have with magstripe (Stearns, 2011). This latter claim vanished when banks declared the authorization process required both account number and expiration date. While account number font was OCR compatible, expiration date was not. Applying OCR would therefore incur new production costs, and so it had no advantage over other suggested technologies pertaining to this aspect. Moreover, standardizing font to comply with OCR requirements was opposed by cards manufacturers who produced different types of fonts, and standardization would force them to lose part of their business.

This however did not completely burn OCR bridges of becoming the standard as concerns about magstripe security were on the rise. A representative of Western States Bankcard Association questioned whether the new standard was preventing fraud or facilitating it. The simplicity of security principles behind magstripe made copying card data from one card to another an easy task. In addition, the probability of fraud increased with the inconsistency between data used for authorization (data in magstripe) and data used for settlement (card embossed characters in sales draft), a risk that did not exist with OCR which used the same embossed data for authorization and settlement (Brooke, 1971a).

For ABA simplicity was inescapable to make POS terminals economically feasible to all merchants, especially low-volume ones who could not afford a more sophisticated technology. Nevertheless, the task force acknowledged that no technology was 100% secure or enough to attain security, experiments underway should guide future improvements in magstripe security, while banks security procedures for detecting fraud should work to complement it. ABA's lack of concern regarding these claims can be explained by the cashless society vision other banks might have ignored. In a cashless society, all financial transactions would be automatically performed by Electronic Funds Transfer (EFT) system. Sales draft thus would only act as a sales receipt for customers, not a device for claiming funds, so the inconsistency claim would be irrelevant (Stearns, 2011).

Debates over magstripe security did not settle, and concerns were reverberated again nearly two years after when in April 1973 Transaction Technology Inc. (TTI), a subsidiary of First National City Corp., planned a competition among students for breaking the security of magstripe. In a press release, TTI announced the security of magstripe could be compromised using simple cheap devices (Brooke, 1973b). With this announcement Citicorp challenged the industry standard and introduced its more secure technology (called Magic Middle), and started developing and installing compatible POS terminals in various merchants and bank branches sites (Tyson, 1973).

These continuous security challenges kept the industry from stabilizing on a certain standard, offering no clear direction of how securing card transaction was going to be achieved, hindering POS terminal automation. Banks through their testing experiments concluded that for POS automation to be economically justifiable, terminals needed to be shared between banks, and standardization would enable this sharing. Further, POS was part of a larger system, EFT, and any problems in automating POS would only cause delays in implementing EFT systems (Brooke, 1973c; Stearns, 2011). So there was an urgent need to approve on a standard technology. Various actors sought to end this limbo state; bank leaders reiterated their support for magstripe stressing the overall value of the technology outweighed the security concerns (Brooke, 1973c), and ABA set criteria for any accepted credit card technology. First, the technology had to be publicly available to any card issuer with no fees or licensing agreements. Second, it must have enough capacity to record all needed information. Third, it must be open to issuers outside the banking industry as well (The American Banker, 1973). Apparently the criteria were tailored to match only magstripe and foreclose any competing technologies. Citicorp new credit card was based on a proprietary technology violating the first criteria. Embossed character recognition (through OCR) did not meet data capacity condition. Finally, besides meeting the first two criteria, magstripe was already in use in other industries, such as airlines, formally claiming itself the sole legitimate nationwide standard.

While agreement on an industry standard was crucial for allowing the development of POS terminals to progress, the industry faced another complication that interrupted POS terminal automation. In May 1973, the Department of Justice (DoJ) antitrust department declared it would not permit any joint efforts to develop unified POS terminals, and it could seek court support to prevent this kind of action. A joint venture was presumed to weaken competition, produce a monopolized system, kill incentives to develop new innovative POS terminals and deny consumers the right to choose a system that best serves their needs and by so burdening them with extra costs of services they might not use. The department also argued that electronic banking was an emerging phenomenon and running into the conclusion that sharing POS was the optimal solution was still early to decide. Instead, regulations should ensure the survival of various competing systems and let the public choose ones that would stay in the market (Baker, 1974).

From the banks perspective, DoJ confused functions banks compete through with those they do not. Automating POS terminals was a technical task for building a unified switch and processing center, and this resided outside banks competition territory. Banks compete through their products (credits, loans, overdrafts) not technologies that deliver these products. A joint venture for shared POS terminals could not therefore be considered violating antitrust laws. In addition, sharing would facilitate the enrolment of small-size financial institutions who could not tolerate the technology's high development costs, giving customers the freedom to choose from a large base of financial institutions (Brown, 1972; Fisher, 1974).

The implications of DoJ announcement threatened the automation of POS terminals. If sharing was disqualified, banks would either need to develop a new mechanism for authorizing transactions or develop different terminals that would be piled up at merchants' checkout counters. This latter proposition was completely opposed by both parties. Merchants set a single POS terminal that accommodates all banks' cards on the top of their demands for enrolling into POS automation project (Asher, 1974; Banking, 1975). And without collaboration, banks would find it economically infeasible to develop their own POS as mentioned previously.

To resolve the endless clamour over POS terminals along with other issues regarding EFT, the Congress established National Commission on Electronic Funds Transfer (NCEFT) in October 1974 to investigate and develop a national policy for EFT. The investigation that lasted for 21 months concluded sharing POS terminals would be pro-competitive, and served the interest of both the consumers and the industry as a whole. However, it maintained the right to challenge this pro-competitive sharing on a case-by-case basis as the effect on competition varies according to the geographic and product market, and the number and size of sharing players (National Commission on Electronic Fund Transfers, 1977). The commission's decision removed another obstacle deterring the development of POS terminals, after which the process moved smoothly allowing merchants to authorize *all* transactions (floor limit became zero) and shifting the liability for fraudulent transactions to issuing banks. Nevertheless, the high cost of these terminals that could reach up to $2000/each drove reluctance in adopting them, especially for low-volume merchants (Stearns, 2011).

As no prevention measure would be useful if it was not diffused, Visa took several actions to solve this problem. Among these was relying on competition between technology vendors to develop cost effective terminals. GTE, Northern Telecom,

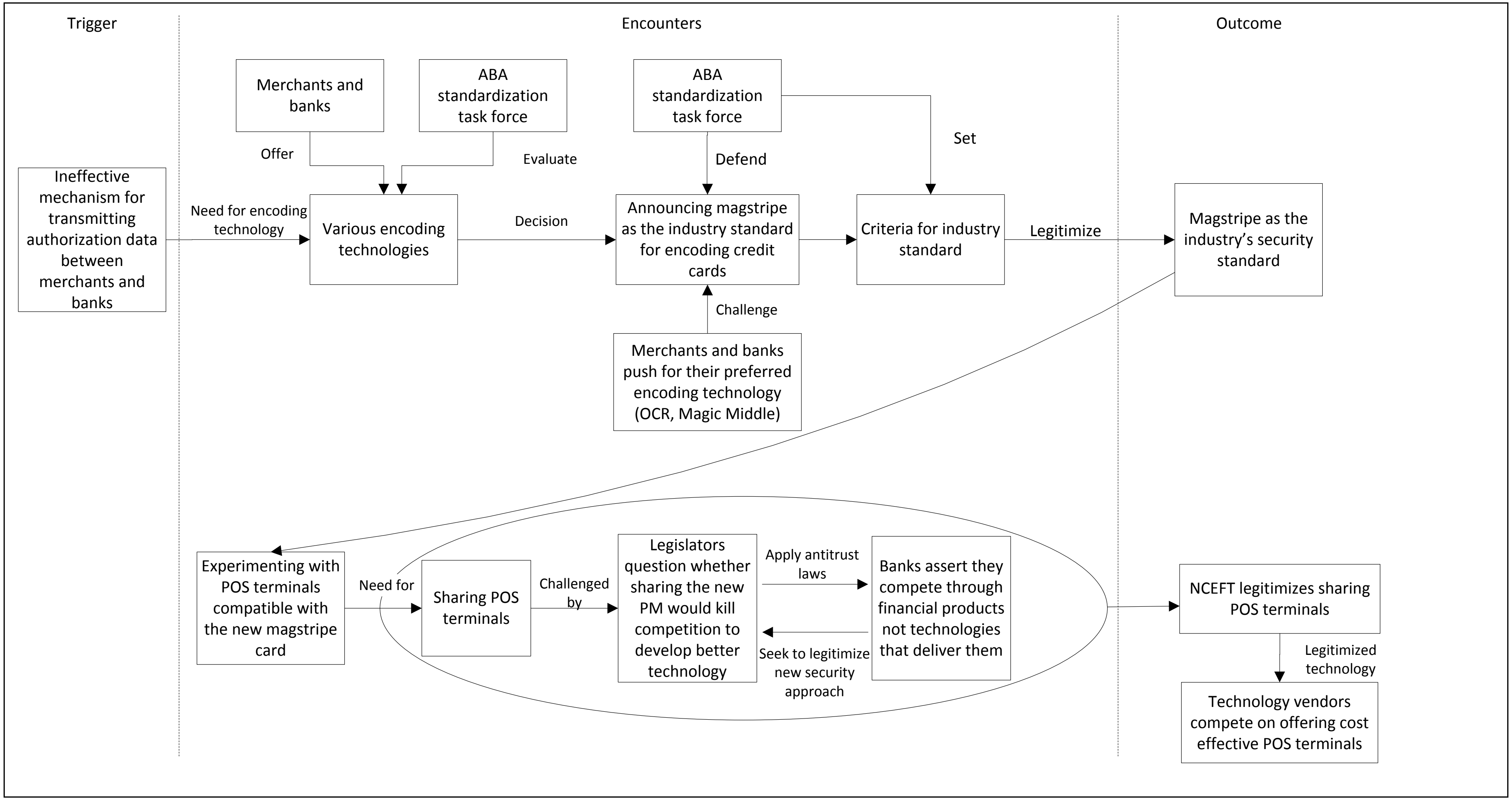

Trigger
Encounters
Outcome
Merchants and banks
ABA standardization task force
ABA standardization task force
Offer
Evaluate
Defend
Set
Ineffective mechanism for transmitting authorization data between merchants and banks
Need for encoding technology
Various encoding technologies
Decision
Announcing magstripe as the industry standard for encoding credit cards
Criteria for industry standard
Legitimize
Magstripe as the industry's security standard
Challenge
Merchants and banks push for their preferred encoding technology (OCR, Magic Middle)
Experimenting with POS terminals compatible with the new magstripe card
Need for
Sharing POS terminals
Challenged by
Legislators question whether sharing the new PM would kill competition to develop better technology
Apply antitrust laws
Banks assert they compete through financial products not technologies that deliver them
Seek to legitimize new security approach
NCEFT legitimizes sharing POS terminals
Legitimized technology
Technology vendors compete on offering cost effective POS terminals

Figure 5-3 *Prevention encounters in automating POS terminals*

Sweda, and TalTek offered their prototypes for a pilot test, with the goal of evaluating these low-cost terminals and ensuring a workable authorization system (ABA Banking Journal, 1980; Stearns, 2011). The company also lowered its interchange fee increasing by this merchants' profitability (Neumann, 1983; Stearns, 2011). These efforts paid off and by mid-1980s POS terminals were widely adopted, all transactions were authorized and fraud dropped significantly.

5.2.4 Prevention Encounter 4: Smart Card vs. Magstripe

After nearly ten years of announcing it the industry standard, and with fraud losses reaching up to more than $2 billion in mid-1980s, the card industry started considering whether magstripe had become obsolete and it was time to adopt another technology (Kutler, 1986d) (see Figure 5-4). Smart cards, mainly adopted in Europe, used an embedded microprocessor chip that authenticated cardholders through personal identification number (PIN), proved to offer a higher level of security against fraud as the card's chip could not be easily duplicated or copied (Walker-Leigh, 1982).

The card industry's response to the new technology was controversial. MasterCard was one of the biggest supporters for smart cards; its experiments showed that participating members witnessed a significant decrease in fraud losses. The company's high investments in experimentations reflected its belief in the technology perceiving it as an effective solution to staggering fraudulent activities that had plagued the industry. Smart cards could not only address counterfeiting but also credit loss problems. The card could be programmed to shut down when cardholders reach their credit limit (Kutler, 1986c; 1986d).

Visa, on the other hand, was more sceptical about smart card's feasibility. The result of a study the company sponsored along with other organizations revealed security alone could not render smart card economically feasible; investing in smart cards cost nearly $15/card while magstripe cost was less than $1/card; the card had to offer other new services to make its costs justifiable (Kutler, 1986b; 1986c). Upon these findings, Visa contracted with Smart Card Internationals to produce a multifunctional chip embedded card (called super-smart card) that would incorporate other services such as a calculator, a clock, and a calendar. The card would further store information regarding numerous account types (credit, savings, check), and be designed with a keyboard and a screen display to enable cardholders to access and manage their different accounts (Berglund, 1987; Weinstein & Marshall, 1985). Proponents of the technology however claimed that economic feasibility should not be a problem when considering magstripe shorter expiration cycle that significantly adds to its costs in comparison to smart cards (Kutler, 1986a; 1988).

Debates between Visa and MasterCard continued with Visa stressing the industry not to rush in taking the decision to transition to smart cards and reminding it about the massive investments incurred in magstripe while MasterCard criticising the clinging on to an obsolete technology and advocating smart card's feasibility and effectiveness in cutting fraud. The contradiction between the two card associations' approaches, Visa's evolutionary and MasterCard's revolutionary, rendered the industry in limbo with no clear path of whether smart cards would replace magstripe or not. The vision got clear in 1988 when Visa announced that smart card was still an immature technology and magstripe would be the primary payment technology in the 1990s, opening the opportunity for technology vendors to arm it with further security features (Kleege, 1993; Kutler, 1988).

5.2.5 Prevention Encounter 5: Strengthening the Legal System

Though automating the authorization process contributed immensely in preventing fraud, the industry found itself facing a new wave of fraud that was accelerating. Card counterfeiting and alteration became the dominant modes of conducting fraud. Criminals obtained card account number by stealing cards and copying information encoded in the magstripe through handmade skimmers, or by simply looking for carbon sales draft in trash cans (called dumpster-diving). This information was then used to produce counterfeited cards, or use the card account number in phone or mail orders. Visa estimated that losses from such activities could cost the banking industry more than $10 billion in 5 years.

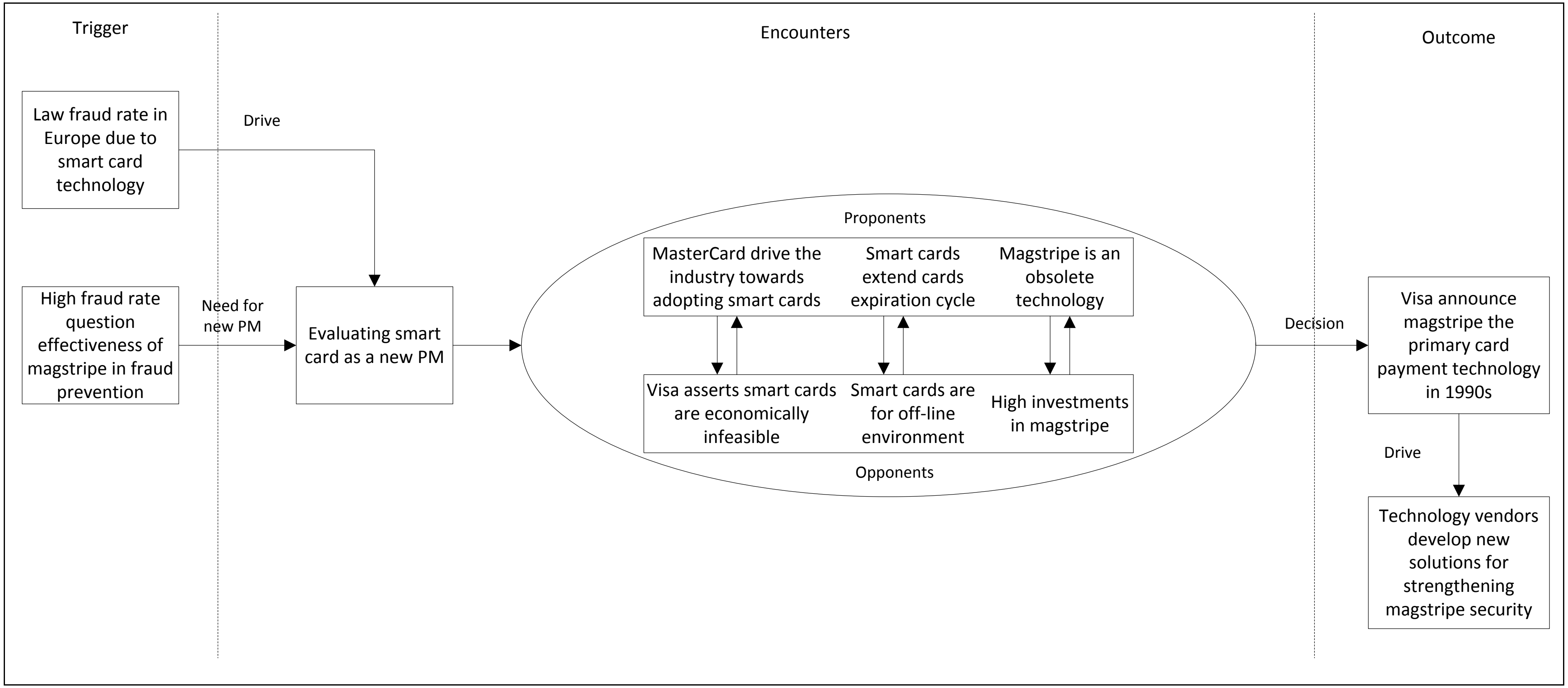

Trigger
Encounters
Outcome
Law fraud rate in Europe due to smart card technology
Drive
High fraud rate question effectiveness of magstripe in fraud prevention
Need for new PM
Evaluating smart card as a new PM
Proponents
MasterCard drive the industry towards adopting smart cards
Smart cards extend cards expiration cycle
Magstripe is an obsolete technology
Visa asserts smart cards are economically infeasible
Smart cards are for off-line environment
High investments in magstripe
Opponents
Decision
Visa announce magstripe the primary card payment technology in 1990s
Drive
Technology vendors develop new solutions for strengthening magstripe security

Figure 5-4 *Prevention encounters in adopting smart card technology*

Despite Visa’s efforts to strengthen the security of the magstripe card by adding different security features, such as holograms, fine line printing, and an encrypted numeric value called Card Verification Value (CVV) encoded in the magnetic stripe, fraud remained staggering high. The legal system did not consider illegal use of credit card numbers a criminal activity; credit cards were restricted to “any card, plate, coupon book or other credit *device* existing for the purpose of obtaining money, property, labor, or services on credit” (Truth in Lending Act, emphasis added). Since credit card number is not a device, courts could not press charges on fraudulent use of card numbers. This encouraged fraudulent use of card numbers, Visa’s statistics revealed that losses from card counterfeiting jumped from $750000 in 1981 to $10.9 million in 1982. Similarly, MasterCard reported an increase in losses of $19.8 million in 1982 in comparison to losses in 1981. With these staggering losses Visa along others in the card industry relayed their concerns that weaknesses in the legal system had a central role in intensifying the phenomenon. Acknowledging these problems and the need for reinforcing current prosecution and preventive tools, legislators initiated several congressional hearings proposing different bills on how to best address these weaknesses (See: the Credit Card Protection Act (1983); Counterfeit Access Device and Computer Fraud and Abuse Act (1983, 1984); the Credit and Debit Card Counterfeiting and Fraud Act of 1983 (1983); and Joint Resolution (1984)). During these hearings that involved a wide range of actors such as, card associations, ABA, National Retail Merchants Associations, Credit Bureau, U.S. Secret Service, and U.S. Postal Inspection Service, concerns were raised regarding the inadequacy of current statutes that are used to prosecute credit card fraud. Truth-in-Lending Act, mail fraud and wired fraud statutes currently used by prosecutors did not accommodate fraud committed using credit card number, not the card itself. It was not a federal crime to deal and traffic in card account number. Law enforcements’ efforts to fight credit card fraud were hindered by such gaps in the legal system. This deficiency further played a role in mobilizing criminal activities. The lack of federal laws made it difficult to trace criminals. Local law enforcement efforts were bounded by their jurisdiction, a constraint that criminals could easily bypass by shifting their activities to another state. With the absence of federal laws Attorney General was hesitant to become engaged in prosecuting these types of criminal activities. The geographic scope of credit card fraud expanded to cover the whole nation threatening the integrity of the entire payment system. Credit card fraud evolved from being solo-crimes to organized-ones with fraudsters mobilizing their activities across the nation.

Realizing the enormous impact the current legal system had on fraud, actors negotiated different approaches to strengthen the legal system. Besides discussing a redefinition of what a credit card fraud was, other loopholes that could be used to avoid prosecution were also important to close. This involved criminalizing the possession of counterfeited cards and counterfeiting equipment, determining the conditions under which these crimes were entitled to federal intervention, whether amending current statutes used to fight fraud is sufficient or more comprehensive revision was needed, and whether computer crimes should be associated with credit card fraud.

The hearings resulted in enacting Credit Card Fraud Act of 1984, a chapter in U.S. Code (Figure 5-5 displays prevention encounters in enacting the new law). The act solved the narrow definition of credit card fraud by using the term ‘access device’ instead of ‘device’ when determining card fraudulent activity, and defined access device by “any card, plate, code, account number, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)”. The act further criminalized possession of counterfeited equipment, and expanded federal jurisdiction to cover an aggregate value of $1000 or more in fraudulent activities regardless of the number of credit cards used to obtain it (previously the $1000 was conditioned to a single card fraud) (Joint Resolution, 1984).

5.2.6 Prevention Encounter 6: Security in Card-Not-Present Environment (E-commerce)

The card industry’s fight against fraud remained mainly concentrated on situations where the card was present at the time of the transaction. Radical change to this security approach occurred in mid-1990s with the emergence of the Internet and the opportunity to do business in a virtual environment.

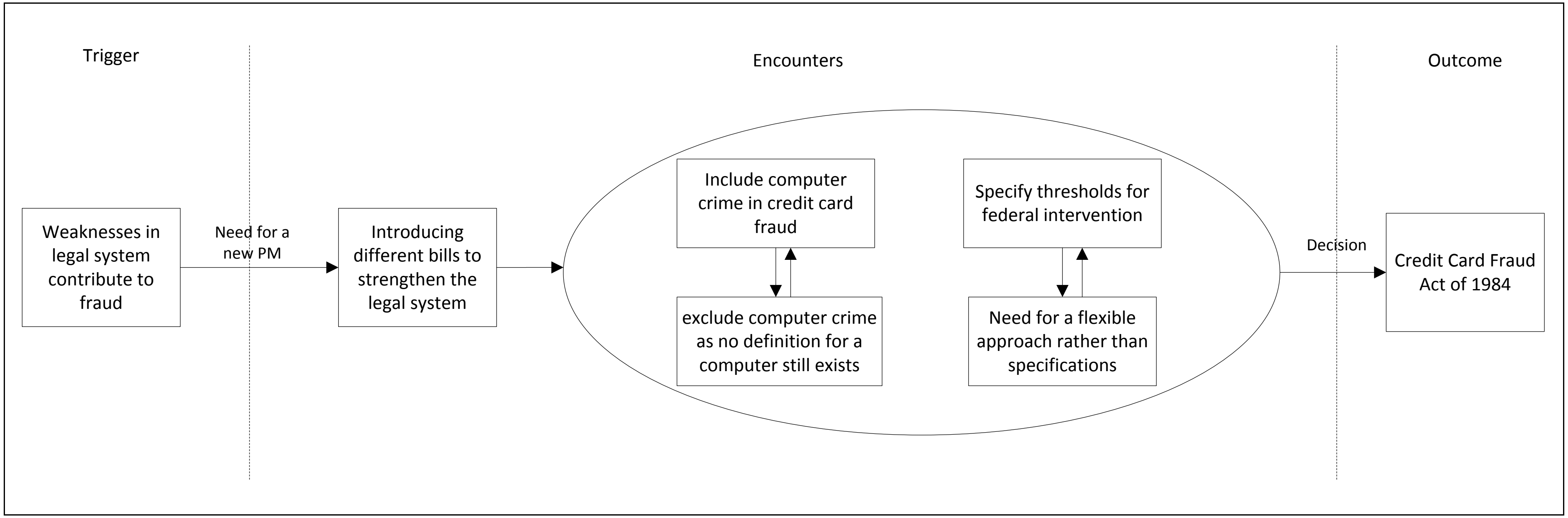

Trigger
Encounters
Outcome
Weaknesses in legal system contribute to fraud
Need for a new PM
Introducing different bills to strengthen the legal system
Include computer crime in credit card fraud
exclude computer crime as no definition for a computer still exists
Specify thresholds for federal intervention
Need for a flexible approach rather than specifications
Decision
Credit Card Fraud Act of 1984

Figure 5-5 *Prevention encounters in strengthening the legal system*

E-commerce rendered many of the security innovations that targeted credit card itself (e.g. hologram, fine-printing, CVC) useless. Merchants and financial institutions who rushed to exploit the new business opportunity only found the current security procedures inapplicable to online payment. A new technology that secured credit card transactions in a card-not-present environment had to be developed (see Figure 5-6).

With increase pressure on card associations to provide a secure channel for accepting payments over the Internet (Kutler, 1996), Visa collaborated with Microsoft and in 1995 released Secure Transaction Technology (STT), a protocol to secure cards payment transactions in cyberspace. Banks did not respond favourably to Visa's STT. Most of them were also members of MasterCard, which itself and in collaboration with Netscape, IBM, Cybercash and GTE developed another protocol for securing e-commerce (Secure Electronic Payment Protocol). The two protocols were not compatible; banks had to bear the cost of installing two systems and manage working on two different operating procedures. They rejected this unnecessary cost and forced the two card association to cooperate and develop a single standard (Bloom & Kutler, 1996; Merkow, 2004).

In February 1996, Visa, MasterCard, GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems, RSA, and VeriSign established Secure Electronic Transactions (SET) consortium to resolve the conflict between the two protocols and develop a unified one. In 1997, Visa and MasterCard released SET protocol announcing it the standard for securing e-commerce transactions. SET authorized transacting parties based on digital certificates and a digital signature that validated the identity of all participants through the use of encryption keys (Cerne, 1996). Upon this announcement, vendors like IBM, Microsoft, and Hewlett-Packard started developing different security solutions based on the new standard (Kutler, 1997a; 1997b; Tracey, 1997).

This situation did not last long. The application of digital signature to secure online transactions faced a roadblock. States started regulating the use of the technology, setting different conditions on when digitally signed documents were considered legal. For instance, some states (e.g. Hawaii, Maryland, Michigan) required the application of public key cryptography for the digital signature to have the same legal effect as manual signatures, others (e.g. California, Florida, Georgia) left the choice of the technology open. This fragmentation meant that technology vendors need to develop their security products in multiple ways to conform to different states regulation. Such an unnecessary increase in implementation costs would stifle development efforts and eventually hinder the growth of e-commerce. Furthermore, no transacting party would risk getting involved in a contract that could be challenged elsewhere (SEAL, 1998).

At first, legislators were not convinced of the need for a federal law and how state regulations regarding digital signature were hindering e-commerce growth. Visa, financial institutions and technology vendors all had to participate in multiple congressional hearings to change this passive attitude (Anason, 1997; Power, 1997). Those actors aired their concerns of how inconsistent regulations added more financial burden on those seeking to secure the Internet and the fact that it could make the infrastructure more vulnerable to threats as it constrained the application of digital signature with a certain technology (e.g. public key cryptography) that could become obsolete given the rapid advancements in information technology. In addition, having a nationwide validation of digital signature could not be considered an extraordinary claim as foreign countries had already done so, leaving the U.S. only behind (Electronic Authentication and Digital Signature, (1997); The Federal Role in Electronic Authentication, (1997); SEAL, (1998); E-SIGN, (1999)).

Actor’s efforts paid off with the enactment of Electronic Signatures in Global and National Commerce Act in 2000. The Act validated the use of digital signature technology giving it the same legal effect as manual signatures. The act further maintained flexibility and adaptability to changes in technologies by being technology-neutral with no specific technical requirements on digital signature (E-SIGN, 1999). This legal certainty allowed heterogeneous actors to contribute to securing credit card transactions by either acting as a “Certificate Authority” (CA) to issue and validate digital certificates, or developing security products end users can implement to ensure safe online payment transactions. The technological neutrality also increased competition among technology vendors who were free to keep pace with technological evolution and embrace any authentication technology to offer solutions that best serve the needs of their customers.

Passing this legal complexity, Visa sought to diffuse the adoption of SET standards by eliminating chargeback fees on online transactions that comply with SET. Chargeback fees became unnecessary since SET ensured that each transacting party possessed a digital certificate authenticating its identity, therefore preventing repudiation. Visa also eliminated consumer liability in an initiative to alleviate their fear about the security of e-commerce transactions (Credit Card News, 1998).

5.2.7 Prevention Encounter 7: Shifting Security Direction: Unified Industry Standards

The use of credit cards in online transactions further increased the ubiquity of the technology as a payment medium. This made it challenging to develop a certain technological solution that accounts for the different needs of the business environments where the card was being used. In June 2001, Visa announced its Cardholder Information Security Program (CISP) specifying security standards members, merchants, and service providers had to follow in order to ensure the security and privacy of cardholders' information wherever it resides (Credit Card Management, 2001). Similar programs were initiated by other card companies; such as Site Data Protection for MasterCard and American Express' Data Security Operating Policy. The multiplicity of security standards made compliance efforts less successful, merchants and acquirers raised their concerns about the costs associated with complying with different standards that in their core sought to meet the same goal. To end this fragmentation and ease actors' anxiety, Visa collaborated with MasterCard among other card companies to align the multiple standards and produce unified global security requirements. The joint efforts resulted in announcing Payment Card Industry Data Security Standards (PCI DSS) in 2004. The standards cover various technical and operational areas aiming to offer best security practices for securing cardholder information.

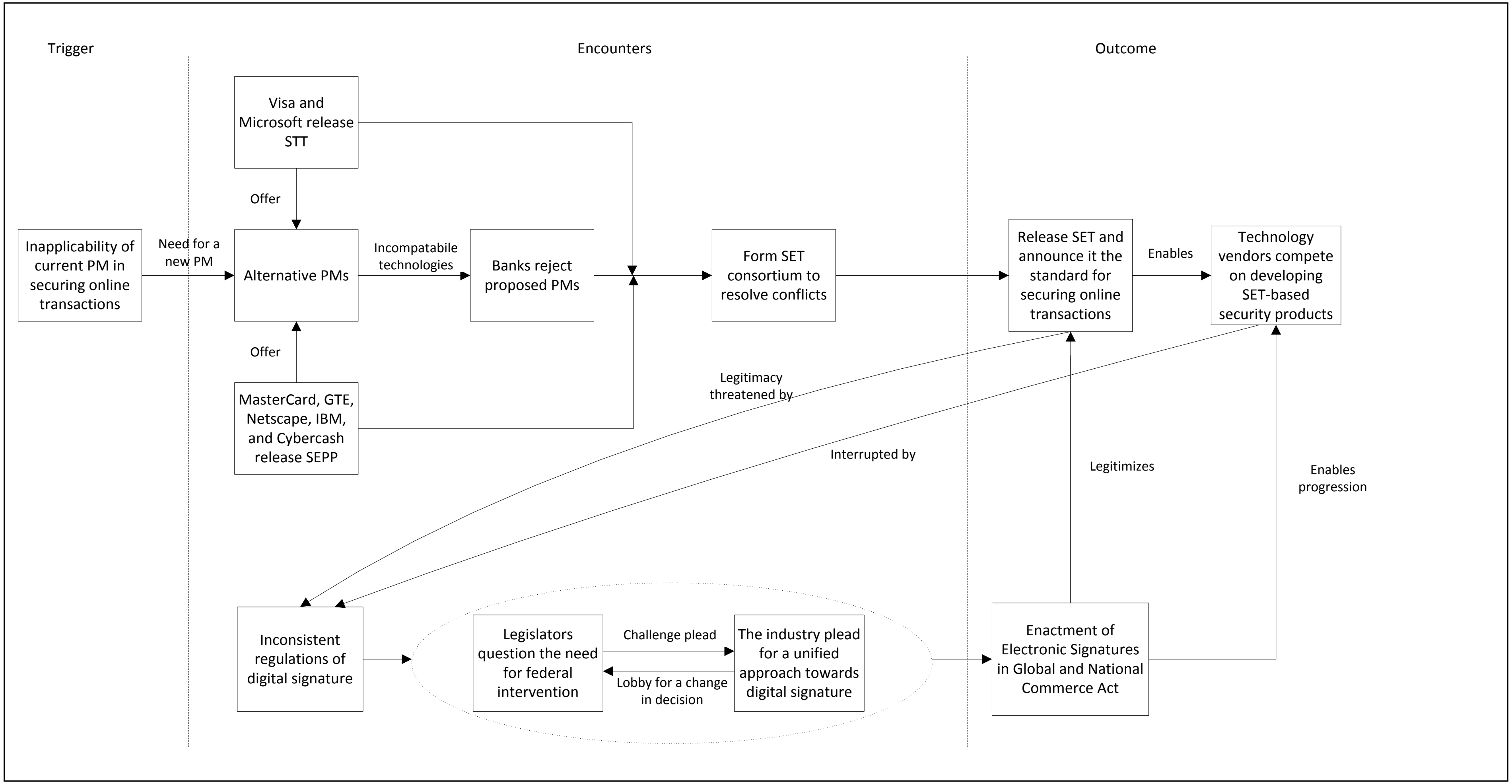

Trigger
Encounters
Outcome
Visa and Microsoft release STT
Offer
Inapplicability of current PM in securing online transactions
Need for a new PM
Alternative PMs
Incompatabile technologies
Banks reject proposed PMs
Form SET consortium to resolve conflicts
Release SET and announce it the standard for securing online transactions
Enables
Technology vendors compete on developing SET-based security products
Offer
MasterCard, GTE, Netscape, IBM, and Cybercash release SEPP
Legitimacy threatened by
Interrupted by
Legitimizes
Enables progression
Inconsistent regulations of digital signature
Legislators question the need for federal intervention
Challenge plead
Lobby for a change in decision
The industry plead for a unified approach towards digital signature
Enactment of Electronic Signatures in Global and National Commerce Act

***Figure 5-6** Prevention encounters in securing e-commerce transactions*

Nevertheless, the standards suffered from different interpretations and contradictory requirements, subsequent versions had to be released to address those issues along with new security threats. In 2006, actors in the joint effort decided to shift the responsibility for maintaining and distributing the standards to a newly formed Payment Card Industry Security Standards Council (PCI SSC) while maintaining responsibility for validation and enforcement tasks.

The Council's responsibilities span over multiple security standards such as: Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. Various actors; such as merchants, financial institutions, technology companies, trade associations, processors, can play a part in developing and changing these standards by acting as "participating organizations". After releasing the standard, the industry is given almost a year to implement and assess the proposed changes. Through Community meetings participating organizations share their views and provide feedback to the Council from their experience with the new standard and suggest improvements or modifications especially in light of evolving security threats. The feedback is compiled and reviewed by the Council's PCI DSS Technical and Working Group (TWG) who determine the appropriate course of action (no action, issuance of new version, issuance of revision, developing supporting documents (ex. best practices)) (PCI SSC, 2010). By this, PCI standards not only provide one referral point to comply with multiple card associations' security requirements, but also reflect the needs and concerns of the various stakeholders involved.

Involving such a wide range of actors made the standards prone to multiple interpretations that can hinder its implementation. To lessen this ambiguity, the Council manages different training programs for firms or experts who seek to be qualified data security companies or professionals. Once certified, those, and only those, will be considered qualified to validate compliance with PCI standards, and be listed in PCI SSC website (PCI SSC, 2016).

Despite solving the fragmentation in security requirements, PCI DSS received wide criticism of its high compliance costs. It is estimated that tier 1 merchants spend on average $225,000 on PCI auditor expenses alone (Ponemon, 2010). Table 5-1 shows

Table 5-1 *PCI standards compliance criteria and requirements (Source: Visa U.S.A)*

Level	Merchant criteria	Validation requirements
1	Merchants processing more than 6 million transactions annually.	Annual compliance report by Qualified Security Assessors (QSA) and quarterly scan by Approved Scanning Vendors (ASV).
2	Merchants processing 1 to 6 million transactions annually.	Annual Self-Assessment Questionnaire (SAQ) and quarterly network scan by ASV.
3	Merchants processing 20000 to 1 million e-commerce transactions annually.	Annual SAQ and quarterly network scan by ASV.
4	Merchants processing less than 20000 e-commerce transactions annually and all other merchants processing up to 1 million transactions annually.	Compliance validation requirements set by merchant bank. Other validation requirements such as annual SAQ and quarterly scan by ASV are recommended.

Visa's compliance criteria and requirements which vary according to transactions' volume and potential risk. In an attempt to address this and accelerate compliance, in December 2006 Visa announced its Compliance Acceleration Program offering financial incentives to acquirers whose level one or two merchants (consuming more than 60% of Visa's transactions) are certified as compliant by March 31, 2007 or August 31, 2007 and had not been involved in security breach incidents. The program however deprived those acquirers from Visa's best interchange rate in case of noncompliance after 30 September, 2007, and they might also find themselves eligible to $25000 fine per noncompliant merchant (Cardline, 2007; Wolfe, 2006).

Prevention encounters surrounding the industry security standards are displayed in Figure 5-7.

5.2.8 Prevention Encounter 8: Beyond Magstripe: Tokenization and Chip Cards

Despite the card industry's efforts to maximize the security of cardholder information through PCI standards and merchants' substantial investments to achieve compliance, security breaches remained pervasive with much of the costs borne by merchants. Facing this complexity, merchants started to rethink their security doctrine. In a letter to PCI SSC, National Retail Federation (NRF) conveyed merchants' concerns about the industry's current security approach and whether it was how security is best attained. The letter raised a critical question of why it was

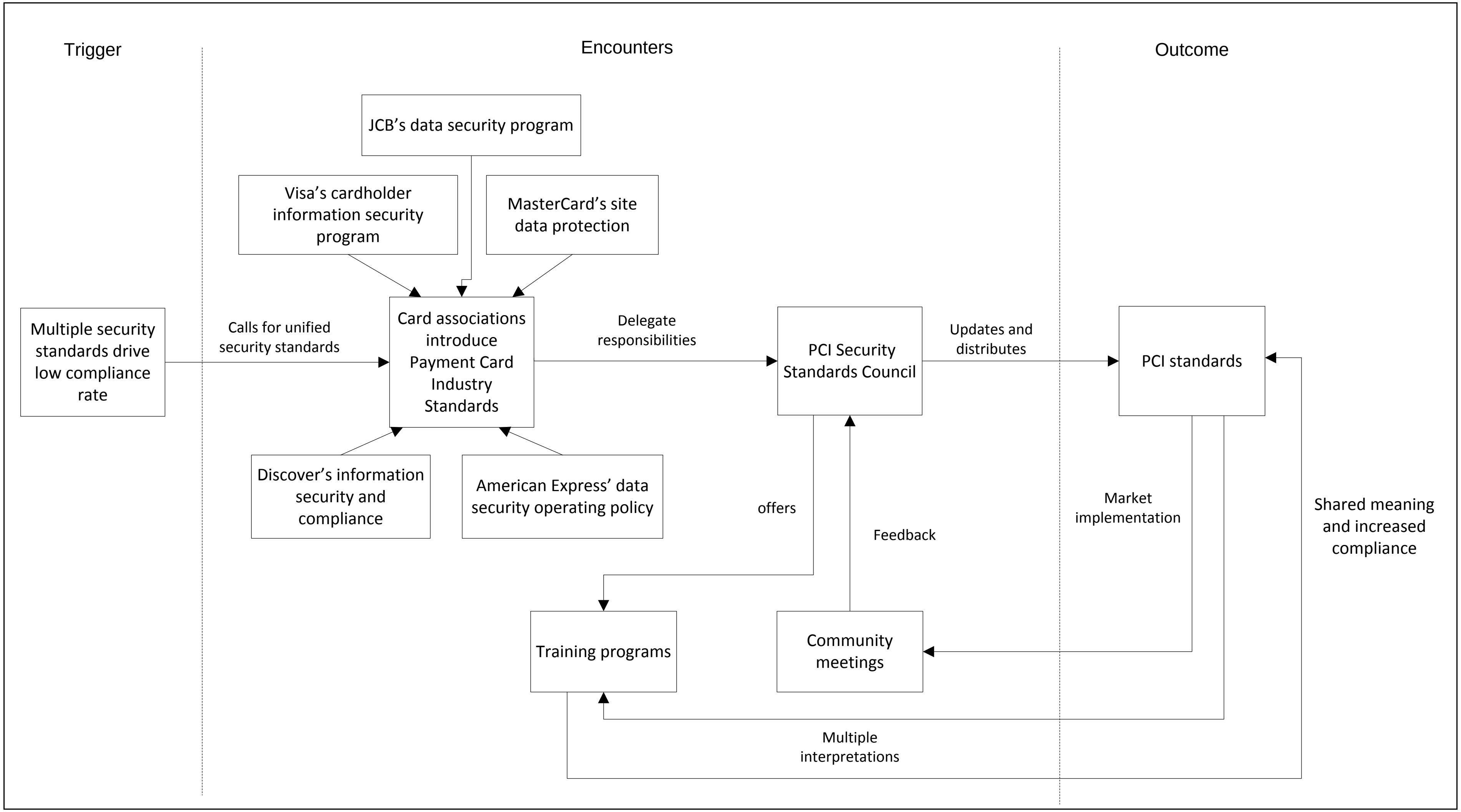

Trigger
Encounters
Outcome
JCB's data security program
Visa's cardholder information security program
MasterCard's site data protection
Multiple security standards drive low compliance rate
Calls for unified security standards
Card associations introduce Payment Card Industry Standards
Delegate responsibilities
PCI Security Standards Council
Updates and distributes
PCI standards
Discover's information security and compliance
American Express' data security operating policy
offers
Feedback
Market implementation
Shared meaning and increased compliance
Training programs
Community meetings
Multiple interpretations

***Figure** 5-7 Prevention encounters in developing industry security standards* merchants' responsibility to protect financial institutions' data and spend millions of dollars to achieve that though the data was not theirs and security was not their core competency. Merchants claimed they were forced to retain card information as part of dispute resolution process where banks ask merchants for details about a certain transaction identified through the credit card number. NRF pleaded for a use of a different technology that would eliminate merchants' need to store card information while retaining the ability to distinguish each transaction, primarily through the use of tokens (substitute identifiers). Adopting such a concentrated security approach that reallocates sensitive data to reside on few locations instead of being distributed across the nation was expected to offer better security (Hogan, 2007). Moreover, they urged for a need to keep pace with the rest of the world in adopting chip and PIN technology and abandoning the obsolete magstripe that was only adding to fraud losses.

Merchants' change proposal did not resonate very well and was dismissed. The matter took a more serious turn in 2009 following a congressional hearing regarding the effectiveness of PCI standards in fighting security threats (Do the payment card industry data standards reduce cybercrime, 2009). In their opening remarks, members of the Congress advocated the transition to chip and PIN that had been successful in thwarting fraud. Merchants again reiterated their concerns about the industry's security doctrine and that change was needed to move the fight against fraud forward. The first step to achieve that was to consider the implementation of emerging technologies such as tokenization, chip and PIN and end-to-end encryption (See also: Privacy in the Digital Age, (2014); Protecting Personal Consumer Information from Cyber Attacks and Data Breaches, (2014); Safeguarding Consumers' Financial Data, (2014)).

Calls for change were better perceived with PCI SSC acknowledging the need and working with technology vendors to evaluate the proposed solutions and how they could strengthen and simplify security requirements. Nonetheless, the Council stated that due to the high cost associated with implementing end-to-end encryption it would be impractical to mandate its usage in the standards as small merchants do not have the required resources. Visa also clarified that it does not require the storage of card account number, and merchants should work with their acquirers/processors in producing a token to reference transactions' details. In addition, the company released guidelines and best practices to aid actors who wish to use tokens (Visa, 2009; 2010).

Despite supporting the need for rethinking security practices where technological solutions (as tokenization) were no longer directed towards protecting a valuable asset but rather depriving it of its value, and therefore making it less attractive to criminals, this did not exceed being a lip service with no serious intentions in taking efforts to develop the technology further. To be able to implement tokenization, significant changes in the payment infrastructure needed to take place with the engagement of all actors to ensure consistent and compatible solutions. With no collaborative efforts to agree on how tokens are generated and mapped to the original card number, and who is responsible for the card-token vault, adopting tokenization to improve the payment system's security is doubtful.

Serious efforts to go beyond magstripe and adopt tokenization and chip technologies started with a change in the marketplace evident in the prevalence of digital payment devices, such as mobile phones and tablets, offering opportunities for contactless payments that chip technology facilitated. In preparing the payment infrastructure for mobile payments, Visa announced in August 2011 its plans to accelerate migration towards contact and contactless chip technology. Plans included expanding its Technology Innovation Program to U.S. merchants. The program waived merchants whose at least 75% of their Visa transactions originate from chip-enabled terminals from annual validation of compliance with PCI standards. In addition, new fraud liability shift rules would apply to actors not adopting chip (Visa, 2011). To accelerate the adoption of tokenization and ensure interoperability across payment systems around the globe, in 2013 Visa, MasterCard, and American Express collaborated to develop tokenization standard to allow the industry's different players to offer secure and reliable payment experience with no fear of compatibility problems (Visa, 2013).

Figure 5-8 depicts prevention encounters in moving beyond magstripe.

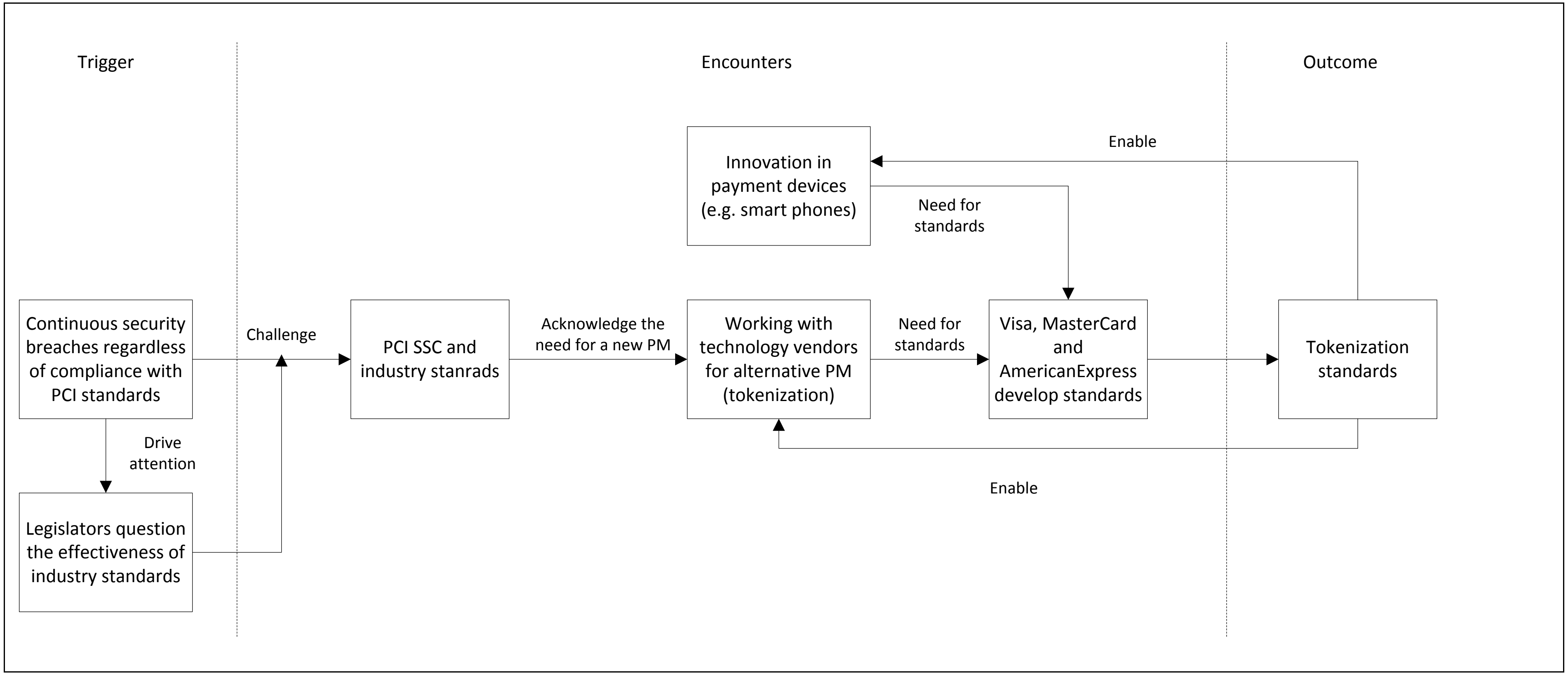

Trigger
Encounters
Outcome
Innovation in payment devices (e.g. smart phones)
Enable
Need for standards
Continuous security breaches regardless of compliance with PCI standards
Challenge
PCI SSC and industry stanrads
Acknowledge the need for a new PM
Working with technology vendors for alternative PM (tokenization)
Need for standards
Visa, MasterCard and AmericanExpress develop standards
Tokenization standards
Drive attention
Legislators question the effectiveness of industry standards
Enable

Figure 5-8 *Prevention encounters in moving beyond magstripe*

6 ANALYSIS

6.1 Introduction

The previous chapter described prevention encounters in the credit card industry since its inception till 2013. In this chapter, I develop a process model of how security networks achieve prevention. I first provide a summary of the eight prevention encounters in the case of credit card fraud. I then, following CR approach, present an analysis of structure and context which is seen essential to derive prevention mechanisms. The three prevention mechanisms are then introduced and discussed. After that, I draw on the empirical analysis to further develop the three forms of incentives synthesized from the literature and better explain how actors are mobilized to prevent fraud despite their diverged interests. Finally, I present the process model of prevention encounters.

6.2 Prevention Encounters in Developing and Adopting Prevention Measures

The case study shows that security threats prevention is a continuous process that necessitates the involvement of heterogeneous actors. With each having particular perspective on how credit card fraud is best prevented, negotiations and conflict resolution become a characteristic of prevention encounters.

Table 6-1 lists the eight prevention encounters identified while preventing credit card fraud and the incentive mechanisms used to mobilize actors towards supporting a certain prevention measure.

Table 6-1 *Prevention encounters*

Period	Prevention encounters	PE triggers	Description	Changes (interruptions) in security approach	Actors	Incentive mechanisms
1958 - 1970	Credit card mass mailing	Public outrage drove legal attention to the ineffectiveness of banks practices in preventing fraud (social pressure)	The rampant fraud rate, resulting from mass mailing of credit cards due to theft and improper use, instigated an investigation of the phenomenon. After several negotiations and debates between banking industry and legislative authorities, where the former tried to offer solutions banks can undertake to prevent fraud that keeps legislators at arm's length, the latter considered them not enough and took a decisive decision that enacted a new law to ban mass mailing of credit cards.	Moving from a situation where financial institutions were the responsible actor for card security to one that made legal intervention part in preventing fraud.	General public, financial institutions, FRS, ABA, FTC, regulators, US post	Actors supporting a banning law sought to mobilize others by showing the negative consequences credit cards have on society. Those against it tried to change those beliefs by stressing the perverse effect of a banning law (Transformative).
1966 - 1973	Automating card transactions	Prevalence of different authorization problems across banks called for a different approach to prevent fraud (social pressure)	Increased fraud losses, due to slow authorization procedures, drove banks to call for joint efforts to address the shared problem and create a nationwide authorization system. Banks, cards associations, and merchants participated in discussing the different proposals for the joint effort. Fear of competition and antitrust laws however caused Master Charge and National BankAmericard Inc. (NBI) (later becomes Visa) to reject these joint effort proposals. NBI consequently adopted a unilateral approach to develop an authorization system (BASE), which it launched in 1973.	Revolutionizing authorization procedure by using technology to coordinate traffic between authorization centers.	Merchants, customers, financial institutions, NBI, BofA, American Express, Master Charge, law, BASE	Though a unified authorization system might seem favourable to actors NBI changed this perception and stated that a joint effort to develop an authorization system is counterproductive as involved actors will be liable to antitrust laws (Transformative).

1970 - 1977	Automating POS terminals	Prevalence of different authorization problems across banks called for a different approach to prevent fraud (social pressure)	With the need for a machine readable card to fully automate the authorization process, different merchants and banks submitted their proposal to American Bankers Association (ABA) card standardization task force that was formed to evaluate the different encoding technologies. Based on certain criteria the force announced magnetic stripe as the encoding technology to be adopted in the banking industry. However actors challenged the security of the new industry standard and offered their own more secure solutions. ABA task force worked to reconfirm the legitimacy of magstripe as the encoding technology and respond to these challenges. After intense negotiations the industry stabilized again on magstripe. Automating POS terminals was further interrupted by DoJ announcement that sharing POS terminals may be subject to antitrust action. Following considerable debates between the banking industry and DoJ, the Congress established National Commission on Electronic Funds Transfer to investigate the subject matter. The commission declared sharing POS terminals is legal allowing development efforts to proceed.	Eliminate human intervention in authorization process by automatically capturing and transmitting data at merchants' site, allowing authorization of *all* transactions.	ABA task force, encoding technologies, merchants, financial institutions, Western states bankcard association, City Corp, DoJ, regulators, NCEFT	Full automation of authorization process was indispensable to eliminate floor limits, hot card lists, and shift liability for fraudulent transactions from merchants to issuing banks (Captive). Opponents of magstripe tried to change actors' beliefs about the security of the technology and how in fact it increases fraud (Transformative). In response to countermoves supporters stressed that reaching a consensus on an encoding technology is needed to pursue the vision of cashless society (Captive). Further, they argued that security should be seen resulting from the payment system as a whole not only the card encoding technology (Transformative). Supporters of magstripe were able to mobilize actors towards accepting the technology ending by this the instability in the

						market facilitating automation efforts to continue (Preparatory). Financial institutions sought to clarify misconceptions held by the DoJ about sharing POS terminals and how it ensures the involvement of all actors regardless of their size (Transformative). The negotiations resulted in legalizing sharing providing with this legal certainty for the worthiness of investment in this technology (Preparatory).
1982 - 1988	Smart card vs. magstripe	Staggering fraud rate forced banking industry to consider a new technology to prevent fraud (technology)	The evidence of the effectiveness of smart cards in preventing fraud drove the industry to start experimenting with the new technology. With the two card associations adopting different approaches, Visa supporting an evolutionary approach while MasterCard a revolutionary one, and each actor trying to counter-argument the other, the industry was in a limbo; not knowing which direction to take. Supported by the heavy investments in magstripe that made banks skeptical about smart cards, as well as results from its experiments with the technology, Visa was	Changing industry standard by proposing chip-enabled cards to replace magstripe in preventing fraud.	Smart card, Visa, MasterCard, financial institutions	Proponents of magstripe mobilized actors around the technology and maintained belief that magstripe is the best technology for preventing fraud by highlighting the big investments the industry endured in magstripe and the fact that smart card is for offline environment rather than U.S. online one (Transformative). Visa

			able to end the limbo state and re-stabilize the industry by reconfirming its commitment to magstripe while encouraging banks and technology vendors to come up with new ways of increasing magstripe security.			also incited competition in strengthening the security of magstripe by announcing it the standard for the next decade (Preparatory)
1983 - 1984	Strengthening the legal system	Industry players lobbied for stronger laws after recognizing weaknesses in the legal system that added to fraud (social pressure)	Several congressional hearings took place with the participation of different actors to address gaps in the legal system and how best they can be closed. Actors held different perspectives on this matter; some advocated the need for comprehensive card fraud law revision, while others opted for minor amendments. The hearings resulted in approving and passing Credit Card Fraud Act to redefine fraudulent activities by criminalizing illegal use of card account number or possession of counterfeited equipment.	Redirecting security efforts towards protecting what is of real value in the technology, which is the credit card number itself rather than merely protecting its materiality as with previous PM that focused on card design security features.	Visa, MasterCard, National Retail Merchants Associations, DOJ, FRS, ABA, US Post	The enactment of a new law armed law enforcement agencies with tools necessary to fight fraud (Preparatory)
1995 - 2000	Security in card-not-present environment (e-commerce)	Banks and merchants wanting to do business online pressured card associations to develop a secure online payment infrastructure (social pressure)	Given the pressure for a secure online payment infrastructure, the two giant card associations each collaborated with technology vendors to produce a secure protocol. The incompatibility between the two protocols caused banks to reject them, and force the two card players to merge their efforts and produce a unified standard called Secure Electronic Transaction (SET) in 1997. With the standard in place technology vendors started developing security products. This was interrupted however by states' inconsistent approach	Challenges to conventional security methods due to the emergence of a new lucrative virtual business environment that called for new security approaches to tackle fraud in card-not-present environment.	Financial institutions, Technology vendors, Visa, MasterCard, SET, regulators	To enable competition between technology vendors in developing innovative technologies to secure e-commerce transactions, Visa and MasterCard announced an industry standard to act as a baseline for security products (Preparatory). Proponents of digital

			towards digital signature (one of SET component) that created unnecessary extra cost for compliance. Actors went through multiple negotiations to convince legislators how such inconsistency was affecting the industry and the security of online financial transactions. In 2000, Electronic Signatures in Global and National Commerce Act was passed to give digital signatures the same legal status as written signatures, legitimizing by this the use of the technology.To encourage the adoption of SET, Visa changed its chargeback policy to eliminate chargeback fees for merchants complying with SET.			signature worked to legitimize the technology and gain legislators support by signifying the perverse effect current state behaviour had on the growth of e-commerce and how the current fragmented state threatened the efficiency of the nation's payment system (Transformative). Actors further confirmed that without a consistent approach towards digital signature there will be no e-commerce (Captive). Adopting SET to secure online credit transactions was encouraged by tying cost savings with the technology (Captive).
2004	Shifting security directions: unified industry standards	Widespread usage of credit cards, as well as the multiplicity of security programs drove major card associations to combine their efforts and	To ensure the security of cardholder information wherever it resides, major card associations resorted for security programs that industry players should conform with. Disparities between these programs made them less successful in achieving their goals and attaining compliance. Given the shared purpose of all them, the major card associations coordinated their efforts and produced a unified standard called Payment Card Industry Standard Data	Relying on general standards rather than a specific finalized technological solution to prevent fraud, expanding by this fraud prevention network to include all those storing/processing	Card associations, security standards, merchants, acquirers, PCI standards, PCI SSC	Recognizing the diversity of business environment and its security needs, security standards was introduced to give actors the flexibility they need to adopt security practices that best match their requirements. To further support actors' commitment to fighting

		produce a unified standard (technology)	Security Standard (PCI DSS) in 2004. In 2006, Payment Card Industry Security Standard Council (PCI SSC) was formed to maintain and distribute the standards as well as producing multiple versions to address rising security concerns. Through Community meetings members provide feedback on the different versions of the standards.	credit card information.		fraud, major card players announced a unified version of the various security standards reducing with this compliance cost (Preparatory). Visa also tied favorable interchange rates with compliance to PCI standards (Captive).
2007 - 2013	Beyond magstripe: tokenization and chip cards	Continuous data breach incidents in merchants' system caused them to rethink security practices and push for new technologies (social pressure)	In a letter sent to PCI SSC, National Retail Federation (NRF) aired merchants' views about the constant data breach incidents despite all investments made to comply with the industry standards, urging the council to rethink how the fight against credit card fraud should proceed. NRF accused card companies of having a role in the continuous breaches since it is their rules that required merchants to store card details, making them attractive targets. The effectiveness of PCI standards in preventing security threats was further challenged by legislators. Visa clarified it does not require the storage of card data by merchants, and the latter should work with their banks to develop an alternative for distinguishing card transactions other than card number (mainly through tokenization). PCI Counsel emphasized its commitment to security through its feedback mechanism with participating organizations and collaboration with technology vendors on the possibility of	Adopting a new approach to security that devalues the technology by replacing its most critical element (credit card number) with a token reducing its attractiveness to criminals.	NRF, PCI SSC, PCI standards, regulators, Visa, MasterCard, American Express, tokenization standards, Chip cards	NRF sought to attract mobilization against PCI standards and gain support for new technological solutions by claiming that banks procedures propagate security breaches not thwart them (Transformative). Visa and PCI Counsel stressed the complexity of security threats and that security is a shared responsibility. The emergence of mobile payments incited Visa to support migration towards Chip cards. Visa also collaborated with MasterCard and American Express to introduce tokenization standard to capture this business opportunity (Captive).

			incorporating new technologies within the standards. The advent of mobile payment was followed by more serious attempts to adopt tokenization and chip card., Visa, MasterCard and American Express introduced tokenization standards to ensure compatibility among different payment systems. Visa expanded its Technology Innovation Program to accelerate the migration to chip technology. Also, merchants who apply tokens can save costs by waiving compliance with PCI DSS.			The standard allowed technology vendors and merchants to pursue their development effort and ensure interoperability between various solutions (Preparatory). Merchants are induced to adopt tokenization and chip cards by coupling it with certain financial savings (Captive).

6.3 Structural and Contextual Analysis

According to CR, mechanisms emerge in virtue of the nature of the entities that possess them. Part of explaining therefore becomes identifying entities' properties that enable the prevention mechanisms to exist. These properties should be differentiated from contextual conditions that trigger mechanisms. Sayer explains "although causal powers exist by virtue of the objects which possess them, they are contingent on conditions for activating them". In other words, the role of properties is enabling mechanisms while the role of context is activating them. Following CR, there are two tasks to undertake: "to explain the causal properties of each entity in terms of its internal structure and to explain the occurrence of particular events in terms of conjunctures of the causal properties of various interacting mechanisms" (Porpora, 1998, p.343). Besides identifying properties and mechanisms, we also need to identify contextual conditions that activate the mechanisms. In what follows I identify entities' properties and the contextual conditions that are seen causally relevant in the events taking place while preventing credit card fraud. I then integrate them with the prevention mechanisms and explicate their role in the emergence of the three prevention mechanisms in Section 6.4.

6.3.1 Entities and Properties

In identifying properties of the structural entities that enable prevention mechanisms, I seek to answer the following question: "What is it *about* the structures which might produce the effects at issue?" (Sayer, 1992, p. 95). As structures (constitute entities of interest) are at the center of attention here, decomposing them first to their constituent elements such as, actors, organizations, systems, relationships, is necessary (Wynn & Williams, 2012).

Elements of structure, or structural entities, in security networks include: regulatory agencies (FTC, FRB), financial institutions, laws, operating procedures, prevention technologies (BASE, PCI standards), card associations (Visa, MasterCard), customers, merchants, technology vendors. These elements are assembled into three groups: social actors, operating system, and technology. Social actors involve individuals such as legislators, customers, merchants or organizations as FTC, Visa, financial institutions that interact in security networks to prevent threats. Operating system refers to laws, rules and regulations that govern and shape actors' interactions. For example, in the second prevention encounter branching laws prohibited banks from opening branches in different states. This forced BofA to expand its card business through license agreements which had implications on the authorization procedures and fraud rates. Finally, technology refers to the collection of technological solutions developed over time to prevent fraud.

Analysis of these three structural entities identified three properties that are causally relevant to events taking place while preventing fraud: heterogeneity of role, inherited complexity, and technological novelty (summarized in Table 6-2).

By definition security networks comprise heterogeneous actors as seen clearly from the case study. These actors are positioned differently in the network and therefore inhabit different roles and interests. These roles are defined within the context of the network they belong to (Callon, 1991). Actors can be challengers, arbitrators, stabilizers or enablers. While those assuming the *challenger* role contest prevention measures and refuse to inhabit roles assigned to them by other actors, *arbitrators* seek to formally resolve conflicts between actors through examining the contested issue and evaluating possible alternatives in order to make a final verdict. Others work as *enablers* to provide foundational cornerstones that other actors can utilize to build prevention measures. Finally, *stabilizers* confront interruptions in security networks prevention efforts and work to re-establish stability to allow actors to continue their efforts in implementing a particular prevention measure.

Inherited complexity describes the interconnected nature of the legal system that transcends to interfere with security network's prevention efforts. Inherited complexity is derived from the U.S. legal system that is based on interrelated systems of legislative, judicial and executive branches that exist on *both* federal and state level. The legislative system is responsible for making laws and is represented by the Senate and House of Representatives, which together form the Congress. These laws are interpreted and applied by the judicial system represented by state and federal courts. The executive system headed by the president legitimizes and enforces the laws. As a product of federalism, each state has its own constitution and legal system. Controversies across states are expected, and thus the U.S. constitution specifies the conditions where federal courts have exclusive jurisdiction.

This multi-layered structure of the legal system where there is a branch for enacting laws and another for interpreting them create an atmosphere of uncertainty as actors lack definite knowledge of how actors in the legal system would react to actions they undertake to prevent fraud. Moreover, laws by themselves are intertwined and can lessen the impact of one another. Enacting or modifying one law can create ripple effects throughout the legal system. For example, the enactment of a new law that would allow federal law enforcements to investigate fraudulent activities clashed with Right to Financial Privacy Act that restricts financial institutions from reporting crimes and thus hindering federal agencies' card losses investigations as it constrains their access to financial records. Amending Right to Financial Privacy Act then becomes inevitable to enable the progression of investigation efforts.

Finally, technological novelty captures the dynamisms in security networks and the necessity to keep pace with new emerging threats. It shows how *new* technologies, whether they are payment technology, preventive technology or medium technology, shape collective security efforts. Given the rapid innovations in information technologies the subject of new technologies receives wide attention in both academic and business world (Rotolo *et al.*, 2015) where the concept is often associated with a multiplicity of definitions. In this research technological newness refers to the use of a new principle to achieve a similar purpose (Arthur, 2007). That is for a technology to be considered new it has to build on or need different basic principles to prevent security threats than those used before. This definition corresponds with the research conceptualization of prevention encounters as the latter denote challenges in current security practices that call for re-evaluating existing prevention measures.

Novel (new) technologies thus have a disruptive impact on established social, economic and legal practices. They challenge existing institutions as knowledge about their applicability and outcomes is incomplete (Garcia & Calantone, 2002) making them ambiguous with uncertain future. Actors try to sense their way through *experimenting* different solutions to prevent fraud to gain better knowledge about the technology and its consequences. In addition, new technologies are known of being *interpretively flexible* (Pinch & Bijker, 1987) and so ascribed with different and sometimes conflicting meanings. They therefore create confusion over future directions for security efforts and necessitate time and interactions between actors to develop a common understanding of the technology. At the same time, novel technologies can transform organizations' business model and offer new *business opportunities* and lucrative markets (Arthur, 2007) creating new security challenges.

Table 6-2 *Properties of structural entities in security networks*

Property	**Definition**
Heterogeneity of role	Different positions actors occupy in security networks to achieve prevention that range between challengers, arbitrators, stabilizers and enablers.
Inherited complexity	The multi-level nature of the legal system that transcends to interfere with security network's prevention efforts.
Technological novelty	Newness of the technology that requires the use of different principles to prevent security threats.

In summary, the effect of technological novelty is observed in terms of experimenting with the technology, the different interpretations ascribed to it, and business opportunities it offers.

Evidence of these properties across the case study is described in Table 6-3.

Table 6-3 *Structural entities properties mapped with prevention encounters*

Prevention encounter	**Heterogeneity of role**	**Inherited complexity**	**Technological novelty**
Credit card mass mailing	• Actors such as FRB and FI acted as challengers and contested solutions proposed by legislators.		• The novelty of credit card stirred various interpretations of the technology and its impact on economy.
Automating card transactions			• The advancements in computer technology drove experimenting its use in automating transactions • A unified authorization system was

			interpreted differently among actors.
Automating POS terminals	• ABA task force was formed to evaluate the technologies and give recommendations (arbitrator) • Some actors' challenged magstripe security and called for a different standard. • DoJ considered sharing POS terminals anticompetitive and liable to antitrust laws (challenger) • ABA task force role shifted to defend its endorsed technology (stabilizer) • Financial institutions clarified they do not compete over technology products (stabilizer) • NCEFT was formed with the role of investigating the issue and resolve conflicts over legitimacy of sharing POS terminals (arbitrator)	• Although the executive branch of the legal system considered sharing POS terminals against antitrust laws, the legislative branch nonetheless required further information to judge whether it resides within antitrust laws or not.	• The need for new encoding technology in card authorization drove experimentations of multiple technologies. • The fact that magstripe was not an established technology opened chances for considering other alternatives to become the standard. • POS terminals revolutionized how merchants and banks interact and blurred industrial boundaries which allowed actors to view the technology in different ways (interpretation). • DoJ argued that POS terminal is an emerging technology and so there is still room for experimenting with other technologies that may better serve the public.
Smart card vs. magstripe	• Visa wore the stabilizer hat and announced smart card is still a premature technology and magstripe is the standard for the next decade.		• The emergence of smart card as a new technology to prevent fraud drove actors to experiment with the technology in order to gain better understandings of its potentials and test its technical and economic feasibility.

			• While some actors perceived smart cards as the new fraud prevention technology others interpret it as a solution finding a problem.
Strengthening the legal system		• The mobility of credit card fraud across the nation was facilitated by the layered nature of the legal system where fighting fraud is present only on state level but not federal level drove actors to call for federal intervention. • Different approaches for federal intervention between legislative and executive branches enabled negotiations to determine the best approach to follow.	• The innovative forms of credit cards fraud drove actors to reinterpret what constitute a credit card and credit card fraud. • The use of computers to conduct fraud was new and required a legal definition of a computer. Nonetheless, actors negotiated an exclusion of some proposed solutions that relate to the use of computers as shared understanding on the meaning of the technology has not been developed yet (interpretation).
Security in card-not-present environment (e-commerce)	• Financial institutions challenged Visa's and MasterCard's proposed security protocol and argued for a need of a single standard (challenger) • Card associations played as infrastructure providers and through SET consortium offered technology vendors a security protocol they can use when developing their	• The multi-layered nature of the legal system produced inconsistent approach towards digital signature and forced actors to re-negotiate security over the Internet.	• The internet gave rise to new business opportunity to do commerce for merchants and banks, and for technology vendor to develop solutions to secure online transactions. • Due to the novelty of the Internet legislators needed multiple hearings to give meaning to the technology and understand

	own prevention measures (enabler). • The legal complexity surrounding digital signature hampered developing security products efforts, the industry consequently worked to gain legal certainty to allow implementation efforts of prevention measure to proceed (stabilizer).		how different state regulations hinder the growth of e-commerce (interpretation).
Shifting security directions: unified industry standards	• To facilitate the adoption of PCI standards, PCI SSC maintain and update the standards and ensure shared understanding of the security requirements through training programs (stabilizer). • PCI DSS TWG works to evaluate the thousands of inputs from participating organizations related to proposed changes and prepare a draft for the new standard (arbitrator).		• Following the release of a new standard actors start assessing it in order to give their feedback and propose changes to be discussed in Community meetings especially in light of new security threats (experiment).
Beyond magstripe: tokenization and chip cards	• Merchants rebelled against PCI standards and drove adoption of another technology (challenger). • PCI SSC contested claims about the ineffectiveness of PCI standards and worked to clarify the Council’s commitment toward security and keeping pace with advanced security solutions (challenger)		• Tokenization gave actors the opportunity to capture new revenues through securing mobile payments.

	• Visa, MasterCard, and American Express cooperated to provide technological infrastructure for tokenization. (enabler)		

6.3.2 Contextual Conditions

Mechanisms’ effect is contingent on conditions responsible for activating them. The analysis showed actors’ actions in prevention encounters were triggered by dissatisfaction with current prevention measures and the fragmented approaches towards security. Those two were further behind the prevention encounters triggers witnessed in the case.

Dissatisfaction with prevention measures stemmed from the fact that they were no longer effective in preventing fraud as ways of countervailing them were on the rise. For instance, the slowness of early authorization procedure coupled with the lack of proper control over the process allowed merchants to bypass it, proving its ineffectiveness in thwarting fraud, which called for a new prevention measure. Similarly, the continuous security breaches despite the implementation of PCI standards drove the need for another more effective prevention measure. Inapplicability of current prevention measures to a certain environment is another source of dissatisfaction. The fact that laws defined credit cards as a device made it difficult to apply them when prosecuting criminals on cases that contained an illegal use of credit card numbers. Laws therefore were unable to maintain their deterrence effect. Likewise, prevention measures that relied on the physical presence of the card at the time of transaction were useless in an e-commerce environment. In both cases, it was the inapplicability of prevention measures that drove actors’ actions in security networks to develop another prevention measure that matches the new context.

Dissatisfaction with prevention measures was not the only condition for triggering collective efforts in security networks. Fragmented security approaches were a source of frustration for actors that initiated prevention encounters. When states started regulating the use of digital signature specifying when it is considered legal, actors swiftly acted and lobbied for a unified approach towards the technology. Along the same line, the numerous security programs initiated by card associations to protect card information which in their essence had the same goal placed unnecessary extra costs on merchants and processors suggesting a need for a change.

After understanding events in fraud prevention and identifying entities and properties that had a significant role in outcomes observed along with the contextual conditions that triggered prevention encounters, I will move now towards identifying prevention mechanisms.

6.4 Prevention Mechanisms

Analysis of prevention encounters showed that there are three mechanisms that explain how security networks achieve prevention. To facilitate the explication of these mechanisms, I describe the relationship between them and entities' properties that support them. I show how context, structural entities and their properties interact to produce the outcome observed.

Figure 6-1 shows the structure of causal explanation after identifying the missing elements.

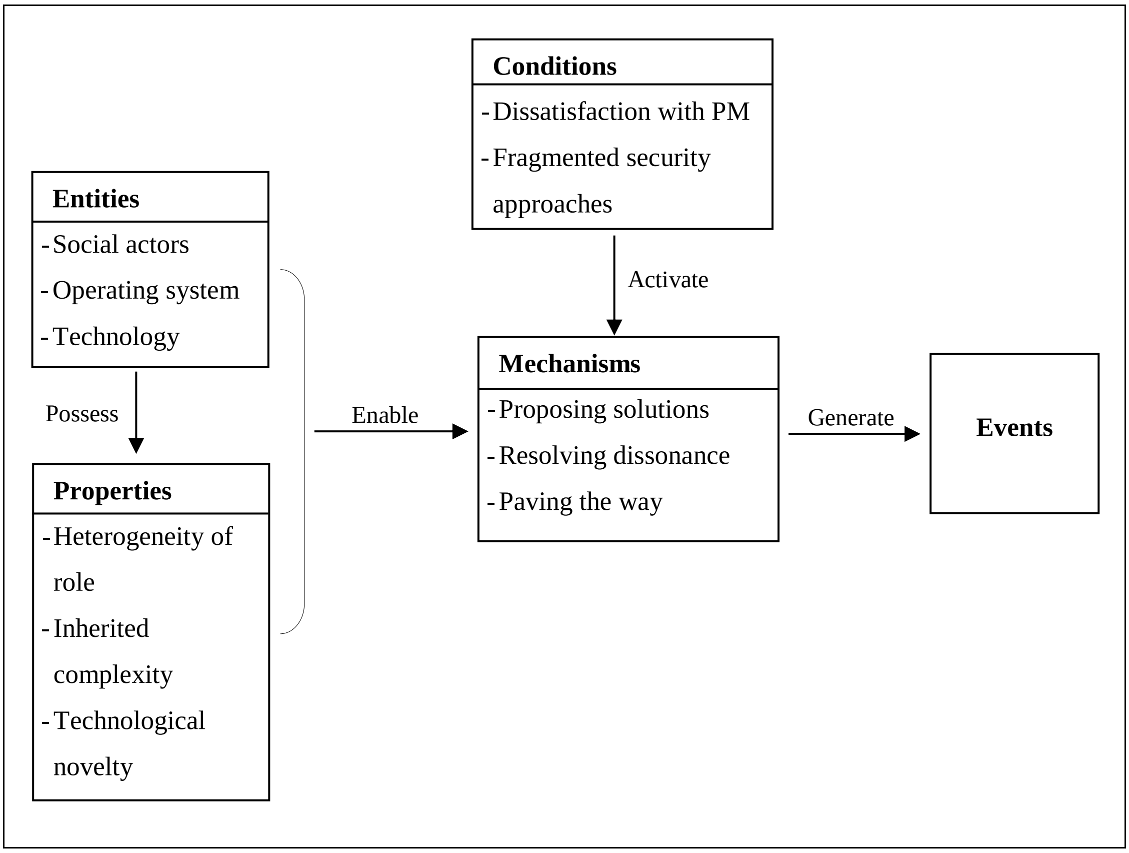


Figure 6-1 *The complete structure of causal explanation in security networks*

6.4.1 Proposing Solutions Mechanism

The first mechanism identified is proposing solutions mechanism. This mechanism emerged from the interactions between actors on how best to tackle the issue at hand. It refers to the process by which actors realizing the need for a change in security practices propose different solutions to prevent security threats.

It was apparent with the huge outrage that followed the introduction of credit cards to the market that a change in banks security practices is needed. What the change would be varied according to how actors interpreted the new payment technology (technological novelty). As providers of credit cards, financial institutions' suggestion of modifying mailing procedures to include a more rigorous check of customers' credit worthiness reflected their desire to protect their new business from any legal intervention and constraints that might be placed on their actions. This proposition nevertheless conflicted with how legislators perceived the new technology. For members of the Congress, the credit card was an inflationary device.

Through cards, customers gained easy access to a considerable amount of money which could increase their spending and eventually inflation rate. Besides, contractual agreements between merchants and acquirers and acquirers and issuers involve paying merchants an amount less than the price of the merchandize. There were further concerns that merchants will pass on this loss to customers through higher prices, which can add to inflation. As legislators seek to protect the interests of the general public, which for them could be only ensured by enacting a new law that regulates credit cards, sponsors of the new law aimed through it to reduce the number of credit cards circulated. This should result in lessening the negative ramifications credit cards have.

The novelty of credit cards as payment devices continued to be seen even after years of its introduction. Being a new technology, it was not easy to envisage ways in which credit card fraud can be conducted. This was complex not only due to the newness of the credit card itself but also to the advancements in information technology that could be used to infiltrate credit cards. For example, strengthening the legal system prevention encounter showed the different bills introduced to tackle the system's weaknesses. While some focused on redefining credit cards and prohibiting buying, selling, or possession of equipment used to produce fraudulent cards or accounts, others in addition to these modifications recognized developments in information technology and understood credit card fraud in conjunction with computer crime and so included a prohibition of the use of computers to commit fraud or disclose information without authorization in their proposals.

The role of technological novelty in the emergence of proposing solutions mechanism is not limited to the technology interpretive flexibility aspect but can extend it to include other aspects as well as evident in automating POS terminals prevention encounter. The benefits credit cards offered made them desirable to banks, merchants, and technology vendors (business opportunity). For banks and technology vendors they provided a new mean of doing business and increasing profits, while for merchants they released them from back office headache concerning administrative and accounting functions. Therefore, when there was a need to electronically transmit card information between merchants' sites and issuing banks, merchants, financial institutions, and technology vendors collectively engaged in enhancing the efficiency and security of the authorization process and participated in experimenting with a variety of technologies for encoding card data. This process resulted in proposing 44 solutions to ABA task force for evaluation. In a similar vein, when computers processing power starting to be evident in late 1960s, processors began experimenting with computers to revolutionize credit card authorization process and test computers capabilities. Omniswitch started offering its services in 1970 and National Data Corporation (NDC) joined Omniswitch two years later. These experiments proved the feasibility of this technical solution and accordingly NBI and other card associations worked to propose their own authorization system.

Business opportunities accompanying new technologies proved crucial in driving actors to engage in proposing solutions that would maintain credit card security. When merchants in 2007 rebelled against PCI standards and called for adopting tokenization to prevent fraud, card associations’ response came only to verbally support merchants’ claims and delegating the responsibility of negotiating and implementing the new solution to acquiring banks, and no further action was taken. It was only when the diffusion of tablets and smartphones offered new means of payment and opportunity to expand services and increase credit cards usage that card associations took tokenization (as well as chip cards) seriously and started collaborating to offer a standard that would facilitate the utilization of tokens to secure mobile payments. This was also the case in securing transactions over the Internet where Visa and MasterCard rushed to propose their security protocols in order to capture the new revenue stream.

Although technological novelty is the dominant property for enabling proposing solutions mechanism to emerge, heterogeneity of role and inherited complexity played a role in some prevention encounters. On the one hand, moving beyond magstripe prevention encounter showed that actors can rebel against roles defined to them and seek to reorganize the network around a different prevention measure. Merchants, who suffered from continuous security breaches, defied PCI standards and proposed tokenization and chip cards as alternative technologies to prevent fraud.

On the other hand, looking at the prevention encounter in strengthening the legal system show how the legal system can have a hand in exacerbating fraud. The structure of the legal system that is divided into state and federal laws enabled proposing solutions mechanism to emerge. Despite the presence of state laws that criminalized fraudulent activities, the mobile nature of credit card fraud made it bypass state jurisdictions. Counterfeiting the cards, for instance, can be based in one state while distributing them in another. The fact that federal laws did not criminalize such activities opened opportunities for actors to offer different proposals on how federal laws can be amended to fight fraud.

Through collective efforts to enhance current situation and prevent fraud in a more effective way, proposing solutions mechanism was manifested in actors' attempts to sense their way to credit cards security through offering different prevention measures. This was mainly driven by the uncertainty associated with novel technologies that made it difficult to know in advance the prevention measure that would best prevent fraud and meet actors' interests. Actors therefore were forced to experiment with different solutions to obtain knowledge about their feasibility and effectiveness. In addition, the presence of opportunities to increase profits incited competition and supported the rise of multiple solutions.

Table 6-4 summarizes entities properties that enabled proposing solutions mechanism to emerge in each prevention encounter.

Table 6-4 *Structural entities properties in proposing solutions mechanism*

Prevention encounters	**Heterogeneity of role**	**Inherited complexity**	**Technological novelty**
Credit card mass mailing			Actors held different <u>interpretations</u> of credit cards, for example, legislators perceived it as an inflationary device while FI perceived it as an innovative payment method. This directed the solutions each proposed.
Automating card transactions			With the rise of computers processing power actors started to

			experiment the use of computers to automate the authorization process.
Automating POS terminals			Use of a card encoding technology to automate authorization changed interactions between merchants and banks and resulted in experimenting with different encoding technologies.
Smart card vs. magstripe			The emergence of smart card as a new technology to prevent fraud drove actors to experiment with the technology in order to gain better understandings of its potentials and test its technical and economic feasibility.
Strengthening the legal system		The mobility of credit card fraud across the nation was facilitated by the layered nature of the legal system where fighting fraud was present only on state level but not on federal level. This drove actors to call for federal intervention.	The innovative forms of credit cards fraud forced actors to reinterpret what constitute a credit card and credit card fraud and propose prevention measures accordingly.
Security in card-not-present environment (e-commerce)			The Internet disrupted actors’ business model and called for means to secure the new environment. Visa and MasterCard each rushed to capture this business opportunity to expand the use of their cards and hence offered security protocols.
Shifting security directions: unified industry standards			Following the release of a new standard actors start assessing it in order to give their feedback and propose changes to be discussed in Community meetings especially in light of

			new security threats (experiment).
Beyond magstripe: tokenization and chip cards	Continuous security breaches even with the adoption of PCI standards made merchants question the effectiveness of the standard and call for new prevention measures (challenger).		Innovations in payment technology necessitated new prevention measures to secure mobile payments and be able to take advantage of the new revenue stream (business opportunity).

6.4.2 Resolving Dissonance Mechanism

The entangled relationships between actors and the availability of different solutions to prevent fraud forced actors to engage in a negotiation process to reach consensus on which prevention measure to adopt. This was a complicated task as actors challenged each other’s solution in an attempt to rule out all others except theirs. Proposed solutions went through several iterations of *exclusion* and *refinements* before the network sealed on one of them. Resolving dissonance mechanism emerged from diverged perspectives on means of achieving security and preventing fraud. It refers to the process by which actors engage in negotiations to solve conflicted views about the proposed prevention measures to reach consensus on the best approach to take to prevent security threats.

As described in the prevention encounters, different positions were held on how credit card fraud should be tackled. Having these conflicted views drove actors to negotiate and find their way into a solution that satisfies them all. Throughout these negotiations, actors sought to develop a shared understanding of the technology itself and how the problem at hand can be best approached. When legislators introduced a bill that constrained mailing credit cards by means of registered mail and only in response to written application, the financial industry rejected such a bill as registered mail was too costly, and experiments with other means to enter the credit card market such as what was proposed in the bill (sending applications) proved to be ineffective and generated low response rate when compared to mass mailing (heterogeneity of role). Failing to reach consensus, financial institutions proposed sending a pre-mailer to notify customers and make them aware of their credit cards.

This method ensured customers become knowledgeable of the credit card and gave them the freedom to either accept or reject it and hence could not be considered an invasion of privacy. Legislators however did not see any difference between this new distribution method and mass mailing. They argued sending pre-mailers placed a burden on customers to respond in situations where they do not wish to receive the card and perceived this as an inconvenient practice.

Legislators faced similar situations representing opportunities for multiple interpretations in automating POS terminals and strengthening the legal system prevention encounters. In the former, the use of POS terminals completely changed the conventional form of communication between merchants and banks creating confusion over where the boundaries lie anymore and opening the opportunity to negotiate whether sharing POS terminals was anti-competitive or not. In the latter, bills proposed to strengthen the legal system involved acknowledging the role of computers in conducting fraud. The newness of the technology however made actors (DoJ, FBI, Department of Treasury, states representatives) reluctant to support such bills as agreement on a definition for a “computer” and what would constitute a computer crime had not been reached yet and was still under investigation. They accordingly negotiated for segregating computer fraud problems and addressing those related specifically to credit card fraud.

While the above mentioned prevention encounters demonstrate how the newness of the technology allowed it to be perceived in multiple ways and therefore affecting the network’s prevention efforts, security in card-not-present environment showed that because the technology (the Internet) was new legislators were unable to ascribe it with a specific meaning. Several hearings had to take place to provide necessary information for them to develop an understanding of the technology and be able to judge whether federal intervention was needed or not.

Failing to reach common understanding prolonged the negotiation process and increased the number of solutions proposed. Besides the multiple interpretations surrounding credit card and its prevention measures (technological novelty), heterogeneity of role further supported resolving dissonance mechanism, whether that was through actors’ rejection to take a role in the network or the emergence of entirely new roles. Consensus was thought to be reached when ABA supported a bill that allowed unsolicited mailing with the conditions that the FRB prescribes regulations for customers illegible to unsolicited cards. However, the unwillingness of the FRB to take responsibilities in the area of consumer protection, along with the continuous social pressure rising from the large number of letters that were repeatedly sent to the FTC complaining about banks' mailing behaviour, and testimonies from various actors regarding the role of credit cards in individual bankruptcies and criminal activities, drove legislators to be more stringent on their ruling and the bill was eventually modified to ban mass mailing all together.

Challenger role was strongly evident in several other prevention encounters denoting its pivotal influence on the emergence of resolving dissonance mechanism. The simplicity of magstripe security features and the significant investments undertaken in other prevention measures made actors contest magstripe as the industry standard and opened the doors for considering other prevention measures. Likewise, PCI SSC challenged claims about the ineffectiveness of PCI standards in preventing security breaches and through negotiation sought to clarify the role of the Council including its initiatives towards incorporating different solutions in new versions of the standards.

Security was not the only aspect that attracted challenges to a certain prevention measure. In automating POS terminals, it was the anti-competitive nature of the prevention measure (sharing POS terminals) not its security aspect that drove DoJ to contest its legality and encourage searching for other solutions. And in securing online transactions, the incompatibility between STT and SEPP was the driver for banks' rejection of the proposed solutions and the basis for negotiating for a single security protocol.

In addition to rejecting (challenging) roles, resolving dissonance mechanism was supported by the emergence of new roles that enrolled new actors to the network. The multiplicity of change proposals created a need for a formal body to evaluate them and determine what the future change would be. Arbitrator role thus emerged, and accordingly actors such as ABA task force and PCI DSS TWG arose to occupy that position.

Sudden exposure to new technologies incited conflict and negotiation. The possibility of introducing smart cards to the U.S. credit card industry was behind the extensive experimentations Visa and MasterCard undertook to check its applicability to the U.S. environment. Through these experimentations, actors developed assumptions and meanings of the technology which shaped the negotiation process. MasterCard was convinced smart cards were the new revolution in fraud prevention. Its heavy investments echoed its belief. Visa's position, in contrast, showed how it interpreted the technology through its economic feasibility rather than its security promises. Building a whole new infrastructure to support smart cards could not be justified based on security reasons solely. Based on this reasoning, negotiations were enriched by Visa's call for discovering new card applications that can make the technology more economically feasible. Proponents of magstripe saw smart cards as a solution that is finding a problem. It was a success in Europe because it solved poor communication lines problem between merchants and financial institutions that made online authorization impossible, a problem that did not exist in the U.S. The hazy future of smart cards with opponents and proponents and the conflicted approaches of the two major card players gave actors the opportunity to raise their concerns or interests regarding the technology so that a unified approach towards it can be reached.

Prevention encounters surrounding alternative encoding technologies that challenged magstripe is another example that shows how technological novelty enabled resolving dissonance mechanism to emerge. Encoding card information with magstripe was not an established practice and magstripe had not *yet* been widely diffused in the credit card industry. Its announcement to become the standard came after ABA's task force recommendations. This timeframe between its announcement and its wide diffusion gave the opportunity to negotiate other alternative technologies before it was too late. Consequently, actors against magstripe rushed to propose other technologies such as OCR and Magic Middle that can address security weaknesses in magstripe.

Building shared understanding during negotiations can be challenging when considering the nature of the industry's operating system. The legal system that governs the banking sector had constrained many efforts for collective action to prevent fraud (inherited complexity). When negotiations for developing a unified authorization system for interchange transactions were underway, actors soon excluded this solution because of antitrust laws. Such collaborative efforts if presumed could be viewed by the DoJ as a collusive practice that creates a monopoly and hinders fair competition. This was also seen in automating POS terminals where different branches in the legal system held different views on the legality of the sharing behaviour. While the executive branch perceived sharing terminals anti-competitive and liable to anti-trust laws, the legislative one saw that little is known about this behaviour and what alternative solutions lie on the table and thus required more information to determine its legality. Divergent approaches between the executive and legislative branches stemmed negotiations in prevention encounters in strengthening the legal system as well. Although actors reached consensus on the need for a stronger federal presence in fighting credit card fraud, they nevertheless had to negotiate the conditions that would warrant federal intervention. Federal thresholds suggested in proposals were in terms of either the possession of a particular number of counterfeited cards (10 or more, 5 or more) or an aggregate amount of fraudulent activities ($5000) or both (10 or more and $5000). Despite recognizing the standard procedures in the Federal Government where specifying the loss amount is necessary to ensure its enrolment, actors representing the DoJ opted for a more flexible solution that would give them the ability to be involved in situations regardless of the loss amount. Legislators however argued that states can have better prosecution laws and enforcement procedures that should not be overruled by federal regulations. Therefore, there should be a policy that clarifies when a federal jurisdiction is triggered. Following these discussions, consensus was reached and a new law was enacted that limited federal intervention to crimes that involve the possession of 15 or more counterfeited access device and have an aggregate value of $1000 in fraudulent amount.

The effect of inherited complexity on resolving dissonance mechanism is not limited to interactions on the federal level but can also rise from those occurring at the state level. The divergence of the U.S. legal system into 50 state laws where each state started to regulate the use of digital signatures created a plethora of inconsistent regulations that hindered the implementation of the prevention technology and stirred actors to demand a federal law that would pre-empt states conflicting laws.

A summary of entities properties that enabled resolving dissonance mechanism to emerge in each prevention encounter is presented in Table 6-5.

Table 6-5 *Structural entities properties in resolving dissonance mechanism*

Prevention encounters	**Heterogeneity of role**	**Inherited complexity**	**Technological novelty**
Credit card mass mailing	Actors such as FRB and FI acted as challengers and contested solutions proposed by legislators.		The different interpretations assigned to the new credit cards distribution methods enabled resolving dissonance mechanism.
Automating card transactions			Actors negatively interpreted the joint efforts plans and perceived them as a mean to control the industry.
Automating POS terminals	ABA task force acted as arbitrator to evaluate proposed encoding technologies and decide on an industry encoding standard. Banks and merchants who invested in an encoding technology other than magstripe challenged the security of the technology in an attempt to redirect the industry towards their solution (Challenger). DoJ considered sharing POS terminals anticompetitive and liable to antitrust laws (Challenger)	Although the executive branch of the legal system considered sharing POS terminals against antitrust laws, the legislative branch nonetheless required further information to judge whether it resides within antitrust laws or not.	As magstripe was still not established in the credit card industry; that is it has not been widely diffused and adopted for a long time, allowed negotiations of alternative technologies to emerge. Space for experimenting with other technologies still existed. POS terminals revolutionized how merchants and banks interact and blurred industrial boundaries which allowed actors to view the technology in different ways (interpretation). DoJ argued that POS terminal is an emerging technology and so there is still room for experimenting with other technologies that may better serve the public.

Smart card vs. magstripe			While some actors perceived smart cards as the new fraud prevention technology others interpret it as a solution finding a problem.
Strengthening the legal system		Different approaches for federal intervention to criminalize credit card fraud between legislative and executive branches enabled negotiations to determine the best approach to follow.	The use of computers to conduct fraud was new and required a legal definition of a computer. Nonetheless, actors negotiated an exclusion of some proposed solutions that relate to the use of computers as shared understanding on the meaning of the technology has not been developed yet (interpretation).
Security in card-not-present environment (e-commerce)	Financial institutions challenged Visa's and MasterCard's proposed security protocol and argued for a need of a single standard (challenger).	The multi-layered nature of the legal system produced inconsistent approaches towards digital signature and forced actors to re-negotiate security over the Internet.	Due to the novelty of the Internet legislators needed multiple hearings to give meaning to the technology and understand how different state regulations hinder the growth of e-commerce (interpretation).
Shifting security directions: unified industry standards	PCI DSS TWG works to evaluate the thousands of inputs from participating organizations related to proposed changes and prepare a draft for the new standard (arbitrator).		
Beyond magstripe: tokenization and chip cards	PCI SSC contested claims about the ineffectiveness of PCI standards and worked to clarify the Council's commitment toward security and keeping pace with advanced security solutions (challenger).		

6.4.3 Paving the Way Mechanism

The case analysis showed that once conflicts were resolved and consensus on the mean to prevent fraud was reached, efforts to take the prevention measure into practice started. Paving the way mechanism refers to the process by which actors engage in materializing the agreed on solution and eliminating obstacles that may derail development efforts.

The agreement on a prevention measure amongst a pool of measures available enabled actors to concentrate their resources and delineate their future security path. Upon announcing magstripe the encoding technology standard technology vendors focused on developing POS terminals that could read magstripe rather than any other technology. Vendors such as GTE, Northern Telecom, Sweda International, and AT&T started marketing their terminals to banks who then sold them to merchants. Large scale pilot tests ran through the industry to evaluate the authorizing network, the low-cost terminals, as well as ensuring merchants' satisfaction.

Events taking place in this mechanism are mainly supported by the heterogeneous roles actors inhabited with a strong presence for stabilizer and enabler roles (see Table 6-6). The analysis showed that in certain prevention encounters taking the prevention measure into practice involved the enrolment of new actors to the network as new roles emerged. The agreement on developing a unified standard to secure e-commerce transactions created a need for an actor to be responsible for combining the two proposed protocols (STT and SEPP) and resolve compatibility problems, and so SET Consortium was formed to inhabit this role. Developing the protocol was vital because other actors in the network depended on it to pursue their security efforts (enabler). Technology vendors awaited the release of SET to incorporate it into their security products before offering them in the market. Microsoft, for instance, announced its secure e-commerce payment solution, Microsoft Wallet, based on SET. Similarly, Verifone, the leading POS terminal manufacturer, incorporated SET in its financial software vGATE. Interdependencies among actors continued with a new role emerging from the release of SET itself. The technology used digital signatures and digital certificate to secure online financial transactions. Certificate Authorities that issue and validate these digital certificates were thus enrolled in the network.

Putting the prevention measure into practice did not always run smoothly however and in some prevention encounters it was interrupted forcing actors to *re-negotiate* their security practices. These interruptions were driven mainly by the novelty of the technological solution that offered space for re-negotiations as with the magstripe security case discussed in resolving dissonance mechanism, or because the technology caused many old barriers to fall creating confusion in the network. For instance, the use of POS terminals introduced not only a new technology to the market but also a new process for handling credit card transactions. It revolutionized how merchants and banks interacted, confusing the functions of each. It was no wonder therefore that sharing POS terminals was interpreted by the DoJ as anti-competitive behaviour though the development of POS terminals does not lie within banks tasks. This misinterpretation associated with implementing an unfamiliar approach in authorizing credit card transactions necessitated re-negotiating the industry’s security practices to clarify and redress the meaning of the new prevention measure. During this process, financial institutions acted as a stabilizer seeking to regain stability which was critical for the progression of the development efforts. Their efforts nonetheless were to no avail, the irreconcilable differences between actors while negotiating sharing POS terminals created a need for a thorough investigation of the phenomenon to formally resolve the conflict. NCEFT was formed and assumed a new role (arbitrator) that after two years of examination announced the legality of sharing POS terminals and allowed the implementation efforts to proceed.

Stabilizer role turned to be critical in this mechanism as interruptions to implementation efforts were evident in several prevention encounters. Because there should be legal acceptance of technologies used in electronic authentication, states rushed to regulate digital signature technology. This resulted in a multiplicity of inconsistent laws that undermined certainty and hindered the implementation of SET. Facing these conditions, actors as financial institutions, card associations, and technology vendors moved to stabilize the environment and obtain national uniformity towards electronic authentication. They engaged in negotiations with legislators claiming the need for a law that would provide certainty and flexibility to adapt to innovations in information technology. Their efforts came to fruition and Electronic Signatures in Global and National Commerce Act was enacted legalizing digital signatures with no specifications on the kind of technology that should be used.

Interruptions in security networks prevention efforts were also seen in situations where a state of vagueness dominated the industry and clarifications on how to move forward were needed. Following the intense experimentations in smart cards by the major card associations, confusion whether it would replace magstripe prevailed in the network. Technology vendors lacked knowledge on which technology they should direct their investments. To end this state, Visa wore the stabilizer hat and announced magstripe the industry standard and that all efforts should be directed towards making it more secure giving technology vendors the stability and security they need for their financial investments. Likewise, the possibility of interpreting PCI standards in multiple ways hindered their implementation. PCI SSC hence provides training programs to ASV and QSA to ensure unified understanding of the meaning of the standards that would facilitate compliance with the agreed on prevention measure (stabilizer).

It is important to mention that actors' roles are not static and can shift to match the new context. During the negotiations of the best encoding technology to adopt, ABA task force acted as arbitrator to evaluate the several proposed encoding technologies. However, due to challenges the task force faced upon announcing its recommendation that disrupted the legitimacy of magstripe, the force shifted its role to act as a stabilizer to regain endorsement of magstripe. The task force resorted to solve the conflicts by tailoring the requirements for the industry standard in a way to exclude other solutions except magstripe. It by this succeeded in re-establishing the network stability needed to continue investments in and implementation of the technology.

Table 6-6 *Structural entities properties in paving the way mechanism*

Prevention encounters	**Heterogeneity of role**	**Inherited complexity**	**Technological novelty**
Credit card mass mailing			
Automating card transactions	---	---	---
Automating POS terminals	Facing interruptions from challengers, ABA task force acted as a stabilizer to regain endorsement of magstripe from the industry's actors. FI sought to clarify the area where they compete in order to relax DoJ anticompetitive concerns (stabilizer) and allow implementation to continue. Facing the multiple views on sharing POS terminals held by actors in the legal system and actors in the credit card industry NCEFT acted as an arbitrator to evaluate the different possible solutions and announce a final verdict of the legality of the contested issue.		
Smart card vs. magstripe	Following the confusion created in the card industry of whether smart card will overrule magstripe Visa announced the latter to continue to be the industry standard and urged actors to direct their efforts to make the technology more secure (stabilizer).		
Strengthening the legal system			
Security in card-not-present environment (e-commerce)	Card associations played as infrastructure providers and through SET consortium		

	offered technology vendors a security protocol they can use when developing their own prevention measures (enabler). The legal complexity surrounding digital signature hampered developing security products efforts, the industry consequently worked to gain legal certainty to allow implementation efforts of prevention measure to proceed (stabilizer).		
Shifting security directions: unified industry standards	To facilitate the adoption of PCI standards, PCI SSC maintains and updates the standards and ensures shared understanding of the security requirements through training programs (stabilizer).		
Beyond magstripe: tokenization and chip cards	Visa, MasterCard, and American Express acted as infrastructure providers and offered tokenization standard to facilitate the implementation of payment solutions based on tokenization (enabler).		

Table 6-7 summarizes the definition of each prevention mechanism.

Using Pawson and Tilley's (1997) conditions-mechanisms-outcome structure, Figure 6-2 presents a tentative process model of how security networks achieve prevention.

Table 6-7 *Prevention mechanisms*

Preventive mechanism	**Definition**
Proposing solutions	The process by which actors realizing the need for a change in security practices propose different solutions to prevent security threats.
Resolving dissonance	The process by which actors engage in negotiations to solve conflicted views about proposed prevention measures to reach consensus on the best approach to take to prevent security threats.
Paving the way	The process by which actors engage in materializing the agreed on solution and eliminating obstacles that may derail development efforts.

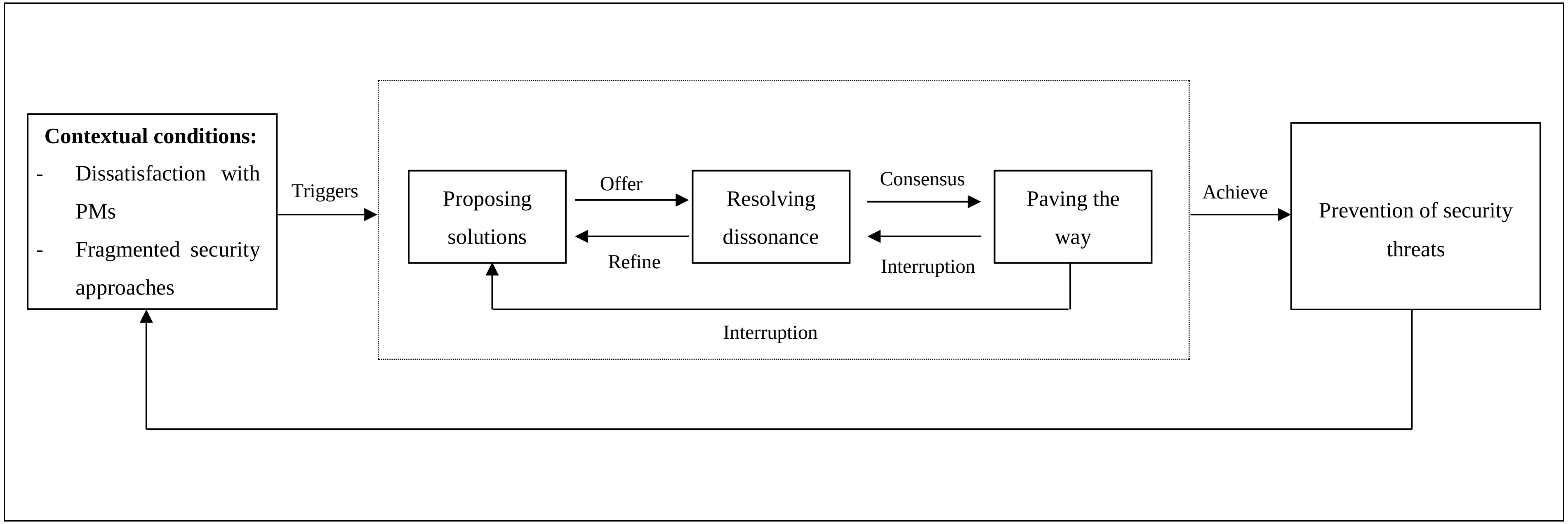

Contextual conditions:
- Dissatisfaction with PMs
- Fragmented security approaches
Triggers
Proposing solutions
Offer
Refine
Resolving dissonance
Consensus
Interruption
Paving the way
Interruption
Achieve
Prevention of security threats

Figure 6-2 *A process model of prevention encounters (tentative)*

6.5 Incentive Mechanisms

The process model of prevention encounters showed that security networks’ work processes involve interactions between heterogeneous actors who inhabit different roles and have divergent interests. Fraud prevention processes were therefore full of contestation and disagreements. To maintain the network stability and ensure collective security efforts, it was critical not only to align actors’ interests but to *continuously* do so as the case showed interruptions may disrupt an already stable network. This alignment and re-alignment processes to mobilize and recruit actors to prevent fraud were achieved by utilizing a collection of incentives to influence actors’ behaviour and motivate them towards the desired goal. Drawing on the initial conceptualization of incentives I now detail the mobilization processes. In doing so and in cases where the spokesperson of the actors is not self-evident, I will adopt the viewpoint of the financial industry in general and Visa in particular and describe processes they/it undertook and incentives used to build a network of allies (Latour, 1987). I first present the three incentive mechanisms and what do they mean drawing on insights from the case, then I detail which of these incentives were used in each prevention encounter to mobilize actors.

Transformative Incentive Mechanism

The first incentive mechanism is transformative incentives. The case showed that actors in security networks held various beliefs on actions either pursued or needed to prevent fraud; some were supportive while others were obstructive. This mechanism emerged as actors got engaged in a negotiation process to resolve differences and correct, what they viewed as, misconceptions held about their actions or technologies developed in order to transform old beliefs and replace them with new supportive ones.

“Rhetorical war” can best describe many of the events taking place in security networks. Efforts to mobilize actors were confronted with counter-mobilization ones that sought to take the industry in another direction. Transformative incentives mechanism refers to efforts taken to mobilize actors towards a certain issue by changing their belief about it through adopting one or more rhetorical devices and/or drawing on vocabularies of motive repertoire.

Preparatory Incentive Mechanism

The second mechanism to converge actors in security networks is preparatory incentives. This mechanism emerged as actors sought to smooth the path for developing prevention measures. The analysis showed preparatory incentives came in two forms, either to provide *legal certainty* or *operational certainty*.

Legal certainty refers to the condition where a stable legal framework exists to foster collective security efforts and protect actors' security investment, while operational certainty refers to the condition where a baseline for security efforts is established through the provisioning of foundational standards and laws that direct future security path. Preparatory incentive mechanism therefore refers to efforts taken to mobilize actors towards a certain issue by manipulating their environment to make it more legally and operationally desirable.

Captive Incentive Mechanism

The third incentive mechanism is captive incentives. Actors employing this mechanism sought to influence behaviour by placing the prevention measure (technology) between actors and their interests, making enrolment an *inevitable* outcome. Captive incentive mechanism refers to efforts taken to mobilize actors towards a certain issue by making the latter indispensable for them to achieve their personal goals.

6.5.1 Prevention Encounter 1: Credit Card Mass Mailing

As described in the first prevention encounter, following public outrage and regulatory intervention due to massive fraud rates, the credit card industry found itself in a situation where it has to defend its practices and change current beliefs about their passive attitude to prevent fraud (transformative incentive). In doing so, different actors from the industry participated in rhetorical wars to mobilize legislators and fight against a prohibition law. They based their debates on perversity and futility arguments, while adopting a variety of vocabularies of motive along the way (see Table 6-8).

In their negotiations, the financial industry (represented by FRB, ABA, banks) *de-escalated problems* arising from mass mailing while problematizing the proposed solutions by escalating the negative future consequences that would follow a complete ban on this practice. They argued that legislators' optimum *role* is ensuring the benefit of the public through enacting rules and regulations to meet this aim. However, enacting a law to ban mass mailing seems to contradict with this mission and leave the industry and the public in a worse situation (perversity). The proposed law would give financial institutions that have already resorted to mass mailing a competitive advantage over ones that yet seek to enter the credit card market. It was well known among financial institutions that mass mailing is the most effective and efficient solution to enter the new market as it had high response rate compared with other entry solutions, as applications sent by mail. Without mass mailing, Interbank (currently known as MasterCard) would not have been able to acquire a large customer base and so compete with BankAmericard. Legislators who always defended competition will now only hurt it by erecting barriers to entry. Furthermore, enacting such a law would reflect legislators' position regarding innovations in the financial industry and send a negative signal that discourages institutions from investing in innovative payment solutions.

The financial industry also utilized futility argument in their defence. They stated banks already have *self-motivation* to prevent fraud to protect their profits and reputation. Corrective actions were already in place making the new regulation of little impact to thwart fraud or incite banks to enhance their security controls.

Though these arguments seemed solid enough to transform held beliefs, the industry faced counter-mobilization efforts from supporters of the new law who also utilized a collection of rhetorical arguments and developed their own vocabularies of motive to reinforce legislators' current beliefs and forbid transformation efforts. Statements from state representatives and bankruptcy division stressed the importance of the

Table 6-8 *Belief transformation tools in credit card mass mailing*

	Rhetorical devices	**Vocabularies of motive**
Against banning law	Perversity, futility	Role conflict, anti-competitiveness, self-motivation, problem de-escalation
Supporting banning law	Perversity, jeopardy	rapid growth (urgency), spawning problems

new law which without the society would only suffer more (perversity). The arguments revolved around the threat the rapid diffusion of the new payment technology had on society. Credit cards, and the act of unsolicited mailing, did not only increase criminal activities but also *spawned* economic problems such as inflation and bankruptcies. Credit cards increase purchasing power and decrease savings trends, and so they jeopardize the country's whole economy which is based on thrifts (jeopardy). Besides this national impact, mass mailing could also threaten consumers clean credit records and credit rating as shown by the statement of the director of President's Committee on Consumer Interests,

> The principle problem is of jeopardy or potential jeopardy to a consumer's credit rating, since the intended recipient of an unsolicited credit card may not be aware an account has been opened in his name if he never gets the card (Meade, 1969, p.64).

These actors collectively pressed the *urgency* for legislative intervention to control banks' behaviour as the phenomenon is *growing rapidly*.

The strength of the counter-movement arguments, which was supported by real evidence such as statistics of economic consequences, for example for bankruptcies, and a considerable amount of consumers' complaint letters, precluded any disruption in legislators' beliefs regarding the danger mass mailing had on society and helped in reinforcing them giving legislators comfort about their ruling.

6.5.2 Prevention Encounter 2: Automating Card Transactions

The second prevention encounter presented the use of transformative incentives as well. However, it showed the failure of BofA's attempts to mobilize actors towards joining its proposal for a unified effort to build a national authorization system instead of developing different systems that serve the same goal. BofA's efforts were not received well by actors in the credit card industry, especially the two newly established card associations. NBI and Master Charge sought through rhetoric to change beliefs about the proposed prevention measure. They raised *scepticism* about BofA's true intentions and spread the word that this was a move by the bank to control the industry and centralize power in one actor. Moreover, joint efforts proposals neglected the regulatory environment that governs banks' actions. Antitrust laws prohibit collusive practices, and cooperation between the industry players to develop one unified system could be considered one (*anti-competitiveness*). Such efforts will then be ineffectual since they will be liable to legal scrutiny that could dissolve them (futility).

These arguments and the lack of counter-mobilizing moves from BofA and American Express (Table 6-9) succeeded in shaking actors' beliefs about the value of the joint efforts and enabled NBI to convince banks that pursuing unilateral authorization path is the most viable solution.

Table 6-9 *Belief transformation tools in automating card transactions*

	Rhetorical devices	**Vocabularies of motive**
Against unified system	Futility	Scepticism, anti-competitiveness
Supporting unified system	---	---

6.5.3 Prevention Encounter 3: Automating POS Terminals

This prevention encounter provided evidence of the use of the three incentive mechanisms in response to how automating POS terminals process was evolving.

The beginning of the process revealed how *captive* incentives facilitated actors' engagement in the process. When there was a need to transform the authorization process during the early days of credit cards, banks and merchants both had interests to collaborate with each other in this reform. The authorization process still required human intervention to communicate transaction details to the issuing bank. The process was prone to human error that would only prolong authorization and lower customer satisfaction. Moreover, as part of fraud prevention procedures, merchants were still required to consult hot card list for transactions below the floor limit. This did not reflect a trust relationship between them and their customers and in many situations they bypassed this authorization step taking the risk in cases where the card was fraudulent. Merchants therefore were eager to automate merchants-banks communication through card encoding technology. This allowed them to ensure high-quality customer service, increase store traffic and shift the liability for fraudulent transactions to issuing banks.

For banks, full automation of the authorization process would help in reducing credit card fraud losses that were massive. Using a card encoding technology to transmit data between merchants and banks eliminated the need for a floor limit allowing all transactions to go through issuing banks for authorization. In addition, hot card lists themselves were not up-to-date, and it took several days for a card to be registered on the list. Full automation would enable them to realize higher profits from the credit card business. With these mutual benefits, experimenting with different encoding technologies to automate merchants-banks communication witnessed active engagement by both parties.

The alignment of interests between actors however did not last. After announcing magnetic stripe as the card encoding technology, negotiations started of whether magstripe was the best alternative available to prevent fraud. As described in the third prevention encounter, actors who have already invested in other encoding technologies did not want their investments to go in vain, and they worked to change how others see magstripe. Opponents’ debates focused on whether a drastic change in the card design is in need to fight fraud. They argued why would banks incur extra costs associated with redesigning the card and developing new POS terminals when an *available familiar* technology (OCR) was already in use and would so relief both banks and merchants from an unnecessary financial burden. Banks who seek to increase their profit margin can find in OCR a mean to do so. Another attempt to disrupt beliefs in magstripe shifted towards focusing on the *simplicity* of the technology that even an amateur could break its security features. They aimed to raise *scepticism* about the security of magstripe and illustrate how its crudeness, in fact, encouraged criminal activities and increased fraud rather than fight them (perversity).

Proponents of magstripe had to stand up against these belief transformation attempts in order to secure the path for magstripe as the credit card industry standard (see Table 6-10). To restore network stability and belief in its standard, ABA task force stood against these claims and started refuting them one after the other. Through this, both transformative and captive incentive mechanisms were utilized to mobilize wide acceptance of magstripe.

The task force claimed that while adopting OCR was presumed to save costs, it actually did not since the card needed to be redesigned in any case to make the expiration data in OCR format (futility). Therefore, OCR had no superiority over magstripe regarding this aspect. Also, the task emphasized that to ensure *fairness and equality* across all actors in the industry; especially small merchants who could not afford a sophisticated solution, the technology had to be simple to allow maximum enrolment. Although magstripe has its vulnerabilities, fraud prevention measures in participants institutions should mitigate security risks and support building a safer payment system. By this, the task force shifted the *locus of security* from one about the encoding technology to one involving the entire payment system.

In addition, ABA task force drove the attention away from magstripe security to the visionary future of cashless society. Regardless of what encoding technology was to be adopted, banks and merchants both shared the same interest of automating not only the authorization process but also clearing transactions. Allowing money to transfer seamlessly and electronically among actors in the industry promised great reductions in administrative costs and facilitated timely settlements. A standard technology to transmit data across the network was the first step in achieving this vision (captive incentive). Conflicts that prevailed over the industry standard at that time were seen as a road block between actors and their interests. This created a sense of urgency to reach consensus and resolve disagreements regarding magstripe, as it was the fastest way for actors to attain their interests.

Table 6-10 *Belief transformation tools in challenging magstripe*

	Rhetorical devices	**Vocabularies of motive**
Against magstripe	Perversity	Scepticism, simplicity, availability
Supporting magstripe	Futility	Fairness and equality, locus of security

The task force strategic manoeuvre in shifting the argument from one about security to one of a higher goal was a clever move that along with transformative incentives succeeded in gaining actors support for magstripe and sealing the network on this encoding technology.

As work on automating POS terminals proceeded the network stability was disrupted again by DoJ antitrust division unanticipated enrolment to the network that challenged actors' security behaviour specifically regarding sharing POS terminals. The division worked on creating a network of allies around its belief of how security should be attained. To achieve this, it employed perversity argument to convince legislators of the need to put an end to banks' behaviour of sharing POS terminals. Its arguments sought to frame sharing as an *anti-competitive* behaviour, which contradicted with legislators' *role* of encouraging competition and free market. If sharing behaviour was to continue, actors in the credit card industry would have no incentives to develop innovative solutions. It would be natural for them to prefer joint ventures to minimize their risk, sharing thus kills competition. The emerging nature of EFT supported DoJ attempts to mobilize legislators to their side. As an emerging phenomenon, spaces for experimenting with other innovations existed. It would be too early therefore to judge that sharing was the best alternative to serve consumers' demand (*temporal fitness*).

Questioning the legitimacy of sharing POS terminals had its ramifications. Preventing fraud depended highly on technology vendors to manufacture and develop terminals that can be implemented at merchants' sites. The rapid diffusion of credit cards gave vendors a new business opportunity to increase their profits and acquire new customers. As a result, competition spurred and multiple brands were available in the market. This state however was disrupted by DoJ announcement that created an obstacle to continuing technology vendors' developments efforts. It was known in the industry that sharing allowed investment in POS terminals to be economically feasible. The technology was expensive; it was not only composed of terminals but also cards, telecommunication lines, computer processing facilities, and switches to route the message across the network. Technology vendors realized that without sharing, banks would opt for another more feasible technology. Therefore, when the legitimacy of sharing was on the line, they had no more incentives to continue their development efforts in POS terminals.

There was a need therefore to mobilize legislators (transformative incentive) to legitimize sharing and re-enrol technology vendors to the network and allow them to pursue their efforts (preparatory incentive). To achieve the former, the industry players' competing discourse focused on the perverse effects of DoJ's arguments (see Table 6-11). While DoJ claimed sharing denies consumers their freedom of choice, reality was the other way around. Small financial institutions who do not have sufficient resources to develop their own terminals conveyed their concerns of being excluded from market competition if they were not given access to other's POS terminals. Sharing then would allow the enrolment of more financial institutions giving consumers more choices. It was necessary to decrease market power concentration and foster a healthy competitive environment that supports *fairness and equality*. The industry's discourse also challenged DoJ's competition appeal. They argued the debates regarding competition were based on an incorrect belief, questioning by this the *validity* of the arguments. POS terminals are delivery systems for banking functions, and banks competed on the latter not the former. Sharing terminals therefore could not be considered anticompetitive.

Arguments supporting sharing were well-perceived and succeeded in changing conceptions about banks' behaviour as evident in NCEFT recommendations that came to legitimize sharing POS terminals and restore the network's stability. This Decision created a relatively *certain legal environment* that can ease vendors concerns and facilitated the progression of POS terminals development.

Table 6-11 *Belief transformation tools in sharing POS terminals*

	Rhetorical devices	**Vocabularies of motive**
Against sharing POS	Perversity	Role conflict, Anti-competitiveness, temporal fitness
Supporting sharing POS	---	Fairness and equality, validity

6.5.4 Prevention Encounter 4: Smart Card vs. Magstripe

This prevention encounter demonstrated the tension in the card industry following the recognition of a new technology that could achieve better results in preventing fraud. Visa and MasterCard held different beliefs about smart cards, and each worked to gain actors' support to their side (Table 6-12). The latter perceived it as the future of payment cards. Its arguments tried to drive the industry toward a radical change by following a revolutionary adoption approach. MasterCard believed magstripe had become an *obsolete technology*. The continuous and mounting fraud losses because of magstripe high vulnerability to counterfeiting (perversity) were not going to be solved by adding more security features to the card. The technology proved its ineffectiveness in countering innovations in fraud techniques, and the industry should be looking for ending not extending its life. Smart cards could offer a *comprehensive* solution to many problems troubling banks. Its chip technology made it difficult to counterfeit and intelligent enough to block transactions when consumers reach their credit limit, saving banks from massive losses. At the same time, MasterCard acknowledged the concerns over the high production costs of smart cards. But it claimed they could be countered by the *derivative value* of the technology that enabled the extension of the card expiration lifecycle and thus cutting re-issuance costs.

Visa took an opposite position. It employed the three rhetorical devices, perversity, futility and jeopardy to update actors' perception of smart cards and their beliefs of how the industry should move forward. The major card association challenged the reduction in losses obtained through smart cards. It argued an abrupt transition to smart cards would leave financial institutions $40 million worse off than they were currently (perversity). This was due to the high costs associated with this transition that included card renewal, modifying and installing new POS terminals. Moreover, credit card business volume was growing at a faster rate than that of fraud losses. The problem hence had been overstated (*de-escalating problem*).

Table 6-12 *Belief transformation tools in smart card vs. magstripe*

	Rhetorical devices	**Vocabularies of motive**
Against smart cards	Perversity, futility, jeopardy	Problem de-escalation, problem redefinition, temporal fitness
Supporting smart cards	Perversity	Obsolete technology, comprehensiveness, derivative value

Visa continued refuting MasterCard's arguments and finding weak points in its debate. For instance, it admitted that credit losses were high in number, nevertheless no technology whether it was magstripe or smart card had to do with tackling this matter (futility). It was rather banks' credit policies that were responsible for any credit losses, a problem that could be prevented through internal procedural change (*redefining the problem*). Despite the fact that the latter problem was argued to be solved through smart cards, banks would be reluctant to utilize the technology's blocking feature as it deprived them of one main revenue stream in the credit card business (jeopardy).

Besides refuting MasterCard's arguments, Visa presented its own as well. It offered a powerful claim on how the new technology jeopardized the great investments and immense efforts the industry incurred in magstripe (jeopardy). Smart card would require restructuring the whole card payment system that took the industry more than a decade to stabilize. It meant abolishing the long-standing infrastructure only to start constructing a new unnecessary one. It would be a bad investment to dedicate resources to a technology that was designed to operate in a contradicting environment than the one featured in the U.S. This rendered smart card impractical to apply (futility). To further support their belief transformation efforts, Visa focused on shifting the argument from that of adoption *decision* to one about the *time* of adoption. Visa acknowledged the superiority of smart cards in reducing losses however it questioned whether it was the appropriate time for transitioning to smart cards. Its research showed that for smart cards to be a feasible solution the card has to offer benefits besides security. Smart card was an emerging technology in the U.S. and time should be allowed to innovate and incorporate new services to the card to increase its economic value.

Visa's persuasive arguments that utilized a variety of rhetorical devices reinforced its belief system and facilitated its transference to other actors, who after that perceived the new technology through Visa's eyes. This allowed Visa to take a decisive decision and announce that magstripe will continue to be the standard for the next decade, and that new technological solutions should be directed towards making magstripe cards more secure.

The impact of this announcement was crucial because the strident debates between Visa and MasterCard left the card industry in limbo, and technology vendors at a crossroad not knowing where to direct their investments. For them, committing resources to both magstripe and smart card to satisfy both card associations was not viable not only because of the economic burden it placed on vendors but also because one technology would eventually prevail, leaving investments in the other a costly missed opportunity. The announcement came to re-stabilize the industry and re-enrol vendors to fraud prevention network. It provided the *operational certainty* vendors needed to efficiently direct their resources, and returned to the market its positive state of one that offers favourable conditions for organizations to compete and derive business value (preparatory incentive). Accordingly, the 1990s witnessed the emergence of multiple technological innovations targeting magstripe security. In 1994, Visa and Citibank started testing 'watermark magnetics' that could determine whether information in the magstripe has been tampered with. Similarly, card associations were invited to test 'magnetic fingerprint' that relied on the physical properties of magnetic stripe itself and its particles arrangements to validate the card. Other fraud protection technologies included ones that measure the magnetic field the card emitted to ensure its authenticity and holomagnetic that encoded card data in a hologram as well, making the card difficult to counterfeit.

6.5.5 Prevention Encounter 5: Strengthening the Legal System

This prevention encounter showed the importance of preparatory incentives in prosecuting fraudsters. The case was triggered by the inadequacy of existing federal laws that were used to fight credit card fraud such as Truth-in-Lending Act and the Electronic Funds Transfer Act in addressing emerging innovative ways in committing fraud as credit card counterfeiting. The absence of a reliable *legal infrastructure* for prosecuting criminals contributed significantly to staggering fraud rates. Not only because existing laws could be circumvented but also because some activities, such as fraudulent use of credit card numbers, were not even covered by any law. Actors in courts and law enforcement agencies level of involvement and investigative and prosecution efforts were constrained by these deficiencies. This contributed to the mobility of criminal activities across the nation. Assistant State Attorney from Miami attested,

> … I think one of the reasons you need Federal legislation is that the very existence of the statute becomes a "power on" switch for the prosecutor and without it, you don't have any power on (Falco, 1984, p.222).

There was a need therefore to heighten the legal environment. The enactment of the new law supplied those actors with new tools to attack criminals and strengthened their prosecution case by basing it on a clear legal foundation.

6.5.6 Prevention Encounter 6: Security in Card-not-Present Environment

As with automating POS terminals, this prevention encounter revealed the use of the three incentive mechanisms following the evolution of the prevention efforts.

The opportunity to do business over the Internet opened up a new revenue stream for technology vendors the same as it did for merchants and financial institutions. Nonetheless, the anonymity of the medium required a new generation of prevention measures to ensure security in situations where neither the card nor its holder is present during the transaction. Given the universal acceptance of credit cards as a payment method, there was a need for global guidelines and frameworks that would lead the development of online security products. To recruit vendors and enable them to achieve their goal, the card associations were committed to laying the foundations of a secure financial infrastructure over the Internet (*operational certainty*). They developed SET protocol to serve as a building block for technology vendors' security products. With SET different products for e-commerce security became available in the market such as Microsoft's walletPassport and Yahoo! Wallet.

To encourage the adoption and diffusion of the standard, Visa took several initiatives to mobilize merchants and customers. The card association tied the exemption of chargeback fees on online transactions with adopting SET-based security products. This constituted a compelling motivation for merchants as chargeback fees consumed a considerable amount of their e-commerce revenues. To motivate customers to purchase through online channels, Visa relieved them from any liability in situations where fraudulent activities took place (captive incentive).

The favourable environment for developing security products based on SET did not last long. In building confidence in e-commerce, it was important to have legal recognition of electronic authentication and digital documents. Accordingly, states enacted laws that legally validated electronic authentication technologies. These laws however were inconsistent with one another as enacted or during judicial interpretation. Furthermore, federal laws themselves were subject to multiple interpretations by the judicial system, and cases showed that courts did not consider the use of technology in communication between transacting actors as binding or legally valid because contracts were not "signed in ink". This interstate inconsistency and federal regulation deficiency disrupted the ongoing efforts to develop security products to secure online transactions. It created an unfavourable climate for investing in electronic authentication by increasing compliance costs for actors, such as Certification Authorities, and limiting their ability to operate nationally. The presence of fifty different regimes further impeded the mobilization of new market entrants in e-commerce business. The Internet revolutionized the way organizations did business, and its openness and geographical breadth should be reflected in the legal environment to enable the private sector to compete and serve the nation. A national uniformity was thus necessary to mobilize businesses to take part in this new technologically-enabled market reform. Chairman Bennett observed,

> Unfortunately, financial institutions and other businesses across the country have hesitated to fully invest in the available technologies. Why? Because the law on

> electronic authentication does not currently provide the support necessary to justify such a substantial investment (Bennett, 1998, p.1).

The importance of having a proper environment with favourable competitive conditions was also seen in calls for adopting a technology-neutral approach that was not legislatively biased towards a particular technology as with some states laws,

> In addition to the problems of inconsistency … another unfortunate and perhaps unintended effect of certain of the current States' initiatives has been to impose by the force of statute business requirements and/or technical standards that may prove inconsistent with the rapid change in the business and technology environment. These statutory standards will be difficult to revise as technology changes, and as market forces develop new products and useful roles for electronic authentication (Lieberman, 1998, p.8).

To restore the network stability and realign actors' interests, federal intervention was needed. Through congressional hearings, actors ensured to build a robust and flexible legal infrastructure that is both consistent and predictable in terms of how electronic authentication is treated. In doing so, they employed transformative incentives and relied on perversity and jeopardy arguments as well as captive incentives to change legislators' beliefs about the technology and what their *role* should be.

In hearings about electronic authentication and digital signature and the federal role in this technology, representatives from financial institutions, technology vendors, and card associations among others applauded states fast initiatives to enact laws that support e-commerce. Nonetheless, they stressed electronic authentication should be viewed within the context of a rapidly changing economy that was shaped by technological innovations. E-commerce cut across state and federal jurisdiction and the current fragmented regulatory environment was not supporting but rather hindering the development of e-commerce (perversity). This effect was noted by actors supporting the need for federal intervention. In his testimony, the associate counsel for government affairs of one of credit companies noted,

> Recent advances in electronic and digital technology severely test the ability of the most diligent government policymakers, regulators and legislators to remain knowledgeable. Moreover, these rapid developments easily outdistance the traditional legislative and regulatory process. Therefore, all too often laws, regulations and rules designed to stimulate and encourage commerce have, on the contrary, become outdated at best, impediments at worst (Mossburg, 1997, p.4).

Mobilization attempts further involved invoking a *common national* interest. Actors (ex. Electronic Commerce Forum, financial institutions, card associations, certificate authorities) tied their claims about the need for federal intervention to enforce a unified approach with the national goal of economic prosperity. They argued without national recognition of digitally signed documents, the growth of e-commerce would stifle. The U.S. legal system that has always fostered an attractive business environment that contributed significantly to the country's economic prosperity will only now and because of its unstable regulatory framework hinder the realization of one significant opportunity for economic growth. Doing business online required a mean to authenticate the identity of the transacting parties. Providing the technology to achieve that was not sufficient alone, there had to be a consistent legal acceptance of the use of the technology nationwide. Without nationally recognizing the legitimacy of electronic authentication technologies, both technology vendors and consumers would be reluctant to take advantage of e-commerce and the U.S. would fall behind this new age of commerce. As the vice president of the Technology and Intellectual Property legal area for Citibank put it:

> It is our view that electronic commerce won't happen without electronic banking, and electronic banking, particularly Internet banking, won't happen without electronic authentication, and in turn electronic authentication won't happen unless we have some sort of national uniformity in this area (Nugent, 1997, p.8).

The mobilization discourse also emphasized that inconsistent laws led to incompatible and less secure authentication systems which threatened not only the efficiency of the *nation's payment system* but also the *leadership* position the U.S. always enjoyed in terms of supporting technological advancements (jeopardy),

> The European Commission has recognized this potential for chaos and is aggressively working to bring Europe into the forefront of electronic commerce by writing the first internationally applicable standards for regulation of digital signatures ... In fact, with all of the activity surrounding electronic commerce in Europe, including extensive government sponsored pilots and studies, it is clear that Europe has established itself as a leader in this area (Konstantaras, 1997, p.6).

Several countries; Japan, Italy, Germany, were providing legal recognition of electronic authentication technologies facilitating competition. If U.S. companies were to compete globally, uniformity needed to exist at a national level first. Further, international negotiations were undergoing regarding an international law for electronic authentication, and for the U.S. to take part in these negotiations and maintain its technological leadership position it had to correct its fragmented approach first as noted by the representative of Electronic Commerce Forum:

> However, before the United States can play a significant role internationally, it is necessary to examine the wisdom of the current multiplicity of state laws. The lack of uniform nationwide rules may inhibit America's ability to influence developments beyond its borders. As a result, it may be appropriate to consider the establishment of a federal standard or guidelines (Dorey, 1997, p.4).

Actors also showed the role national uniformity had on fostering a competitive environment that promoted values of *fairness and equality*. Differing state laws increased the cost of conducting business over the Internet. Where large actors might be able to bear unnecessary compliance costs, it was doubtful that smaller ones could. A unified approach would facilitate the participation of all actors in e-commerce. Supporters further strengthened their case by relating it to the *presidential policy* on global information infrastructure. Their claims for federal intervention to enact a unified approach were consistent with the policy's principles that called for a predictable legal environment for e-commerce.

These rhetorical arguments (Table 6-13) succeeded in overcoming legislators' scepticism about the need for an overarching federal law and resulted in passing Electronic Signatures in Global and National Commerce Act that nationally legitimized the use of electronic authentication.

***Table 6-13** Belief transformation tools in legitimacy of digital signature*

	Rhetorical devices	**Vocabularies of motive**
Supporting consistent and universal approach towards digital signature	Perversity, jeopardy	Role conflict, leadership, fairness and equality, national goal, national payment system

The *legal certainty* provided by the enactment of Electronic Signature in Global and National Commerce Act realigned actors' interests and re-stabilized the network. The act facilitated the use of digital signature and other electronic authentication technologies in e-commerce allowing technology vendors to resume their development of technological solutions to ensure security over the Internet. Furthermore, its technology-neutral approach gave the private sector the flexibility needed to adapt to market changes and technological advancements and encouraged competition among electronic authentication service providers.

6.5.7 Prevention Encounter 7: Shifting Security Directions: Unified Industry Standards

In the year 2000 and what follows, securing credit card data rested in card associations announcing security requirements merchants and other actors who store or transmit card information had to follow. Despite providing the flexibility for actors to adopt the technology that best serves their business environment, the network stability started to fade. Merchants began complaining about the various card protection programs they must comply with and the burden that added on their financial resources. The card associations agreed to collaborate and introduce a single standard that would re-enrol actors in security networks and ensure the network's durability. Having a unified security standard for the whole industry helped to favourably influence merchants' behaviour by altering their assessment of the environment. Instead of perceiving it as complex and driving confusion and cost, PCI standards provided a simple environment that made it easy for actors to adopt the prevention measure.

To further build a supportive compliance environment, PCI SSC offers training programs to firms and experts so that they can help merchants and other actors in their compliance efforts and ensure correct interpretation of the standards. Moreover, the Council facilitates the adoption of the standards by providing a list of secure devices merchants and financial institutions can consult when making the purchase decision. By this, PCI SSC's efforts aim to provide actors a general framework to guide their security decisions while ensuring them their efforts meet the industry's best practices (*operational certainty).*

Besides the use of preparatory incentives to motivate actors to adopt PCI standards, Visa (along with other card associations) offered a collection of financial incentives through its compliance acceleration program (as mentioned previously in the case narrative). The program which targeted acquiring banks rather than merchants directly tied financial rewards and penalties to the compliance of their merchants. Being the enforcement agency of PCI standards, merchants' banks worked to ascertain the compliance of their merchants in order to be entitled to the favourable interchange fees or to be waved from costly penalties (captive incentive).

6.5.8 Prevention Encounter 8: Beyond Magstripe: Tokenization and Chip Cards

Following the continuous data breaches at merchants' sites even after adopting PCI standards shook the network's stability and stirred questions regarding the effectiveness of PCI standards in thwarting fraud and the financial industry's true intentions in safeguarding consumer private data. Efforts to push the industry towards new prevention measures commenced and involved the use of the three incentive mechanisms.

While legislators focused their attention on policy procedures such as notification laws, NRF sought to reorient their focus and argued that the real problem did not lie in how fast the industry should notify consumers about the breach. The vital question that needed to be asked was why these breaches keep happening despite immense investments in fighting fraud (*redefining the problem*). NRF General Counsel and Senior Vice President claimed the answer lied in the *U.S. outdated card payment system*. When compared with the rest of the world, *the U.S. stands oddly alone* in terms of fraud prevention technologies. Chip and PIN cards were proved to significantly prevent fraud and were "already deployed successfully in nearly all of the industrialized world (and much of the Third World)" (Duncan, 2014). Yet, the U.S. card payment system was still outdated relying on the vulnerable and obsolete signature and magstripe.

Realising where the problem is was further emphasized by a consumer advocate, who stressed that offering after fraud services should not be mixed with security solutions against fraud,

> The provision of credit monitoring … really creates a false sense of security. It will not stop fraud on your existing accounts, and it will not stop identity theft (Mierzwinski, 2014, p.21).

From this point of view, the problem was not related to PCI standards per se but rather to the fact that these standards were associated with an obsolete technological platform. The credit card market that is based on duopoly pursues solutions that serve the interests of its two major card associations and refuse to widen the competition base *lessening competition*. Migrating to another safer technology was thus challenging. Further, policymakers should encourage investments in new technologies to prevent fraud so that the U.S. does not lag further behind the rest of the world.

Facing these charges, the financial industry started to counter this negative publicity and correct perceptions about its security measures (see

Table ***6-14***). In responding to reasons why the U.S. lagged behind the rest of the world in adopting chip and PIN despite facts of its effectiveness in preventing fraud, Visa argued that it was the U.S. advanced telecommunication infrastructure in terms of high speed and efficiency that allowed this delay. The reliable infrastructure facilitated real-time network authorization and fraud analytics making the benefits offered by chip and PIN less prevalent (futility). Nonetheless, witnessing the increase in breach incidents the card industry is shifting towards chip-enabled cards, encouraging signature and chip rather than PIN and chip. In her testimony, Visa's chief enterprise risk officer and chief legal officer, acknowledged that about 70% of fraud in brick and mortar stores is caused by counterfeited cards. As PINs reduce lost and stolen card fraud it does not do anything in preventing card counterfeiting, which is the big problem (redefining the problem), a point that was also confirmed by PCI SSC. She further argued that constant debates about signature vs. PIN and the focus on the latter will only slow the migration process and increase overall costs (perversity).

Table 6-14 *Belief transformation tools in tokenization and chip cards*

	Rhetorical devices	**Vocabularies of motive**
Against PCI standards and financial industry's position	---	Problem redefinition, outlier, outdate card payment system, anti-competitiveness
Supporting PCI standards and financial industry's position	Perversity, futility, jeopardy	Commitment, shared responsibility, collective work, locus of security, validity, problem redefinition, threats complexity

In congressional hearings held to investigate what security practices and technologies were used to strengthen the security of the payment system, ABA emphasized the industry's *commitment* to security:

> Even with the recent breaches, our payments system remains strong and continues to support the $3 trillion that Americans spend safely and securely each year with their credit and debit cards, and with good reason: Customers can use these cards confidently because their banks protect them by investing in technology to detect and prevent fraud, reissuing cards and absorbing fraud costs (Reuter, 2014, p.18).

ABA representative further stressed that banks were often the first to be blamed for security breach incidents since in many times suffered retailers' identity are intentionally not revealed leaving banks to take the reputation hit themselves. Security is a *shared responsibility* and should not be mistakenly perceived to fall solely under the financial industry's arena,

> Protecting the payments system is a shared responsibility. Banks, retailers, processors, and all participants in the payments system must share the responsibility of keeping the system secure. That responsibility should not fall

> predominantly on the financial services sector. Banks are committed to doing our share, but cannot be the sole bearer of that responsibility (Reuter, 2014, p.19).

In a similar vein, the chief technology officer of the PCI SSC underlined the *complexity* of security threats that made collective efforts inevitable,

> … the recent breaches underscore the complex nature of payment card security. A multifaceted problem cannot be solved by a single technology, standard, mandate, or regulation. It cannot be solved by a single sector of society. Business, standards bodies, policymakers, and law enforcement must work together to protect the privacy interests of consumers (Leach, 2014, p.24).

Visa as well acknowledged the shared responsibility of fraud prevention and the seriousness of the phenomenon as the continuous threats jeopardize consumers' trust in the payment systems actors *collectively worked* to establish over the last 50 years (jeopardy). The major card association faced its critics by stating the different prevention measures the company applies in protecting cardholder information. It assured other players that it does not require the storage of credit card information as has been claimed. On the contrary, in 2006 Visa promoted "drop the data" campaign to discourage merchants from storing sensitive information while acknowledging that they should remain tentative since data can be stolen in transit (*locus of security*). Accordingly, a shift in security practices was taking place, and the industry was moving from data protection to data devaluation approach. This shift was strongly evident when the innovation in payment methods through the use of smartphones and tablets to make contactless payment created a gap in security solutions that tokenization and chip technologies offered to fill (captive incentive). To capture the new business opportunity and ensure its worldwide dominance, Visa got more engaged in both technologies. The card association collaborated with MasterCard and American Express to release a global standard that supported new payment products such as Apply Pay and Google Wallet while maintaining the compatibility with the existing infrastructure.

Releasing tokenization standards by the card association and announcing guidelines for implementing the technology by PCI SSC was critical for taking the technology into practice (preparatory incentive). First, the standards provided the tools needed to build an interoperable environment. They offered a consistent framework between transacting actors on how tokens are generated and processed allowing the payment process to run smoothly. Issuers, for instance, need to be able to authorize tokenized transactions regardless of the devices or operating systems used in the payment process, or the tokenization solution adopted by processors. Tokenization standards enabled issuers' participation in the new wave of digital payment. This was crucial as issuers are the ones who inhabit the authorization role and their enrolment was necessary to progress with digital payment. The standard therefore allowed scaling up the technology to enlist and serve more actors. Second, despite the availability of security systems based on tokenization, merchants were reluctant to implement this technology although it promised them better security and reduction in compliance costs. Merchants are under contractual obligation to comply with the industry's security standards. With the absence of formal guidance within PCI standards on tokenization, they lacked the incentive to invest in a technology that might not conform to future changes in security requirements. PCI SSC guidelines relaxed merchants' fears and offered a baseline for evaluating the different tokenization solutions available in the market while at the same time reassuring merchants of their compliance with PCI security requirements.

To further encourage the move towards tokenization and chip cards, Visa waved merchants who adopt the new technologies from certain security requirements under PCI standards. This allowed merchants to evade a complex, costly and mandatory prevention measure and achieve considerable savings in security investments (captive incentive). In 2011 Visa announced the expansion of its Technology Innovation Program to merchants in the U.S. to accelerate the migration to chip cards and therefore adoption of mobile payments.

What can be deduced from these encounters is that the card industry succeeded in changing beliefs about its PCI standards and commitment to security. There was a consensus among actors that finger pointing is not going to solve contested issues. One can also infer that retailers as well succeeded in creating necessary pressure for adopting chip technology. Actors agreement that chip-enabled cards, with or without a PIN, remains better than the current magstripe, can lead us to presume that Visa, at the present time, was able to convince actors to adopt chip and signature. I should note however that debates surrounding PIN vs. signature is not over and continues after 2014 which marks the end of the data collection period for this prevention encounter.

Figure 6-3 incorporates the three incentive mechanisms and offers a complete view on the process model of prevention encounters.

6.6 Summary

Drawing on the case of credit card fraud and how its prevention measures developed over time, this chapter presented an analysis of how security networks achieve prevention and what incentives come into play to ensure convergence and network stability. The analysis showed that preventing security threats revolves around three prevention mechanisms: proposing solutions, resolving dissonance and paving the way, that interact with one another. Being a social and political process, collective security efforts do not go smoothly and can sometimes be interrupted prolonging the prevention process. The chapter further showed that the structure of security networks in terms of their constituent entities and their properties have a great influence on the networks' prevention efforts. Properties of security networks such as heterogeneity of actors' roles, the complexity of the legal system and technological novelty enabled prevention mechanisms to emerge. Their impact however was not constant but varied across the three prevention mechanisms.

Bringing actors together to prevent credit card fraud was challenging. Convergence process relied on employing a variety of incentives. In transformative incentives mechanism actors mobilized others by adopting different rhetorical arguments and vocabularies of motive in an attempt to change their belief to one that supports their case. In a different context, manipulating the environment to make it more favourable was the key for actors' enrolment in security networks. Captivating actors to the network by tying their interests with the desired behaviour was another successful convergence strategy.

In the next chapter, I discuss the knowledge gained from the process model and relate it with the relevant literature.

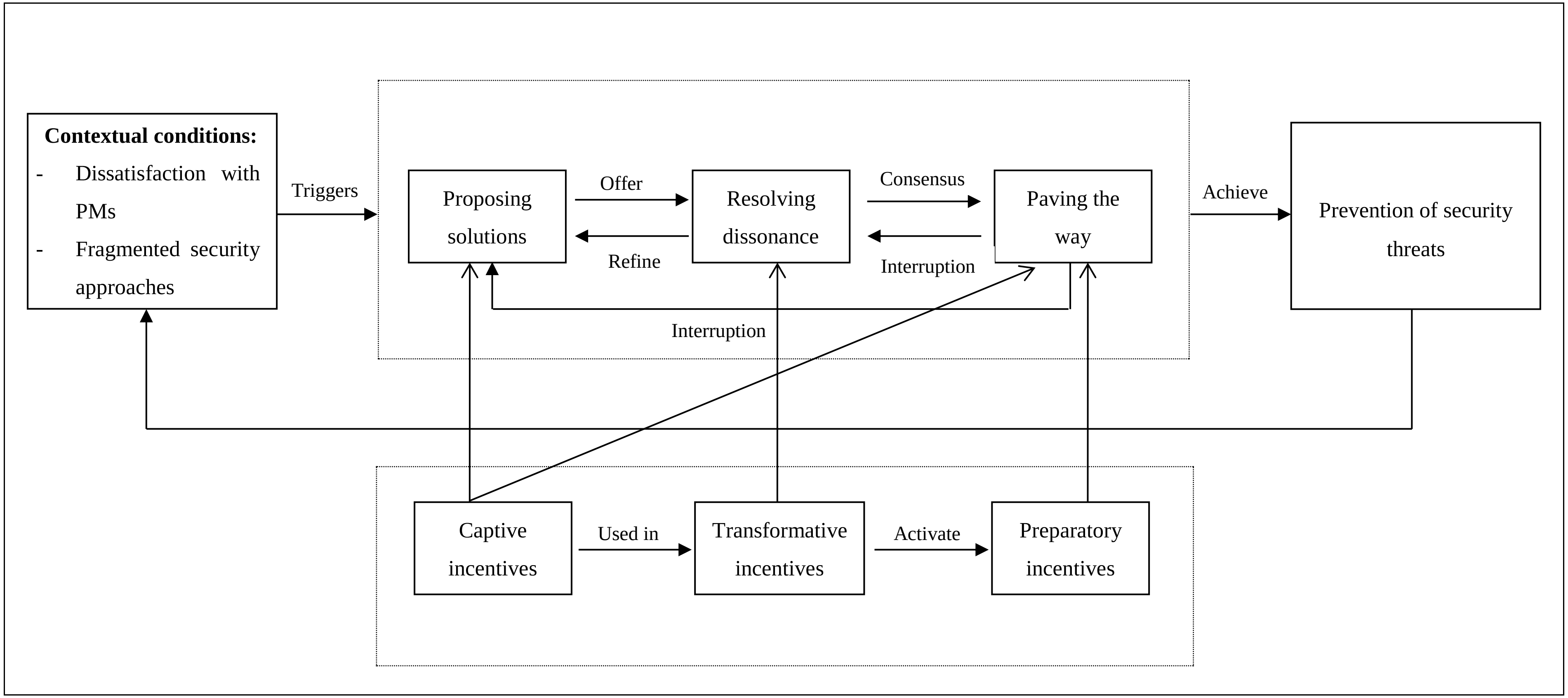


Figure 6-3 *The process model of prevention encounters with incentive mechanisms for convergence*

7 DISCUSSION

7.1 Introduction

In the current security networks literature, collective security efforts are manifested in information sharing alliances, outsourcing relationships, and vulnerability disclosure networks. This literature adopts an equilibrium-focus approach in studying security networks where variance models that take a snapshot view of the phenomenon constitute the foundation for knowledge about these security networks. Accordingly, little is known about how security networks achieve prevention. This research adopted a disequilibrium process-oriented approach and developed a process model of prevention encounters in security network. The model offers a detailed explanation of the prevention process. It explicates prevention and incentive mechanisms along with contextual conditions that trigger collective security efforts. In this chapter, I discuss the research findings with the current literature and show how they support and extend knowledge of security networks, while at the same time challenge common wisdom offering new insights. First, I discuss the prevention process in security networks. Then I move to examine the structure of security networks. Incentives for converging actors in collective security are discussed next. The chapter concludes with a brief examination of contemporary security threats to substantiate the findings under different settings.

7.2 Prevention Process in Security Networks

The prevention process starts with a dissatisfaction of current prevention measures because they are no longer effective or applicable in thwarting security threats. Furthermore, the common goal of attaining security and preventing threats made fragmented security approaches trigger collective security efforts. Realizing a need for a change in their security practices, and driven by captive incentives where taking action is necessary to realize personal benefits, actors in security networks start to experiment with innovative technological solutions that are more capable of facing the rising security threat. Proposing solutions mechanism results in a variety of security approaches. Accordingly, actors have to negotiate and discuss these different propositions in order to reach consensus on the best approach to follow. This is a challenging process because of many reasons. The interpretive flexibility of the proposed technologies facilitates a multiplicity and often conflicted beliefs about what should be the next prevention measure. Actors in resolving dissonance mechanism acted as challengers and refused to accept roles assigned to them by the network. Challengers therefore can drive the network back to proposing solutions in order to offer new alternatives. Furthermore, the presence of challengers give rise to a new role, arbitrator, who formally investigate the conflicted issue and resolve conflicts in the network. The complexity of the legal system, with its three interrelated branches that exist on both state and federal level (in my case), also played a role in instigating conflicts in the network. The prevalence of conflicted views in resolving dissonance mechanism make transformative incentives essential to shape others' beliefs and mobilize their support towards a certain prevention measure. Once actors are mobilized and consensus has been reached, actors start to take the agreed on prevention measure into practice. The prevention process does not end here however as prevention efforts can be interrupted triggering paving the way mechanism. In here, actors face these disruptions by renegotiating the prevention measure and acting as stabilizers and enablers to re-stabilize the network and allow the prevention efforts to proceed. Preparatory incentives hence become important to create a favourable environment that enable security efforts to move forward.

The prevention process offers several insights about security network's prevention efforts that contrast, compliment, or confirm the current literature. This is discussed next.

In their prevention efforts, actors are rational; they have predetermined objectives that maximize their benefits (Gordon *et al.*, 2003; Liu *et al.*, 2014), and the path to reach these objectives among available options is known (Lee *et al.*, 2013). Actors relationships in security networks are thus governed by the extent to whether the issue at matter meets their goals or not (Cezar *et al.*, 2014; Lee *et al.*, 2013) and so are based on a 'take it or leave it' approach. For instance, MSSPs offer their services to clients who have the freedom to accept or reject them (Zhao *et al.*, 2013). My study indicates however that goals and interests are not static and actors shape them in response to the context they find themselves in. Prevention process is hence fluid and actors can be *lenient*. Whereas banks' interest was initially to protect their credit card business from any legislative intervention, continuous debates and interactions with other actors made them more flexible, and they started negotiating the formation of the new law. Actors are not solely takers but they try to *manipulate* options to make them better fit their interests, which have already shifted in the course of the prevention process.

Interactive communication is thus critical in how security networks achieve prevention. Actors actively engage with one another throughout the whole process starting from proposing solutions and ending with paving the way for implementing the agreed on prevention measure. Accordingly, actors in security networks do not merely react to the actions of others in a sequential move pattern as currently described in security networks literature (Arora *et al.*, 2008; Cavusoglu *et al.*, 2007; Kannan & Telang, 2005; Liu *et al.*, 2014) where actors' relationships are interpreted to occur in multi-stage models. For example, in the first stage, a social planner (as CERT) set the protection period. In the second, vendors choose their patch release time and in the third organizations install the patch once it is available. Another example is designing research models to let the infomediary announce its pricing policy regarding rewards for reporting vulnerabilities and subscription fees and then allow discoverers and organizations to react accordingly. Although the process model shows that prevention efforts involve several stages (proposing solutions, resolving dissonance, paving the way) those are far from being static or bidirectional. Direct confrontations and negotiations were a foundational cornerstone in how security networks achieve prevention, making the process cyclical rather than linear. In the attempts of pursuing their own interests, actors challenged propositions offered to prevent credit card fraud moving the network to earlier stages. Therefore, there was not only one version of how security is achieved.

While the current literature tends to view relationships between actors to be unproblematic because actors are rational and have homogeneous beliefs on how to prevent security threats, the process model shows that conflict, heterogeneity of beliefs and uncertainty are key characteristics of collective security efforts. The difficulty of envisioning future consequences of prevention measures was apparent.

Actors struggled with ambiguity that stalled the entire prevention process since the future security path was blurry making it challenging to prefer one alternative over the other. Legislators, for instance, were not able to take a position about digital signature because they had little information to help them make sense of the Internet and its consequences and accordingly any technology related to it. Several hearings were initiated to gain information needed making security a complex cognitive task.

In addition, interdependence between actors add to the complexity of security networks. In the current literature, interdependence is mainly seen to be problematic and an obstacle to collective security efforts because it encourages free riding behaviour in information sharing alliances (Gordon *et al.*, 2003; Liu *et al.*, 2014) and introduces information asymmetry that makes it difficult to observe security efforts in outsourcing contracts (Hui *et al.*, 2012; Lee *et al.*, 2013). The prevention process offers a different view on interdependence. Interdependence can indeed be seen as an obstacle in security networks' prevention efforts but not because it drives actors to renege on security, rather because it prolong the prevention process as actors hold different beliefs about security efforts that force them to engage in negotiations to resolve their dissonance. An example is the different beliefs actors had on digital signature that created an uncertain legal environment. Developing a shared understanding of the technology between actors was necessary in order for the prevention process to proceed.

7.3 The Structure of Security Networks

Examining the structure of security networks, that is their constituent elements, facilitates uncovering components that play key roles in how prevention is attained and therefore allows a better understanding of security networks' prevention efforts. The current literature pays significant attention to individuals in security networks (e.g. a vendor, a competitor, an infomediary), whereby examining their actions it tries to explain collective security efforts. For example, in vulnerability disclosure networks preventing threats is achieved through referencing to vendors' patch release time decision (Arora *et al.*, 2010; Arora *et al.*, 2008) or infomediaries' profit maximization actions (Kannan & Telang, 2005; Li & Rao, 2007; Ransbotham *et al.*, 2012). Similarly, although information sharing and analysis center's goal is not maximizing its own profits but increasing the network's reliability and decreasing losses from security breaches, it still achieves this by leveraging its role in setting the optimal membership fee structure (Liu *et al*., 2014). Explanation is therefore achieved through focusing on individual's actions. This study shows that how security networks achieve prevention cannot be seen resulting from individual's actions alone. Each actor indeed had his own agenda on how prevention should be pursued but in such an interactive process it would be difficult to attribute the efforts of the network to that of one actor alone. Consensus on a prevention measure was rarely made individually. Rather it resulted collectively through negotiating solutions proposed by the network's heterogeneous actors which by themselves (proposed solutions) were modified during the process resulting in the emergence of new solutions that did not exist before. Possible alternatives therefore do not exist in outer space and already known by actors (Arora *et al.*, 2008) but can rather emerge throughout actors' efforts in finding the future security path. Therefore, to explain collective security efforts it is more useful to look at social actors in security networks through their relations with each other and the external environment rather than focusing on individuals' actions alone.

Moreover, although social actors are a key element in the structure of security networks, they offer a limited view on how these networks prevent security threats. This research identified technology and operating system (in terms of laws and regulations that govern actors' interactions) as other critical components that can change how prevention is achieved and thus their role should not be neglected.

Of importance here is to go more in depth and beyond identification of structural components to identify their properties that influence collective security efforts. My research shows that social actors occupy different roles in the network. Similarly the novelty and newness of the technology and the complexity of the legal system makes technology and operating system (respectively) causally relevant to the network's prevention efforts.

Heterogeneity of role refers to the different positions actors occupy in security networks to achieve prevention. Those positions are challengers, arbitrators, stabilizers, and enablers. The case further demonstrated that actors' role is not static and that the same actor can shift between these roles in response to changing context. While Visa's efforts in developing security standards represent its enabler role, the company acted as a stabilizer when there was confusion in the market in the 1980s over whether smart card would replace magstripe or not. Actors thus do not only shift their *security position* such as levels of security investments and information sharing or preference towards a certain patch disclosure policy to fit contextual conditions (Cavusoglu *et al.*, 2007; Hausken, 2007), but also their *network position*. The latter reflects the dynamic nature of security networks where actors move, enter, exit, or even threaten the network. It is crucial not to neglect such changes as they can impact security path as evident in the case of credit card fraud. This can be further inferred from Cavusoglu et al. (2007) study that observed a change in optimal disclosure policies once their single-vendor model was extended to incorporate the presence of multiple vendors in the network. Hausken (2007) also notes that social planner's interference in information sharing alliances should be carefully examined in order for it to result in collectively beneficial sharing conditions. This is because a social planner's actions (e.g. controlling for security investment) can sometimes have a perverse effect and result in an increase in free-riding behaviour. Moreover, it is vital to recognize the heterogeneity of actors in security networks and the impact that has on security decisions. Actors in the network differ in their capabilities to accommodate solutions that lead to better security (Gal-Or & Ghose, 2005; Liu *et al.*, 2014). Because small-size vendors need to be able to accept credit cards payment, security solutions adopted were not always the optimal ones. The fact that the network included small actors actually benefited larger ones in their negotiations and helped them in their mobilizing efforts. This runs contrary to what is frequently assumed that small actors tend to exploit larger ones (Gupta & Zhdanov, 2012).

Inherited complexity is the second property identified to be relevant to prevention efforts. It depicts how the multi-level and interrelated nature of the legal system interferes to constrain actors' security efforts. The study illustrated how such structure created inconsistencies concerning prevention efforts between the different legal branches prolonging the prevention process as well as creating security gaps that could be exploited to conduct illegal activities. The study extends prior research that conceptualizes the impact of the regulatory environment through the actions of *regulators* (e.g., Arora *et al.*, 2010; Gal-Or & Ghose, 2005) to show the impact of the *legal system* as a whole in security networks prevention efforts.

Technological novelty is the final property identified that shape collective security efforts. The research findings show that the effect of new technologies can be seen in three ways. First, actors have to *experiment* with new technologies to gain knowledge about their feasibility and consequences to be able to draw future security path. Second, new technologies are open to multiple *interpretations* that create confusion over how security is best achieved. Actors thus engage in negotiations to develop shared understanding of the meaning of the technology. Third, new technologies are not always seen ambiguous but can offer *business opportunities* that incite competition to deliver best security solutions.

7.4 Incentive Mechanisms in Security Networks

Incentives are essential for the survival of collective security efforts. Prior research stressed the importance of monetary payoffs in converging actors in security networks. This research concurs with this finding but also departs significantly by showing that monetary incentives only partly explain human motivation and that they are one of the three types of incentives to motivate collective security efforts.

The analysis of the case study provides evidence of the three incentive mechanisms conceptualized from the literature: transformative, preparatory and captive. Identifying such a variety of incentives acknowledges the heterogeneity of actors involved in security networks that makes the use of only one form of incentives (monetary) insufficient in succeeding convergence. Moreover, the current focus on rational actors averted attention from meanings and interpretations behind actors' interactions, and their role in the mobilization efforts. Issues such as free-riding behaviour and designing outsourcing contracts received more attention, leaving details about the interactions between actors and how they reach a common understanding about their relationships unexplored, providing by this incomplete picture of incentive mechanisms.

Conflicted beliefs about future security efforts are expected in security networks as clearly seen from the study. This incongruence hindered actors from reaching consensus over a prevention measure. From here, transformative incentives mechanism which targets actors' beliefs is deemed central to mobilize actors towards certain behaviour. The case analysis illustrated this mechanism hinges on utilizing different rhetorical arguments and drawing on vocabularies of motive repertoire to attain belief transformation. In particular, actors employed three rhetorical arguments in their mobilization efforts. In perversity argument, actors emphasized the contradicting effect of a particular behaviour. For example, in mass mailing prevention encounter the credit card industry tried to gain legislators' support by highlighting how enacting a banning law would display inconsistency between legislators' role and their actual actions. Moreover, a banning law would send a message in the industry that legislators oppose innovations in payment solutions. This resonates with 'signalling' incentive identified in security networks literature (Gal-Or & Ghose, 2005; Gupta & Zhdanov, 2012) where, for instance, actors join information sharing alliances to signal their security commitment to stakeholders. This research expands on this idea by offering a deeper understanding that explains that signalling works as an incentive through changing actors' beliefs and therefore can be seen part of transformative incentives mechanism.

Actors employed futility argument to reflect on the uselessness of a certain prevention measure in order to drive acceptance of another. In here, actors open up the discussion by using elements of the social structures to advance their interests. Proponents of magstripe referred to the nature of the U.S. payment environment to build support for magstripe against smart cards. At the same, these elements can constrain actors' collective security efforts as with antitrust laws that rendered a collective approach towards a unified authorization system futile.

The third rhetorical argument evidenced in the case is jeopardy argument which represents actors clinging to status quo and resistance to migrate to an alternative future in an attempt to protect valuable accomplishments. Actors manoeuvre their way to gain support not by attacking the proposed solution, which on the contrary can be accepted, but by shifting the discussion towards its undesirable consequences.

Jeopardy argument was the primary tool employed to stretch the life of magstripe as long as possible before the industry finally redirected towards smart cards.

Diversifying mobilization efforts through applying different rhetorical arguments and vocabularies of motive increase the chances of success. Nonetheless, appealing to an audience is complicated, and mobilization gets more problematic with the presence of counter-mobilizing moves that challenge transformative attempts. The *strength* of the counter-mobilization arguments of proponents of a banning law weakened the credit card industry’s claims, and their efforts to convince legislators of the lack of a need for a new law failed. At the same time, countermovement’s mobilizing arguments can benefit those they aim to oppose rather than incapacitate them. When arguments are built on shallow grounds, they open opportunities for the opposite party to find gaps and weak points that threaten the creditability of the claims. For the audience, this gives a perception that the latter has better knowledge in the matter of interest and therefore drives them to adopt their beliefs and their side of the debate. The research shows how the validity of some claims such as the anticompetitive nature of sharing of POS terminals and the mandate to save credit card numbers by merchants were questioned affecting and diminishing their persuasive effect in changing beliefs.

Vocabularies of motive are situated and vary with different contexts (Mills, 1940). Nonetheless, they can be associated with particular social conditions where some vocabularies become woven with certain behaviour. Mobilizing legislators often used vocabularies that revolved around their mission. Therefore, in more than one prevention encounter actors emphasized the conflict of role found in legislators’ current behaviour whether that was through highlighting the anti-competitive nature of the prevention measure or showing how their actions are impeding innovation and societal benefits. Furthermore, actors were keen to associate the desired action with vocabularies related to national impact and national prosperity that that are of high interest to legislators and at the core of their mission. In other contexts, such vocabularies were of little value and different ones were employed. For instance, when PCI standards were attacked, the Council and the card associations defended themselves by using inclusion vocabularies, such as shared responsibility, locus of security, collective work, threats complexity, which aimed to include other actors in preventing fraud.

Who makes the claim contributes to the success of mobilizing efforts. The credibility of actors involved is essential for a particular belief to resonate (Benford & Snow, 2000). The fact that the use of SET was encouraged by Visa and MasterCard was significant in creating a sense of security for transactions over the Internet among consumers and alleviating their concerns. This finding goes in line with Arora et al. (2010) who found that vendors respond faster to vulnerabilities disclosed by CERT than by other actors. They reasoned this to CERT's strong reputation of being a credible source of information since it investigates vulnerabilities before reporting them to vendors.

While it is commonly assumed that actors need to be incentivized to contribute to security networks, my study revealed that this need not be necessarily the case. Actors' interests can be aligned with those of the network. However, what is holding them from engaging in collective security efforts is the difficulty of pursuing their interests. Technology vendors, for instance, did not need incentives to develop solutions for securing transactions over the Internet; they already had self-interest in capturing the new revenue stream. What they needed was a foundational cornerstone for their development efforts. Therefore, enrolling actors to security networks is not only a misalignment problem but can also be an *advancement problem*. Preparatory incentive mechanism is another form of incentives that is crucial for converging actors in security networks. As actors do not come into a prepared environment, it becomes pivotal to manipulate the latter to make it more favourable for the former to advance their interests. It by this involves *deliberate* attempts to change the context to allocate power to actors and legitimize their efforts.

The analysis revealed that actors sought two kinds of certainty to pursue their security efforts: legal and operational. Prevention encounters demonstrated how actors ensured to comply with both regulatory and industry requirements but ambiguity surrounding any of the two impeded investments in security. National recognition of digital signature was necessary to justify investments in the technology. Legal certainty would enable building a stronger case for security products that are based on digital signature since it increases the scale of adoption. Instead of investing in a solution that can be only adopted in one state, legal certainty allowed it to diffuse across 50 states. The same applies to operational certainty that offers guidelines for security efforts. Merchants' hesitancy in adopting tokenization was due to a lack of legitimate standard recognized by the credit card industry. Prior research that investigated underinvestment in security reasoned that to interdependencies among actors (Kunreuther & Heal, 2003; Zhao *et al.*, 2013). This research offers two alternative grounds for underinvestment: legal and operational uncertainty.

The literature on security networks emphasizes the role of monetary incentives in motivating actors' enrolment. This research acknowledges the importance of this type of incentive it nevertheless shows that monetary incentives are a subset of a larger umbrella of incentives the research refers to by captive incentives. In captive incentives, actors are incited towards a particular behaviour because it is indispensable if they want to achieve their interests. IS security outsourcing offers valuable benefits ranging from cost savings to liability shift that incite actors to engage in outsourcing relationships (Cezar *et al.*, 2010; Hui *et al.*, 2012). Security networks' value hence stems from their ability to *mediate* between actors and their interests. Offering monetary incentives was also evident in the case of credit card fraud. Favourable interchange rates, a waiver from chargeback fees, and lessening the scope of PCI environment all resemble financial benefits actors are entitled to if they enrol to the network. This research complements the literature by demonstrating that actors can be captivated to collective security efforts by means other than financial rewards and penalties. The *common future vision* of a cashless society was behind actors' support for magstripe despite the security challenges surrounding the technology. ABA mobilization efforts aimed to invoke the notion of cashless society and the urgent need to agree on a standard technology in order to pursue this vision. Continuous debates about magstripe were impeding the realization of the vision and until the industry reaches consensus on a standard technology, efforts to build a cashless society would be held off. Tying a common future vision with accepting magstripe as the standard undermined the effectiveness of the opponents' arguments and facilitated mobilizing acceptance for magstripe. My research further provides evidence of the effectiveness of tying desired behaviour with national interest (legitimacy of digital signature case) and business opportunities (tokenization and smart card case) in converging actors in security networks.

The literature on information sharing alliances shows that they suffer from free-riding behaviour among their members because each want to protect its reputation and so renege on sharing security breach information. Besides designing better membership policies that incorporate economic incentives (Gordon *et al.*, 2003), this study indicated that concerns over the industry's reputation have a substantial impact on inciting actors and driving stronger commitment to security. The well-known Target security breach, for instance, cannot be seen as a problem affecting Target alone; its repercussions resonated to the entire credit card industry and drove regulatory attention to measures taken to safeguard consumers' personal information. Scaling the problem from an organization level to an industry level made actors more active in their security efforts.

Captive incentives can also be seen in relation to Gupta and Zhdanov's study that examined the formation of MSSP (Gupta & Zhdanov, 2012). They argue that actors join MSSP network to take benefits of its protective measures and large information base, what they call knowledge effect. However, they show that during the early stage of MSSP formation the network suffers from critical mass problem lessening the effectiveness of knowledge effect in enrolling actors to the network, making for-profit MSSP networks more prevalent in comparison with consortium networks. My study demonstrates that the value of security networks can be derived from benefits other than knowledge effect and members are willing to take the risk and contribute to the network formation because the network is indispensable to reach a broader common interest.

A key contribution of this research stems from examining the role of technology in security networks. Liability for security losses is a widely proposed incentive for driving collective security efforts (August & Tunca, 2011; Cavusoglu *et al.*, 2007; Hui *et al.*, 2012; Liu *et al.*, 2014; Ogut *et al.*, 2005). At the same time, the literature acknowledges that interdependent security and complexity in observing actors' efforts in security networks makes it difficult to determine the actor responsible for the loss, which can render this strategy inapplicable (Kunreuther & Heal, 2003; Lee *et al.*, 2013; Zhao *et al.*, 2013). The case revealed that technology plays a key role in solving this dilemma. Technological prevention measures were coupled with liability shift rules to motivate their adoption. By automating POS terminals, merchants shifted liability of fraudulent transactions to issuing banks. Similarly, security rules are inscribed in PCI standards allowing the technology to shift liability from one actor to another. By this, fraud liability is never definite and in a continuous flux that changes with various technologies. Technology has become the reference point actors revert to whenever security breaches occur to assign liabilities with no reasonable doubt.

Taking these incentive mechanisms together shows how they are related and nested within one another. During their attempts to transform beliefs and recruit supporters (transformative incentive) actors utilized captive incentives to strengthen their arguments. In legitimizing digital signature prevention encounter, for instance, they tied the growth of e-commerce with national recognition of the technology to drive legislators to perceive the importance of the issue at hand. At the same time, transformative incentive was employed to activate preparatory incentive mechanisms. Updating legislators' beliefs about the value of federal intervention to provide a consistent approach towards digital signature was necessary to build a stable legal environment for technology vendors to develop prevention technologies. This shows that security threats prevention is more about *chain of incentives* where providing incentives for one actor requires mobilizing other actors first.

Incentivizing others is therefore a complex *process*. While prior security networks literature recognizes the interdependent nature of security (Ogut *et al.*, 2005; Zhao *et al.*, 2013), the research findings reveal that incentives are, in return, interdependent. This finding extends prevalent understanding of incentives that treat them as ready-made structures that just need to be given to others to stimulate certain behaviour (Gal-Or & Ghose, 2005; Gordon *et al.*, 2003; Liu *et al.*, 2014). In this view, incentives are used to mobilize actors (first arrow in Figure 7-1). According to the chain of incentives view, the interdependence between actors make the provisioning of incentives to mobilize one actor requires the intervention of another actor. The latter actor hence needs to be mobilized first in order to offer the needed incentive

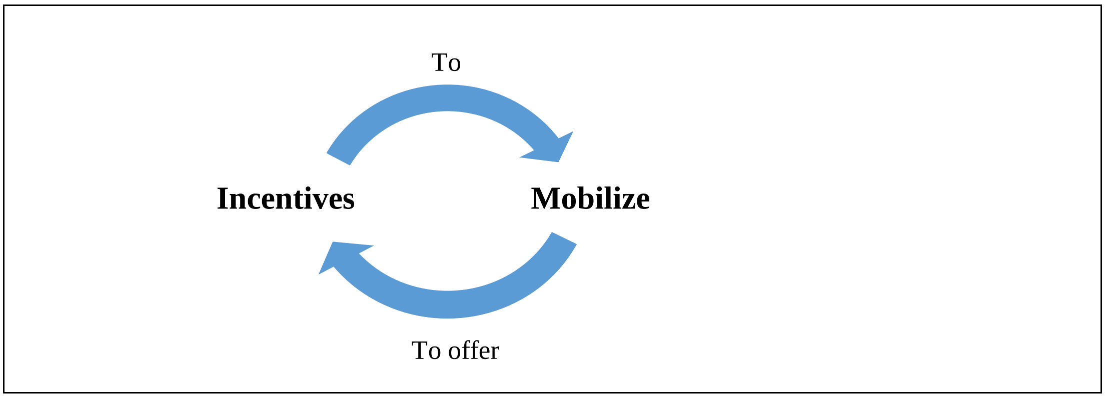


Figure 7-1 *Chain of incentives*

(second arrow in Figure 7-1), which in itself requires the use of incentives and therefore going back to the beginning of the cyclic process. Incentives here become a socially dynamic process rather than a one-time event. Figure 7-1 shows the interplay between incentives and mobilization.

Incentive mechanisms in security networks are more complicated than what is currently portrayed by security networks literature. Another source of complexity arises when considering the networks of organizational relationships. For example, it is assumed that once firms transfer their security risks to another actor through outsourcing or insuring their services, they will have less incentive to invest in security (Zhao *et al.*, 2013). This may not be necessarily true as organizations can have their own security obligations to other actors. Through PCI standards, financial institutions do indeed transfer liability of security breach incidents to non-complying actors, in most cases retailers. Their investments in security solutions however are not lessened since they have obligations under Electronic Fund Transfer Act to protect consumer data. Considering the organization's networks of relationships can reveal *networks of incentives* that are central to achieving security.

Incentive mechanisms are situated and emerge during the prevention process (Archer, 1995). When actors were trying to resolve their dissonance and mobilize others to their goals they had to apply different incentive strategies to meet the nature of the situation and how it was developing. Actors can begin with one form of incentive and in the course of the prevention process moves to another. To illustrate, in automating POS terminal prevention encounter, captive incentives served as the principle mechanism for stimulating actors to propose encoding technologies. However, when later on magstripe was challenged new vocabularies of motives (equality and fairness, locus of security) emerged to cope with the situation. Incentives hence are not fixed because motives and interests change with time, they are rather created during the process by which actors recruit others to perform a particular action.

While incentives are socially constructed, they are at the same time shaped and affected by social structures (Archer, 1995; Fairclough, 2005). Futility and jeopardy rhetorical devices embody the influence of structure in their arguments. Futility recognizes the deep institutionalization of social rules in order to dissuade certain actions and turn the attention to another desired one, while jeopardy achieves the same but by drawing on the value of past structures. Structural relations and historical conditions influence how actors interpret events and how they engage in social encounters.

Accordingly, actors can exist in a constrained context with structures impeding the perusal of certain goals. Laws that do not properly offer appropriate prosecution tools to fight fraud limit law enforcements' involvement in security networks. Transforming pre-existing structures become necessary to provide a proper environment that supports threats prevention. Structures at the same time can be reinforced when they become tools actors draw on when mobilizing others towards a particular behaviour. For instance, actors advocating against a unified authorization system made use of antitrust laws to support their argument. Besides their constraining and enabling effects in creating incentives, structures and incentives might be inseparable. This is in situations where structures have built-in incentives. Financial rewards and penalties for adopting prevention measures were inscribed in technologies developed. Incentives here are not derived from structures but they became part of the structure itself.

Incentives are not constituted of language and communication alone but are also shaped by components of the social system such as the legal and the technological structures. The interplay between discourse and structure during the mobilization process is displayed in Figure 7-2. Structures affect discourse in multiple ways. As a

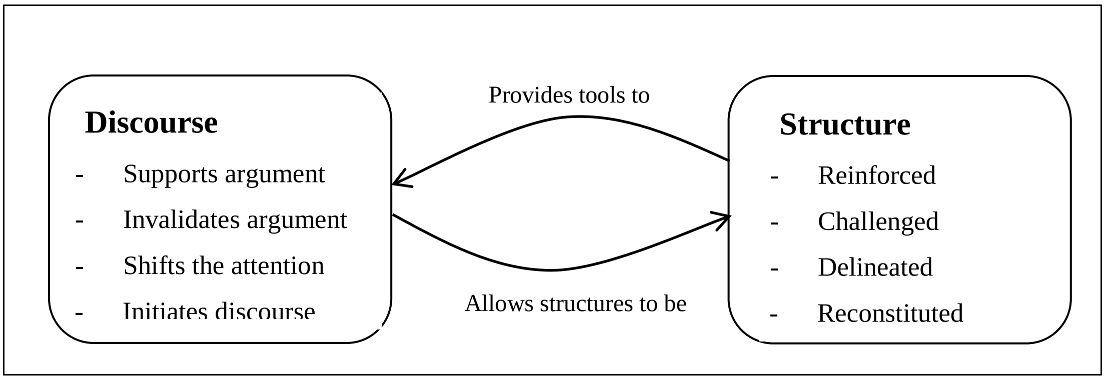


Figure 7-2 *The interplay between discourse and structure in incentive mechanisms*

broader and more general effect they represent tools for constructing arguments and vocabularies of motives which are then used for several purposes. Structures allowed actors to support their arguments, invalidate counter-arguments, shift attention, and initiate prevention communications.

Legislators' role was employed in many prevention encounters to stimulate specific behaviour, especially the role pertaining to encouraging competition and free market. Persuasive discourses focused on how a certain action conflicted with legislators' role in order to support their argument and advance particular security behaviour. Values of fairness and equality in the market also prevailed to support claims. At the other end, actors made use of structures to invalidate assertions. Competition, as a salient market structure, allowed financial institutions to undermine DoJ statement that sharing POS terminals would be anti-competitive by showing how delivery systems do not reside within financial institutions competition area. During mobilization discourse, actors further utilized existing structures to shift attention away from the contested issue. Internal banking procedures for fighting credit card fraud were brought to attention when magstripe security was challenged. Actors argued that security hinges not only on magstripe but the whole payment system including security mechanisms applied in financial institutions. A final impact of structure on discourse lies in its role in initiating it. Inconsistent laws and weak legal infrastructure drove dissatisfaction and instigated negotiations in the network to solve the problem.

As structure influences discourse, discourse in return feedbacks and affects structure. Structural reinforcement takes place whenever actors draw on aspects of the social system during their encounters to support their arguments. Referring to competition and antitrust laws during prevention encounters, for instance, reproduced existing market and legal structures. In certain situations, the discourse aimed to delineate certain aspects of existing structures. Discursive processes to legitimize sharing POS terminals sought to outline the border of competition for financial institutions. At other times, discourse impact on structures is more radical, it challenges existing rules in an attempt to reconstitute them and introduce new rules of conduct. The enactment of new laws is seen to have such reconstitution effect.

Challenging, delineation and reconstitution influences are seen to manifest during novel situations where existing structures hamper innovation. Through them, discourse can overcome structural impediments either by redefining their scope or introducing new ones to serve their interests.

The role of discourse in incentive mechanisms cannot be neglected. In addition to what have been discussed, discourse can be used to revise costs and benefits associated with prevention measures and what would constitute a rational decision. The debates about smart card and magstripe (in the 1980s) show how MasterCard sought through discourse to rework the cost-benefit analysis of the new technology, and the meaning behind its economic infeasibility. In its arguments, MasterCard reinterpreted feasibility to be one that is determined on the long-term not on the short-term as Visa advocated. Taking the expansion in card expiration lifecycle, smart cards can cut costs on the long-run and thus the technology would be economically feasible. Discourse therefore can evoke new meanings for what would be considered a rational behaviour.

A final but important point to mention before moving to the next section is that divergence or failing collective security efforts should not always be seen as a problem of insufficient provisioning of proper incentives or a failure in the communication process to create incentives. Compelling incentives might be offered, however achieving the desired action might not be realized because incentive mechanism’s effect is countered by the exercise of another incentive mechanism. For example, MasterCard offered persuasive evidence of the impact of smart cards in thwarting fraud and one would expect that this would appeal to financial institutions.

However, the presence of counter-mobilization efforts by Visa that stressed on the immaturity of the new technology silenced MasterCard’s incentive strategy. So it is the *interaction* between mechanisms that defines what the end result would be, and hence the actualization of incentive mechanisms is context-dependent.

7.5 The Process Model of Prevention Encounters and Contemporary Security Threats

To substantiate the findings of my research, contemporary security threats such as those arising from innovations in connected cars, wearable technologies, and smart home products[1] are viewed in line with the findings to examine the applicability of the research model in different settings as well as examining how the new cases can inform the research results.

7.5.1 The Case of Connected Cars

Technological innovations are sweeping the automotive industry in efforts to improve the driving experience, reduce fuel consumption and enhance safety. An emergent mode of transport is connected cars. Cars have become connected through various electronic systems such as infotainment and safety monitory tools. Connected cars promise a broad range of benefits from providing information about traffic jams and alternative routes to automatic emergency call upon accidents. However, with opportunities come challenges and connected cars have become the next target for security attacks.

[1] Data for this section has been mainly, but not exclusively, collected from: (FTC workshop on Internet of Things, 2013; Hearing on Internet of Things, 2015; Hearing on Internet of Cars, 2015; Hearing on Examining Ways to Improve Vehicle and Roadway Safety, 2015)

Interests in automotive *cyber* security arose when in 2013 two security researchers, Charlie Miller and Christopher Valasek, demonstrated how they were able to hack a car, disable its braking system and take control over the steering system along with other things (e.g. turn the engine off, honk the horn). More recently, the same researchers wirelessly hacked a Jeep Cherokee through its Internet-connected entertainment system causing Fiat Chrysler to recall 1.4 million vehicles in July 2015. These demonstrations exposed the inapplicability of the current prevention measures (e.g. locks, alarm systems) in ensuring connected cars' security and triggered a need for developing new prevention measures that match the revolution in the transport industry.

Captive incentive mechanism was driving the efforts for proposing prevention measures to fight possible security threats. Connected cars technology opened up new revenue streams for car manufacturers and allowed them to reimagine their business and transform customers' driving experience. However, ensuring the safety and security of connected cars was of paramount importance to build trust in and drive adoption of the new technology. Consequently, several prevention measures were proposed to secure connected cars that differed in their focus (technical, organizational, and legislative). The automobile industry proposed forming an information sharing and analysis center to exchange information and effectively counter threats on a timely basis. Some actors perceived the security of connected cars as a human resource problem and suggested developing automotive cybersecurity programs and degrees to develop the skills and talents needed in this new phenomenon. The National Highway Traffic Safety Administration (NHTSA) solutions for securing vehicle-to vehicle (V2V) communications involved three technologies: symmetric encryption systems, group signature systems, and asymmetric public key infrastructure systems. In their turn, legislators sent letters to 17 major automakers (e.g. General Motors, Ford, Toyota, Honda, Nissan, Volvo, Mercedes-Benz) and NHTSA asking for clarifications on the industry's security efforts. The responses to these letters revealed the different security directions being taken to secure the novel technology and the need to consolidate these efforts, clarify roles and responsibility, and build a national strategy. Accordingly, several bills were proposed to offer an overarching strategy.

In discussing these bills, the heterogeneity of role and the inherited complexity of the legal system enabled resolving dissonance mechanism to emerge. The division of the Congress into two parties; Republican and Democratic incited conflicts among actors (legislators) who acted as challengers and attacked the unilateral process through which the discussed bill was drafted. They argued had bipartisan approach been followed, many of the weaknesses would have been addressed leading to a stronger bill and faster process to achieve security. Other challengers included NHTSA and FTC who aired their concerns about weaknesses in the proposed bill such as assigning more responsibilities to NHTSA without allocating additional necessary funds for the agency to take on the extra work, failing to name an enforcing agency that would ensure car manufacturers compliance with security standards, and setting no minimum requirements for best practices or acknowledging the need for updating them in accordance with emerging threats and technologies. Moreover, defining roles in this emerging technology was itself a challenging task and a source of conflict as different roles were envisaged for various actors. This involved divergent views on whether NHSTA should take a leading role in establishing appropriate security practices and standards or that role should be passed to the private sector. The FTC also revealed concerns about the proposed bill since it undermined its role in fighting improper security practices and argued for a redefinition that would acknowledge the role of the FTC Act in securing connected cars.

The bill further allowed multiple conflicting interpretations of the novel technology. For some (legislators, regulators) it was a threat to the environment since it was associated with carbon emission credits. For others (car manufacturers), connected cars contributed to a cleaner environment. Opponents sought to transform beliefs about the effectiveness of the proposed bill and gain support for their arguments by employing perversity and futility argument. They emphasized the bill’s current security approach does very little in protecting the car and can, in fact, makes it more vulnerable. The bill prohibited all unauthorized access to vehicle data ignoring the fact that security researchers can hack the car for research purposes which contributes significantly in making it more secure. In addition, they argued the proposal of allowing more pollution in exchange for implementing advanced technologies is unnecessary; car manufacturers have already publicly committed to making such technologies (as emergency breaking) a standard feature in new cars, and therefore there was no need to propose this trade-off. Negotiating these bills is still underway[1].

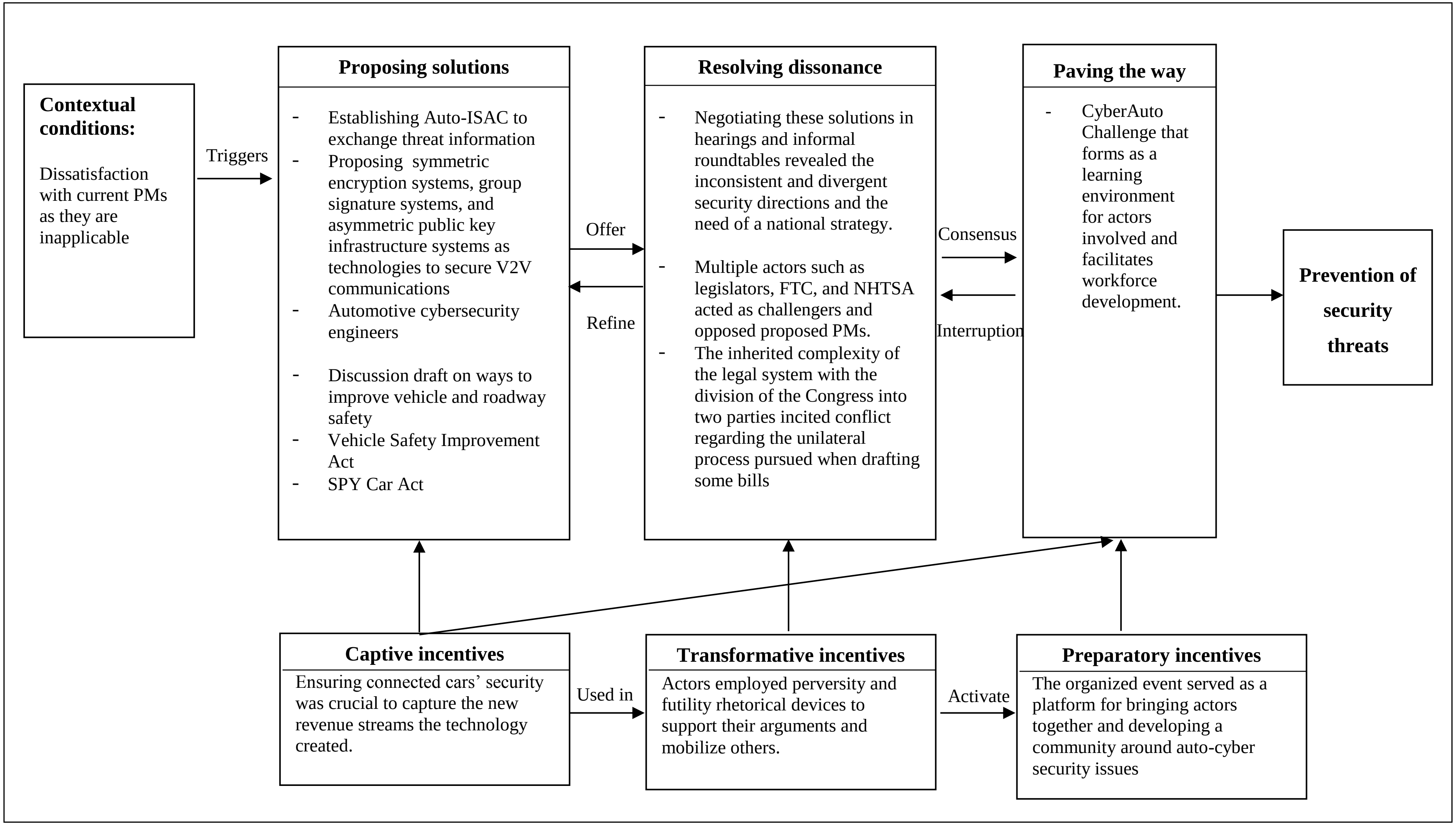
Paving the way mechanism can be seen in auto-specific hackathon such as CyberAuto Challenge that represent an attempt to materialize the proposition for the need of automotive cybersecurity engineers. The event which is held annually brings together automotive engineers, government engineers, students and white hat hackers, and constitutes a learning environment where actors can gain and apply their knowledge and experiment on real cars to identify possible security threats and propose solutions that help in designing more secure cars. The event further provides an opportunity to expose current engineers to the cyber community and develop interest around auto-cyber security issues (preparatory incentive).

Figure 7-3 applies the process model on connected cars case.

7.5.2 The Case of Wearable Technologies

As with the case of connected cars, the research community played a key role in raising the attention to the lack of effective prevention measures for securing wearable technologies. In 2008, academic researchers demonstrated how they were able to attack a defibrillator and change its operations. In 2010 and 2011 researchers illustrated how attackers can intercept insulin pump signal and change the blood-sugar level read on the device alarming the person to adjust their insulin dosage which can be fatal over time. Furthermore, a report by the Government Accountability Office showed the lack of attention towards wearables' cyber security.

[1] There was not sufficient data to show evidence of resolving dissonance mechanism for the other proposed solutions. I should note that data availability constrained evidence of the prevention and incentive mechanisms in this case as well as the next two cases.



Contextual conditions:

Dissatisfaction with current PMs as they are inapplicable

Proposing solutions

- Establishing Auto-ISAC to exchange threat information
- Proposing symmetric encryption systems, group signature systems, and asymmetric public key infrastructure systems as technologies to secure V2V communications
- Automotive cybersecurity engineers
- Discussion draft on ways to improve vehicle and roadway safety
- Vehicle Safety Improvement Act
- SPY Car Act

Resolving dissonance

- Negotiating these solutions in hearings and informal roundtables revealed the inconsistent and divergent security directions and the need of a national strategy.
- Multiple actors such as legislators, FTC, and NHTSA acted as challengers and opposed proposed PMs.
- The inherited complexity of the legal system with the division of the Congress into two parties incited conflict regarding the unilateral process pursued when drafting some bills

Paving the way

- CyberAuto Challenge that forms as a learning environment for actors involved and facilitates workforce development.

Prevention of security threats

Captive incentives

Ensuring connected cars' security was crucial to capture the new revenue streams the technology created.

Transformative incentives

Actors employed perversity and futility rhetorical devices to support their arguments and mobilize others.

Preparatory incentives

The organized event served as a platform for bringing actors together and developing a community around auto-cyber security issues

Figure 7-3 *The application of the process model in the case of connected cars*

These strong pieces of evidence of the possibility of penetrating wearable health devices and posing threats to human life triggered actions to develop better prevention measures for wearable devices. Driven by the captive incentives of the new technology such as improving health and empowering patients, and new business opportunities that would facilitate better personalized services such as insurance plans and premium discounts offers, actors engaged in proposing different solutions that can enhance the security of wearable technologies. Technical solutions such as encrypting the data stored in the devices and while in transit, use of passwords, biometric and smartcard to limit unauthorized access, were proposed. Other actors focused on legislative solutions emphasizing that mobile health applications are not governed by Health Insurance Portability and Accountability Act (HIPAA) and wearables are not subject to security breach notification laws. Companies therefore have no legal obligation to make public disclosure of hacking incidents. Others proposed a more engaging role of regulators as the FTC and suggested the agency should organize a multi-stakeholder group with the mission of building a code of conduct to protect wearables' security.

The heterogeneity of actors involved in wearable technologies enabled resolving dissonance mechanism to emerge. Because actors vary in their interests, some of them challenged the proposed solutions. There was a clear tension between the need to ensure the usability of these devices and the need to secure them. Some actors did not favour technical measures that obliged the use of passwords to protect these devices and the data they contain. They argued that physicians did not favour them either because they saw them as an obstacle towards using the devices and therefore improving patients' health. Furthermore, others challenged the belief that publicly announcing breaches on wearable devices would make consumers more aware of the risk involved in this technology as they believed that consumers have become "alert fatigue" and accustomed to continuous hacking incidents (futility argument). The negotiation process also involved attempts to mobilize legislators in securing wearables by stressing that regulatory barriers and outdated laws were impeding not supporting the advancement of healthcare innovations (perversity argument).

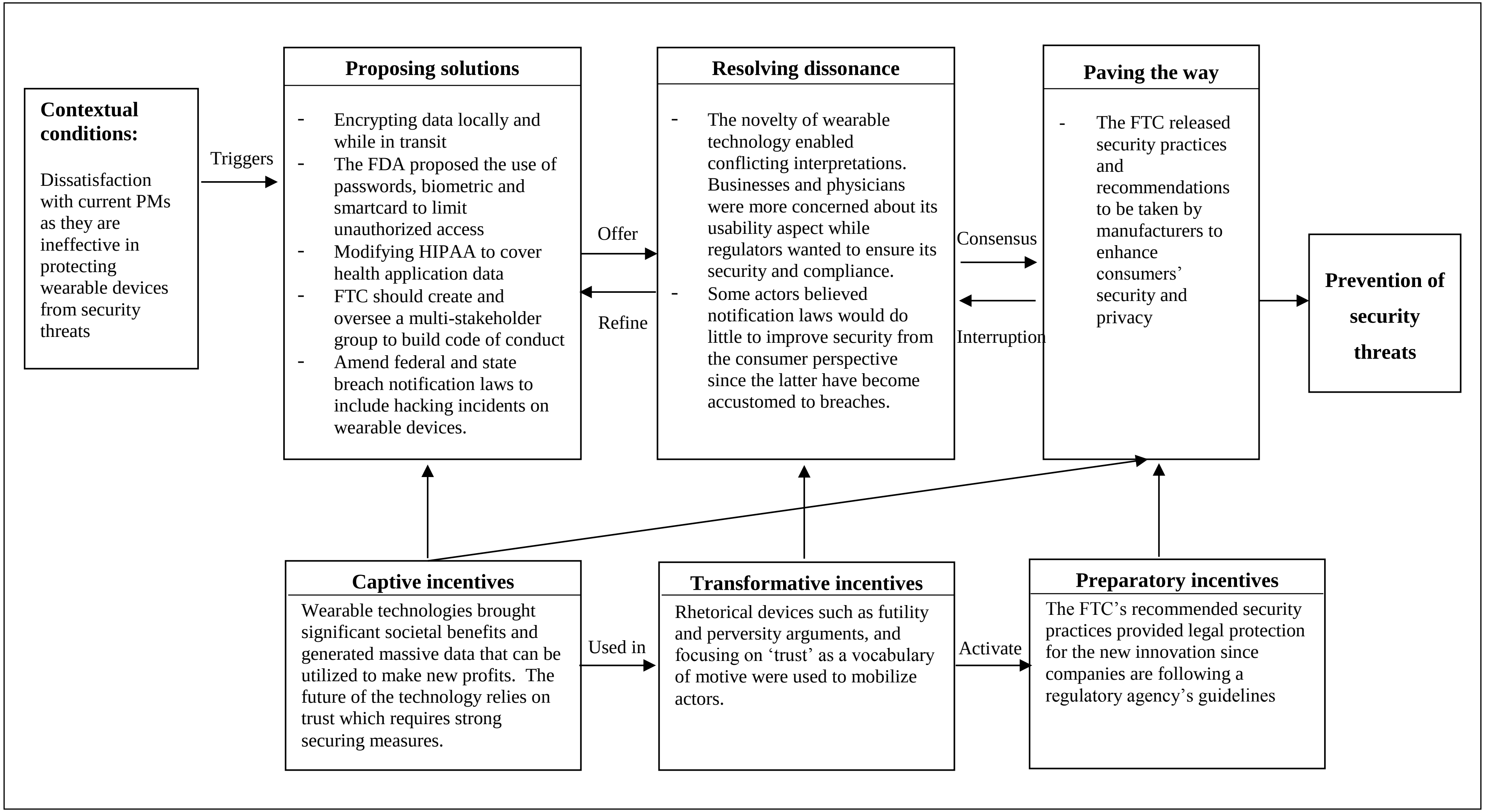
Securing wearable technologies is in its early stages, actors are still finding their way on the best means to ensure security, and most of actors' encounters lie in proposing solutions and resolving dissonance prevention mechanisms. Nonetheless, the FTC's release of security practices and recommendations to be taken by manufacturers can be seen as an attempt to introduce some legal certainty that can protect the new innovation from legal liability because it ensures companies that they are following reliable and trusted guidelines suggested by a regulatory agency.

Figure 7-4 applies the process model on wearable technologies case.

7.5.3 The Case of Smart Home

Attention to the security risks associated with smart home technology was drawn when in January 2012 hackers exploited a vulnerability in TRENDnet IP camera and spied into users' homes exposing the private lives of hundreds on the internet. Following this practical evidence, efforts to secure the technology took place.

Actors started proposing different solutions as security was inevitable to build trust and confidence, and realize the business opportunities and societal benefits the novel technology offers. Smart home products increase efficiency, reduce costs, improve convenience and allow data monetization (captive incentives). Actors however differed in how they interpreted the technology and this was reflected in the type of prevention measures they proposed. Some opted for technical solutions such as applying better security standards (such as ZigBee and Z-wave) in wireless home network. While others focused on the importance of organizational approaches as well technical ones. They saw the problem rising from the fact that most of the companies that offer smart home products were not expert in security. Accordingly, their suggestion was a change in organizational structure and hiring policies to recruit security experts in order to build more secure products. Another proposition was consumer-focused and suggested that educating consumers and creating awareness of the security risks associated with the technology can help in preventing attacks.



Contextual conditions:

Dissatisfaction with current PMs as they are ineffective in protecting wearable devices from security threats

Proposing solutions

- Encrypting data locally and while in transit
- The FDA proposed the use of passwords, biometric and smartcard to limit unauthorized access
- Modifying HIPAA to cover health application data
- FTC should create and oversee a multi-stakeholder group to build code of conduct
- Amend federal and state breach notification laws to include hacking incidents on wearable devices.

Resolving dissonance

- The novelty of wearable technology enabled conflicting interpretations. Businesses and physicians were more concerned about its usability aspect while regulators wanted to ensure its security and compliance.
- Some actors believed notification laws would do little to improve security from the consumer perspective since the latter have become accustomed to breaches.

Paving the way

- The FTC released security practices and recommendations to be taken by manufacturers to enhance consumers' security and privacy

Prevention of security threats

Captive incentives

Wearable technologies brought significant societal benefits and generated massive data that can be utilized to make new profits. The future of the technology relies on trust which requires strong securing measures.

Transformative incentives

Rhetorical devices such as futility and perversity arguments, and focusing on 'trust' as a vocabulary of motive were used to mobilize actors.

Preparatory incentives

The FTC's recommended security practices provided legal protection for the new innovation since companies are following a regulatory agency's guidelines

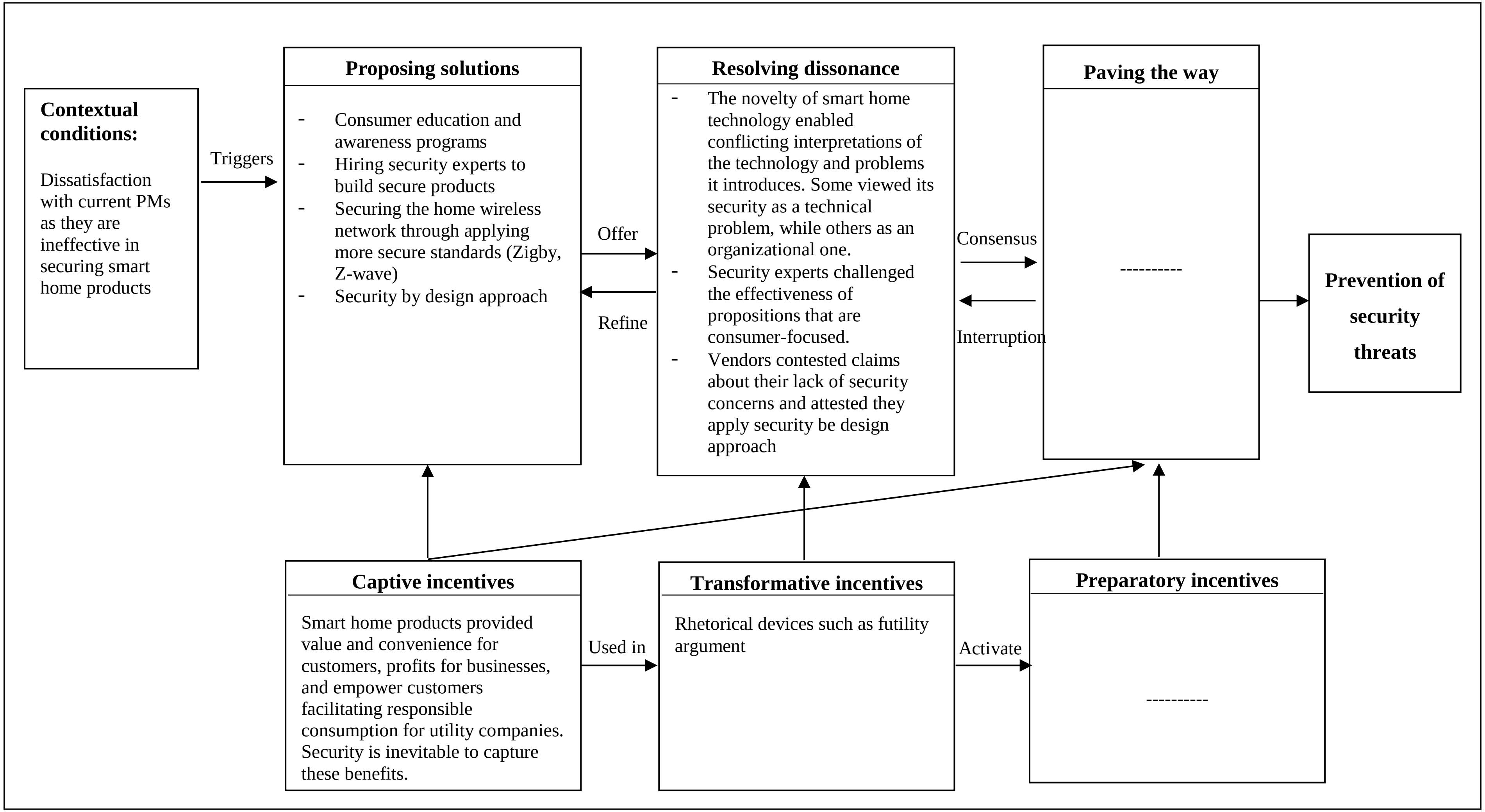
Figure 7-4 *The application of the process model in the case of wearable technologies*

Resolving dissonance mechanism emerged from the diverse views on how smart home technology can be secured. With multiple interpretations of the novel technology and the security problems it introduced (technological novelty), actors challenged some of the proposed solutions (heterogeneity of role). Some believed that the proposition to focus on consumers to attain security through education and awareness programs would achieve very little (futility argument). They supported their claim by drawing on computer security field where immense efforts had been undertaken to educate users, and still security problems remain. For those actors, the real problem lied in the products and the fact that manufacturers themselves do not understand the technology and its security implications. They argued that building strong security requires considerable computing power and storage capacity which significantly consume energy lowering the product’s battery life. Vendors, who aim for value and convenience, therefore do not take security seriously and tend to rely on the security of the home network to prevent threats. In their view, securing smart home technology should start from the vendors who ought to be more responsible and develop expertise in security. Vendors agreed that there is a trade-off between convenience and security. Nonetheless, they refused to be seen as passive and considering security as an afterthought. They contended security by design approach is followed and many devices work only within acceptable parameter ranges making the products more secure.

Figure 7-5 applies the process model on smart home case.

Taking these cases collectively demonstrates and confirms the importance of evidence in gaining *attention* to security and in triggering prevention encounters. Furthermore, the process model reveals that prevention encounters in security networks are dispersed and ramified to cover diverse security aspects: developing required talents, developing technical prevention measures, changing organizational processes, developing industry and government regulations, and enacting and updating laws. While having their own objective, these encounters are nested within one another and interrelated; talents and skills are needed to develop technical solutions, organizations should change their processes to attract new talents and respond to new regulations, regulations are developed to offer best security practices, and laws are enacted to facilitate innovation in prevention measures and ascertain accountability. Actors engage in different encounters and thus become part of various security networks where they move freely between them, making security networks loosely coupled (see Figure 7-6).

Security networks vary in their structure and objective, and they therefore act at a different pace. To give an illustrative example, security networks involved in developing skills and talents in cyber-auto security, such as CyberAuto Challenge is expected to take less time than legislative security networks that aim to support the security of connected cars through enacting laws. In the latter, the case showed that the security aspect of the technology was crowded out by many other issues such as environmental safety, the privacy of collected data, and recall notices that supported conflict between actors and prolonged the prevention process. Consequently, for collective security efforts to be more efficient it has to be *focused*. Taking dedicated steps towards achieving security yield faster results than trying to incorporate security along with other matters. This was seen in strengthening the legal system prevention encounter in preventing credit card fraud where actors advocated segregating computer fraud problems from credit card fraud and addressing those specifically related to the latter. This focus increased the pace of security networks and allowed the new law to be enacted in a shorter time span.


Contextual conditions:
Dissatisfaction with current PMs as they are ineffective in securing smart home products
Triggers
Proposing solutions
- Consumer education and awareness programs
- Hiring security experts to build secure products
- Securing the home wireless network through applying more secure standards (Zigby, Z-wave)
- Security by design approach
Offer
Refine
Resolving dissonance
- The novelty of smart home technology enabled conflicting interpretations of the technology and problems it introduces. Some viewed its security as a technical problem, while others as an organizational one.
- Security experts challenged the effectiveness of propositions that are consumer-focused.
- Vendors contested claims about their lack of security concerns and attested they apply security be design approach
Consensus
Interruption
Paving the way

Prevention of security threats
Captive incentives
Smart home products provided value and convenience for customers, profits for businesses, and empower customers facilitating responsible consumption for utility companies. Security is inevitable to capture these benefits.
Used in
Transformative incentives
Rhetorical devices such as futility argument
Activate
Preparatory incentives

Figure 7-5 *The application of the process model in the case of smart home*

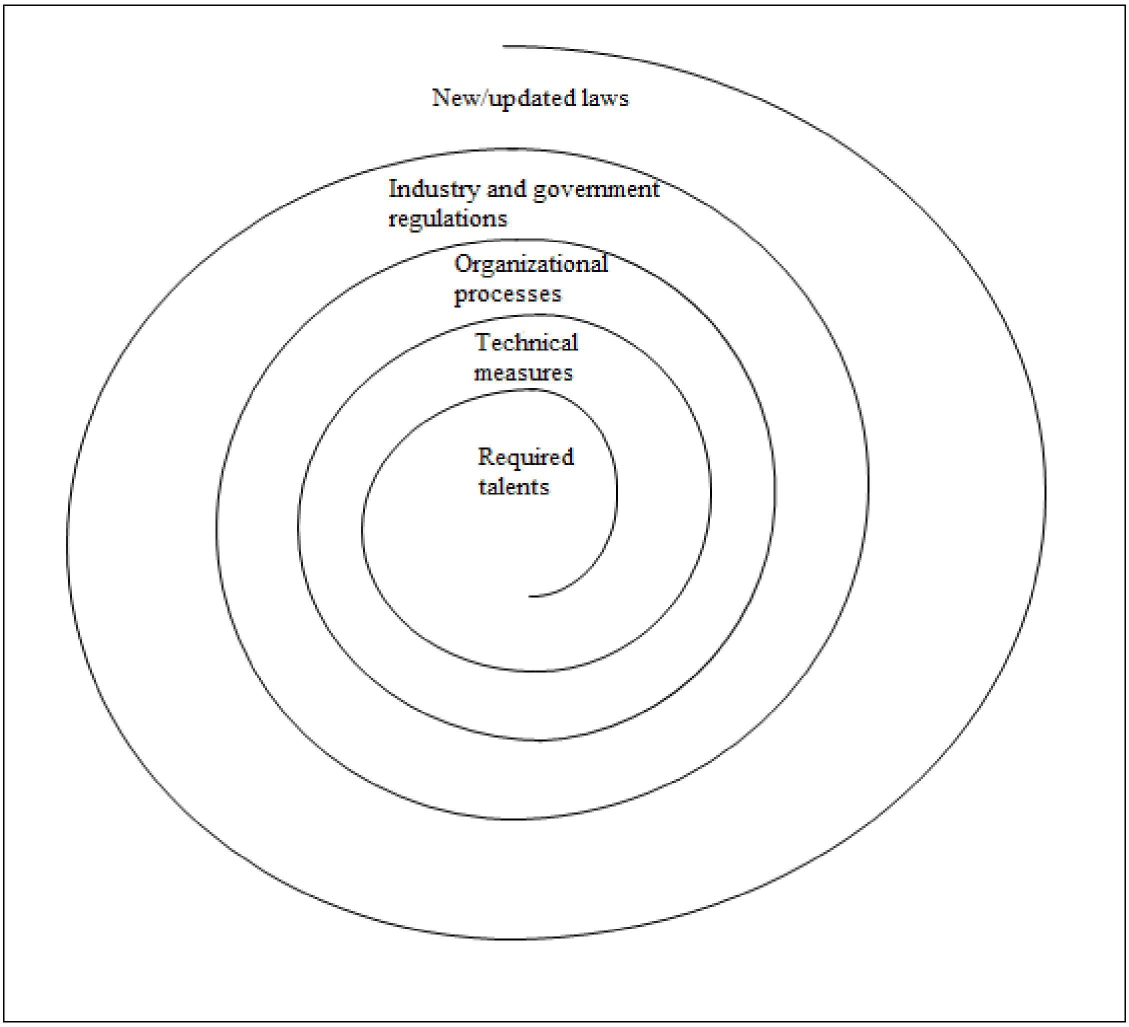


Figure 7-6 *Nested and loosely coupled security networks*

7.6 Summary

This chapter has discussed the research findings in relation to the current literature on security networks. Tracing the causal chain of events occurring while preventing credit card fraud revealed the dynamic and interactive nature of the work processes of security networks. The in-depth analysis of security networks allowed drawing new insights on security threats prevention process and identified elements of importance in these networks that inform and extend knowledge derived from analytical models emphasized by the previous literature. Entities such as the legal system and prevention technologies along with their distinctive properties play a crucial role in enabling the emergence of prevention mechanisms. This chapter further showed how economic incentives alone are not sufficient for converging actors in security networks and how they form part of a larger form of incentives referred to herein by captive incentives.

Finally, contemporary security threats related to the internet of things were discussed through the research lens and proved the applicability of the research model to cybercrime threats. In the next chapter, theoretical and practical implications are described as well as limitations and avenues for future research.

8 IMPLICATIONS AND CONCLUSIONS

8.1 Introduction

The process model of prevention encounters with its underlying prevention and incentive mechanisms provides a detailed explanation of how security networks achieve prevention. The aim of this chapter is to discuss the theoretical and practical implications of the findings of this research. Avenues for future research are explored along with the limitations. Finally, I end with the conclusion.

8.2 Implications for Theory

Previous literature on security networks focuses on causal effects in understanding how certain factors such as security investments, competition, vulnerability disclosure mechanism, and reward/penalty structure in outsourcing contracts affect security behaviour. This research contributes to the existing knowledge of collective security efforts by moving beyond examining *effects* to studying *mechanisms* underlying security networks. That is moving from studying the relationships between *variables* to those between *actors*. This focus on *qualitatively* tracing the causal chain of events in preventing threats is of great importance since it provides a detailed analysis of prevention *processes* and adds the significant element of context when explaining collective security efforts. By this, this research offers useful and deep insights that can enrich the previous literature with its quantitative and analytical models research approach. Explicating prevention mechanisms in security networks can strengthen quantitative research in multiple ways. They can help in explaining anomalies in observations quantitative models cannot justify (Helper, 2000). In addition, they can identify important factors that are often difficult to capture in standard economic thinking (Starr, 2014). For example, this research showed the important role of values such as fairness and equality in driving convergence on a particular prevention measure. Moreover, the qualitative approach can offer guidelines for future research by shedding light on important elements to account for when building quantitative models. For instance, the literature on information sharing alliances examines the relationship between information sharing and security investments and shows that organizations tend to shift their defence line to more information sharing when the cost of security investments increases (Gordon *et al.*, 2003; Hausken, 2007). Deep analysis of security networks' prevention efforts revealed that it is the effectiveness of the prevention measure that influences the adoption of alternative solutions rather than merely its high costs. That is actors are willing to incur high investments in security if these are likely to offer better security and move to adopt another when the prevention measure is ineffective. This is evident in merchants and legislators questioning the effectiveness of PCI standards in thwarting credit card fraud despite the substantial investments that have already been made to comply with the standards and their calls for adopting another more effective prevention measure. This suggests that the effectiveness of security measures is an important element to consider by quantitative researchers when designing their models. Furthermore, preventing threats is path dependent and security investment decisions, along with other security decisions, are not divorced from the past. The research showed how moving to smart cards, although promised a reduction in fraud levels, was hindered by the industry's past investments in magstripe. Security decisions are not influenced by current strategies alone but also past experiences and their impact on how the present is interpreted and how decisions are made should be acknowledged.

This research extends existing understanding of security networks by offering a process model that explains how security networks achieve prevention. By incorporating incentive mechanisms that are necessary to hold the network together, the model reveals the conditions under which diverse interests are likely to converge contributing to the durability of the network. The model shows that preventing threats is full of encounters between security network's actors. Collective security effort is thus not a smooth process as currently portrayed; it is best described as one that entails a combination of *both* conflict and cooperation. Conflict because of the rival opinions and competing interests of the networks players, while cooperation because actors realize that individual pursuit to achieve security is not enough and they need to work collectively with others to attain security. The model makes clear the multilevel dynamics of threats prevention where multiple security networks exist and interact with one another to achieve security. Those networks operate at different levels (e.g. individual, organizational, legal) but their constituent actors can travel across these levels distributing knowledge and facilitating collective security. The process model thus helps us view security networks as nested and loosely coupled formations. This should contribute to better adaptation with the constant emergence of new security threats.

Prevention measures are not carved in stones, and future security paths are not known a priori. In searching for ways to resolve dissonance, actors engage in negotiations that may result in the emergence of new prevention measures. This emphasizes the fact that there is no one best method for preventing a certain security threat. However, unlike prior literature that mainly reasons this to actors' rational behaviour (Cavusoglu *et al.*, 2007) this study shows that there is no standard optimal method because of the continuous conflict in the network that makes it difficult for actors to collectively agree on the prevention measure. The research gives a fine-grained analysis of the causes of such dissonance that surpass rationality and self-interest while acknowledging their importance. The structure of security network, that is its constituent elements, is a main source of conflict that should be taken into consideration. The research findings highlight the role of technological novelty and complexity of the legal system in initiating disagreements and multiple interpretations about prevention measures and which one to adopt.

Another important contribution of this research is introducing the concept of prevention encounters to examine security networks. Researchers that tend to study collective actions usually start by having an existent network or organization to investigate. In security networks, those can be information sharing alliances or vulnerability disclosure networks. Although valuable, with such conceptualization of security networks opportunities for capturing the formation of the network and why it was created can be missed. Examining the phenomenon with pre-determined dimensions of interests assumes researchers already know what is important and worthy of investigation and can result in not only failing to recognize key events that greatly influence future path of security networks but also eliminating the important role of emergence and surprise in explaining social phenomenon (Tsoukas & Chia, 2002). Prevention encounters concept shifts the focus from the network per se towards actors' *actions* that would collectively form the network. It will allow us to unpack the black box of security networks and gain a deeper understanding of the phenomenon including conditions for their emergence and durability. Furthermore, changes that are likely to result in a departure from standard means of achieving security provide better chances for capturing collective security efforts since their impact would ripple through a wide range of actors who will then constitute the network in order to take action. Prevention encounters therefore, with its focus on critical change opportunities, represent an excellent manifestation of collective security efforts and can serve as a useful foundation for future work on security networks.

The paucity of empirical studies is a key shortcoming identified in the previous security networks literature (Arora *et al.*, 2008; Gal-Or & Ghose, 2005; Gordon *et al.*, 2003; Kannan & Telang, 2005; Ransbotham *et al.*, 2012). This research empirical study on credit card fraud answers calls for a need for empirical evidence. Drawing findings from examining real-life events increase the value of the research since the results would be seen more representative (Piore, 2006). Moreover, the insights drawn from this empirical research can boost quantitative research explanatory power since "Unless there is such correspondence between model and reality, the analysis will only offer an as-if story of little or no explanatory value" (Hedstrom, 2008, p.330-331).

Collective security efforts is an incentive-related process, whereby offering the proper incentives is crucial for maintaining security networks. A significant contribution of this study lies in breaking away from a homogenous view on security networks and the underlying incentives to recognizing the heterogeneity of actors involved where motivating one using a certain incentive might not have the same impact on another. The research identifies three forms of incentive mechanisms that have a pivotal influence on motivating collective security efforts and cater for actors' various needs.

Transformative incentive mechanism recognizes the role of beliefs in motivating behaviour. By changing beliefs to be aligned with the desired actions, actors can recruit others to meet a particular goal. Transforming beliefs is attained through employing different rhetorical strategies. The research illustrates the role of perversity, futility and jeopardy arguments in challenging current beliefs and establishing new ones. Moreover, the use of vocabularies of motive can help in encouraging collective security.

Market forces in terms of price, demand, and competition are identified in security networks literature as critical incentives in driving security behaviour (Arora *et al.,* 2008; Cezar *et al.,* 2010; Gal-Or & Ghose, 2005). These are certainly of value however this research revealed that their effect should not be taken for granted. The case showed that in order for market mechanisms (such as competition) to exert their power, they need to be enabled. That is preparing the environment for their activation. This research shed new knowledge on the effect of market mechanisms as incentives through identifying preparatory incentives as a pre-stage that is required for the motivating influence of market mechanisms to take place. The research identified two preparatory incentives: legal certainty and operational certainty. Gal-Or and Ghose (2005) argue for the need to address the role of government intervention in providing incentives to encourage collective security efforts. Besides common incentives that come in the form of subsidies and tax benefits, this study shows that policymakers can intervene to provide legal stability that protects security investments and fosters innovation in developing better security products. The other means identified to prepare the environment is providing operational certainty. In here, mobilizing actors in security networks hinges on empowering them with tools that delineate future security path. By this, preparatory incentive mechanism departs from the current understanding that actors always need incentives to contribute to security networks. This study shows that the interests of the actors and the network can be aligned. The types of incentives needed at this condition are ones that boost actors' interests and remove roadblocks in the way. Therefore, elements of the environment should not be neglected when designing incentive structures.

Finally, captive incentives incorporate the current literature emphasis on financial penalties and rewards but extends that to demonstrate that the power of captive incentives lies in its ability to act as an obligatory passage point (Callon, 1986) for actors to reach their interests, and monetary incentives are only one mean to achieve this. Provoking shared future vision and common national interest and tying those with the desired security behaviour proved effective in mobilizing actors in security networks. This finding provides a possible explanation of why actors would join security networks though the benefits the network offers do not justify such a decision.

This research extends current understanding of incentives as end products by showing how a complex *process* incentivizing can be. Actors need to be continuously motivated to perform the desired action. Moreover, interdependence between actors makes incentives in return interdependent. The research introduced chain of incentives concept to reflect this interdependence where providing incentives for one actor requires mobilizing other actors first. Incentives here become a socially dynamic process rather than a one-time event. What comes of importance as well is acknowledging inter-organizational relationships that can make incentives stem from numerous sources in which actors become involved in networks of incentives. Having this notion in mind help us realize that shifting security liabilities to other actors does not mean that incentives to have proper security measures are diminished. This is because actors are motivated to retain a positive security attitude through their obligations to other stakeholders in their network.

Besides contributing to the security networks literature, the three incentive mechanisms identified, particularly transformative incentive, offers valuable contributions to the literature on behavioural IS security. This literature advocates that users are the key element in protecting organizations against security threats, and therefore there is a need to identify factors that will increase their compliance with information security policies and procedures. In achieving this, research into behavioural security draws on various theories such as deterrence theory, protection motivated theory, theory of planned behaviour, and rational choice theory to derive insights into the effective development of security training and education programs. For example, by mapping volitional security behaviour (e.g. legitimate email handling, account protection) with dimensions of criticality, promotion difficulty, and degree of common sense, Posey et al. (2013) offer a taxonomy of protection-motivated behaviour that provides details on types of behaviour that should be prioritized during security training programs. Puhakainen and Siponen (2010) stress the significant role of cognitive processing in motivating desired security behaviour. They argue that security education programs should be designed to account for users' prior knowledge in order to activate their cognitive processing capabilities. Moral reasoning (Myyry *et al.*, 2009) and beliefs about the costs and benefits of compliance and non-compliance (Bulgurcu *et al.*, 2010) were also seen to influence user's compliance behaviour and so such consequences should be reinforced in security awareness programs. The use of fear appeals (threat messages) further influence users' compliance given the severity of the threat, the susceptibility of being a victim, and personal efficacy in mitigating the threat (Johnston & Warkentin, 2010).

In summary, the current literature on behavioural IS security emphasizes the role of security education and training programs in increasing compliance with organizations' security policies, and offers recommendations to be taken into consideration when designing these programs. This research provides a contribution in this respect and offers an alternative theory, rhetoric, for motivating security behaviour and driving compliance. The role of beliefs in driving compliance is acknowledged in the literature (Bulgurcu *et al.*, 2010). This research suggests the use of different rhetorical arguments to persuade users by questioning their current beliefs about compliance with security policies and then transforming them from negative or neutral ones to positive ones. Perversity, futility and jeopardy bring to light the interactive nature of security and help us understand how achieving compliance is a two-way communication process. While the need for persuasive communication and providing justifications to motivate security behaviour have been implied in the literature (Siponen, 2000), this is often portrayed as a one-side relationship, often a one-way communication from the organization's part, neglecting how employees would react to compliance efforts. The use of rhetorical devices is not limited to educators in security training programs, they are open for everyone to use including employees who can employ them to counter presented arguments. The value of rhetoric stems from its ability to give voice to users through competing discourse. It therefore provides a better picture on the reciprocal interactions between employees and educators in security management programs. This open nature draws attention to the importance of employing more than one rhetorical device to strengthen the argument presented which should increase the probability of transforming users' beliefs. It also caters for the individual differences between users where one might be affected by a particular persuasive strategy rather than another.

Besides the three rhetorical devices, this research suggests the use of vocabularies of motive as another rhetorical tactic that can be applied to motivate compliance. Careful use of language when communicating security policies and selecting vocabularies that are more likely to have an impact on employees' psychology can enhance compliance rates. The case shows that vocabularies of motive are situational because motives themselves are situational. Actors in prevention encounters behaved in a particular way because of the peculiarities of the context they found themselves in. Motives therefore cannot be separated from their contextual conditions and the latter should be accounted for when seeking mechanisms to increase users' compliance.

While the extent literature has researched different means to motivate users to comply with information security policies, which indicates that users are not self-motivated to comply, this research revealed that this might not necessarily be true. Preparatory incentives are evident to have a significant role in achieving security. In here, the environment must offer support for users' volitional compliance efforts. Employees that acknowledge the importance of not sharing account details, for instance, are unlikely to conform to this security procedure in an environment that places task completion a top priority. Pre-existing structures influence users' actions and in situations where they act as constraints they have to be modified to enable the realization of desired actions.

8.3 Implications for Practice

This research offers a number of practical implications. The prevention encounters process model helps practitioners understand how threat prevention in security networks take place. Knowledge of prevention mechanisms is valuable because it allows intervention to improve the process and gives insights on what needs to be done to make it more efficient and productive. The model shows how the prevention process is full of contestations where actors' interests change during interactions. Accordingly, when participating in security networks, organizations must be flexible and move away from having a rigid security agenda. They should be open to and expect alternative views on future security practices. As prevention is a political process, actors ought to recognize that it would be unlikely to reach agreement on a solution that would satisfy all actors. Compromise and tuning interests are necessary to keep collective prevention efforts alive and sustain the network.

The model further shows that prevention processes undergo interruptions that prolong security efforts and increase organizations' susceptibility to security threats. Organizations can avoid this by identifying the causes of interruptions and address them before they occur in order to allow a smooth pursuit of collective security efforts. This research identified two sources for interruptions: legal and operational uncertainty about prevention measures. An important issue for organizations is to ensure the legal legitimacy of their prevention measures. Prevention measures that are susceptible to antitrust laws (or any other law) can disrupt prevention efforts if such legal threat is practiced. Organizations can seek legal authorities' support of their security product to protect it against future complexity. Providing legal certainty has an implication for policymakers as well. As my study illustrated, legal fragmentations towards prevention technologies can hinder investments in these technologies as fragmentation increases risk and compliance costs. Policymakers can encourage technological innovation through clear and integrated laws and enacting ones that protect actors' security investments. Moreover, since both technology and security threats keep evolving, laws should be technologically neutral to promote innovation and retain their adaptability to changing contexts.

The research further demonstrated that the absence of operational certainty in terms of foundational tools for future security efforts hindered the prevention process. The responsible actors (whether policymakers or organizations) should recognize the significance of these tools and work to empower actors with laws and security standards that facilitate their involvement in security networks.

Practical implications for designing security training, awareness and education programs can also be drawn. Perversity, futility and jeopardy arguments offer a strong foundation regarding the *content* of these programs. These programs should communicate appropriate messages to users by stressing, for example, how their reckless security behaviour while seen simple, such as sharing passwords, does not only constitute a threat to the organization's image and profitability but will also extend to jeopardize employees' job security and stability. At the same time, management should be aware of how their security efforts are perceived by employees. If despite great investments in security products and security management programs the organization is still facing considerable security breaches, it would be unlikely that employees would see any value of these security efforts, and therefore their compliance is expected to decline.

In a similar vein, practitioners can benefit from the concept of vocabularies of motive and use ones that are likely to influence behaviour. This implies that they must have knowledge of the organizational culture and their audience in order to be able to intelligently select suitable vocabularies. This strategy can involve *naming* users' act, for example as shameful or unethical to dissuade undesired behaviour. By this, certain vocabularies become woven with certain behaviours that should ultimately drive better security.

In addition, while the focus on employees' behaviour and modes of motivation is certainly crucial to attain security, management should not always assume that employees *need* to be motivated. Research shows that employees can be a valuable resource for maintaining security (Hedstrom *et al.*, 2011; Spears & Barki, 2010). This research revealed ensuring that the organizational environment supports security efforts is another area that deserves management attention. Managers should design the organizational structure in a way that foster security and be compatible with the organization's security requirements mandated in its security policy. For instance, reporting relationships with regards to security issues must be clearly stated, regular updates for security programs should take place, and security checks should be incorporated into functional tasks. Moreover, since preparatory incentive requires changes in the environment to facilitate desired security behaviour, organizations ought to maintain a flexible structure that would allow such changes.

Another practical implication lies in captivating compliance with users' interests. This supports the literature that recognizes the role of rewards and punishments in motivating conformity with security policies. For example, managers can tie yearly appraisal with adherence to security policy. Practitioners however should utilize captive incentives more and look beyond financial gains or penalties. Focusing on higher goals and visions and joining them with proper security behaviour might result in better outcomes that extend achieving security. Informing project leaders, for instance, that access to needed resources is conditioned on following security procedures by team members, not only enables the organization to encourage better security behaviour but also helps it achieve its goals. Naturally, continuous monitoring to ensure security guidelines are being followed is necessary to maintain the incentive’s power (in this example).

8.4 Limitations

As with any other, this research has its own limitations. First, the use of a single case study of credit card fraud places limitations on the generalizability of the findings to other types of security threats. Nonetheless, generalizability according to critical realism is not defined by the ability to apply the findings to other empirical domains but it is more about the ability to go beyond description and delve more in depth to identify mechanisms and contingent conditions that activate these mechanisms (Tsoukas, 1989). The examination of eight prevention encounters in credit card fraud prevention helped in providing this in-depth understanding of the phenomenon and identifying enduring mechanisms that better explain the prevention process and the contingent conditions that facilitate transposing the research model to other settings. The aim hence is not generalizing from sample to population but from case findings to theory in order to offer rich insights on how security threats are prevented (Lee & Baskerville, 2003). As generalizability to other settings is best achieved by actually examining the theory under new settings (Lee & Baskerville, 2003), I have applied the process model on three different contexts and showed how it was able to shed light on cybercrime prevention processes as well.

Another limitation pertains to the fact that this research is a document-based one where no interviews were conducted to collect the data. Although collecting data using different methods is important to facilitate triangulation, Denzin (1989) explains that this is only one strategy for triangulation. Data triangulation is another strategy where triangulation is achieved through collecting data from different sources (using the same method); this includes collecting data at different points in time as well. Accordingly, although methodological triangulation was not accomplished, collecting data on prevention encounters at different times and the use of multiple types of sources (books, trade journals, government documents, newsletters) helped me obtain data triangulation.

Moreover, given the historical nature of the research, documents represent the main and logical sources of data (Marwick, 2001; Mason *et al.*, 1997a). Documents (public sources) are more objective as the researcher has no influence on the data collected. Also, many of the documents I used, especially congressional hearings, can be defined as noninentional social documents (Rowlinson *et al.*, 2014) that are not exposed to subjective distortion as they represent direct reporting of discussions without any external interference (Alvesson & Skoldberg, 2009). Although I was not directly involved in collecting the data, I had an influence in interpreting it, where new meanings and understanding could have been assigned to the events taking place in maintaining the security of credit card transactions, which may go beyond the scope of the evidence. I tried to mitigate this interpretation bias by remaining close to the evidence.

A crucial element in my study was gaining knowledge of the exact time of events and their sequence. Public sources signify excellent resources for establishing timeline of key events as it is common for interviewees not to remember exact dates (Mason *et al.*, 1997a). Accordingly, public sources can be seen more reliable for gaining retrospective knowledge since interview data is more susceptible to recall errors such as selective reporting of events whether intentionally or unintentionally (Glick *et al.*, 1990). Capturing early prevention encounters would thus be difficult using interview data which would result in significantly limiting the prevention encounters examined. The historical analysis of documents facilitated the identification of eight prevention encounters which helped me in building a stronger theory.

Third, security networks are complex and can include large numbers of actors. In order to have focus and draw boundaries, this research focused on Visa's efforts to prevent credit card fraud. Through tracing prevention encounters over time, some actors appeared to be more salient than others. Those were the card associations, technology vendors, merchants, financial institutions, regulators and legislators. This is not to limit prevention efforts to these actors, and future researchers can identify and examine the role of other actors in preventing credit card fraud.

Fourth, the concept of prevention encounters is used to explain how security networks achieve prevention. Accordingly, the research findings are constrained by the research focus on security efforts that disrupt a prior security practice. That is, I only focus on encounters or disequilibrium moments. Episodes of continuous security efforts by different actors in security networks are thus not covered in this research.

Finally, in two prevention encounters (credit card mass mailing and strengthening the legal system) the prevention measure manifested itself in terms of law. Investigating the process preceding the enactment of the law was seen suffice to meet the research objectives and therefore events taking place after the law has passed have not been traced.

8.5 Future Research

The primary focus of this research was to explain how security networks achieve prevention and identify the incentive mechanisms for converging actors in these networks. In answering these questions areas for future research have arisen.

The research findings revealed that interactive communication is a critical element in the functioning of security networks. Future research can benefit from this finding, for example, the literature on vulnerability disclosure networks can focus on the reporting process and communication patterns between vendors and coordinators and examine how that would influence the disclosure process and vendor's decision on when to release a patch.

Properties of the social and technological structures have a significant influence on security networks' prevention efforts. This research identified the complexity of the legal system, the novelty of the prevention measure, and the heterogeneity of roles of the social actors as pivotal in enabling prevention mechanisms to prevent credit card fraud. Identifying other properties under different contexts will deepen our understanding of collective security efforts. Moreover, future research can study whether the fact that the vulnerable technology is new has an impact on patch release time, and accordingly whether the coordinator (e.g., CERT) needs to change its vulnerability disclosure policy for new technologies.

Although this research revealed divergence between actors in security networks and reasoned that to different interpretations of the prevention measure and different beliefs on how security is to be achieved, the main focus was on the convergence rather than the divergence process. A promising venue for future research would be to explore and provide in-depth analysis of the divergence process, which can include the identification of different sources of divergence and how divergence affects the prevention process and the security networks' outcome. This means studying cases where collective security efforts fail and security networks dissolve. This is because convergence herein occurs when the network's actors collectively reach consensus on the mean to achieve security. Although my study revealed one prevention encounter where collective security efforts did not succeed (automating card transactions), this is not enough to offer a robust analysis of the divergence process especially since the later may require a different methodology than the one adopted in this research.

The complexity of security networks and security threats requires varying the incentives used to account for the particularities of the actors involved and the context of the phenomenon. Future research would benefit from the three forms of incentives identified to develop a configurational perspective on incentives for converging actors in security networks. This approach acknowledges equifinality in security networks where not all of the three forms of incentives need to be employed to achieve successful convergence. Future research can investigate this issue and develop combinations of incentives along with their contextual conditions that result in converging actors.

8.6 Concluding Remarks

In our increasingly connected world, achieving security has become distributed across heterogeneity of actors that reside outside organizational boundaries. It is important therefore to envisage IS security as one that is not only about organizational processes, extra-organizational settings deserve scholarly attention to advance the field of IS security. Taking extra-organizational settings as the point of departure, this research aimed to increase our understanding of security networks by extending the current literature that places more emphasis on cause-effect relationships to examine the causal mechanisms behind the prevention efforts of security networks. Towards this aim, prevention encounters concept was introduced to capture the complexity of security networks and the constant upheavals they experience that makes reaching equilibrium a continuous process.

Incentives are crucial for the functioning of security networks. However, it is of paramount importance to acknowledge the heterogeneity of actors involved and thus the need to use a variety of incentives to cater for actors' various interests. This research identified three forms of incentives that aligned actors' interests and allowed the network to achieve its purpose.

The findings of this research provide valuable contributions to the literature on security networks as well as the literature on behavioural IS security. The qualitative and historical research design along with adopting a different philosophical stance than the common interpretivism and positivism offer rich and new insights that have the promise to move the field of IS security forward.

9 REFERENCES

ABA Banking Journal (1980) POS networks announced; one a pilot, one "live". *ABA Banking Journal.* August, 1980: p.104-105.

Abbott, A. (2001) *Time Matters*. Chicago: University of Chicago Press.

Abouchar, R. J. (1969) Bank Charge Cards in the 1970s. *Banking.* October, 1969: p.34, 76, 78, and 80.

Alfranca, O. & Huffman, W. E. (2003) Aggregate private R&D investments in agriculture: The role of incentives, public policies, and institutions. *Economic Development and Cultural Change*, 52 (1): 1-21.

Alvesson, M. & Skoldberg, K. (2009) *Reflexive methodology: New vistas for qualitative research* 2nd edn. Los Angeles ; London: SAGE.

Anason, D. (1997) Congress Asked to Adopt a Federal Standard For Digital Signatures in Internet Commerce. *The American Banker.* 10 July 1997

Andersen, P. H. & Kragh, H. (2010) Sense and sensibility: Two approaches for using existing theory in theory-building qualitative research. *Industrial Marketing Management,* 39 (1): 49-55.

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

Archer, M. (1995) *Realist Social Theory: The Morphogenetic Approach*. Cambridge: Cambridge University Press.

Arora, A., Krishnan, R., Telang, R. & Yang, Y. (2010) An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure. *Information Systems Research*, 21 (1): 115-132.

Arora, A., Telang, R. & Xu, H. (2008) Optimal policy for software vulnerability disclosure. *Management Science*, 54 (4): 642-656.

Arthur, W. B. (2007) The structure of invention. *Research Policy*, 36 (2): 274-287.

Asher, J. (1974) What the point-of-sale revolution means to banks. *Banking* August, 1974: p.32-34; p.77-79.

August, T. & 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.

Bachtler, J. & Raines, P. (1997) Government incentives and the financial services sector in Scotland. *Service Industries Journal*, 17 (3): 456-473.

Baker, D. I. (1974) Competition, Monoploy and Electronic Banking. In The Economics of a National Electronic Funds Transfer System. Proceedings of a conference sponsored by the Federal Reserve Bank of Boston.

Banking (1969) A.B.A. on Unsolicited Credit Cards. *Banking.* November: p.22.

Banking (1973) Mag stripe cards: "Still the answer". *Banking.* May 1973: p.100.

Banking (1975) Retailers list POS demands. *Banking.* July, 1975

Barrett, M., Heracleous, L. & Walsham, G. (2013) A rhetorical approach to IT diffusion: reconceptualizing the ideology-framing relationship in computerization movements. *MIS Quarterly*, 37 (1): 201-220.

Bartling, C. (1967) Midwest plan moves to cut card fraud. *The American Banker* 2 June 1967

Beersma, B., Hollenbeck, J. R., Humphrey, S. E., Moon, H. & Conlon, D. E. (2003) Cooperation, competition, and team performance: Toward a contingency approach. *Academy of Management Journal*, 46 (5): 572-590.

Benford, R. D. (1993) You could be the 100th monkey: collective action frames and vocabularies of motive within the nuclear disarmament movement. *Sociological Quarterly,* 34 (2): 195-216.

Benford, R. D. & Snow, D. A. (2000) Framing processes and social movements: An overview and assessment. *Annual Review of Sociology,* 26: 611-639.

Bennett, R. (1998) Statement to the Senate. Hearing before the Subcommittee on Financial Services and Technology of the Committee on Banking, Housing and Urban Affair. The Digital Signature and Electronic Authentication Law. March 11 1998.

Berglund, N. (1987) Visa Says It Will Have 15,000 'Super Smart' Cards by Yearend. *The American Banker.* 23 July 1987

Bettenhausen, K. & Murnighan, J. K. (1985) The emergence of norms in competitive decision-making groups. *Administrative Science Quarterly*, 30 (3): 350-372.

Bloom, J. K. & Kutler, J. (1996) Two New On-Line Alliances Pair Niche Leaders. *The American Banker.* 21 February 1996

Bonner, W. (2013) History and IS - Broadening our view and understanding: Actor-Network Theory as a methodology. *Journal of Information Technology*, 28 (2): 111-123.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D. & Polak, P. (2015) What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. *MIS Quarterly*, 39 (4): 837-U461.

Bradford, A. & Ben-Shahar, O. (2012) Efficient Enforcement in International Law. *Chicago Journal of International Law*, 12: 375-431.

Brady, H. E., Collier, D. & Seawright, J. (2010) Refocusing the Discussion of Methodology In: Brady, H. E. & Collier, D., eds. *Rethinking Social Inquiry: Diverse Tools, Shared Standards*. 2nd edn. Lanham, Md.: Rowman & Littlefield Publishers: 15-31.

Brickson, S. (2000) The impact of identity orientation on individual and organizational outcomes in demographically diverse settings. *Academy of Management Review*, 25 (1): 82-101.

Brimmer, A. (1969) Statement to the Senate (S.721). Hearing before the Committee on Banking and Currency, Subcommittee on Financial Institutions. Unsolicited Credit Cards. December 4, 1969.

Brimmer, A. F. (1967) Statement to the House of Representatives. Hearing before the Committee on Banking and Currency on H.R. 12646: To Prohibit Federally Insured Banks from Making Unsolicited Commitments to Extend Credit, and for Other Purposes. November 8, 1967.

Brooke, P. (1970a) BofA, Amer. Express postpone reply date as interest lags in national card network. *The American Banker.* 28 May 1970

Brooke, P. (1970b) BofA, American express plan wide card authorization system. *The American Banker.* 15 April 1970

Brooke, P. (1971a) ABA magnetic stripe highly vulnerable to fraud, WSBA staff engineer declares. *The American Banker* 3 November 1971: p.6.

Brooke, P. (1971b) ABA adds to guides for magnetic card coding. *The American Banker* 18 March 1971

Brooke, P. (1973a) Electronic data transmission net linking all US BankAmericard centers is operative. *The American Banker.* 11 May 1973

Brooke, P. (1973b) Citicorp says students find cheap, easy ways to defraud magnetic stripe cards. *The American Banker* 9 April 1973

Brooke, P. (1973c) Bank Credit Card Leaders Back Magnetic Stripe Despite Security Flaw. *The American Banker.* 13 April

Brown, J. E. (1972) The Case for Shared Terminals. *Banking.* October, 1972

Broz, L. J. (1999) Origins of the Federal Reserve System: International Incentives and the Domestic Free-Rider Problem *International Organization*, 53 (1): 39 - 70.

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

Bureau, W. (1971) Magnetic stripe for credit cards urged by ABA unit. *The American Banker* 16 February 1971

Callon, M. (1986) Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. In: Law, J., ed. *Power, Action and Belief: A New Sociology of Knowledge*. London: Routledge & Kegan Paul: 196–233.

Callon, M. (1991) Techno-economic networks and irreversibility. In: Law, J., ed. *A Sociology of Monsters: Essays on Power, Technology and Domination*. London: Routledge: 132-165.

Capgemini & RBS (2013) World Payments Report 2013. [online] Capgemini and Royal Bank of Scotland. Available from: http://www.capgemini.com/wpr13 (Accessed 16/Feb/2014).

Cardline (2007) Visa Reports Increased PCI Compliance Among Merchants. *Cardline.* 26 October 2007

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

Cavusoglu, H., Mishra, B. & 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): 69-104.

Cavusoglu, H., Mishra, B. & Raghunathan, S. (2005) The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, 16 (1): 28-46.

Cavusoglu, H., Raghunathan, S. & Cavusoglu, H. (2009) Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. *Information Systems Research*, 20 (2): 198-217.

Cerne, F. (1996) Taking Those First Few Steps. *Credit Card Management.* November, 1996: p.94-99.

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

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

Chandler, D. (2014) Organizational Susceptibility to Institutional Complexity: Critical Events Driving the Adoption and Implementation of the Ethics and Compliance Officer Position. *Organization Science*, 25 (6): 1722-1743.

Che, Y.-K. & Kartik, N. (2009) Opinions as Incentives. *Journal of Political Economy*, 117 (5): 815-860.

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

Chutkow, P. (2001) *Visa: the power of an idea*. Chicago: Harcourt.

Clark, P. B. & Wilson, J. Q. (1961) Incentive systems: a theory of organizations. *Administrative Science Quarterly*, 6 (2): 129-166.

Corbin, J. & Strauss, A. (1990) Grounded theory research: procedures, canons and evaluative criteria. *Zeitschrift Fur Soziologie*, 19 (6): 418-427.

Credit Card Management (2001) Visa Takes Aim at Database Thieves. *Credit Card Management.* April, 2001: p.6,8.

Credit Card News (1998) The Associations Give Online Merchants a Break...And Are Fighting Over Who Deserves the Credit. *Credit Card News.* 15 January 1998: p.3.

Culnan, M. J. & Williams, C. C. (2009) How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, 33 (4): 673-687.

D'Arcy, J., Hovav, A. & Galletta, D. (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, 20 (1): 79-98.

Denzin, N. (1989) Strategies of Multiple Triangulation. In: *The Research Act: a Theoretical Introduction to Sociological Methods*. 3rd edn. London : Prentice Hall: Englewood Cliffs, N.J.: 234-247.

DeSanctis, G. & Poole, M. S. (1994) Capturing the complexity in advanced technology use: adaptive structuration theory. *Organization Science*, 5 (2): 121-147.

Dhillon, G. & Backhouse, J. (2000) Information system security management in the new millennium. *Communications of the ACM*, 43 (7): 125-128.

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

Dobbin, F. & Dowd, T. J. (2000) The market that antitrust built: Public policy, private coercion, and railroad acquisitions, 1825 to 1922. *American Sociological Review*, 65 (5): 631-657.

Dorey, P. (1997) Statement to the House. Hearing before the Committee on Banking and Financial Services. Subcommittee on Domestic and International Monetary Policy. The Federal Role in Electronic Authentication. July 9 1997.

Dosh, P. (2009) Tactical Innovation, Democratic Governance, and Mixed Motives: Popular Movement Resilience in Peru and Ecuador. *Latin American Politics and Society*, 51 (1): 87-118.

Duncan, M. (2014) Statement to the Senate. Hearing before the Subcommittee on National Security and International Trade and Finance of the Committee on Banking, Housing, and Urban Affairs. Safeguarding Consumers' Financial Data. February 3 2014.

Eisenhardt, K. M. (1989) Building theories from case-study research. *Academy of Management Review*, 14 (4): 532-550.

Eisenhardt, K. M. & Graebner, M. E. (2007) Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, 50 (1): 25-32.

Eisenhardt, K. M. & Zbaracki, M. J. (1992) Strategic decision making. *Strategic Management Journal*, 13: 17-37.

Fairclough, N. (2005) Peripheral vision discourse analysis in organization studies: The case for critical realism. *Organization studies*, 26 (6): 915-939.

Falco, J. (1984) Statement to the House. Hearing before the Subcommittee on Crime of the Committee on the Judiciary. Counterfeit Access Device and Computer Fraud and Abuse Act. March 13 1984.

Ferrara, E., Hayes, N., Koetzle, L., McClean, C. & Mak, K. (2013) *The Forrester Wave: Emerging Managed Security Service Providers, Q1 2013*.

Fisher, J. F. (1974) Discussion. In The Economics of a National Electronic Funds Transfer System. Proceedings of a conference sponsored by the Federal Reserve Bank of Boston.

FTC (2013). Internet of Things Workshop. Novermber 19, 2013.

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

Garcia, R. & Calantone, R. (2002) A critical look at technological innovation typology and innovativeness terminology: a literature review. *Journal of Product Innovation Management*, 19 (2): 110-132.

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

Gerring, J. (2004) What is a case study and what is it good for? *American Political Science Review*, 98 (2): 341-354.

Gerring, J. (2007) *Case Study Research: Principles and Practices*. New York: Cambridge University Press.

Glaessner, T. & Mas, I. (1995) Incentives and the resolution of bank distress. *World Bank Research Observer*, 10 (1): 53-73.

Glaser, B. & Strauss, A. (1967) *The discovery of grounded theory : strategies for qualitative research*. New York: Aldine de Gruyter.

Glick, W. H., Huber, G. P., Miller, C. C., Doty, D. H. & Sutcliffe, K. M. (1990) Studying changes in organizational design and effectiveness: retrospective event histories and periodic assessments. *Organization Science,* 1 (3): 293-312.

Gneezy, U., Meier, S. & Rey-Biel, P. (2011) When and Why Incentives (Don't) Work to Modify Behavior. *Journal of Economic Perspectives*, 25 (4): 191-209.

Goel, S. & Chengalur-Smith, I. N. (2010) Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems*, 19 (4): 281-295.

Gordon, L. A., Loeb, M. P. & Lucyshyn, W. (2003) Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 22 (6): 461-485.

Green, D. P. & Shapiro, I. (1994) *Pathologies of rational choice theory : a critique of applications in political science*. New Haven ; London: Yale University Press.

Gupta, A. & Zhdanov, D. (2012) Growth and sustainability of managed security services networks: an economic perspective. *MIS Quarterly*, 36 (4): 1109-1130.

Hanley, J. M. (1969) Statement to the Senate (S.721). Hearing before the Committee on Banking and Currency, Subcommittee on Financial Institutions. Unsolicited Credit Cards. December 4, 1969.

Hartelius, E. J. & Browning, L. D. (2008) The application of rhetorical theory in managerial research - A literature review. *Management Communication Quarterly*, 22 (1): 13-39.

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. & 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.

Hedstrom, K., Kolkowska, E., Karlsson, F. & Allen, J. P. (2011) Value conflicts for information security management. *Journal of Strategic Information Systems*, 20 (4): 373-384.

Hedstrom, P. (2008) Studying Mechanisms to Strengthen Causal Inferences in Quantitative Research. In: Box-Steffensmeier, J. M., Brady, H. E. & Collier, D., eds.

The Oxford Handbook of Political Methodology. Oxford: Oxford University Press: 319-335.

Heine, K. (2013) Inside the black box: incentive regulation and incentive channeling on energy markets. *Journal of Management & Governance*, 17 (1): 157-186.

Helper, S. (2000) Economists and field research: "You can observe a lot just by watching". *American Economic Review,* 90 (2): 228-232.

Hemphill, C. S. & Lemley, M. A. (2011) Earning exclusivity: generic drug incentives and the Hatch-Waxman Act. *Antitrust Law Journal*, 77 (3): 947-989.

Hesketh, A. & Fleetwood, S. (2006) Beyond measuring the human resources management-organizational performance link: Applying critical realist meta-theory. *Organization*, 13 (5): 677-699.

Hilgartner, S. & Bosk, C. L. (1988) The rise and fall of social problems: a public arenas model. *American Journal of Sociology*, 94 (1): 53-78.

Hirschman, A. O. (1991) *The Rhetoric of Reaction: Perversity, Futility, Jeopardy*. Cambridge, Mass ; London: Belknap Press of Harvard University Press.

Hock, D. (1999) *Birth of the Chaordic Age.* San Francisco: Berrett-Koehler.

Hock, D. (2005) *One of many: Visa and the rise of the chaordic organization*. San Francisco: Berrett-Koehler.

Hoffman, A. J. & Ocasio, W. (2001) Not all events are attended equally: Toward a middle-range theory of industry attention to external events. *Organization Science,* 12 (4): 414-434.

Hogan, D. (2007) *NRF letter to PCI SSC*. Available from: https://nrf.com/sites/default/files/PCI-Letter-Final_1.pdf

Hui, K.-L., Hui, W. & Yue, W. T. (2012) Information Security Outsourcing with System Interdependency and Mandatory Security Requirement. *Journal of Management Information Systems*, 29 (3): 117-155.

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.

Jakobs, K. (2013) Why then did the X.400 e-mail standard fail? Reasons and lessons to be learned. *Journal of Information Technology*, 28 (1): 63-73.

Johnston, A. C. & Warkentin, M. (2010) Fear appeals and information security behaviors: an empirical study. *MIS Quarterly,* 34 (3): 549-566.

Kamenica, E. (2012) Behavioral Economics and Psychology of Incentives. *Annual Review of Economics, Vol 4*, 4 427-452.

Kanfer, R. (1990) Motivation Theory and Industrial and Organizational Psychology. In: *Handbook of industrial and organizational psychology*. 75-170.

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

Kantrow, A. M. (1986) Why history matters to managers. *Harvard Business Review*, 64 (1): 81-88.

Kaplan, S. (2008) Framing Contests: Strategy Making Under Uncertainty. *Organization Science*, 19 (5): 729-752.

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

Kennedy, T. R. (1969) The Plastic Jungle. *Montana Law Review,* 31 (1):

Kim, H. J. & Bearman, P. S. (1997) The structure and dynamics of movement participation. *American Sociological Review*, 62 (1): 70-93.

Kleege, S. (1993) Visa to Try Low-Cost Chip in Fraud Fight. *The American Banker.* September 21, 1993

Konstantaras, A. (1997) Statement to the House. Hearing before the Domestic and International Monetary Policy Subcommittee of the Banking and Financial Services Committee. The Federal Role in Electronic Authentication. July 9 1997.

Kretschmer, T. & Puranam, P. (2008) Integration Through Incentives Within Differentiated Organizations. *Organization Science*, 19 (6): 860-875.

Kumar, R. L., Park, S. & Subramaniam, C. (2008) Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems,* 25 (2): 241-279.

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

Kutler, J. (1986a) Controversy Clouds Useful Answers On Future of Smart Card Technology. *The American Banker.* July 8, 1986

Kutler, J. (1986b) As MasterCard Tests Smart Card, Visa Plans Two-Year Wait. *The American Banker.* March 25, 1986

Kutler, J. (1986c) Smart Card Debate: Visa, MasterCard Face Off; How Bright Are They? . *The American Banker.* 3 July 1986

Kutler, J. (1986d) Smart Card Champions Believe Chip Can Reduce Fraud and Credit Losses. *The American Banker.* July 7, 1986

Kutler, J. (1988) Visa Will Stick with the Magnetic Stripe; Association Maintains Smart Card Technology Is Years Away. *The American Banker.* 25 February 1988

Kutler, J. (1996) Vendors Ready - and Waiting - for E-Commerce. *The American Banker.* 2 February 1996

Kutler, J. (1997a) On-Line Banking: EDS to Use Verifone Internet Payment Technology. *The American Banker.* 6 November 1997

Kutler, J. (1997b) HP Jumps In to the E-Commerce Alliance Game. *The American Banker.* 2 December 1997

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. [online] Bingley, U.K: Emerald e-book. Available from: (Accessed 11/Feb/2014).

Land, F. (2010) The use of history in IS research: an opportunity missed? *Journal of Information Technology*, 25 (4): 385-394.

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

Latour, B. (1987) *Science in action: How to follow scientists and engineers through society*. Harvard university press.

Lawson, T. (1998) Economic science without experimentation / Abstraction. In: Archer, M., Bhaskar, R., Collier, A., Lawson, T. & Norrie, A., eds. *CRITICAL REALISM: Essential Readings* London; New York: Routledge: 144 - 169.

Leach, T. (2014) Statement to the Senate. Hearing before the Subcommittee on National Security and International Trade and Finance of the Committee on Banking, Housing, and Urban Affairs. Safeguarding Consumers' Financial Data. February 3 2014.

Lee, A. S. & Baskerville, R. L. (2003) Generalizing generalizability in information systems research. *Information Systems Research*, 14 (3): 221-243.

Lee, C. H., Geng, X. & Raghunathan, S. (2013) Contracting Information Security in the Presence of Double Moral Hazard. *Information Systems Research*, 24 (2): 295-311.

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.

Li, P. & Rao, H. R. (2007) An examination of private intermediaries' roles in software vulnerabilities disclosure. *Information Systems Frontiers*, 9 (5): 531-539.

Lieberman, K. (1998) Statement to the Senate. Hearing before the Subcommittee on Financial Services and Technology of the Committee on Banking, Housing and Urban Affair. The Digital Signature and Electronic Authentication Law. March 11 1998.

Lindenberg, S. & Foss, N. J. (2011) Managing joint production motivation: the role of goal framing and governance mechanisms. *Academy of Management Review*, 36 (3): 500-525.

Liu, C. Z., Zafar, H. & Au, Y. A. (2014) Rethinking FS-ISAC: An IT Security Information Sharing Network Model for the Financial Services Sector. *Communications of the Association for Information Systems*, 34 (1): 15-36.

Marengo, L. & Pasquali, C. (2012) How to Get What You Want When You Do Not Know What You Want: A Model of Incentives, Organizational Structure, and Learning. *Organization Science*, 23 (5): 1298-1310.

Markus, M. L. & Robey, D. (1988) Information technology and organizational change: causal structures in theory and research. *Management Science*, 34 (5): 583-598.

Markus, M. L. & Silver, M. S. (2008) A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit. *Journal of the Association for Information Systems*, 9 (10): 609-632.

Marwick, A. (2001) History: Essential Knowledge about the Past. In: *The new nature of history : knowledge, evidence, language*. Basingstoke: Palgrave: 22-50.

Mason, R. O., McKenney, J. L. & Copeland, D. G. (1997a) An historical method for MIS research: Steps and assumptions. *MIS Quarterly*, 21 (3): 307-320.

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

Maxwell, J. A. (2004) Causal explanation, qualitative research, and scientific inquiry in education. *Educational researcher*, 33 (2): 3-11.

McKenney, J. L., Mason, R. O. & Copeland, D. G. (1997) Bank of America: The crest and trough of technological leadership. *MIS Quarterly*, 21 (3): 321-353.

Meade, R. (1969) Statement to the Senate. Hearing before the Subcommittee on Financial Institutions of the Committee on Banking and Currency. Unsolicited Credit Cards. December 7, 1969.

Merkow, M. S. (2004) Secure Electronic Transactions (SET). In: *The Internet Encyclopedia*. p.247-260.

Meyer, A. D., Brooks, G. R. & Goes, J. B. (1990) Environmental jolts and industry revolutions: organizational responses to discontinuous change. *Strategic Management Journal*, 11 93-110.

Meyer, A. D., Gaba, V. & Colwell, K. A. (2005) Organizing far from equilibrium: Nonlinear change in organizational fields. *Organization Science*, 16 (5): 456-473.

Meyer, M. W. (1979) Organizational structure as signaling. *Pacific Sociological Review*, 22 (4): 481-500.

Mierzwinski, E. (2014) Statement to the Senate. Hearing before the Subcommittee on National Security and International Trade and Finance of the Committee on Banking, Housing, and Urban Affairs. Safeguarding Consumers' Financial Data. February 3 2014.

Miles, M. B., Huberman, A. M. & Saldaña, J. (2014) *Qualitative data analysis: A methods sourcebook*. 3rd edn. Los Angeles; London: SAGE Publications.

Mills, W. C. (1940) Situated Actions and Vocabularies of Motive. *American Sociological Review*, 5 (6): 904-913.

Mingers, J. (2004) Real-izing information systems: critical realism as an underpinning philosophy for information systems. *Information and organization*, 14 (2): 87-103.

Mingers, J., Mutch, A. & Willcocks, L. (2013) CRITICAL REALISM IN INFORMATION SYSTEMS RESEARCH. *MIS Quarterly*, 37 (3): 795-802.

Mitev, N. & De Vaujany, F.-X. (2012) Seizing the opportunity: towards a historiography of information systems. *Journal of Information Technology*, 27 (2): 110-124.

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

Mookerjee, V., Mookerjee, R., Bensoussan, A. & Yue, W. T. (2011) When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination. *Information Systems Research*, 22 (3): 606-623.

Mossburg, D. (1997) Statement to the Senate. Hearing before the Senate Banking, Housing and Urban Affairs Committee. Subcommittee on Financial Services and Technology. Electronic Authentication and Digital Signature. October 28 1997.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. & Vance, A. (2009) What levels of moral reasoning and values explain adherence to information security rules&quest; an empirical study. *European Journal of Information Systems*, 18 (2): 126-139.

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

National Commission on Electronic Fund Transfers. (1977) *The Final Report of the National Commission on Electronic Fund Transfers: EFT in the United States: Policy Recommendations and the Public Interest*.

Neumann, W. D. (1983) Statement to the House of Representative. Hearing before the Subcommittee on Consumer Affairs and Coinage of the Committee on Banking, Finance and Urban Affairs. The Nature and Scope of Credit and Debit Card Fraud and related issues. May 4, 1983.

Newman, M. & Robey, D. (1992) A social process model of user-analyst relationships. *MIS Quarterly*, 16 (2): 249-266.

Nugent, M. (1997) Statement to the House. Hearing before the Committee on Banking and Financial Services. Subcommittee on Domestic and International Monetary Policy. The Federal Role in Electronic Authentication. July 9, 1997.

O'Sullivan, M. & Graham, M. B. (2010) Guest Editors' Introduction - Moving Forward by Looking Backward:Business History and Management Studies. *Journal of Management Studies*, 47 (5): 775-790.

Ogut, H., Menon, N. & Raghunathan, S. (2005) *Cyber Insurance and IT Security Investment: Impact of Interdependence Risk*. IN: The Workshop of the Economics on Information Security (WEIS).

Orlikowski, W. J. & Gash, D. C. (1994) Technological frames: making sense of information technology in organizations. *ACM Transactions on Information Systems*, 12 (2): 174-207.

Panke, D. (2013) Regional Power Revisited: How to Explain Differences in Coherency and Success of Regional Organizations in the United Nations General Assembly 1. *International Negotiation*, 18 (2): 265-291.

Pawson, R. & Tilley, N. (1997) *Realistic Evaluation*. London: SAGE.

Payments Cards and Mobile (PCM), 2015. *Card Fraud Report 2015*. Available from http://www.paymentscardsandmobile.com/wp-content/uploads/2015/03/PCM_Alaric_Fraud-Report_2015.pdf. Accessed 20/05/2016

PCI SSC (2010) *Lifecycle for Changes to PCI DSS and PA-DSS*. [online] Available from: https://www.pcisecuritystandards.org/pdfs/pci_lifecycle_for_changes_to_dss_and_padss.pdf

PCI SSC (2016) *Program Training and Qualification*. [online] Available from: https://www.pcisecuritystandards.org/program_training_and_qualification/

Pettigrew, A. M. (1990) Longitudinal field research on change: theory and practice. *Organization Science*, 1 (3): 267-292.

Pinch, T. J. & Bijker, W. E. (1987) The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other In: Bijker, W. E. H., Thomas P. & Pinch, T. J., eds. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MassachusettsLondon, England: The MIT Press: 17-50.

Piore, M. J. (2006) Qualitative research: does it fit in economics? *European Management Review*, 3 (1): 17-23.

Png, I. P. L. & Wang, Q. H. (2009) Information Security: Facilitating User Precautions Vis-a-Vis Enforcement Against Attackers. *Journal of Management Information Systems*, 26 (2): 97-121.

Ponemon (2010) *PCI DSS Trends 2010: QSA Insights Report: Recommendations and guidance for achieving compliance from Qualified Security Assessors*. Available from: http://www.tomsnetworking.de/uploads/media/Ponemon__PCI_DSS_Trends-QSA_Insights_010310.pdf

Porra, J., Hirschheim, R. & Parks, M. S. (2006) Forty years of the corporate information technology function at Texaco Inc.–A history. *Information and Organization*, 16 (1): 82-107.

Porra, J., Hirschheim, R. & Parks, M. S. (2014) The Historical Research Method and Information Systems Research. *Journal of the Association for Information Systems*, 15 (9): 536-576.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J. & Courtney, J. F. (2013) Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory diversity for protection-motivated behaviors. *MIS Quarterly*, 37 (4): 1189-1210.

Power, C. (1997) On-Line Banking: Don't Overregulate E-Commerce, Group Warns. *The American Banker*. 10 July 1997

Puhakainen, P. & 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. & Becker, H. S., eds. *What is a Case? Exploring the Foundations of Social Inquiry*. Cambridge: Cambridge University Press: 217-226.

Ragin, C. C. & Becker, H. S. (1992) *What is a case? exploring the foundations of social inquiry*. Cambridge: Cambridge University Press.

Ransbotham, S., Mitra, S. & Ramsey, J. (2012) Are markets for vulnerabilities effective? *MIS Quarterly*, 36 (1): 43-64.

Reuter, J. (2014) Statement to the Senate. Hearing before the Subcommittee on National Security and International Trade and Finance of the Committee on Banking, Housing, and Urban Affairs. Safeguarding Consumers' Financial Data. February 3 2014.

Rotolo, D., Hicksb, D. & Martin, B. R. (2015) What is an emerging technology? *Research Policy,* 44: 1827-1843.

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

Rowlinson, M., Hassard, J. & Decker, S. (2014) Research strategies for organizational history: a dialogue between historical theory and organization theory. *Academy of Management Review,* 39 (3): 250-274.

Salmela, H. (2008) Analysing business losses caused by information systems risk: a business process analysis approach. *Journal of Information Technology,* 23 (3): 185-202.

Sayer, A. (1992) *Method in Social Science: A Realist Approach*. 2nd edn. London; New York: Routledge.

Schechter, S. E. & Smith, M. D. (2003) *How much security is enough to stop a thief?* IN: International Conference on Financial Cryptography. Springer, 122-137.

Schneider, B. R. (2002) Why is Mexican business so organized? *Latin American Research Review,* 37 (1): 77-118.

Sichelman, T. (2010) Commercializing patents. *Stanford Law Review,* 62 (2): 341-411.

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

Smith, G. E., Watson, K. J., Baker, W. H. & 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.

Spears, J. L. & Barki, H. (2010) User participation in information systems security risk management. *MIS Quarterly,* 34 (3): 503-522.

Starr, M. A. (2014) Qualitative and mixed-methods research in economics: surprising growth, promising future. *Journal of Economic Surveys,* 28 (2): 238-264.

Statista, 2016. *Value of payment card fraud losses in the United States from 2012 to 2018, by type (in billion U.S. dollars).* Available from https://www.statista.com/statistics/419628/payment-card-fraud-losses-usa-by-type/. Accessed 23/11/2016

Stearns, D. L. (2011) *Electronic Value Exchange: Origins of the Visa Electronic Payment System*. London; New York: Springer.

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

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

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

Suddaby, R. & Greenwood, R. (2005) Rhetorical strategies of legitimacy. *Administrative Science Quarterly*, 50 (1): 35-67.

Sun, L. L., Srivastava, R. P. & Mock, T. J. (2006) An information systems security risk assessment model under the Dempster-Shafer theory of belief functions. *Journal of Management Information Systems*, 22 (4): 109-142.

Sutherland, R. A. (1981) Automation Speeds Credit Card Authorization; Telecommunications Network Reduces Losses, Fraud and Time *The American Banker* 21 September 1981

Symantec (2009) Symantec Global Internet Security Threat Report: Trends for 2008. [online] Symantec. Available from: http://www.symantec.com/connect/downloads/symantec-global-internet-security-threat-report-trends-2008 (Accessed 14/Feb/2014).

The American Banker (1970) Task force to offer card standardization guideline by Jan.1. *The American Banker* 28 October 1970

The American Banker (1971) Card groups take own authorization paths. *The American Banker.* 29 June 1971

The American Banker (1972) BankAmericard rejects vendor proposals, plans own information processing network. *The American Banker.* 24 February 1972

The American Banker (1973) ABA issues credit card criteria, reaffirms support of magnetic stripe. *The American Banker.* 14 November 1973

Tieben, B. (2012) *The concept of equilibrium in different economic traditions : an historical investigation*. Cheltenham, UK ; Northampton, MA: Edward Elgar.

Titmuss, R. M. (1970) *The gift relationship : from human blood to social policy*. London: Allen & Unwin.

Tosh, J. (2008) *Why History Matters*. Houndmills, Basingstoke, Hampshire ; New York: Palgrave Macmillan

Tracey, B. (1997) Banking on the Net: Microsoft Moves Seen Helping Consumers Get Comfy with SET. *The American Banker*. 15 May 1997

Tsoukas, H. (1989) The validity of idiographic research explanations. *Academy of Management Review*, 14 (4): 551-561.

Tsoukas, H. & Chia, R. (2002) On organizational becoming: Rethinking organizational change. *Organization Science*, 13 (5): 567-582.

Tyre, M. J. & Orlikowski, W. J. (1994) Windows of opportunity: temporal patterns of technological adaptation in organizations. *Organization Science,* 5 (1): 98-118.

Tyson, D. O. (1973) Citibank introduces check card different from others, claimed to be more fraud-proof. *The American Banker* 25 October 1973

United States. H.J.Res. 648: A joint resolution making continuing appropriations for the fiscal year 1985, and for other purposes.

United States House. The Credit Card Protection Act. Subcommittee on Consumer Affairs and Coinage of the Committee on Banking, Finance and Urban Affairs. Hearings H.R. 2885 and H.R. 3622. July 6 and July 27, 1983.

United States House. Counterfeit Access Device and Computer Fraud and Abuse Act. Subcommittee on Crime of the Committee on the Judiciary. Hearings H.R. 3181, H.R. 3570 and H.R. 5112. September 29, November 10, 1983, and March 28, 1984.

United States House. The Federal Role in Electronic Authentication. Hearing before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services. July 9, 1997

United States House. The Electronic Signatures in Global and National Commerce Act (E-SIGN). Subcommittee on Finance and Hazardous Materials of the Committee on Commerce. Hearing H.R. 1714. June 24, 1999

United States House. Do the payment card industry data standards reduce cybercrime? Hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security. March 31, 2009

United States House. Internet of Things. Hearing before the Subcommittee on Courts, Intellectual Property, and the Internet of the Committee on the Judiciary. July 29, 2015.

United States House. Examining Ways to Improve Vehicle and Roadway Safety. Hearing before the Subcommittee on Commerce, Manufacturing, and Trade of the Committee on Energy and Commerce. October 21, 2015.

United States House. The Internet of Cars. Joint Hearing before the Committee on Oversight and Government Reform. Subcommittee on Information Technology and Subcommittee on Transportation and Public Assets. November 18, 2015.

United States Senate. Unsolicited Credit Cards. Subcommittee on Financial Institutions of the Committee on Banking and Currency. Hearing S.721. December 4, 7, and 8, 1969.

United States Senate. The Credit and Debit Card Counterfeiting and Fraud Act of 1983. Committee on the Judiciary. Hearing S.1870. October 31, 1983.

United States Senate. Electronic Authentication and Digital Signature. Hearing before the Subcommittee on Financial Services and Technology of the Committee on Banking, Housing and Urban Affairs. October 28, 1997.

United States Senate. The Digital Signature and Electronic Authentication Law (SEAL). Subcommittee on Financial Services and Technology of the Committee on Banking, Housing, and Urban Affairs. Hearing S. 1594. March 11, 1998.

United States Senate. Safeguarding Consumers' Financial Data. Hearing before the Subcommittee on National Security and International Trade and Finance of the Committee on Banking, Housing, and Urban Affairs. February 3, 2014.

United States Senate. Privacy in the Digital Age: Preventing Data Breaches and Combating Cybercrime. Hearing before the Committee on Judiciary. February 4, 2014.

United States Senate. Protecting Personal Consumer Information from Cyber Attacks and Data Breaches. Hearing before the Committee on Commerce, Science, and Transportation. March 26, 2014

Verma, K., Mitnick, B. M. & Marcus, A. A. (1999) Making incentive systems work: Incentive regulation in the nuclear power industry. *Journal of public Administration research and theory*, 9 (3): 395-436.

Visa (2009) *Visa Releases Global Data Encryption Best Practices.* Available from: https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.1338581.html

Visa (2010) *Visa Best Practices for Primary Account Number Storage and Truncation.* Available from: https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/bulletin-pan-truncation-best-practices.pdf

Visa (2011) *Visa Program Encourages Merchant Adoption of EMV Chips as a Path Toward Dynamic Authentication.* Available from: https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.1526954.html

Visa (2013) *MasterCard, Visa and American Express Propose New Global Standard to Make Online and Mobile Shopping Simpler and Safer*. Available from: http://investor.visa.com/news/news-details/2013/MasterCard-Visa-and-American-

Express-Propose-New-Global-Standard-to-Make-Online-and-Mobile-Shopping-Simpler-and-Safer/default.aspx

von Hippel, E. & von Krogh, G. (2003) Open source software and the "private-collective" innovation model: Issues for organization science. *Organization Science*, 14 (2): 209-223.

Walker-Leigh, V. (1982) US Vanguard Visits France to Look at the Smart Card; More To Follow as Technology There Spurs Interest with Security, Home Banking Potentials *The American Banker* 11 August 1982: Available from: (Accessed

Wang, H. C. & Barney, J. B. (2006) Employee incentives to make firm-specific investments: Implications for resource-based theories of corporate diversification. *Academy of Management Review*, 31 (2): 466-476.

Weinstein, M. & Marshall, J. (1985) 2 Credit Cards with Chips So Small, Which Card Is Smartest of Them All? . *The American Banker* 2 October 1985: Available from: (Accessed

Weistart, J. C. (1972) Consumer protection in the credit card Industry: Federal legislative controls. *Michigan Law Review*, 70 (8): 1475-1544.

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

Wiegold, F. (1971) Omniswitch tests system of merchant-to-bank authorization to aid card use, reduce fraud. . *The American Banker*. 18 June 1971: p.1

Wieviorka, M. (1992) Case studies: history or sociology? In: Ragin, C. C. & Becker, H. S., eds. *What is a Case? Exploring the Foundations of Social Inquiry*. Cambridge: Cambridge University Press: 159-172.

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

Wolfe, D. (2006) Visa Offers Compliance Awards. *The American Banker*. 13 December 2006: p.10

Wynn, D., Jr. & Williams, C. K. (2012) Principles for conducting critical realist case study research in information systems. *MIS Quarterly*, 36 (3): 787-810.

Yayla, A. A. & 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.

Yin, R. K. (2014) *Case study research: design and methods*. 5th edn. Los Angeles: SAGE.

Zhao, X., Xue, L. & 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.