LSE Research Online

THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

Monica Lagazio, Nazneen Sherif, Mike Cushman

A multi-level approach to understanding the impact of cyber crime on the financial sector

Article (Accepted version) (Refereed)

Original citation:
Lagazio, Monica, Sherif, Nazneen and Cushman, Mike (2014) *A multi-level approach to understanding the impact of cyber crime on the financial sector.* Computers & Security, online . pp. 1-32. ISSN 01674048 (In Press)

DOI: 10.1016/j.cose.2014.05.006

© 2014 Elsevier Ltd.

This version available at: http://eprints.lse.ac.uk/57000/

Available in LSE Research Online: June 2014

LSE has developed LSE Research Online so that users may access research output of the School. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in LSE Research Online to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profit-making activities or any commercial gain. You may freely distribute the URL (http://eprints.lse.ac.uk) of the LSE Research Online website.

This document is the author's final accepted version of the journal article. There may be differences between this version and the published version. You are advised to consult the publisher's version if you wish to cite from it.

http://eprints.lse.ac.uk

A Multi-level Approach to Understanding the Impact of Cyber Crime on the Financial Sector

Monica Lagazio[*], *Nazneen Sherif*[†] *and Mike Cushman*[‡]

Abstract: This paper puts forward a multi-level model, based on system dynamics methodology, to understand the impact of cyber crime on the financial sector. Consistent with recent findings, our results show that strong dynamic relationships, amongst tangible and intangible factors, affect cyber crime cost and occur at different levels of society and value network. Specifically, shifts in financial companies' strategic priorities, having the protection of customer trust and loyalty as a key objective, together with considerations related to market positioning vis-à-vis competitors are important factors in determining the cost of cyber crime. Most of these costs are not driven by the number of cyber crime incidents experienced by financial companies but rather by the way financial companies choose to go about in protecting their business interests and market positioning in the presence of cyber crime. Financial companies' strategic behaviour as response to cyber crime, especially in regard to over-spending on defence measures and chronic under-reporting, has also an important consequence at overall sector and society levels, potentially driving the cost of cyber crime even further upwards. Unwanted consequences, such as weak policing, weak international frameworks for tackling cyber attacks and increases in the jurisdictional arbitrage opportunities for cyber criminals can all increase the cost of cyber crime, while inhibiting integrated and effective measures to address the problem.

Keywords: Cyber crime; economic impact; financial sector; system dynamics; causal loop diagram.

1 INTRODUCTION

Human dependency on digital communication and other networked technologies for tasks ranging from simple web browsing for information to far more important and critical tasks, such as monetary transactions and power grid control and operation, has steadily increased since the initiation of the Internet. This dependency has translated into a growing emphasis on the strategic importance of cyberspace to enable achieving fundamental objectives in contemporary societies: innovation, collaboration, productivity, competitiveness and leadership.(Sharma, 2010) The expansion of cyber functionalities has, however, also opened up new opportunities for people to carry out criminal activities online, and/or to use the Internet as a medium for their criminal objectives. The advantages of the Internet come with risks. While organisations and individuals are exploiting its business benefits they may not realise that cyberspace confers the same benefits on those who wish to attack them. Hacker groups, criminal organisations and espionage units worldwide have access to powerful, evolving capabilities, which they use to identify, target and attack their victims. They even have well-developed market places for buying and selling the tools and expertise used to target and execute cyber attacks. These attacks do not only represent technological threats. If we accept the argument that modern, economically developed societies are increasingly becoming 'information societies', then, it follows that threats to information can be seen as threats to the core of these societies (Eriksson and Giacomello, 2006).

Although nobody disputes the importance of protecting cyberspace from criminal activities, our understanding of cyber crime and its consequences, both economical and social, is still limited. The literature on cyber crime is vast, but still theoretically thin and underdeveloped. This is because there are still many different perspectives and a lack of consensus on many fundamental aspects of cyber crime. Thus lack of consensus extends to definitions, classifications, economic implications, security

[*] Dr Monica Lagazio, Partner, Trilateral Research & Consulting, Crown House, 72 Hammersmith Road, London, W14 8TH, UK, monica.lagazio@trilateralresearch.com, +44(0) 207 559 3550.
[†] Nazneen Sherif, Assistant Technical Editor, Incisive Media, 32-34 Broadwick Street, London, W1A 2HG, UK, nazneen.sherif@gmail.com.
[‡]Mike Cushman Department of Management, London School of Economics and Political Science, Houghton Street, London, WC2A 2AE, UK, m.cushman@lse.ac.uk.

standards and solutions. Furthermore, among the factors undermining our appreciation of cyber crime and its impact are intangible pre-conditions, such as lack of awareness, general fears and feelings of insecurity as well as perceptions of trust, risks and 'the virtual world'[4] These intangible pre-conditions can themselves have significant consequences.

Experience of cyber crime can also be fragmented. Experience might be spread across the different levels of the value network[5] and of society. The different actors involved each holding only part of the overall 'puzzle', might often be unable or unwilling to share their knowledge for fear of perceived consequences. Because of this fragmentation, and given the existence of the intangible pre-conditions referred to above, more flexible and multi-level approaches are needed in order to appreciate the complexity of cyber crime activities and their consequences.

As part of the emerging debate about the need to embrace more complex and interactive models for assessing the impact of cyber crime (Anderson *et al.*, 2008) this article suggests a multi-level approach aimed at mapping and at shedding further light on the interaction of both interdependent and differentiated factors, which together can facilitate or deter cyber crime, while increasing and/or decreasing its economic and social costs. This approach makes use of system dynamics (Forrester, 1958) methodologies. Although system dynamics models are neither a panacea nor always appropriate, we demonstrate they provide a useful methodology that has not been sufficiently exploited in the context of cyber crime analyses. In this article we analyse cyber crime in the financial sector by adopting a multi-level approach, based on system dynamics theory. We have selected this sector because financial services and products, notably card payments, are a major target of cyber criminals (Trustwave, 2012).

The structure of this article is as follows:

- **Section 2** briefly reviews the existing debate and research on the consequences of cyber crime, while identifying existing research challenges and gaps.

- **Section 3** introduces the system dynamic approach and briefly discusses the definitions, the data for the model and model development.

- **Section 4** presents some of the results and insights on the impact of cyber crime on the financial sector as emerging from the developed multi-level model.

Many of the issues covered in this article are still under development and are the subject of continuing dispute among specialists. Our aim is to contribute to the debate on, and examination of, these issues rather than provide conclusive answers.

2 THE IMPACT OF CYBER CRIME: STATE OF THE PLAY AND CHALLANGES

The notion of cyber crime, referring to "criminal acts committed using electronic communications networks and information systems or against such networks and systems"(European Commission,

[4]Virtual activities are perceived as happening and developing in a virtual world, sometimes with little association to the material one. In this virtual environment, crime breakers tend to underestimate the impact of their actions and therefore ethical considerations are somehow less constraining on actors. So far, there is little perceived human suffering associated with cyber actions (Geers, 2011, p. 109).

[5] Value networks are any web of relationships that generates both tangible and intangible value through complex dynamic exchanges between two or more individuals, groups or organisations. Any individual, organisation or group of organisations engaged in both tangible and intangible exchanges can be viewed as a value network, whether individual consumer, private industry, government or public sector (Bauer, et al, 2008).

2007, p2) [6] is primarily a social concept defined by the intention of actors in relation to norms laid down by law. Cyber crime regulations and policies address intention and behaviour with regard to social and economic consequences. Technology is only a means and, at most, a proxy. As Ross Anderson (2001) has pointed out, many failures of information security could often be better explained in the language of economics rather than by technological shortcomings. Building on Anderson's work (and on Gary Becker's (1968) seminal study on the economics of crime and prosecution), the interdisciplinary security community has started to develop economic interpretations of cyber crime (see, for example, Kshetri, 2006; Anderson *et al*., 2008; van Eeten and Bauer, 2008; Moore et al, 2009). Not all cyber crimes can be fully assessed and understood through an economic perspective; for instance, economic considerations are less prominent in case of ideological attacks, revenge and other crimes of passion. In these cases, cost-benefit approaches often involve psychological and ideological benefits, while the perceived costs are often ignored by the attackers, including the likelihood and impact of getting caught. However economic explanations are helpful when cyber attackers are mainly driven by economic factors. The core argument of this approach is both sound and un-complicated: essentially, cyber crime is driven by rational cost-benefit calculations. People engage in such crime if their risk-adjusted expected benefits outweigh the cost of committing it. However, the correct application of the approach in a complex and dynamic environment, such as the Internet and, more broadly, technologically advanced societies, is all but straightforward. Due to this complexity, assessing the impact of cyber crime has been characterised by controversies and criticisms.

Firstly, studies sponsored by the security industry have been criticised for obscure methodology, vested interests, and extrapolation errors due to asymmetric responses in samples which are heavily biased towards people without direct cyber crime exposure (Herley, 2011).

Secondly, most of the studies on the impact of cyber crime have produced no robust and replicable findings. This is possibly due to: inadequate data, partly at least due to underreporting and other forms of inaccuracies affecting available data sources (The Economist, 2012); different specifications, or theories; complexity; or simply random variation. Consequently, questions remain about the practical power of such analyses and validity of their findings. Could it be that cyber crime is not as big a threat as it is said to be? That threats to cyberspace engender cost is not disputed. However, the magnitude of this cost is uncertain, as is its incidence across the different levels of the value network and society at large (Bauer *et al.* 2007). Anderson *et al*.'s (2012) most recent work has paved the way to addressing some of these well known issues by both providing more reliable data on cost and developing a broader framework to assess cost. Anderson *et al*.'s cost framework was broadened so as to include: defence costs (the cost involved in the implementation of security measures); and opportunity costs (the costs involved in missed opportunities arising from a certain cyber crime being carried out, irrespectively of its outcome, in circumstances where the security measures developed and implemented by end-users divert attention away from other activities). Anderson *et al.*'s work has made an important contribution by providing better data and defining better metrics for assessing the cost of cyber crime. However, it has hardly started to address other fundamental problems, such as the incidence of cyber crime cost on the value network and society at large.

Next, both tangible (such as financial losses and cost) and more intangible drivers (including trust, loyalty, and society utility) of cost are important and sizeable consequences of cyber crime. Public perceptions of, and attitudes towards, cyber crime (Wall, 2008), together with issues of awareness, trust and societal utility, cannot be ignored. For instance, there is the risk that an exaggerated concern with security in cyberspace could reduce the generativity of the Internet to put information technology to many different and, perhaps initially, unforeseen uses. Such an extension of uses has been identified as central to the development of the online economy.

[6] The 2007 report, together with the European 2001 Convention on Cyber crime, has harmonised terminologies related to cyber crime and defined a minimum standard for the criminalization of cyber crime among the ratifying countries. Both documents set a baseline for effective cyber crime policy, in particular for cross-border crime.

Finally, the way in which citizens, society and industry players are engaged in responding to cyber crime is of importance. Defence measures taken in the fight against cyber crime can be ineffective without citizens', society's and industry's engagement and may be considered illegitimate without citizen support. Indeed, the controversy over universal identification, which has in part been presented as an effective solution to address issues of cyber crime attribution, has polarised the debate between those who believe that international or national agencies could legitimately provide Internet identity credentials, based on other identification systems (passports, national identity cards, driver's licences, etc.), and those who assert that attempting to build such a system is futile, and will only give criminals and hackers new ways to hide, while impacting societal utility and hindering fundamental rights (Schneier, 2010).

These debates have raised additional questions related to which data, methods and techniques we should develop to capture and unpack the complex issues of 'economics of security'. Possible approaches range from the development of general and specific measures of societal utility and resilience to more empirical approaches to capturing the behavioural economics of security and calculating the financial return on security investments (ROSI) and economic incentives for cyber security. In recent years, further methods and techniques have been tested for validity and robustness and implemented. However, these methods have typically focused at the level of the individual company and organisation without analysing the economic cost on the entire value network and society at large (Gordon and Loeb, 2006). It is only very recently that van Eeten *et al.* (2009) have started to investigate the impact of specific security incidents across the value network, while taking into account second-round effects. Van Eeten *et al.* identify such second-round effects as those effects that impact not only the immediate targets of the attacks but also on other relevant actors. Such actors may be as different as end-users, e-commerce sector, law enforcement agencies and society at large. This work, together with the analysis of Anderson *et al.* (2012) clearly indicates the need to move toward a more comprehensive and multi-level accounting framework for assessing the impact of cyber crime. While addressing several issues of previous cost models, these more recent attempts have also opened up further challenges. Second-round impacts are not easy to assess and often require an attempt to assess implicit costs: those known impacts of security breaches, which are difficult to measure unambiguously. A typical example of implicit cost is revenue loss due to reputation damage and/or the slowdown in the adoption of online services by market players and end-users, which could both arise from security incidents. Although it may be possible to find proxies for implicit costs, their dynamics and interactions with other types of direct and more explicit costs are not fully understood and require additional investigations.

Building on these new developments within cyber security study, we have sought to use system dynamics methodologies (Forrester, 1958) to investigate the impact of cyber crime on financial institutions. By developing a system dynamics approach we aim to further investigate the multi-level dynamics of second-round impacts and to map some of the key interactive relationships among the key drivers of cyber crime costs at the different levels of society.

3 A SYSTEM DYNAMIC FRAMEWORK TO ASSESS THE IMPACT OF CYBER CRIME ON THE FINANCIAL SECTOR

This section considers why a system dynamics approach is suitable for studying the impact of cyber crime and briefly discusses the system dynamics method, the definitions and data used, and the model development phase.

3.1 THE SYSTEM DYNAMICS APPROACH

System dynamics (SD) is a methodology and mathematical modelling technique for framing, understanding, and unpacking complex issues and problems. System dynamics methods help explain

the dynamic behaviour of complex social systems, over time, through causal theory, feedback relationships and delays, while capturing all these complexity through computer modelling (Lane, 2008). All SD methods share one simple assumption: the structure of any system - the many circular, interlocking, sometimes time-delayed, relationships among the system's components - is just as important in determining the system's behaviour as its individual components. By applying this assumption, SD methods try to resemble the modelled reality structurally, so as to review structures in the world for usefulness and consistency. Furthermore, they provide a way of seeing the ramifications of that simplification through simulation and, thus, a means of testing hypotheses (Sterman, 2000).

The most common approach in developing SD models is initially to map the dynamic relationships, believed to be at stake within a system, or specific problem of interest, and then use a variety of methods to understand the possible consequences of those relationships, while developing theories about them. Essentially this approach makes use of very sophisticated forms of program logic or concept mapping. Examples of these forms and methods of SD include the causal loop diagrams (CLDs), developed by Forrester at MIT (1971) and popularised by Senge (1994). A CLD is a diagramming convention that helps in representing feedback structures in problems. Essentially, CLDs are causal diagrams that aid visualisation of how interrelated variables affect one another (Sterman, 2000). In some cases, CLDs take delay durations and polarity of feedback into account to ascertain likely stability and oscillation issues, as well as oscillation frequency. Typical causal-loop diagrams define causal links (i.e., relationships) representing causes and effects. The CLD diagram consists of a set of nodes representing the key variables of a complex system, connected together via links. These links, or relationships, among variables, visualised by arrows, can be labelled as positive or negative. Notation 'S' indicates a *positive causal link* and means that the two nodes, or variables, change in the same direction: if the node in which the link starts decreases, the other node also decreases. Similarly, if the node in which the link starts increases the other node likewise increases. By contrast, notation 'O' indicates a *negative causal link* and means that the two nodes change in opposite directions: if the node in which the link starts increases, then the other node decreases, and *vice versa*. The '||' symbol shows delayed effect. A reinforcing loop is formed when there is zero or an even number of 'O', or negative links, in a loop. A balancing loop is formed when there are odd numbers of 'O', or negative, links. As the name suggests, reinforcing relationships cause more growth or more decline (representing positive feedback) and balancing loops tend to correct or balance these reinforcing effects (representing negative feedback).

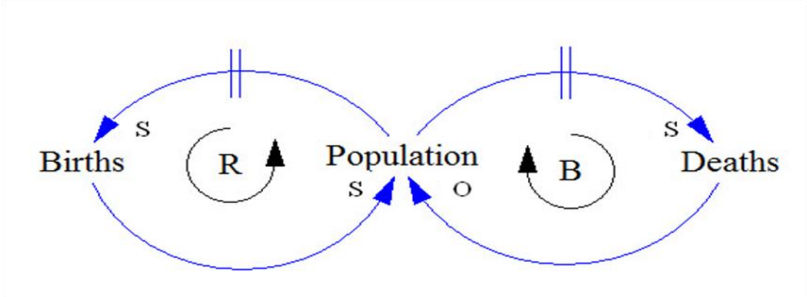

Figure 1: Example of CDL mapping

A typical example of a positive link is the relationship between number of births and population growth. We know that, all else being equal, more births lead to a greater population, and fewer births lead to a lower population. In Figure 1 above, this relationship is represented by labelling the arrow head with a 'S' sign. By contrast, the relationship between number of deaths and population growth represents a negative link. More deaths lead to a lower population, and fewer deaths lead to a greater population. As illustrated in Figure 1, this can be represented with an 'O' sign on the arrow head. These causal links are true independently and they are also simultaneously true. However, on their own, they do not tell us what is actually happening to the population. If we apply CLD mapping and introduce some feedback into the model then a more complex picture will emerge. While more births

lead to a greater population, a greater population also leads to more births since more people make more babies (assuming, of course, a constant birth rate). Therefore, we can draw a positive causal link (S) from population back to births. This link represents the first feedback loop, shown on the left side of the Figure 1 above.

A feedback loop is the name given to a set of relationships where one variable leads to a change in another variable that eventually leads to a change in the original variable. To read a feedback loop, one picks a variable to start with together with an arbitrary direction – either 'S or 'O'. If, on Figure 1, we start with population and S, we will discover another feedback loop. More population leads to more births which lead to more population. This is called a reinforcing feedback loop (marked with an 'R' in Figure 1). This is because more births today lead to more births in the future, i.e. births reinforce births. Similarly, fewer births would lead to a lower population, which would lead to fewer births in the future, indicating that the reinforcing process works in the opposite direction too. If this were the only feedback loop in the population system and people did not die, then we would see exponential growth in the number of people. We see a different type of feedback loop when we examine deaths. More deaths today lead to fewer deaths in the future. This is because more deaths today will cause the population to fall, which means fewer people will be alive to die later. These types of loops are called balancing feedback loops (marked with a 'B' in Figure 1) since more leads to less or less leads to more, meaning that the original change is balanced by a change in the opposite direction. In Figure 1 there are also two hash marks, '||', on the causal links between population and births and between population and deaths. This is because it takes time for an individual to be old enough to have a child meaning that there is a delay between population and births. Likewise, it takes time for individual to get old and die.

For modelling the multi-level impact of cyber crime on the financial sector, we have selected the CLD method. SD in general, and CLDs in particular, are suitable choices for modelling the impact of cyber crime for a number of reasons. Firstly, an SD approach is widely recognised as a clear method for communicating ideas and complex structures to those with little working knowledge of the particular problem studied. Secondly, based on more recent analyses on the impact of cyber crime, the economic variables involved appear to follow feedback structures more closely than linear causal relationships. Some of these causal relationships also seem to be characterised by delayed effects, which can be well represented by a SD model. Finally, given the lack of comprehensive and robust data on cyber crime, CLDs can offer a useful alternative to more data-driven models. In particular, it is possible initially to develop a CLD for cyber crime with partial data and then further define the mathematical relationships in the SD model as and when more data become available. Modelling the initial framework for cyber crime impact with SD will therefore, facilitate further refinement of the model in the light of more data, while providing, in the meantime, new insights into the problem.

3.2 DEFINITIONS AND CLASSIFICATION OF FINANCIAL CYBER CRIME

The concept of cyber crime is problematic because it is open to a variety of social, political, practical and scientific interpretations and explanations. Most of the definitions of cyber crime take into consideration the utilisation and mediation of cyberspace[7] in the perpetration of cyber criminal activities, while distinguishing those criminal activities that are heavily dependent on cyberspace from those that are not. According to Wall (2007, p187), "true cyber crimes are criminal behaviours transformed or mediated by the Internet". This encourages the study of how digital opportunities and technological innovations have transformed traditional crimes into cyber crimes. Following Wall, we have adopted a broader, but still cyber-space-based, definition of cyber crime. This definition includes all cyber activities that support crime in any of its aspects, while also emphasising how the Internet has transformed traditional crimes and projected them to a much larger scale.

[7]Cyber space stands for the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online interaction and communication takes place.

Adopting this broader approach, we regard as cyber crime:

(1) *Traditional crimes* that are to be regarded as *cyber* when they are conducted online and are exploiting cyberspace as providing more opportunity for crime (e.g., traditional fraud, piracy, espionage, stalking, trading sexual material).

(2) *Hybrid cyber crimes* which are traditional crimes whose effectiveness, nature and modus operandi have significantly changed as a result of new opportunities provided by the Internet (e.g., ID theft, hacking, hactivism, illegal online sex trade),

(3) *True cyber crimes* consisting of opportunities created purely by the Internet and carried out only within cyberspace (e.g., spam, denial of service, phishing, illicit cyber sex) (Wall, 2003).

(4) *Cyber platform crimes* such as the use of botnets to facilitate other crimes rather than being used to carry out criminal activity directly.

Based on the above categorisation and Wall's initial classification of cyber crime in general, we have catalogued a taxonomy of financial cyber crimes, which is based on the nature of the crime (Table 1).[8] By nature we mean the main focus of the criminal activities. We have considered as financial cyber crime, crimes that directly target financial organisations (e.g., ID theft) or heavily rely on financial instruments to perform other type of criminal activities (e.g., online scams).

[8] In order to explicate a taxonomy of cyber crime, based on the nature of crime, we developed a cognitive map (Bryson *et* al., 2004) based on previously developed classifications in order to create clusters of concepts and ideas related to specific criminal activities. The map was developed in Decision Explorer software (http://www.banxia.com/dexplore/).

Objectives	Means	Examples
1. ID related fraud *Account related financial fraud* Account take-over Opening new account Online shopping *Acquiring financial products* Mortgage Fraud Medical Insurance Fraud *Acquiring employment, key positions or immigration status* *Tax Refund Fraud*	Hacking, Phishing, Malware, Trojan, virus	In the UK alone, 7% of the population, which is around 4 million people, have been victims of identity fraud. Mortgage fraud increased 500% in the U.S.A from 4,000 cases in 2001 to 17,000 cases in 2004. Canadians annually lose $1.5 million due to mortgage fraud.
2. Espionage *Economic Espionage* *Industrial Espionage*	Hacking, Phishing, Malware, Trojan, virus	In 2009, a chemist at Valspar Corporation attempted at taking data on secret formulas to a new job in China. In 2006, an employee at Ford Motor Company reportedly copied sensitive data into an external hard drive in order to procure a job in China.
3. Exploiting existing financial infrastructures *Money Laundering*	Complex legitimate transactions exploiting the online financial infrastructure	HSBC multi-billion dollar money laundering scam in 2012.
4. Disruptive attacks *Hacktivism* *Cyber-terrorism* *Recreational Hacking* *Extortion*	Denial of service, web defacement, Botnets, Hacking, Attack on critical infrastructure	Jonathan James, a juvenile hacker, hacked into the NASA system and stole information worth US$1.7 million in 1999. In 1989, a group named WANK (Worms Against Nuclear Killers) penetrated the United States Department of Energy and NASA Vax VMS machines. The Chinese triads, a type of criminal organisation, have taken the help of specialists in carrying out Distributed denial of service attacks against commercial sites for ransom.
5. Content related crime (indirectly related to financial cyber crime) *Obscenity* Trading illegal sexual material Trading illegal sexual services	Spam, Web-redirection	Russian criminal groups like Russian Business Network, and Yambo Financial began their journey in crime through child pornography and online casinos.
6. Online scams and piracy crime (indirectly related to financial cyber crime) *Piracy* Selling counterfeit products CD and software pirating *Scams* Online gambling fraud E-auction scams	Spam, Web-redirection	Pfizer's Viagra pill that sells for several dollars is supplied to merchants from Indian factories for less than a dime. Lost revenue due to software piracy has been estimated at US$ 53 billion in 2008, with nearly 41% of software installed on computers obtained illegally.

Table 1 Taxonomy of financial cyber crime based on nature of crime

3.3 MODEL DEVELOPMENT: PRIMARY DATA

In order to study the impact of cyber crime on the financial sector via a CLD model, we initially needed to capture: organisational spending on cyber security; the number of specific incidents faced

by financial companies on a yearly basis; and industry perceptions on the impact of cyber crime. Relying on previous studies and statistical publications is not enough. Publically available statistics tend to focus on the number of incidents on specific types of cyber crime, such as fraud losses or ID theft (Financial Fraud Action UK 2012, 2012), furthermore, financial statements of companies do not provide specific break down of spending for cyber crime risk management. As a result, we sought additional primary data from a sample of industry representatives through surveys and interviews.

The financial sector is heavily affected by cyber crime (The Ponemon Institute, 2010). However, the competitive nature of the industry leads to practices such as under-reporting and lack of information sharing (The Economist, 2012); there is a tendency for financial institutions not to share information about cyber crime incidents in order to protect their reputation and market share. Given the well-known difficulties in gaining information from the sector, we decided to follow a qualitative approach, combining the insights from a small number of surveys with followed up in-depth interviews. We also restricted the data collection to the UK financial sector; the UK provides an insightful single country view, since it has a mature online economy with a well-functioning financial sector and well- informed users on the risks of cyber crime (European Commission, 2007). This approach allowed us to build a more detailed and informative, although less representative, picture of how the financial sector experiences and perceives the impact of cyber crime. Table 2 below shows the number of surveys and interviews aimed for and the responses received.

Industry sub-sectors	Survey and interview requests	Responses received
Banking	32	2
Cards	6	1
Insurance	4	0
Retail	5	0
Online payment providers	3	0
Financial services	8	3
Government fraud service	1	0
Total	**59**	**6**

Table 2 Number of surveys sent and responses received

The response rate of both surveys and interview was low but those we were able to interview held roles which gave them an overview of potential and actual cyber crime in the sector. Consequently, we were still able to identify seven key observations and five key insights from the survey and interview data, which were used for developing feedback causal loops in the CLD model. These initial observations and insights are summarised below, while they appear to be robust further future interviews of a wider sample will confirm or amend them:

Key observations from survey and interviews

1. Overall, industry representatives make a clear distinction between fraud and cyber crime as they see fraud as something that could happen even without the existence of cyberspace. Hence, these numbers are reported separately by financial companies.

2. The percentage of revenue spent on preventive measures against cyber crime was around 1-2% of the IT budget according to 2 respondents. 4 respondents said that this figure will increase in the next year, indicating either a move towards better protection or increased efforts in tackling the growing number of cyber attacks on their business.

3. 4 respondents revealed that compromised cards and accounts were the most common cyber crime incidents bringing maximum financial losses to the company.

4. 3 respondents said that attacks to IT infrastructures occur often and 3 said they occur occasionally.

5. 4 respondents said there is a focus on preventive measures to avoid compromised customer accounts and online scams targeting customers. This indicates the importance for financial companies of protecting customer trust in their business, products and services.

6. 2 respondents stated that the impact of cyber crime on their business is significant (3 on the 5-point rating scale used in the survey), while 2 stated that it is minor and 1 said there is no impact.

7. 2 respondents stated that so-called 'hacktivist' motivated attacks against the financial sector and leaks of sensitive information have been common in current times. Most of the time, hacktivists would like to be caught so they can use a successful attack as a platform to disseminate their propaganda against financial organisations.

Key insights from survey and interviews

1. Perception of the occurrence of cyber crime remains fragmented and, at times, contradictory within the sector. While the banking and cards sub-sector claim that the overall number of cyber incidents is very low, the financial advisory services sub-sector argues that cyber incidents happen on a consistent basis. This fragmented view may be due to under-reporting or it could be that for large companies, even a few hundred incidents contribute to negligible losses. The tendency of the industry to consider fraud and cyber crime as two separate and mutually exclusive types of crime and risk may also have a part to play in this. Fraud and cyber crime losses are reported separately following the rationale that fraud could happen through any means and not just through cyberspace.

2. The occurrence of cyber crime offers financial organisations a variety of strategies that might affect their spending on how to manage cyber risks. Large companies in the financial sector tend to over-spend on security as this gives them some scope for defending their reputation and their management of cyber risks, after successful attacks (if it appears that we have done everything we could to avoid cyber attacks then our reputation and risk strategies should be judged as sound). Appearing to be more protected than their competitors is also a way to market a company's products and boost sales. This means that any financial companies that can afford high-end security measures will install them irrespectively of whether they face serious cyber threats. However, for small and medium sized companies, it may be cheaper to carry out speedy recoveries after attacks, restoring to business-as-usual conditions quickly and recovering losses on customers' account, rather than pre-emptive spending on preventive measures. Small and medium sized financial companies have also observed that speedy recovery is effective in increasing customer trust and loyalty. By effectively and efficiently solving issues when occur, in this case a cyber crime incident, companies create those important 'moments of truth' (Beaujean *et al*, 2006) helping to transform wary or sceptical customers into strong and committed brand followers. This in turn prompts the question of whether customer trust and/or loyalty is what ultimately drives the spending on preventive measures as direct cyber crime losses do not seem to be the main driver.

3. Making companies' more risk averse is also another important impact of cyber crime, which can significantly affect companies' strategic behaviour and choices. Some respondents stated that cyber incidents cause companies to be risk averse, which in turn leads to an increase in the opportunity cost of lost businesses as some business opportunities might be regarded too

risky after experiencing cyber crime. Often, this risk aversion can also lead to a reduced customer experience due to more burdensome authentication measures, implemented in order to protect companies' customer accounts from cyber crime.

4. The advisory services sub-sector claims that cyber crime losses are negligible for large companies. This can explain why our respondents from the banking sub-sector reported a minor impact of cyber crime. However, a few cyber crime incidents against small and medium size financial, and other sector, companies would still add up to significant losses for the companies involved. Big banks also tend to over-spend on protective measures. However, smaller companies cannot afford high-end security measures. This in turn may affect customer trust and sales, even for large companies. Smaller companies may become the weak link within the sector, opening a door for cyber attacks: a vulnerability in one company may open a door to the operations of an otherwise better protected, but linked, business which may not even be on the same continent. This raises two questions. Does cyber crime have a major impact only on small and medium companies? Are the weaknesses of smaller companies concealed by the confidence of large banks that the overall problem of cyber crime is under control?

5. The majority of respondents believe that weak links will always exist. Criminals will always be able to find those vulnerabilities through which they can penetrate the business network and carry out their activities. Furthermore, new technological criminal avenues can, sometimes be offered by the technologies designed to fight cyber crime. Therefore, it becomes necessary for larger companies, with high-end security measures, to support other companies, not only those in the financial sector, to become better protected. Furthermore, it is also becoming essential for both large and smaller financial companies to increase their own resilience against cyber attacks. All these will reduce the risk that large financial companies' own systems are broken into, while supporting speedy recovery even though complete avoidance of risk is an impossibility. Enterprise risk management must be extended to embrace cyber resilience, which is the organisational capacity to withstand cyber attacks (Information Security Forum, 2011, p2).

3.4 MODEL DEVELOPMENT: COST APPROACH

In relation to accounting for the cost of cyber crime, we have followed the cost methodology, suggested by Anderson *et al* (2012) but further adapted it based on the observations and insights from the surveys and interviews. We then developed logics, relationships and feedback loops, based on this approach, and built them in the CLD model.

Costs of cyber crime can be split up into three main categories:

- **Direct losses:** monetary losses, damage, or other suffering experienced by the targeted end users and organisations as a consequence of a cyber crime.

Examples of direct losses include: loss due to fraud; legal costs; recovery and clean-up cost; regulatory fine; loss of customer accounts; and loss of customer trust and/or loyalty. Loss of trust and loyalty was the largest cost borne by the targeted company and is best considered as a direct cost.

- **Indirect losses:** the monetary losses and opportunity costs imposed on organisations and society when a cyber crime is carried out, no matter whether successful or not.

Examples of indirect losses include: opportunity cost of reduced sales (due to disruption and reduced customer trust); cost of recovering unanticipated damage to infrastructures; overall reputational damage extending beyond a company's own customers; wider citizens' loss of trust in the sector and online economy; competitive disadvantage due to intellectual property (IP) thefts; and opportunities

costs due to shifts in priorities and strategies in response to cyber crime (the opportunity costs of risk aversion and of failure to migrate to online systems, processes, services and products).

- **Defence costs:** direct defence costs of development, deployment and maintenance of cyber crime measures and indirect defence costs arising from inconvenience and opportunity costs caused by the defence measures.

Examples of defence costs include: cost of security measures, such as spam filters and antivirus; security services provided to individuals and industry, such as training and awareness measures; law enforcement; and all the opportunity costs caused by spending and implementing defence measures (the opportunity costs of lengthy security procedures and of increased spending on security at the expense of revenue generating activities).

3.5 MODEL DEVELOPMENT: FINALISATION OF MODEL LOGICS

So far, we have discussed some of the key relationships and logics that we have considered for the CLD model. They emerge from the primary data and literature, mostly in the form of cost-benefit insights, classifications of various types of cyber crime, costs and proxies for the more indirect costs of crime. However, what is still missing is an understanding of the dynamic interplay and the multi-level interactions among the various factors that drive the cost of cyber crime, above all from the differing viewpoints of value network actors. To take one example, there has been a growing concern about jurisdictional arbitrage opportunities of which cyber criminals take advantage by launching crimes from countries with inadequate cyber laws (Kshetri , 2005). Effective policing of cyber crime would require better public and government awareness about the scale of the problem. Such awareness has so far produced such global efforts as the 2001 Convention on Cybercrime. This called for the establishment of an international legal framework to address the impact of cyber crime internationally. It seems fair to assume that although political attention to issues such as these can be speeded up by public and media pressures, it may, nonetheless, be undermined by hiding of the real picture due, for example, to industry under-reporting. Furthermore, in relation to this awareness-government-effort interplay, some key questions remain unanswered. For instance, whether under-reporting prevents awareness and better global policing; and whether government policies and policing should take a back seat in comparison to the protection of the reputation of companies that under-report? Also, technological advances and corresponding improvement in protective measures are all positive developments, but what happens when cyber criminals also advance? These questions indicate that there is a need for the CLD model, to take the government and societal level into account as well as the evolution of various variables and their effects over time (such as the timescale for migrating banking services to new online systems and how long cyber criminals would take to find loopholes in the newly implemented systems).

Another example of dynamic interplay is associated with defence spending. We know that the majority of industry players feel the need to install better security systems, at least so that they are better protected than their competitors. In other words, their attitude typically is, ‘I don’t have to outrun the bear; I just need to outrun you’. Consequently, it would be informative to understand the trade-offs such players adopt when formulating their IT security budgets and whether there is an upper cost ceiling that companies will not break. Furthermore, it is also important to understand the impact of individual companies’ defence spending on the overall sector and on society as whole. Finally, from a customer’s view point, what sorts of things would make a bank customer stay loyal: speedy compensation after being a victim or only significantly reduced risk of, or even complete absence of, crime?

All these possible interplays indicate that cyber crime in the financial sector is characterised by multiple players, seeking different ends. Indeed our aim, while developing the CLD model, has been to bring the perspectives of all these players together and try to simplify this rather complex problem. The CLD SD model tries to factor in time and multiple feedback loops to lay out the structural behaviour of this complex phenomenon and presented it a systemised way. Although detailed data is

not easily available, the inputs from some of the industry's biggest banks, cards businesses and leading financial services firms have provided very practical and strategic insights that have helped fill many gaps and unknowns in the academic literature. From the literature, interviews and surveys, we have identified the major variables that form the key causal links in our model. In the following paragraphs, we will explain how we have developed these key interplays and multi-level relationships and how we have linked them together by applying logical extrapolations to fill in the missing causal links to develop our final system dynamics model so as to fathom a complex system.

First of all, the different, if at times, contradictory, perceptions of the impact of cyber crime emerging from the surveys and interviews reveal that under-reporting is indeed a major issue. The extent of under-reporting may depend on the actual numbers of cyber-attacks faced by a company. For example, the cause might be that the number of attacks it experiences is so high that the company believes there might be a risk of reputational damage if the numbers are revealed. Another impact of under-reporting that financial companies may have in mind relates to the cost of insurance for cyber crime losses (Detica, 2011). All these factors drive severe under-reporting by financial organisations. In order to capture this condition, we have identified the actual number of cyber crime incidents faced by the industry and the figures reported by the industry as two separate variables with two separate effects in our CLD model. Extrapolating from the problem of under-reporting, we make the logical assumption that the *actual* number of cyber crime incidents in an organisation determines its direct cost of cyber crime and cost of defence, while the *reported* number determines how governments and the media assess cyber crime threats and, in turn, affects public pressure for legal frameworks to tackle the issue. Of course, the figures reported also have a bearing on companies' reputations. This impacts on levels of general public trust in financial companies and, in turn, on financial companies' and the sector's ability to provide secure products and services.

Secondly, a degree of agreement emerges from the literature about some broad categorisation of cyber crime Based on the taxonomy developed in Section 3.2 above, and the results of the survey, we have identified specific types of cyber crime that are particularly relevant to the financial sector. These are: identity related crime, money laundering, disruptive attacks (hacktivism), IP thefts and cyber espionage. From Anderson *et al.*'s (2012) study and the insights from the surveys and interviews, we have also considered the main effects of these cyber crimes as: direct financial losses for financial companies; financial loss to customers; unanticipated damage to IT infrastructures (due to the knock on effects on the IT systems); reduced customer trust in new products and services; and disruptions affecting business functions. We have also considered some indirect costs as more generalised losses and opportunity costs imposed on the sector and society. Out of all these cost variables, loss of customer trust appears to be producing the most important and negative consequences. Companies wish to avoid such consequences at all cost in order to preserve sales of their financial products and services to their existing and potential customer base. However, we have also included in our CLD model the observation by one of the respondents that quick and effective compensation of losses incurred by customers due to fraud on their accounts, often leads to an increase in customers' trust and as a result growth in product and service use and sales. In relation to IP thefts and hacktivism, although there have been disagreements in the literature on their specific impact (Detica, 2011; Anderson *et al.* 2012), the interviews suggest that the sector has experienced a recent increase in IP thefts and hacktivist attacks. Therefore, both types of attacks have been included in our CLD model. It would be interesting to explore, in an extension to this study, the sales losses these produce. This could be done, for instance, by estimating these losses via the R&D costs of compromised products and use this as cost proxy (Office of National Counterintelligence Executive, 2011) together with sales figures before and after the occurrence of crime. Increased hacktivist attacks on IT systems also render companies risk averse, above all in relation to migrating to businesses models more dependent on IT platforms.

Thirdly, as mentioned earlier, the technological aspects of cyber crime have changed the face of traditional crimes. Wall (2005) has pointed out that technological advance may open up further avenues for criminals to exploit. Clearly, this requires some delay accounting for the time cyber criminals take to catch up with these technological developments and find new loopholes.

Technological advance also means increasing pressure, within the sector, to migrate business functions, products and services to online platforms, which bring productivity gains through larger servicing capacity, while avoiding the transaction costs of offering financial products and services through physical channels. On this point, based on the findings from the survey and interviews, we extrapolate the conclusion that the incentive of increased profit through cost cutting (Anderson *et al.* 2012) could cause companies to migrate anyway despite the risk of vulnerability to online attacks.

Fourthly, in relation to defence costs the following logics have been identified. The majority of our respondents stated that the main requirement, with regards to protection against cyber crime, is to have better security systems in place than competitors. This is primarily due to the needs: to win customer trust; and to avoid being considered a weak link that could be easily targeted. However, this attitude does not always translate into automatic spending on high-end security measures. For a small-to-medium sized company, state-of-the-art security measures may not be affordable. Indeed, while the majority of large companies will try to be as well protected as possible regardless of security cost, smaller companies might think of trade-offs between an acceptable level of security and the costs involved. All these costs, together with the opportunity costs of the losses and the opportunity costs of chosen strategies to deal with cyber crime, add up to give our total cost of cyber crime. We have used this total cost in our CLD model, reflecting both tangible and intangible factors. Furthermore, we have discovered from the surveys and interviews that the overall cost of cyber crime within the sector can produce two contradictory effects. The first is related to the high cost of cyber crime increasing pressures within the sector to be better protected, therefore driving-up security costs even more. However, in the longer term a second effect will emerge. The higher cost of cyber crime may affect companies' revenues, forcing them in the longer term to cut IT budgets since financial companies may become less able to afford expensive security systems on a consistent basis; it may become cheaper for companies to compensate customers. However, in the case of large banks, this is unlikely. For a large bank which perceives a negligible cost of cyber crime, affordability would not be an issue. As a result such banks would just continue striving for better protective measures to secure customer trust and maintain their brand reputation.

All of the above interactions are represented in our CLD model as variables connected by causal links and feedback loops. This has allowed us to start building into our model an initial multi-level view of how interdependent and differentiated factors interact to create complex and non-linear loops of interactions that both facilitate and/or deter cyber crime, while increasing and/or decreasing its economic and social costs. As a result our model of the impact of cyber crime on the financial sector uses both tangible and intangible factors and feedback characteristics. It takes into account the perceptions of the industry and the trade-offs and strategic decisions companies are forced to face on a daily basis when dealing with cyber crime and is illuminated by relevant academic discourse

4 MODEL RESULTS

We now discuss the final results of our SD model, implementing a CLD approach. We have developed our model in *Vensim PLE*[9] and focused on all the types of cyber crime from the taxonomy that are relevant to the financial sector (as discussed in Section 3.5 above). As underlined in Section 3.5, the causal relationships and feedback loops built into the model are all taken from the integration of insights emerging from the survey and in-depth-interviews (see Section 3.2 above) with previous studies, in particular from Anderson *et al.* (2012) and van Eeten (2009). Furthermore, we have made the following assumptions when designing the model:

- The actual number of cyber crime incidents faced and the figures reported by the industry are assumed to be distinct variables

[9] For details of hesoftware see. http://vensim.com/

- Apart from government's awareness of the dangers of cyber crime, public and media pressures are also needed for better efforts in law enforcement.

- Better reporting and awareness of the effects of cyber crime will not lead to all governments striving for global enforcement. Some governments set themselves other priorities higher than cyber crime, while others may not be culturally and historically inclined to international and/or cyber crime legislation. However, in general, a better awareness of the impact of cyber crime could trigger efforts from governments to tackle this issue. Therefore, the assumption made in the model is that increases in the reported number of cyber crime figures, as well as public media pressures, will push governments towards global enforcement and policing strategies.

- Revenues and profits of a company are affected by many factors. However, in our model, we have taken a simplified approach and assumed that an increase in company growth, due to higher sales, increases revenues and profits, while the losses due to cybercrime reduce profits.

- We have made another simplifying assumption in relation to the overall growth of cyber crime and IP thefts: as the number of cyber crime incidents increases so does the likelihood of compromised IP or sensitive data.

The main causal reinforcing and balancing loops of our model are explained in detail in Figures 2 to 8 below.

Reinforcing Loop R1 "Customer trust and security measures":

This loop explains why financial companies want to migrate to systems which support online products and services to perform their transactions and why customer trust in these new products and services is important. In this loop, the variable, "customer trust in new products" refers to the trust that financial customers (account holders, business clients, etc.) have in their financial products and services, and in the company which provides them. As shown in the loop, the higher the degree of customer trust, the higher the "transition to electronic payment systems". This leads to reduced transaction cost, as online payments have lower operating costs than traditional systems. This, in turn, leads to an increased "productivity gain" for the company (Anderson, R. *et al.*, 2012). This increased productivity can promote "growth of the company" and in time, lead to better "market cap/size of the company". This could, in consequence, boost company "revenue" and "profits". Higher "profits" lead to better "affordability of high-end security measures" and better "security infrastructure in place" within the company. This eventually serves the purpose of being able to "position the company in the market using enhanced security as a selling point".

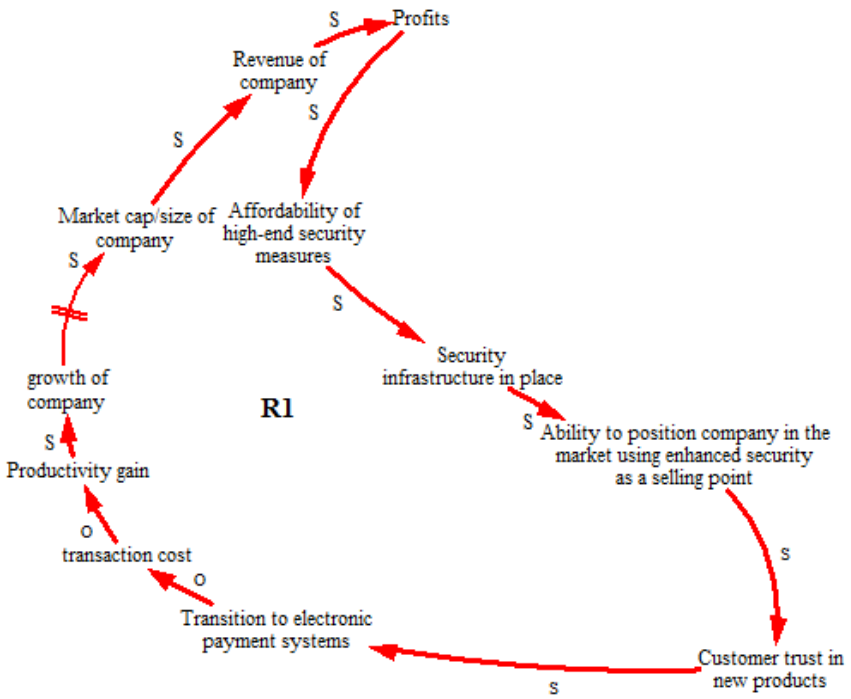

Figure 2: Customer trust and security measures loop

From loop R1, we can observe that compromising on customer trust leads to lower growth for companies as this can lead to smaller or no market expansion and lower or no transition to online systems. Loss of customer trust and/or loyalty is a major consequence of cyber crime. Therefore, in order to protect companies' growth, a focus on maintaining and/or improving customer trust and loyalty in the event of a cyber attack is important. This could lead to strategic moves towards not only preventive measures but also recovery measures, where the focus is more on efficiently and effectively recovering losses and greatly reducing inconveniences experienced by the customer following cyber attacks.

Reinforcing loop, R2 "Security infrastructure in place and strategic positioning"

The interviews revealed that customer trust is an important driver for spending on defence measures against cyber crime. However, defence spending also implies some opportunity costs. This has been captured in reinforcing loop, R2. In Figure 3, better "customer trust in products" leads to increased "sales of financial products and services". Conversely, lower customer trust could lead to lower sales, which may boost "the opportunity cost of foregone sales" for the company. This eventually contributes to the overall "cost due to cyber crime" within the sector. This increased cost could drive down "profits" and eventually lead to lower "security infrastructure in place" and even lower "customer trust" for a company.

Cost of cyber crime alone is not the only factor in determining the level of security infrastructure in place within a company. Indeed, as indicated by the surveys and interviews, certain companies implement high-end security measures just for strategic positioning and marketing their products and services more effectively in the market place. This is explained by the variable "strategic positioning through implementing better security measures as compared to competitors", which relates to how a company will position itself and its brands within the market vis-à-vis its competitors. Some companies feel that as long as they are more protected than their competitors, they have less need to worry about criminals targeting their systems because they assume that criminals will target the more vulnerable companies and their systems first. As a result, "strategic positioning through implementing

better security measures as compared to competitors" could also drive more "security infrastructure in place".

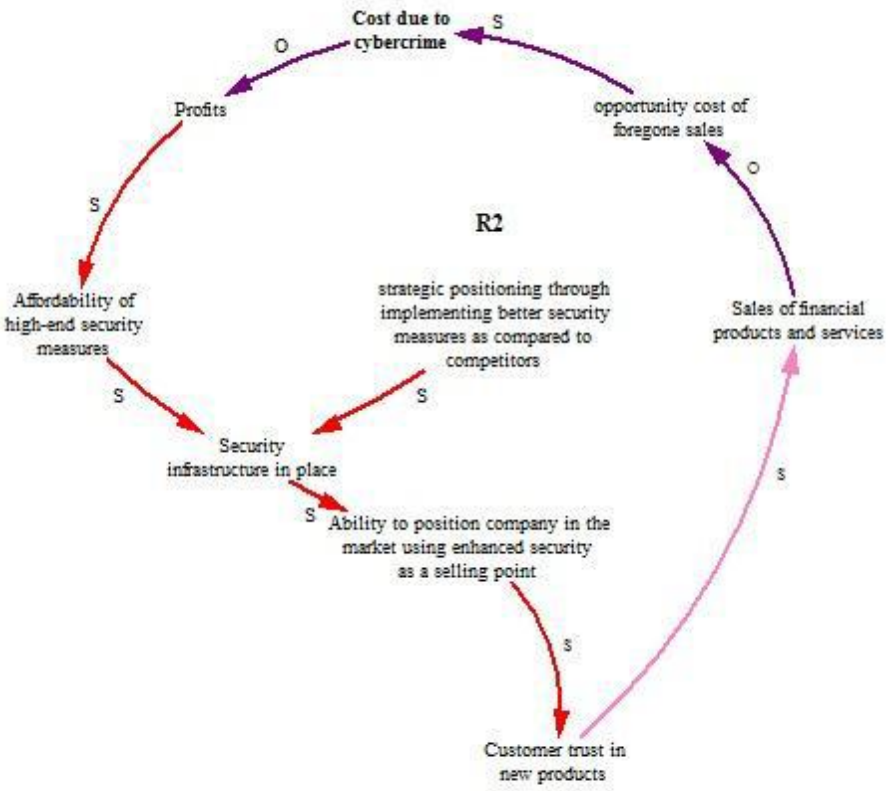

Figure 3: Security infrastructure in place and strategic positioning loop

Loop R2 shows a reinforcing behaviour where lower customer trust could affect a company's profits and send them into a spiral of decline. Some companies believe that better "strategic positioning through implementing better security measures as compared to competitors" can protect them from such spiralling decline. This strategic position is not driven by any empirical factors, such as number of successfully experienced cyber crime incidents and/or failed cyber attacks. It is, rather, a strategic position driven by the belief that competing in security measures can indeed increase customer trust and loyalty and protect these assets in case of a successful cyber attack.

Reinforcing loop, R3, and balancing loops, B1 and B2 "recovery and preventive security measures":

R3, B1 and B2 loops show similar variables to R2 loop but they include two additional factors: "the pressure within organisations to be well protected" and "efficiency of recovery after cyber crime incident". As shown in Figure 4 when there is more "security infrastructure in place", this drives up the "cost of security of cyber crime", which includes both direct and opportunity costs of preventive measures. This raises the "cost due to cyber crime" overall within the sector, which in turn increases "the pressure within organisations to be well protected". These relationships form the reinforcing loop R3. R3 shows how excessive security measures drive up the cost of cyber crime overall if companies do not adopt strategies to balance and achieve optimal spending on security. B1 also shows the balancing action for the over spending in R3. Here, the high cost of cyber crime within the sector reduces "affordability of high-end security measures" for companies, which in turn means that they will spend less for defence measures since they have less money to allocate to defence and therefore the cost of defence will go down. In loop B2, better "security infrastructure in place" raises "customer trust" and "sales of financial products" and eventually drives up the cost of cyber crime since more

sales will create more crime opportunities and more defence spending to protect more customer accounts. All these loops show how security measures affect sales as well as the overall cost of cyber crime. R3, B1 and B2 loops indicate that organisations need to limit irrational spending on security and find optimal solutions. B2 also shows that if the "efficiency of recovery after cyber crime incident" is high, this leads to more customer trust in the company, its products and services. More trusted products and services will increase sales. The customers would then feel that no matter the risk of cyber attacks, they need not to worry about the loss of money and time as the company would reimburse their losses and restore their products (e.g., accounts).

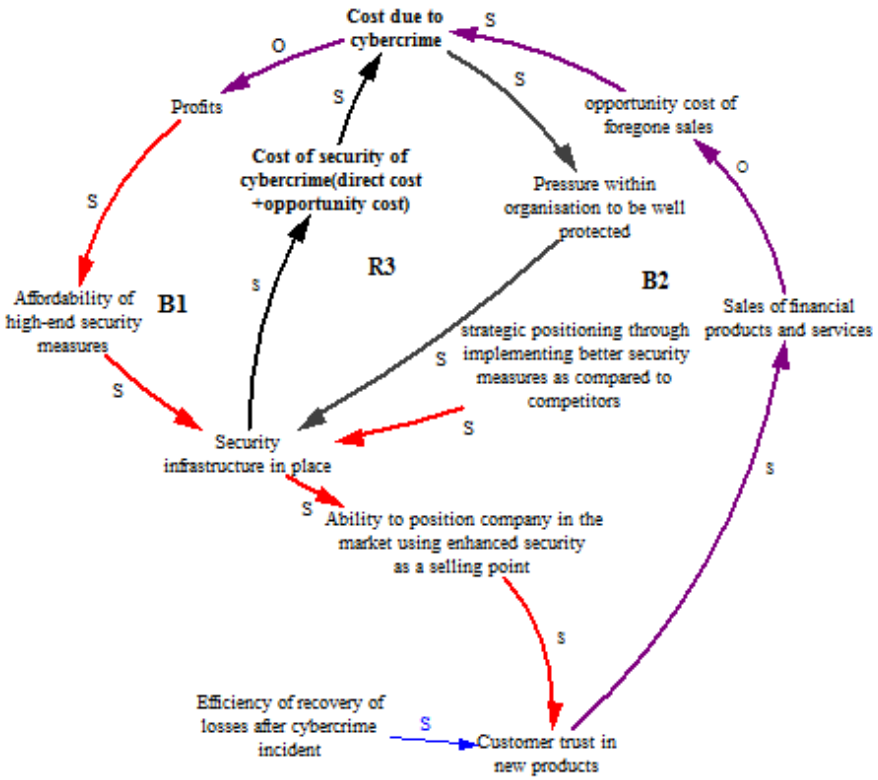

Figure 4: Recovery and prevention security measures loops

As already underlined in loop R2, companies that can afford better security will invest in defence measures in order to improve their strategic positioning; the marketing of their products and services; and customer trust and/or loyalty. However, loops R3, B1 and B2 indicate that fast clean-up and efficient recovery may be less expensive and more effective in winning customer trust rather than preventive measures alone. Therefore, companies' key concern does not always need to be on preventing cyber crime alone but also increasing company resilience through effective clean up and fast recovery. R3, B1 and B2, also stress that the key motivation for the industry in relation to security spending is not driven by the need to reduce the number of cyber crime attacks or incidents but rather to maintain customer trust and therefore high sales. As a result, there may be excessive spending in protective measures by certain companies, which in turn adds to the cost due to cyber crime. This spending could be significantly more than the losses incurred due to cyber attacks. Hence, a trade-off is needed between the cost of security measures and the level of protection actually needed for effective functioning of the business.

Reinforcing loop, R4 "under-reporting"

We have already highlighted the tendency of the financial sector to conceal cyber attacks to prevent reputational damage. Loop R4 (Figure 5) aims to illustrate the impact of under-reporting. R4 indicates that the higher the number of "cyber crime incidents", the higher the scope of reputational damage

perceived by a company. Based on this perception, companies decide to under-report cyber crime incidents. This leads to more "under-reporting", which drives down the "figures reported", which in turn reduces the "government estimation of impact" of cyber crime. The lack of awareness about the real extent of cyber crime then leads to lower "state effort to reduce cyber crime", fewer "global enforcement measures", lowers "organised nature and specialisation in policing cyber crime" and increased "jurisdictional arbitrage". All these will hinder "effective policing of cyber crime" and lead to growth of "cyber crime incidents".

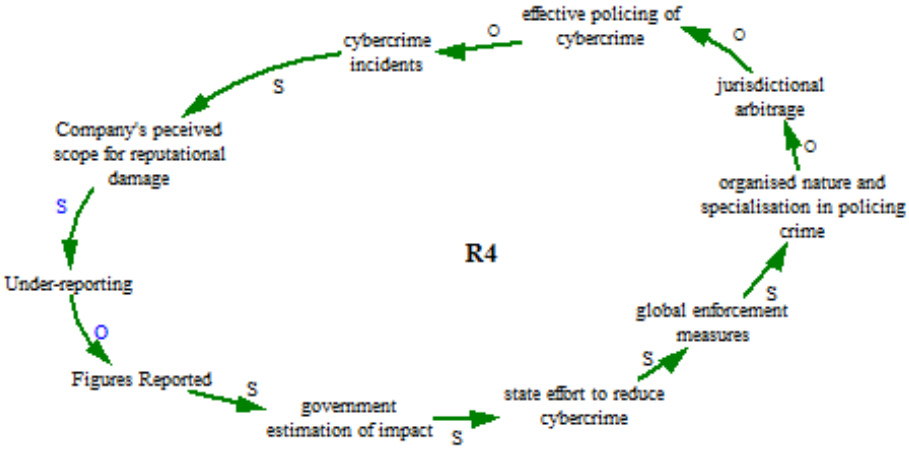

Figure 5: Under-reporting loop

Loop R4 sums up one of the biggest issues in understanding the impact of cyber crime. Cyber crime figures, reported by financial companies, determine the awareness of the cyber crime problem and in turn government measures to tackle cyber crime. When these figures are manipulated, it affects formulation of effective national and global strategies for policing and tackling cyber crime.

Balancing loop, B3 "Propaganda and reputational damage":

Balancing loop B3 (Figure 6) introduces the impact of reputational damage. B3 shows that the higher the number of "cyber crime incidents", the higher the probability that some of those incidents relate to "compromised IP and sensitive data", which increases the "possibility of sensitive information leak" and therefore propaganda campaigns against the financial sector, eventually leading to "actual reputational damage" for the company and the sector overall.

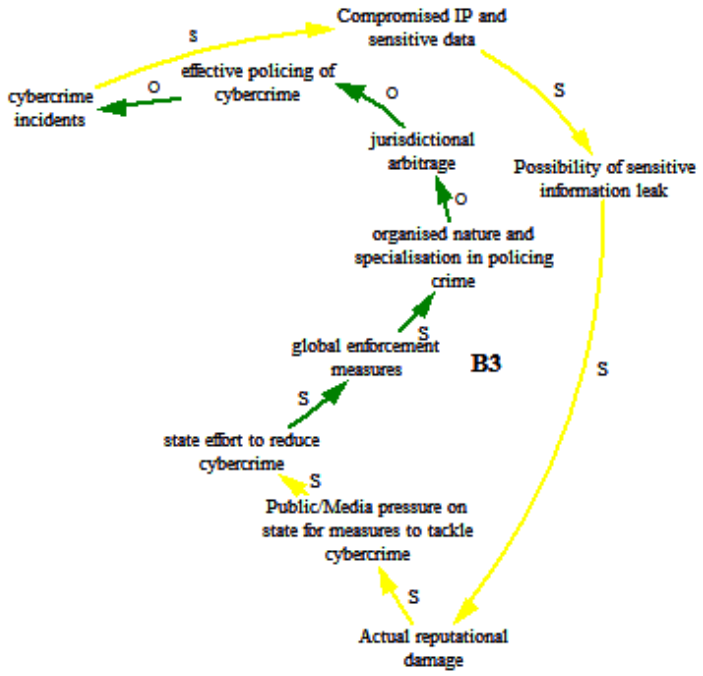

Figure 6: Propaganda and reputational damage loop

However the "actual reputational damage" in loop B3 also raises awareness of cyber activities and lead to more "public and media pressure to tackle cyber crime", which could work in the favour of increasing global enforcement and strategies for tacking cyber crime. Therefore, sensitive information leaks, possibly triggered by hacktivist attacks such as WikiLeaks, could have an initial negative impact on companies and the sector but an overall positive impact on society in the medium and longer term. This describes the public exposure of vulnerabilities in existing IT infrastructures and ways of dealing with cyber crime, prompting the design of more collaborative and effective measures to address those vulnerabilities and gaps.

Reinforcing loops, R5 and R6 "under reporting":

In addition to the problems that under-reporting produces in the previous loop R4, Figure 7, the reinforcing loop R5, shows that the lower the "figures reported", the lower the "actual reputational damage" faced by the company. However, this in turn can reduce the "public/media pressure to tackle cyber crime", which could lead to less awareness and fewer efforts by governments to address cyber crime, which in turn would increase the number of cyber crime incidents, leading to further manipulation of reported figures by companies.

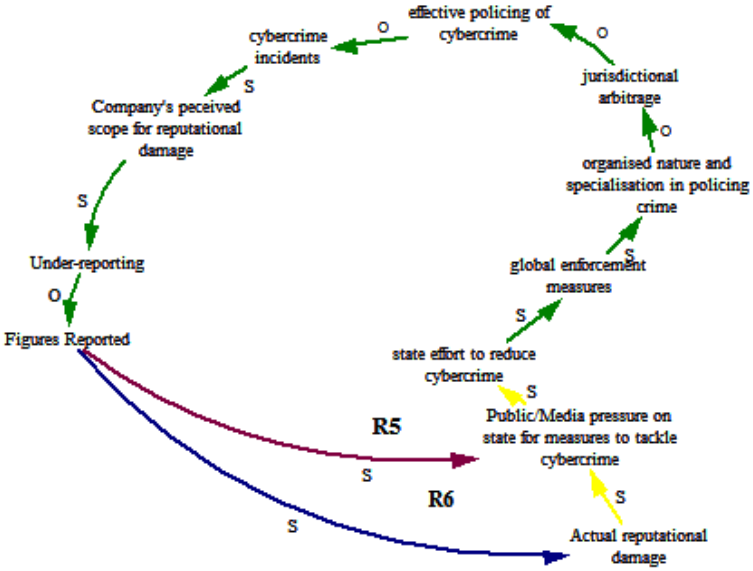

Figure 7: Reinforcing loops for under-reporting

The two loops, R5 and R6, work towards reinforcing the undesirable attitude of companies related to manipulating reported figures, which could lead to a social system where cyber crime is rampant. In this social system, companies will continue hiding the issue in order to protect their brand and market positions. As a result cyber crime is not properly addressed through integrated and effective measures, leading to companies continuing in their isolated and ineffective battles against cyber crime. Sofaer *et al.* (2001) describe how existing attempts to fight cyber criminal activities have only been deemed partially effective and usually provide short-lived results. Efforts tend to focus only on single-domain measures, these being solely legislative, technological, social and organisational, or cultural. Given the interdependent and multi-faced nature of cyber crime, anti-cyber crime responses need to be based on multi-actor co-operation, which will enable a full range of integrated responses.

Linear relationships:

There are many variables in our CLD model that do not form part of a loop and are instead part of linear linkages, directly connecting a cause to an effect. Too many linear relationships in CLD models specifically, and system dynamic models in general, are undesirable, as these models assume that in order to understand any system behaviour we need to focus on its feedback structures rather than its simple components. However, since our research uncovered an equal mix of linear and feedback relationships, we have allowed both relationships to be built in the model structure, but then we have focused only on the most important ones. The linear and causal loops discussed in this paper give us the final CLD model shown in Figure 8. The linear relationships in this model are intuitive and straight forward.

1. More cyber crime incidents leads to more “direct financial loss to company”. It also leads to higher “financial losses to customers” as certain costs are not recoverable. The distress suffered by customers is not included as it is difficult to simulate (Anderson *et al*., 2012, p5).

2. Growing numbers of cyber attacks also increase “risk aversion of companies”. This in turn reduces business appetite for exploiting new opportunities, such as migrating to a new online system, while leading to an increase in “opportunity cost of lost business due to risk aversion”.

3. There could be unanticipated damages of IT infrastructures due to certain cyber crimes. For instance, the immediate direct damage of the IT infrastructures may be small but the clean-up

cost of reinstating business-as-usual conditions may be high (ibid, p4). Therefore, an increase in cyber crime incidents could also increase the "cost of recovery of unanticipated damages to infrastructure".

4. Companies are insured against many risks. If the figure for cyber crime reported by a company is high, this could increase its "insurance premium".

5. Cyber crime incidents also cause "disruptions affecting business", which leads to a lower volume of sales, or no sale at all, during the disruption. If a financial company is unable to effectively and efficiently restore pre-cyber attack conditions, these disruptions also cause "inconvenience to customers due to restoration activities", which leads to lower customer trust. Another factor that affects sales is "compromised IP and sensitive data". This could lead to a higher probability of "selling of trade secrets" of a company, which could increase its "competitive disadvantage" and therefore reduce the company's ability to sell or market its products and services.

6. The "actual reputational damage", caused to a company by its publically known failures to deal with cyber crime attacks, could lead to lower "public trust in the company's brand and products". This is somewhat similar to a customer losing trust in the company's financial products and services as well as in the providing company as a whole due to being a victim of cyber crime (see loop R1 in Figure 2). However this causal connection refers to the amplified impact that reputational damage could have on a company's entire and potential customer base as a result of the company having publically suffered cyber crime failures, which in turn could drive down sales. All of these elements increase "the cost due to cybercrime".

7. In our CLD model, when delayed impacts are considered, "security infrastructure in place" is shown not to have an effect on the number of "cyber crime incidents". This is because even if one company is well protected, it will not be long before criminals seek out other companies whose infrastructures are more vulnerable (Jones, 2012) to perform their attacks. Technological advance may immediately reduce cyber crime incidents; however, criminals will soon catch up by exploiting loopholes in the new systems and products and therefore bringing the number of cyber crime incidents to what they were before the implementation of new security infrastructures (Wall, 2005). In addition, "overall technological advance" can increase both cyber crime incidents (i.e., the catching up argument) thereby decreasing sales, and also online activities, thereby increasing sales. Technological advance also leads to "pressure to migrate to online systems", which in turn leads to more "transition to online systems" after a delay and therefore more sales. The delay accounts for time needed by companies to test new systems and win over customer trust.

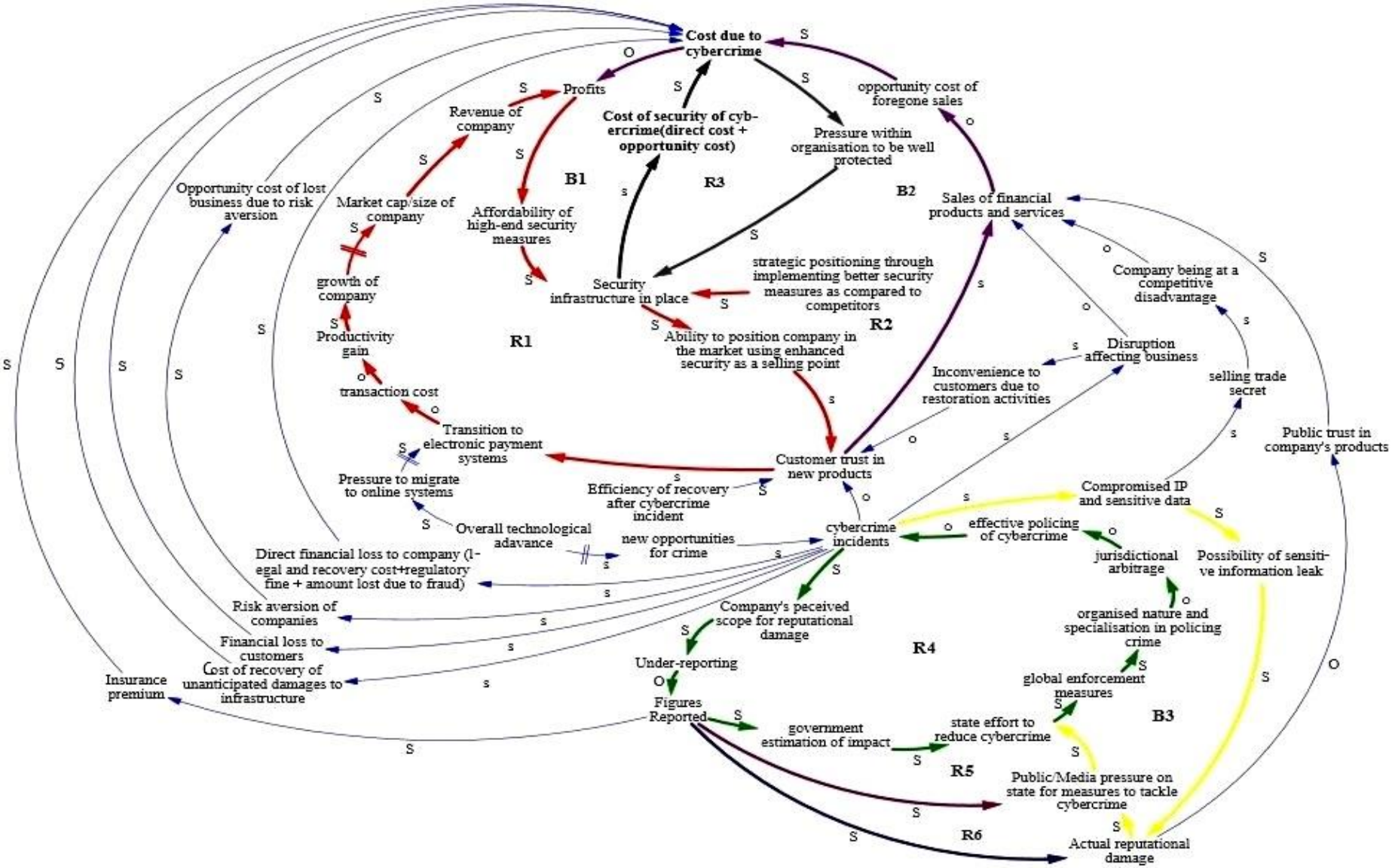

Figure 8: The full system dynamics model on the impact of cyber crime on the financial sector

From the linear relationships identified in the model, we can infer three interesting conclusions. First, as in the case of the more complex loops discussed earlier linear links indicate that for financial companies, better security infrastructures are mostly the result of considerations related to enhancing strategic positioning and customer trust. Secondly, there are also other ways to maintain and win customer trust. These strategies do not only rely on prevention but rather focus on fast and effective recovery after cyber attacks. Thirdly, two types of cyber crime incidents emerge as highly risky for financial organisations, namely IP thefts and leaks of sensitive information. Differently from the other types of cyber crime attacks, fast and effective recovery might not work in the context of these cases. Potentially, the reputational damage caused by them could be of such a scale that financial companies might find difficult and slow to recover the lost reputational ground.

5 CONCLUSIONS

In this article, we have described a SD framework, based on the CLD approach. It aims to understand the impact of cyber crime on the financial sector. Our results show that shifts in strategic priorities, having the protection of customer trust and/or loyalty as a key objective, together with considerations related to market positioning vis-à-vis competitors, are very important factors in determining the cost of cyber crime. Most of these costs are not driven by the number of cyber crime incidents experienced by financial companies, but rather by the way financial companies choose to go about protecting their business interests and market positioning in the presence of cyber crime. As underlined by the over-spending on defence measures and chronic under-reporting, financial companies' strategic behaviour as response to cyber crime has also an important consequence at sector and societal levels and, potentially drives the cost of cyber crime even higher. Unwanted factors, causally driven by other elements of the model, such as weak policing, weak international frameworks for tackling cyber attacks and more jurisdictional arbitrage opportunities for cyber criminals can all increase the cost of cyber crime, while delaying integrated and effective measures to solve the problem.

Our results show that strong dynamic feedback loops among tangible and intangible factors, affect cyber crime cost and occur at different levels of society and value network. This is consistent with recent theories and findings but we provide additional explanations absent elsewhere. Even with the limited number of data and variables used in our CLD model, highly interactive and multi-level relationships among the different factors appear to be a consistent feature of the nature of the impact of cyber crime. Ignoring this methodological and theoretical position could only delay future developments in the field. Cyber security theorists and methodologists should carry forward the task of understanding the systematicity and complexity of cyber crime activities and their consequences.

Acknowledgements: The paper draws on research performed for the European Commission under Grant Agreement numbers: SEC-2011.6.3-1 and SEC-2013.2.5-2. The authors prepared based on research on behalf of Trilateral Research & Consulting LLP in collaboration with the London School of Economics. The authors also acknowledge discussion of elements in this paper with David Wright and Kush Wadhwa and editing comments from Andrew Neish.

References

Anderson, R. "Why Information Security is Hard. An Economic Perspective". Annual Computer Security Applications Conference, 2001.

Anderson, R., R. Böhme, R. Clayton and T. Moore. "Security Economics and European Policy". Workshop on the Economics of Information Security, Tuck School of Business, Dartmouth College, NH, 2008.

Anderson, R., C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore and S. Savage. "Measuring the Cost of Cyber crime". Workshop on the Economics of Information Security, Berlin, Germany, 2012.

Beaujean, Marc, Jonathan Davidson and Stacey Madge. "The 'Moment of Truth' in Customer Service". *McKinsey Quarterly*, February 2006.

Bauer, J. M., M. J. G. Van Eeten and T. Chattopadhyay. "ITU Study on the Financial Aspects of Network Security: Malware and Spam", *ITU Report*, 2008. http://www.itu.int/ITUD/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

Becker, G. "Crime and Punishment: An Economic Approach". *Journal of Political Economy*, Vol.76, No. 2, 1968, pp. 169-217.

Bryson, J. M., F. Ackermann, C. Eden and C.B. Finn. *Visible Thinking: Unlocking Causal Mapping for Practical Business Results*. Wiley, Chichester, 2004.

Detica. *The cost of cybercrime*, Cabinet Office, London, 2011.

Eriksson, Johan, and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (IR)relevant Theory?". *International Political Science Review*, Vol. 27, No. 3, July 2006, pp. 221-244.

European Commission. *Towards a General Policy on the Fight against Cyber Crime*, COM 267, 2007.

European Commission. "Special Eurobarometer 390 Cyber security," 2012, http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf.

Financial Fraud Action UK 2012. http://www.financialfraudaction.org.uk/Fraud-the-Facts-2012.asp. 2012.

Forrester Jay. "Industrial Dynamics: A major breakthrough for decision makers". *Harvard Business Review*, Vol.26, No. 4, 1958, pp. 37–66.

Forrester, Jay. "Counterintuitive Behaviour of Social Systems". *Technology Review*, Vol. 73, No. 3, 1971, pp.52–68.

Geers, Kenneth. *Strategic Cyber Security*. CCD COE Publication, Tallinn, Estonia, 2011.

Gordon, L. A., and M. P. Loeb. *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, McGraw-Hill, New York, 2006.

Herley, C. "Sex, Lies and Cyber crime Surveys". Workshop on the Economics of Information Security, Washington, DC, 2011.

Information Security Forum. *Cyber Security Strategy*. Information Security Publication, 2011.

Kshetri, N. "Pattern of global cyber war and crime: A conceptual framework". *Journal of International Management*, Vol. 11, 2005, pp. 541-562.

Kshetri, N. "The Simple Economics of Cyber crimes". *IEEE Security & Privacy*, Vol. 2, No. 1, 2006, pp. 33-39.

Lane, D. "The Emergence and Use of Diagramming in System Dynamics: A critical Account". *Systems Research and Behavioural Science*, Vol. 25, 2008, pp. 3-23.

Moore T., R. Clayton and R. Anderson. "The Economics of Online Crime". *Journal of Economic Perspectives*, Vol.23, No. 3, 2009, pp. 3-20.National Cyber Leap Year Summit. *Co-Chairs' Report*, Washington, DC, 2009.

Jones, Neira. "Failing Gracefully", *Net Focus.* Weblog [Online]. March 2012. http://netfocus.baptie.com/blogs/neirajones/archive/2012/08/03/failing-gracefully.aspx .

Office of National Counterintelligence Executive. "Foreign spies stealing US economic secrets in cyber space*". Report to Congress on Foreign Economic Collection and Industrial Espionage*, October 2011.

Schneier, Bruce. "Schneier-Ranum Face-Off: Should we ban anonymity on the Internet?". *Information Security*, February 2010.

Senge, Peter, Art Kleiner, Charlotte Roberts, Rick Ross and Bryan Smith. *The Fifth Discipline Fieldbook*, Doubleday, New York, 1994.

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends". *Strategic Analysis*, Vol. 34, No. 1, 2010, pp. 62-73. http://www.tandfonline.com/toc/rsan20/34/1.

Sofaer, Abraham D., and Goodman, Seymour E. "Cyber crime and Security. The Transnational Dimension", in *The Transnational Dimensions of Cyber crime and Terrorism*, Hoover Institute, Stanford, CA, 2001, pp. 1-34.

Sterman, John D. *Business Dynamics: Systems Thinking and Modelling for a Complex World*. McGraw-Hill, New York, 2000.

The Economist. A Spook Speaks, Business and Cyber-security, 30th June 2012. http://www.economist.com/node/21557817.

The Ponemon Institute. *2010 Global Cost of a Data Breach*, April 2010.

Trustwave, *Global Security Report 2012*, 2012.

van Eeten, M. J. G. and J. M. Bauer. "The Economics of Malware: Security Decisions, Incentives and Externalities". *OECD Science, Technology and Industry Working Paper No. 2008/1*, 2008.

van Eeten, Michel, Johannes M. Bauer and Shirin Tabatabaie. "Damages from Internet Security Incidents. A Framework and Toolkit for Assessing the Economic Costs of Security Breaches". *TU Delft OPTA*, February 2009.

Wall, David. "Mapping out Cyber crimes in a Cyberspatial Surveillant Assemblage", in F. Webster and K. Ball (eds.), *The Intensification of Surveillance: Crime, Terrorism, and Warfare in the Information Age*, Pluto, London, 2003, pp. 112–136.

Wall, David. "The Internet as a Conduit for Criminals", in April Pattavina (ed.*), Information Technology and the Criminal Justice System*, Thousand Oaks, Sage, California, 2005 (Chapter revised March 2010), pp. 77-98.

Wall, David. "Policing Cyber crimes: Situating the Public Police in Networks of Security within Cyber space". *Police Practice and Research: An International Journal*, Vol. 8, No.2, 2007, pp. 183-205.

Wall, David. "Cybercrime, media and insecurity: The shaping of public perceptions of Cybercrime". *International Review of Law Computers and Technology*, Vol. 22, 2008, pp.45–63.