New Economic Models in the Digital Economy

Case Study on Coordination of Cybersecurity Risk Management in the UK Insurance Sector

Paul Klumpes

Professor of Finance and Risk Accounting

Nottingham Business School

Nottingham Trent University

Newton Building

Nottingham NG1 4BU

UK

Paul.Klumpes@ntu.ac.uk

Direct: +44 (0) 115 8486512

ABSTRACT

This paper reviews the literature on the impact of government interference and public policy developments on recent trends in cybersecurity risk and cyberrisk insurance in te UK insurance industry. A complexity theory approach is then used to outline a short case study documenting these efforts, based on the interviews conducted with relevant stakeholders, regulator representatives and other key gatekeepers as to most relevant areas and highlights efforts by the Bank of England to coordinate the industry's resilience against cyber attacks.

1.Aims and Objectives

London is currently the world's leading financial centre within the increasingly integrated, technologically sophisticated and growing global financial system. Moreover the UK financial services sector provides a significant contribution to the overall wealth of the UK, and is therefore a key element of the nation's Critical National Infrastructure (CNI).[1] Moreover, responsible financial service entities operating in the UK have recent years become increasingly sensitive to and concerned about cybersecurity risk.[2] It is therefore important to develop more integrated and timely monitoring systems that effectively communicate the associated information risk from the IT and operational risk areas to the board. However there are currently still no UK regulations that specifically address either the appropriate protocols for networks to mitigate against these threats, or to the reporting of such risks to the board, regulators and key stakeholders.[3] There are also internal governance implications. Dutta et al. (2002) argue that cybersecurity risk management is a management issue, and not an IT issue. However these two issues have not been previously studied in a single paper.

There is limited evidence in the corporate governance literatures concerning the effects and likely impact of cybersecurity threats on the overall resilience of financial service and insurance organisations specifically. Klumpes *et al.* (2013) examine the risk reporting

[1] Cybersecurity is the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access. CNI is defined as "certain 'critical' elements of infrastructure, the loss or compromise of which would have a major, detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life".

[2] According to The Financial Times, cybersecurity attacks on companies has doubled in 2012-13 compared with the previous financial year (Financial Times, 21/10/13). The latest Lloyd's (2013) risk index survey reveals that cybersecurity risk is now the third most important perceived risk faced by UK business, significantly higher than in 2011 when it was only ranked 12th.

[3] In the US, the Securities and Exchange Commission requires registrants to disclose, as part of the management discussion and analysis part of their annual report filing ("10-K") the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. However Ferraro (2013) argues that these SEC disclosure requirements are too vague and not sufficiently informative.

practices by a sample of Global 25 largest insurers in the period 2006-2012. They find limited evidence of disclosures related to cybersecurity threats especially in the non-US firms. The ICAEW (2012) provides an overview of current practices concerning the ethical and other implications of recent developments in cybersecurity threats. Wang *et al*. (2013) find evidence that capital markets are sensitive to the disclosure of security risk factors by corporations.

There is more extensive literature on this issue in the computer science discipline, but is mainly limited to the non-financial sector. Ma and Abdulatif use various formal methods, including knowledge based theory (Ma *et al*. 2004, 2005a, 2005b, 2005c, 2005d, 2006a, 2008, 2010) and linear temporal logic (Abdulatif *et al*. 2012, 2013a, 2013b) to systematically and mechanically analyse the potential security challenges to and possible flaws contained in security protocols, some of which have been widely used. The syntax, semantics as well as the type theory of such methods have been carefully investigated (Ma *et al*. 2006b) to ensure that they are effective and robust. As cloud computing is now becoming more extensively used in data and information management, the security concerns have been thoroughly studied by Ma (2012). Due to the increasing reliance on sophisticated computer databases, the security attacks on them, especially tracker attacks on statistical databases, have been analysed and countermeasures have been proposed by Ma (2011a, 2011b). In addition, Simpson *et al*. (2008a, 2008b) and Russell *et al*. (2009) have proposed new approaches to secure data sharing in healthcare sector, resisting cyber-attacks on confidential information transmitted over Internet. These findings and results can be extended to the financial sector.

Most recently the UK government has joined forces with insurers on cybersecurity, as part of its efforts to manage cyber risk within the UK government Cyber Essentials Scheme (UK Government, 2013) and more generally to implement its Cyber Security Strategy (UK Government, 2011). However there is little or no literature evidencing the effectiveness of

such coordination efforts to mitigate or prevent cyber attacks. The report seeks to contribute to this topic. Specificially it briefly reviews the relevant literature in order to identify and review best practices facing insurance firms in managing the trade-off between seeking value added benefits from big data and cloud computing developments and assuring data integrity of their systems against cyberattacks. It then briefly outlines a short business case that documents latest efforts by the UK regulators, firms and both professional and international bodies to coordinate with the insurance industry and key professional bodies to enhance resilience against cyberattacks

The rest of this report is organised as follows. The next section provides the institutional background to the study. Section 3 provides a brief literature review of salient research. Section 4 outlines the conceptual framework used to analyse recent developments. Section 5 provides an overview of the research methods used. Section 6 reports the results of the discussions. Section 7 provides a conclusion.

2. Institutional Background

Key UK insurance firms trade-off the benefits of enhancing their business model through exploiting developments in cloud computing and big data, with the costs of investing in cyber risk management, and the strategies employed (e.g. via insurance, regulatory compliance and operational management). The case documents the dynamic and increasingly integrated threats from various sources:

- Frictional risks from increased direct and hidden costs of complying with existing and developing EU and UK data protection laws (Grady and Parisi, 2006).

- There are significant and material investment in cybersecurity resilience based audit and IT departments. Consultants regularly offer competitive and new digital security insurance and risk management solutions across the sector and best practices used by key insurance firms to identify fraud losses and potential theft of personal data held by organisations, related to both internal and external parties.
- The rapid growth of information technology-based solutions has facilitated globalisation of services and transformed business models.
- Current UK Protection laws and EU proposals for upgraded data protection laws and consider their likely impact on corporate responsibilities to comply with cybersecurity law, such as the international convention on cybercrime, human rights, national security, as well as civil and criminal law related to money laundering, data collection and identify fraud.

The report focuses primarily on recent issues related to cyber risks affecting key insurance firms, regulators and professional bodies to help better understand how these developments inter-relate with best practices in information risk governance, data and information management arising from recent technological advances. It also informs the business and academic community generally about the nature and outcomes of regulatory efforts to coordinate resilience of insurance firms against cyberrisk.

UK insurance entities are particularly susceptible to cybersecurity attacks because the integrity of their business models involves inter-connected responsibilities for maintaining resilience of their systems to various gatekeepers (e.g. regulatory agencies), actors (e.g. other financial services entities), and stakeholders (e.g. shareholders, consumers) which create pressures to ensure best practices in information risk governance, data and information

management. To achieve success in international markets, UK-based global service providers and professional attestation firms face challenges of moving towards competing on being able to offer unique, high quality assurance and innovative integration solutions to their financial services clients. Newly evolving EU and US based regulations impose complex risk-based reporting and capital adequacy rules, which requires firms to increasingly rely on complex web-based financial models for integrated data assurance and cybersecurity risk management.

A key challenge facing such firms is to demonstrate sufficient ethical management, and ensure high quality data integrity capabilities in order to meet increasingly stringent and complex requirements imposed by regulators. This however also requires firms to face the need to trade-off investment in high quality of regulatory compliance monitoring mechanisms, with providing high quality value added services and performance to their clients and investors, respectively. However, the financial services industry generally, and the insurance industry specifically, particularly in globally exposed markets such as the UK, faces unique challenges in a changing regulatory environment. Enhanced infrastructure protection is also a key concern for financial service firms and their stakeholders. New Solvency II regulations and the proposed overhaul of existing Basle II regulations (where relevant) require greater reliance on complex financial models that require integration with existing financial, regulatory and customer databases.

3. Literature review

There is relatively little empirical, conceptual or analytical academic research specifically on cyber risk and/or cyber insurance that is of relevance to this study. Shackleford (2011) argues that firms should adopt a proactive approach to safeguard their assets against attack in a competitive environment. Biener et al. (2015) provide evidence of the insurability of cyber

risk in a European and US context and find that there are significant problems in the market due to adverse selection problems, resulting from highly inter-correlated losses, lack of data and severe information asymmetry. They also provide evidence that there is a distinct lack of cyber insurance coverage available in the European context, in contrast to the US, possibly due to the lack of public policy engagement and reluctance of firms to disclose breaches.

The lack of literature bearing on this topic contrasts with the frequent and often contradictory financial press coverage of these issues. For example the Computer Weekly (2014a,b,c,e) contains frequently contradictory articles in the benefits and costs of cyber risk insurance, perhaps because the authors are seeking to publicise their own consultancy services in this area. The Financial Times provides regular articles on this topic, but mostly focuses on the impact of cyber-attacks on the banking sector (e.g. Braithwaite and Kuchler, 2014, Bonner, 2014, Arnold, 2014, FT Reporters, 2014; Solman, 2014).

By contrast there are relatively few articles on the direct impact of cyber-attacks, or the incidence of cyber insurance (Gray, 2014a, b). More recently the Bank of England penetration testing or CBEST was launched in October 2014, with the intention of testing financial services firms' systems resilience against "ethical hacking" by BofE staff, the existence of such practices were first documented in April 2014 (Fleming 2014). However there is no public announcement of such efforts apparently due to the confidentiality issues (Solman, 2014).

This situation contrasts with that in the US, where the Securities and Exchange Commission has issued guidance on disclosure of security breaches by US corporations. This in turn has facilitated empirical studies on the effectiveness of such disclosure requirements (e.g. Dutta den McCroban, 2002; Wang et al., 2013; Ferraro, 2014).

Despite the lack of evidence on coordination efforts, there are a number of studies sponsored by consultancies (e.g. the Ponemon Institute, 2013, 2014; Datamonitor Financial, 2013), insurance firms (e.g. Atlantic Council and Zurich, 2014; Marsh 2014) and professional organisations (e.g. AIRMIC, 2013; ICAEW, 2012 and Institute of Risk Management, 2014; World Economic Forum, 2013) on various issues pertaining to both cybersecurity risk management and cyber risk insurance. However none of these studies focus specifically on the insurance industry. Although there are regularly held conferences on this topic (e.g. Institute of Risk Management, Association of British Insurers) these have not resulted in contemporary publications that shed light in this area.

4. Conceptual Framework

This section briefly outlines the theoretical basis for the research, identifies the key users and beneficiaries, and sets out the key research questions addressed.

4.1. Theoretical Antecedents

The case study draws on elements of both systems theory and complexity theory on corporate governance (Goergen *et al.* 2012) to examine the inter-connectedness of cybersecurity risk management both at the corporate governance level and the IT governance level. Further, key gatekeepers, such as regulators, auditors, IT and risk management professional advisers play a key role in determining the property rights and information production costs associated with assuring data and information integrity (Klumpes, 2013).

The proposed conceptual framework for this project directly addresses key priorities of the RCUK (2011) programme concerning close connection to requirements of users in policy and business sectors, and the wider public by integrating elements of complexity theory and systems theory. This is because specific types of best practices that are identified by the application of the conceptual framework to deal with cyber-attacks for both data and information management and broader reporting processes, require the close engagement and interaction of major actors in the UK financial services sector, their internal and external stakeholders and key gatekeepers. Further, the project is broadly relevant to the managing multidimensional complex risks that require cross-disciplinary analysis of complex risks, through the collaboration of business school and computer science department expertise to integrate knowledge of the impacts of cyber-attacks in the corporate governance and IT governance. Finally, by focusing on a specific industry sector, the outcomes arising from the project will specifically assist financial service sector organisations operating in critical infrastructure areas to achieve sustainable compliance with corporate governance and legal requirements regarding the management of cybersecurity risk. It will ensure greater integrity and resilence of data and information management, and risk reporting processes. The integration of these services will also be of much broader interest to both the financial services entities, regulators, professionals, industry association and academic communities.

4.2. User and Beneficiary Engagement in Implementation of Research

The project involved primary engagement with key industry-based organisations that are concerned about cyber-attacks, secondary engagement with industry associations in the relevant sub-sectors, and academic programmes on equivalent topic(s).

The primary beneficiary of the analysis is the Bank of England, which participated in all stages of the research project, including the development of the conceptual framework,

archival data analysis, content analysis, survey questionnaire design and conference participation. The Bof E also participated a business roundtable on the impact of cyber-attacks on the board.

In addition, the project also invite industry associations that represent the four key sub-sectors of the UK financial services sector to participate in the survey and conference participation elements. These include key industry players, both in terms of cybersecurity risk management and providers of cyber risk insurance, as well as BofE which has recently conducted research on the potential impact of cyberattacks jointly with the cabinet office, HM Treasury and the Financial Conduct Authority. Other professional bodies consulted included AIRMIC Ltd, and the Institute of Risk Management, which has recently published a report on risk resilience and tolerance issues within the financial sector (IRM, 2014), aswell as the Institute and Faculty of Actuaries, which has recently set up a working party on cyber risk management.

4.3 Research questions

The conceptual framework helps clarify the interrelations betweeen how UK-based insurance firms can manage information risks associated with cyberattacks to provide greater assurance to their key internal and external stakeholders, gatekeepers as well as the broader public as to the integrity and resilience of existing data and information databases to sustain cyber attacks.

This framework was then applied to analyse the interactions between financial service entities, regulators and other parties to ensure transparent, resilient and robust management of cybersecurity threats in order to address the following specific questions.

1. What is the impact of latest regulatory developments and the effectiveness of recent efforts to coordinate the ability of the UK insurance industry (e.g. via the BofE's CBEST initiative) to assure the resilience of their systems against cyber attacks in the light of recent innovations in cloud computing and big data and evolving regulatory and societal pressures to assure integrity of these resources?
2. What is the impact of these ongoing developments on best practices by insurance firms seeking value added benefits from exploiting big data and cloud computing innovations?

5. Research Methods

The following research methods will be used to examine the above research questions:

(i) ***Case study.*** A case study will document current digital economy trends on key UK insurance firms

(ii) ***Interviews.*** Used to identify best practices by insurance firms in seeking to benefit from the CBEST initiative to enhance their systems against cybersecurity threats.

5.1 Case study – Key Stakeholders and Gatekeepers

In this section, we briefly overview the major gatekeepers, industry participants and other stakeholders in the cybersecurity risk management of the UK insurance industry. This discussion is kept at a fairly brief level.

5.1.1. Bank of England and other Regulators of Cybersecurity in the UK

Operational and Cybersecurity Risk Management is a fundamental concern to all financial organizations in a digital economy and is an important subset of enterprise risk management.

The use of the internet has significantly increased the vulnerability of financial organisations to information theft, vandalism, and denial-of-service attacks, thereby bringing information security issues to the forefront of the agenda for business innovators and corporate risk management executives. At the same time, there has been increased demand by regulators, shareholders and rating agencies and customers for credible and more sophisticated techniques for capital management and financial guarantees to meet new and developing IFRS, FSA-based individual capital assessment and Solvency II requirements. This in turn led to an increased demand for and the associated use of sophisticated computer systems and scenario stress testing models in the banking, finance, insurance and investment industries.

The UK Government (2011) has raised awareness about the importance of information risk and its link to corporate governance effectiveness.[4] While issues of security, confidentiality, integrity, availability, accountability, non-repudiation and reliability are the foundations of computer security generally (Gollman, 2011) there are specific issues for financial service providers, particularly related to the potential for loss or misuse of sensitive regulatory and consumer-related data.[5] The UK Data Protection Act requires that "appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."[6]

Recently the issue of cybersecurity threats and its relevance to corporate governance effectiveness in managing information risk have received extensive coverage in the financial press. However an important issue is the trade-off between ensuring that ethical responsibilities to disclose cyber attacks and their financial consequences to stakeholders are

[4] Information risk is defined as the "guardianship and management of information in all its aspects (integrity, availability and confidentiality) that is crucial to public service delivery" (UK Government, 2008, 6).

[5] Latest statistics suggest that data theft by employees is pervasive, especially for financial services firms (Computer Weekly, 2 September 2013). The Financial Conduct Authority (2013) has reported receiving reports that fraudsters are using the name or other details of a genuine firm.

[6] Schedule 1, Principle 7 of Data Protection Act (1998). However neither the Act nor the Information Commission Office charged with implementing the Act provide any specific guidance for financial services.

met, and the potential loss of privacy and the information production costs associated with making effective disclosures in the public domain. However, there is also little research concerning the financial consequences of such trade-offs in cybersecurity risk management of insurance firms.[7] Moreover the

The UK government has already committed £650 million to the National Cyber Security Programme (NCSP) launched in 2010. However since then there have been increasing threat posed by state industrial espionage, and international e-crime committed for political or personal purposes (Home Affairs Committee, 2013). The Intelligence and Security Committee (2013) raised issues of potential ethical conflict between commercial imperative and national security as a result of increasing private ownership of telecommunications networks that are considered to be part of the UK's critical national infrastructure.

However, although the quality of investment in cybersecurity risk management processes is essential to meet regulatory needs and enhance the robustness and integrity of financial services firms' data and information exchange, its impact on key external stakeholders and gatekeepers has not been previously systematically studied.[8] There is also a lack of information sharing and engagement about these issues among firms and key gatekeepers.[9]

On 17 September 2014, the Financial Reporting Council (FRC) issued an updated version of its UK Corporate Governance Code including the related document *Guidance on Risk Management and Internal Control and Related Financial and Business Reporting*. The revised Code will apply to accounting periods beginning on or after 1 October 2014. The new code requires firms to disclose their principal risks, their policies for mitigating risks and the

[7] The Australian government established the Computer Emergency Response Team which annually surveys the impact of cyber crime and security issues affecting businesses comprise Australia's CNI.
[8] In March 2013 six South Korean banks were affected by a North Korean cyber attack, disrupting financial services worldwide and costing £500million to clear up (Guardian, 16 October 2013).
[9] The Australian Strategic Policy Institute (2013) recommends greater geopolitical engagement on cyber security attacks, but did not focus distinctly on the financial system. The BBA (2013) recommended greater regulatory coherence in financial services but did not refer to cybersecurity issues specifically.

monitoring mechanisms used by the board to ensure effectiveness and risk culture. However there is no specific application to insurance.

The Bank of England's Prudential Regulatory Authority, which was only fully effective in 2013 under the Financial Services Act, specifically is responsible for the preducential regulation of insurers and other financial service firms. It works together with the Financial Conduct Authority to provide a twin peaks regulatory structure. However the 2013 latest annual report of the PRA makes no specific mention of cybersecurity risks nor of the cyber risk insurance activities of the UK insurance sector.

5.1.2. Stakeholders – Industry Players

The major insurance companies are both part of the UK's critical infrastructure and major players in the cyber risk market. A recent Geneva Association conference held in London highlighted the importance given to cyber risk management and insurance issues by key players such as Zurich, Aviva as well as smaller insurance firms. Most of the issues covered concerned the lack of coordination between regulators and the industry in addressing concerted cyber-attacks, notwithstanding the recent UK government consultation with the industry. Because of the competitive nature of the market as well as the lack of uniform mandatory disclosure of cyber breaches in the UK and/or the EU (in contrast to the US) there is a distinct unwillingness to voluntarily disclose breaches. This situation contrasts with the UK banking industry, where large UK banks regularly report such breaches and whose efforts to mitigate them involve active coordination by the relevant industry body (The British Bankers' Association). By contrast, neither the equivalent industry body for insurance (the Association of British Insurers) nor that of insurance brokers (The British Brokers

Association) currently (to the best of the author's knowledge) have any active programme of consultation with the industry on such issues.

5.1.3. Professional Bodies

As mentioned above, both AIRMIC Ltd and the Institute of Risk Management issued publications on cyber risk management and insurance. However they did not specifically address insurance issues. The Institute and Faculty of Actuaries presently do not have an active research programme of publications in this topic, although it is currently under development.

5.1.4. Gatekeepers – Consultants and Advisers

Consultancy and advisory organisations specialising in cyber risk management and/or insurance produce annual publications in these areas (e.g. Marsh, Ponemon Institute) although these tend to be US, rather than UK or EU oriented. The Big 4 accountancy firms occasionally issue reportst to their clients on current developments although these lack specificity. It appears that a large number of consulting actuarial firms and other consulting firms have strong interest in the area although none were prepared to be interviewed and did not produce publicly available regular surveys, specifically in connection with the UK and/or EU insurance industries.

5.2. Interviews

A series of interviews were held with representatives of the BofE, industry players and key professional bodies with explicit interest in the topics of risk management and/or insurance of cyber risk as connected to the UK insurance industry.

The Bank of England representatives included the Chief Information Security Officer as well as various officials from the Prudential Regulatory Authority Department of BofE that are connected to the supervision of the UK insurance industry. Some of the interviews were in a round table session hosted by an insurance brokerage firms. No representative from the Financial Conduct Authority could be identified for interview within the project scope. An official from the Department of Business Innovation and Skills with supervisory authority in the cyberrisk area did not respond to requests to be interviewed.

Key industry players interviewed included Aviva, QBE Insurance and Zurich. A number of other insurance firms declined to be interviewed. Views on the relevant topics were solicited from attendance and participation in a Geneva Association conference held in London in October 2014.

Professional bodies interviewed included the IRM and Institute and Faculty of Actuaries (IFOA). Representatives of industry and/or trade bodies or associations such as ABI and BBA, declined to be interviewed. Actuaries specialising in these topics were interviewed following the author's presentation of a paper at an IFOA sponsored "GIRO conference" held during September 2014. However only a small proportion of those attending the session subsequently agreed to be interviewed. An accountancy regulatory body and some consultants and other professional industry associations were also approached but did not respond to requests for interview.

A number of consultants and advisers were also approached, but declined to be interviewed. Some discussions were held informally. It would appear that a combination of confidentiality issues, and seeking to retain competitive advantage contributed to the poor response rate.

6. Discussion of Interviews

A total of 10 interviews were conducted over a period of five days in London during October-November 2014. Of these, 3 interviews involved BofE and/or PRA officials, 3 interviews involved industry players and/or insunce brokers, and the remainder were held with Professional bodies such as the IFOA and IRM representatives. The major results of these interviews are discussed below. For confidentiality reasons, the names and affilliations of those interviewed has been withheld.

6.1 Bank of England and/or PRA

The BofE has three major areas of interest in cybersecurity risk management and insurance issues within its remit. First, it has a responsibility to ensure systemic risk avoidance through the coordination of cyber attack mitigation in coordination with key players of the UK financial services industry. Second, it has a specific responsibility, through its insurance division located within the Prudential Regulatory Authority department, over the audit and quality monitoring of cybersecurity risk management systems of major players. Third, it has a responsibility to monitor and supervise insurers offering cyber risk insurance. The interviews addressed issues related to all three of these areas, the major result of which are briefly outlined below.

The CBEST initiative was specifically instigated by the BofE to assure the intrigity of standards of cyber risk management of the UK financial services industry, of which the insurance industry is a key component. It is also connected to the UK government's policy on cyber risk as documented above. The Chief Information Security Officer of BofE had recently been interviewed on international and national efforts to coordinate defence of the

banking industry to cyber attackes (Amar, 2014) but did not mention the insurance industry. He did not refer to any specific initiatives focusing solely on the insurance industry, however noted the recent consultation between the government and key industry players.

Other officials from the PRA were interviewed as part of a broader industry roundtable that was hosted by a key insurance broker. Some officials were responsible for supervising the cyber risk insurance market, while others monitored activities by key players with significant cyber security risk exposure. It became apparent that regular coordination between various officials within the PRA was lacking and an outcome of the meeting was to improve this. However the officials did not respond to further requests for interview to clarify these comments subsequently.

6.2. Industry key players

The industry sector has a strong interest in ensuring adequate monitoring of the cyber risk management systems. Additionally there are issues relating to how cyber risk insurance should be "priced" for soon-to-be-implemented European wide Solvency II capital adequacy requirements. The representatives of the two major insurance companies interviewed claimed to have sophisticated and regular monitoring of such attacks, but declined to name instances of such attacks. They also admitted that the design and implementation some of the relevant protection software was outsourced to third party consultants.

A further issue concerned the pricing of cyber risk insurance. An interview was held with senior managers and underwriters of a major insurance broker in this market. It was aapparent that there is a lack of publicly available data on the instances and severity of recent cyber attacks on the UK insurancce industry. The lack of such generally available data reduced the efficiency of the market but also created more opportunity to operate in what was regarded as a fairly lucrative market. The absence of any recently publicly known severe

cyber attacks on key industry players (in contrast to the banks) contributed further to the lack of actuarially fair pricing of insurance.

Senior management representatives of both large and small insurance firms discussed the growing importance of these issues at a Geneva Association conference held in London in October 2014. However the author had only limited opportunities to follow up specific issues with the key speakers. It appears that cyber risk management is a key and major consideration for most of these firms. However by contrast the cyber risk insurance market is seen as being "high risk" and creates complications for both actuarial fair pricing and capital modelling purposes. There appeared to be a lack of consensus among speakers as to the growth potential of this market in the European context, although all agreed it was a significant and major issue for boards of companies.

6.3. Professional bodies and Industry Associations

Various industry bodies, including AIRMIC Ltd, IRM were interviewed but did not appear to have strong views on the topic beyond general concerns about the quality of risk management processes and documenting various descriptive issues concerning accessing cyber risk insurance policies. Both bodies have recently published guidance to members on these issues as noted above and plan to continue to do so in the near future as the cyber risk insurance market develops. It was noted this was an area lacking regulatory oversight and guidance and that the professional bodies played an important role in education and in providing support to members.

Despite a number of its members playing key roles as senior management and/or consultants to the insruance industry, the IFOA has not published any definitive position papers or

guidance on this topic. The author is an honorary fellow of the IFOA and has made presentations on this topic to IFOA working parties and to IFOA-sponsored conferences during 2014. The IFOA is currently is in the process of setting up a working party on cyber risk management, of whch the author has been invited to participate. It is expected that this working party will produce a literature review on the topic and generate some ideas for discussion within the UK actuarial profession in the early part of 2015.

7. Comclusion

This paper provides an overview of the current literature in the areas of the coordination of cyber risk management and cyber risk insurance by UK regulatory authories and key players in the UK industry. It appears there is no existing literature that either documents such processses or provides an analysis of how such issues bear on the future growth on the cyber risk insurance market.

In order to address this issue, a conceptual framework based on complexity theory to identify key players, stakeholders and gatekeepers was applied to analyse the views of regulatory officials, major industry players, professional bodies and consultants to the industry on this topic. A series of interviews were held in London during October –November 2014 to elicit views on major developments and trends in the market generally and the likely impact of regulatory coordination efforts.

It is apparent that this is a very sensitive and commercially valuable area for many participants. This may explain the relatively poor response rate to requests for interview, particularly by consultants. Further, high-level coordination between the UK government in seeking to implement public poliy on national cyber security strategy and the industry is in very early stages. Further, relevant industry players appear reluctant to provide greater public transparency on cyber attacks, and appear to be hostile to efforts to sponsor publicly available

databases on such incidents. The lack of engagement by key industry associations and other professional bodies on issues specific to the insurance industry also compound the issue. This situation is in contrast to that in the banking industry. The consultants in particular seem wary of maintaining their competitive advantage in providing specialist services to the major players seeking to mitgate against cyber risk attacks.

From a public policy perspective, there appears to be a growing awareness by key regulatory supervisors such as the BofE's PRA to hold more regular and detailed monitoring and coordination with key industry players. Further specialist professional bodies such as the IRM generally and the IFOA specifically are still the process of developing major thought leadership on such issues.

Further research is needed to identify and analyse the impact of coordination efforts on the pricing of cyber riskk insurance. Currently existing models of pricing do not appear to consider the impact of public interference or oversight on the activities of major players. Further there is a lack of shared knowledge at the public level concerning the nature, incidence and severity of cyber attacks, relative to the US, which may lead to inefficiencies in the pricing of cyber risk insurance. This might explain the lack of current depth of this market relative to the US, although most industry players appear to recognise that this is a growing and increasingly significant market. Further efforts to develop such a public database of such incidents, and/or public regulatory demands for increased transparency by firms of such attacks as is already the case in the US, may assist in facilitating more general awareness of the issues, and facilitate more informed and rigorous academic research into this increasingly important topic.

Acknowledgements

The author wishes to express his gratitude to the RCUK for sponsoring this research, and to the various interviewees and organisations who were willing to be interviewed.

References

Alabdulatif, A. **X. Ma** and L. Nolle. 2012. A Framework for Cryptographic Protocol Analysis Using Linear Temporal Logic. International Conference on Information Society (i-Society 2012), London, UK, June.

Alabdulatif, A., **X. Ma** and L. Nolle. 2013a. Analysing and Attacking the 4-Way Handshake of IEEE 802.11i Standard. The 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), London, UK, December 9-12.

Alabdulatif, A. **X. Ma** and L. Nolle. 2013b. A Framework for Proving the Correctness of Cryptographic Protocol Properties by Linear Temporal Logic. *International Journal of Digital Society*, 4(1): 749-757.

AIRMIC. 2013. AIRMIC Review of Recent Developments in the Cyber Insurance Market. AIRMIC: London.

Alloway,T. 20114. AIG Offers Insurance Against Cyber Injury. Financial Times: 23 April.

Amar, S. 2014. Banking on IT, RM Professional, Autumn, 19-20.

Arnold. M. 2014. Banks Face Rising Threat from Cyber Crime. Financial Times: 7 October.

Austin, R. D. 2007. The iPremier Company (A): Denial of Service Attack. Harvard Business School Publishing: Case 9-601-114.: HBS Publishing: Boston MA.

Atlantic Council and Zurich, 2014 Risk Nexus: Beyond Data Breaches: Global Internnections of Cyber Risk. Zurich: Switzerland.

Bank of England Prudential Regulatory Authority. 2014. Annual Report and Accounts 2014. Prudential Regulatory Authority: London.

Bonner,S. 2014. How Much to Reveal of Cyber Breaches? Financial Times: April 29.

Biener,C., M. Eling and J.H. Wirfs 2014. Insurability of Cyber Risk: An Empirical Analysis.

Braithwaite, T. and H. Kuchler. 2014. US Probes Wave of Cyber Attacks on Banks. Financial Times: 28 August.

Computer Weekly.com. 2014a. UK Government Joins Forces with Insurers on Cyber Security.

-----. 2014b. Cyber Insurance Complements Security Controls, Says Aon.

-------. 2014c. It's Time to Add Cyber Insurance to Your Security Strategy.

-------. 2014d. Cyber Liability Insurance Isnt' Worth the Cost.

Datamonitor Financial. 2013. UK Cyber Insurance: Potential for Growth in the Smaller End of the Market. Datamonitor: London.

Dutta, A. and K. McCrohan. 2002. Management's role in information security in a cyber economy. *California Management Review* 45: 1, 67-87.

Ferraro, D. 2014. "Groundbreaking" or "Broken"?: An Analysis of SEC cybersecurity disclosure guidance, its effectiveness and implications. *Albany Law Review* 77 (forthcoming).

Fleming, S. 2014a. Bank of England to Oversee "Ethical Hacking" of Financial Groups. Financial Times: 21 April.

-------. 2014b. Bank of England to Probe Banks' Computer Defences. Financial Times: 11 June.

FT Reporters (anonymous). 2014. JPMorgan Data Breach Triggers Calls for Deeper Collaboration.

Goergen, M., C. Mallin, E. Mitleton-Kelly, A. Al-Hawamdeh and I.Hse-Yu Chiu. 2010. *Corporate Governance and Complexity Theory*. Edward Elgar Publishing: London.

Gray, A. 2014a. Disasters Shake Up Insurance Industry. Financial Times: 27 April.

---------. 2014b. Cyber Insurance Market Tempts New Participants: 6 October.

Institute of Chartered Accountants in England and Wales. 2012. *Building Trust in the Digital Age: Rethinking Privacy Trust and Security*. ICAEW: London.

Institute of Risk Management 2014. Cyber Risk. IRM: London.

Intelligence and Security Committee (House of Commons). 2013. *Foreign Involvement in the Critical National Infrastructure: The Implications for National Security*. Stationery Office: London.

Klumpes, P.J.M, X Ma and S. Srinivasan. 2013. Towards Sustainable Compliace in Complex Organisations.

Marsh. 2014. UK and Ireland 2014 Cyber Risk Survey Report. Marsh & McLennan: London.

Ponemon Institute. 2013. Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age.Ponemon Institute:

----------. 2014. 2014 Cost of Data Breach Study: United States. Ponemon Institute:

Shackleford, S.J. 2011. Should your firm invest in cyber risk insurance? SSRN 1972307

Solman, P. 2014. Chief Information Security Officers Come Out from the Basement, Financial Times, 29 April.

United Kingdom (HM) Government. 2011. The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World. Cabinet Office: London.

United Kingdom (HM) Government. 2014. Cyber Essentials Scheme. Department for Business, Innovation and Skills: London.

United Kingdom (HM) Government Cabinet Office. 2013. Progress Against the Objectives of the National Cyber Security Strategy: December 2013.

Wang, T. K.N. Kannan and J.R. Ulmer. 2013. The Association Between the Disclosure and the Realization of Information Security Risk Factors. *Information Systems Research* 24(2): 201-218.

World Economic Forum. 2013. Global Risk Report. WEF: Geneva.