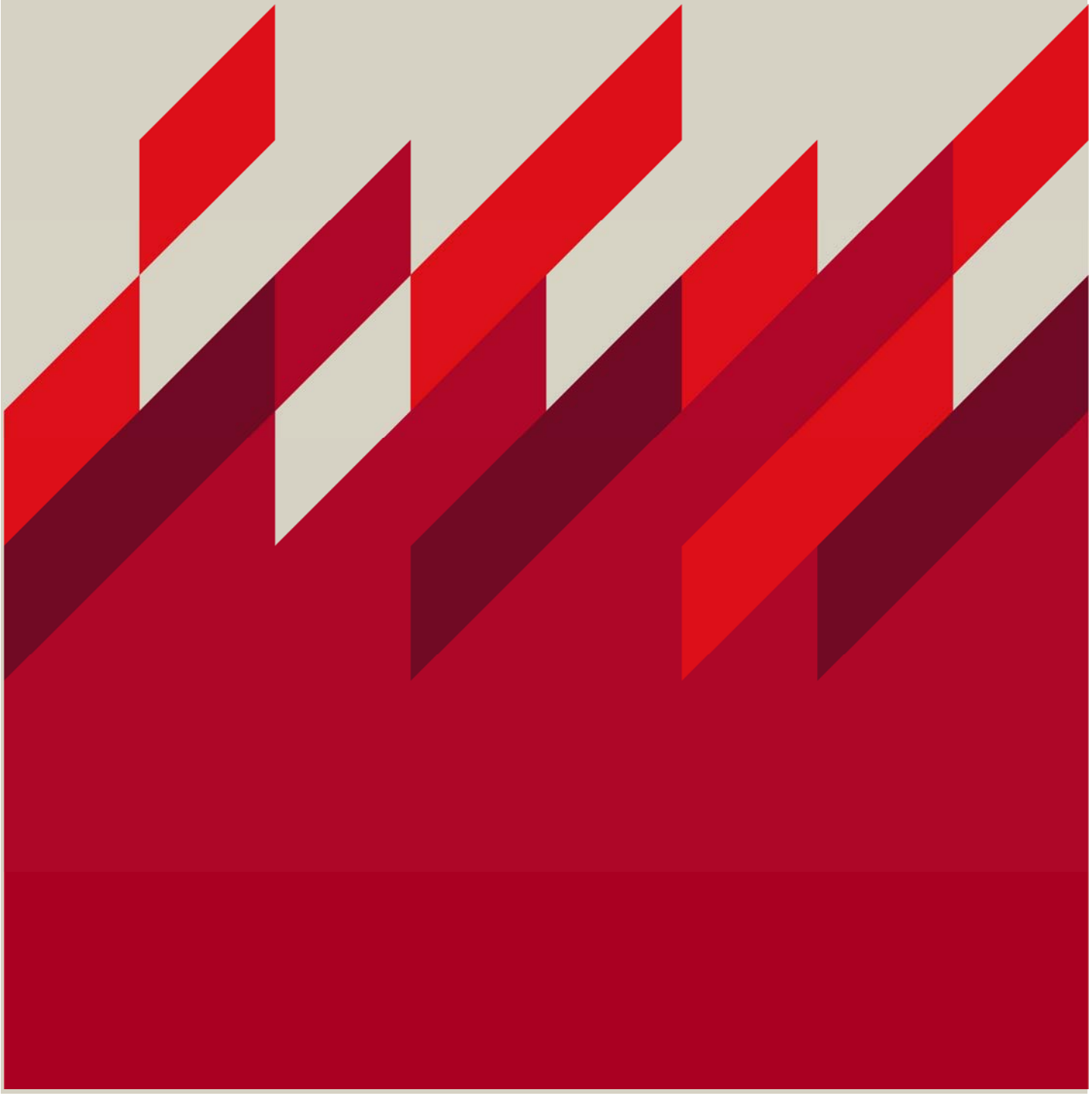
CENTRE FOR
FINANCIAL RISK
Faculty of Business and Economics

MACQUARIE
University

Understanding Cyber-Risk and Cyber-Insurance

WORKING PAPER 18-01

Gareth W. Peters, Pavel V. Shevchenko, Ruben D. Cohen



Understanding Cyber-Risk and Cyber-Insurance

Gareth W. Peters[a,*], Pavel V. Shevchenko[b], Ruben D. Cohen[c]

[a] *Department of Actuarial Mathematics and Statistics, Heriot-Watt University, Edinburgh, UK*
[b] *Department of Applied Finance and Actuarial Studies, Macquarie University, Sydney, Australia*
[c] *Consultant, MP Capital, London*

Abstract

In this manuscript we explore a range of perspectives being adopted by industry and regulators in order to classify cyber crime or cyber risk loss processes. The purpose of this is to better understand and discuss the emerging perspectives on this class of risk process in order to inform management practice, data collection and ultimately loss modelling. In the second part of the manuscript we discuss the emerging market of cyber risk insurance and the challenges faced by this market resulting from the diversity of insurance coverage on offer and uncertainty relating to potential exposures and vulnerabilities associated with this risk class. Furthermore, we discuss the challenge of moral hazard that can arise in developing such insurance markets. In the third section, the manuscript discusses regulator and industry responses to cyber risk management, mitigation and insurance. We conclude with insights and perspectives on whether cyber risk is a loss process that should be primarily covered by capital management practice, or whether it is better suited to an insurance mitigation or risk transfer based approach.

Keywords: financial technology (FinTech), risk management, cyber risk, cyber crime, operational risk, cyber insurance, cyber regulation, information technology risk, business disruption

*Corresponding author: garethpeters78@gmail.com

1. What is Cyber Risk from a Financial Risk and Insurance Perspective?

There is an increasing focus on IT and cyber related risk and insurance. The primary reason is that organisations of all sizes in both the public and private sectors are increasingly reliant on information and technology in order to execute business processes that support the delivery of services.

If there is a breakdown or failure in these systems, the organisation will realise a direct negative impact on the processes it supports, resulting in reduction of service and disruptions that ultimately impact on the organisations ability to meet its objectives.

Emerging fintech firms have taken on increased importance to improve risk management with financial technology. Given the importance of cyber risk and the trends of increasing risk- management techniques, to a wide spectrum of organisations and individuals, it is not a surprise that there is a variety of views on how to classify and think about cyber risk loss event types.

In this section we begin with an introduction to the different views of cyber risk that have emerged in recent years, which includes an overview of cyber risk from the perspective of operational risk (OpRisk), as some would argue that many aspects of cyber risk losses and cyber risk management would fall under the remit of OpRisk management according to Basel II regulatory requirements BCBS (2006). An overview of the many categories of OpRisk and how the data and models should be handled in this risk management domain can be found in comprehensive works such as Cruz et al. (2015), Peters and Shevchenko (2015) and Shevchenko (2011), and in recent discussions on OpRisk modelling in Peters et al. (2016). This is also timely discussion given the current trend that[1]:

> "*Regulators are taking a heightened interest in organizations risk management and underlying cultures, with the spotlight shifting somewhat from banks to insurers.*"

In this paper, we focus on an emerging type of OpRisk known as cyber risk and highlight techniques to both measure and manage this exposure. This area of risk is increasingly gaining prominence in banking and risk management areas and we believe

[1] `www.thecroforum.org/2017/10/06/a-guide-to-defining-embedding-and-managing-risk-culture/`.

that financial institutions are increasingly aware of the threats that can arise from cyber related crimes. Consequently, they are actively continuing to strengthen their defences against these threats. However, in response, cyber criminal organisations, cyber crime attack types are also becoming increasingly highly sophisticated.

Cyber crime is frequent, in that the crimes and attacks are increasingly being perpetrated on a massive scale, over a range of different actors in society. Cyber attacks increasingly hit individuals in their personal environment as well as organisations. In this chapter we are primarily focused on the view of institutions in this ongoing battle against cyber attacks.

Cyber crime is also a risk type that affects a large array of different organisations worldwide, eg, government agencies, universities, financial sectors and generally all industries, including important infrastructure units that play a key role in population security and safety, such as emergency services and healthcare.

Next, it is worth highlighting the evolution of cyber crime attack types. To achieve this we resort to an organisation that has tracked cyber crime, producing an annual report on cyber related incidents in the US since 2001: the FBIs Internet Crime Complaint Center (IC3).[2]

We summarise the leading fraud categories from these reports since 2003, these are the percentage of all referred fraudulent complaints as of January 1 to December 31 each year, outlined in Table 1.

The wide variety of these cyber- events introduce unique risk measurement and risk management challenges. The categories used in Table 1 are those proposed by the FBIs Internet Crime Complaint Center (IC3) to classify different types of cyber event. These classifications differ from those we will present from a typical operational risk classification, but we believe they are quite informative and may also provide guidance on classification of cyber events for financial organisations, mapping loss types to OpRisk/ cyber risk categories. The definitions of relevant classes of cyber event (see Appendix 1 in the 2007 Internet Crime Report of IC3)[3] are as follows.

[2] `https://www.ic3.gov/default.aspx`.

[3] `https://pdf.ic3.gov/2007_IC3Report.pdf`.

Table 1: IC3.org Cyber crime number of victims/events as percentages of yearly total events over time. Note: (i) Where more than one year is included the results are averaged over years reported in top 10 worst categories of cyber crime in the US. (ii) NA is utilised for crime types not reported in a given year or period by IC3.org. In 2014 half year results are reported for some fraud types - these are doubled for the year. (iii) Average per loss is for complaints reporting a loss. (iv) Numbers will not add to 100% as these categories only include the top ten fraud types per year.

Cyber Event Type	2003 - 2006	2007 - 2010	2011 - 2013	2014	2015	2016
Advanced Fee Fraud	NA	8.7	10	7.1	5.7	5.0
Auction Fraud	60.0	18.2	10	7.3	7.5	NA
Business Fraud	1.2	NA	NA	1.1	2.7	NA
Business Email Compromise	NA	NA	NA	NA		4.0
Computer Fraud	1.5	6.3	NA	NA	NA	NA
Check Fraud	2.6	5.7	NA	NA	NA	NA
Confidence Fraud	1.2	7.3	NA	4.4	4.3	4.9
Credit/Debit Card Fraud	6.0	6.7	NA	5.8	6.0	5.3
Corporate Data Breach	NA	NA	NA	0.3	0.9	1.1
Denial of Service	NA	NA	NA	0.3	0.4	0.3
FBI Scams& Gov. Imperson.	NA	14.9	10	NA	4.1	4.1
Financial Institutions Fraud	0.7	2.5	NA	NA	NA	NA
Identity Theft	1.0	5.9	9	6.6	7.6	5.6
Investment Fraud	1.1	NA	NA	0.5	0.6	0.7
Intellectual Property Rights	NA	NA	NA	0.6	0.7	0.9
Non-delivery	17.8	21	7.1	23.6	23.4	27.1
Overpayment Fraud	NA	6.3	5.9	8.6	10.7	8.6
Phishing	NA	NA	NA	4.8	5.8	6.5
Personal Data Breach	NA	NA	NA	3.8	6.8	9.2
Scareware/Ransomware/Malware	NA	NA	0.7	1.6	2.0	1.8
Spam	NA	6.6	NA	3.2	NA	NA
Social Media	NA	NA	NA	NA	7.0	6.3
Tech Support Fraud	NA	NA	NA	NA	NA	3.6
Threat/Extortion	NA	1.9	3.2	13.3	5.1	11.2
Virtual Currency	NA	NA	NA	NA	0.7	0.6
# Events (total) (,000)	187	281	289	269	288	299
Total USD Loss Reported	111.18Mil	354.5Mil	530.7Mil	800.5Mil	1.071Bil	$\geq$1.33Bil
Ave. or median USD per Loss	424.14	728.67	5,001.67	6,472	8,421	NA

- Financial Institution Fraud: is the purposeful misrepresentation of the truth or concealment of a material fact by a person to induce a business, organisation or other entity that manages money, credit or capital to perform a fraudulent activity. We also note that, as banks continue to dis-intermediate various services to fintech firms, financial institution fraud is taking on increased importance. Credit/debit card fraud is an example that ranks among the most commonly reported offenses to IC3. Identity theft also falls into this category; cases classified under this heading tend to be those where the perpetrator possesses the complainants true name identification (in the form of a social security card, driving licence or birth certificate), but there has not been a credit- or debit-card fraud committed.
- Gaming Fraud: to risk something of value, especially money, for a chance to win a prize when there is a misrepresentation of the odds or events. Sports tampering and claiming false bets are two examples of gaming fraud.
- Communications Fraud: a fraudulent act or process in which information is exchanged using different forms of media. Thefts of wireless, satellite or landline services are examples of communications fraud.
- Utility Fraud: when an individual or company misrepresents or knowingly intends to harm by defrauding a government- regulated entity that performs an essential public service, such as the supply of water or electrical services.
- Insurance Fraud: a misrepresentation by the provider or the insured in the indemnity against loss.
- Government Fraud: a knowing misrepresentation of the truth, or concealment of a material fact, to induce the government to act to its own detriment. Examples of government fraud include tax evasion, welfare fraud and counterfeit currency.
- Investment Fraud: deceptive practices involving the use of capital to create more money, either through income- producing vehicles or through more risk- oriented ventures designed to result in capital gains. Ponzi/pyramid schemes and market manipulation are two types of investment fraud.
- Business Fraud: when a corporation or business knowingly misrepresents the truth or conceals a material fact, such as bankruptcy fraud and copyright infringement.

- Confidence Fraud: reliance on anothers discretion and/or a breach in a relationship of trust resulting in financial loss.
- Auction Fraud: non-delivery of payment or merchandise, which are both types of confidence fraud and are the most reported offences to IC3.
- Credit/Debit Card Fraud: unauthorised use of a credit or debit card with the purpose of obtaining anything of value with the intent to defraud.
- Check Fraud: forgery, alteration, counterfeiting or knowing issuance of a cheque on an account that has been closed or has insufficient funds to cover the amount for which the cheque was written.
- Computer Fraud: in the broadest sense, computer crime is a violation of law involving a computer. As defined by the Office of Special Investigations (a department within the US General Accounting Office), computers can be used as tools to commit traditional offences. This means that the functions specific to computers, such as software programs and Internet capabilities, can be manipulated to conduct criminal activity.
- Identity Theft: is the illegal use of another persons identifying information (such as a name, birthdate, social security and/or credit- card number).
- Nigerian Letter Fraud: any scam that involves an unsolicited email message, purportedly from Nigeria or another African nation, in which the sender promises a large sum of money to the recipient. In return the recipient is asked to pay an advance fee or provide identity, credit card or bank account information. Subsequently, the recipient loses all monies they have entrusted to the sender of the message and they get nothing in return.

Other taxonomies or classifications of cyber risk also have been developed in recent years to try to capture the classes of loss process event types that this category of risk management may entail. For instance, in the white paper "A Taxonomy of Operational Cyber Security Risks" [4] (see Cebula and Young (2010)) one can find a detailed overview of a taxonomy of cyber risk categories that are largely aligned with the categories proposed

[4]report CMU/SEI-2010-TN-028 at URL `http://www.dtic.mil/get-tr-doc/pdf?AD=ADA537111`.

by the Basel II/III banking regulation categorizations of events such as cyber crime in a financial organization.

The Defense Technical Information Center[5], as per this taxonomy provide the following definition and categorization of cyber crime. "*Operational cyber security risks are defined as operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems. [$\cdots$] [one can ...] identify and organize the sources of operational cyber security risk into four classes:*

- *actions of people,*
- *systems and technology failures,*
- *failed internal processes, and*
- *external events.*

Operational risks are defined as those arising due to the actions of people, systems and technology failures, failed internal processes, and external events."

Furthermore, they provide the following decomposition in Cebula and Young (2010) as a taxonomy of Cyber Security Risks from the CMU Software Engineering Institute[6]:
Class 1 Actions of People:

- inadvertent - mistakes, errors and omissions;
- deliberate - fraud, sabotage, theft and vandalism; and
- inaction - skills, knowledge, guidance and availability.

Class 2 Systems and Technology Failures:

- hardware - capacity, performance, maintenance, obsolescence;
- software - compatibility, configuration management, change control, security settings, testing; and
- systems - design, specifications, integration and complexity.

Class 3 Failed Internal Processes:

[5] `http://www.dtic.mil/dtic/`
[6] `https://www.sei.cmu.edu/`

- process design or execution – process flow, process documentation, roles and responsibilities, notifications and alerts, information flow, escalation of issues, service level agreements, task hand-off;
- process controls – status monitoring, key risk indicators, key performance indicators and key control indicators, periodic review, process ownership; and
- supporting processes - staffing, funding, training and development, procurement.

Class 4 External Events:

- hazards - physical damage (weather, fire, flood, earthquake);
- legal issues - regulatory compliance, legislation, litigation;
- business issues - supplier failure, market and economic conditions; and
- service dependencies - utilities, fuel, transportation.

We also note that they assert that within the cyber security space, the risk management focus is primarily on operational risks to information and technology assets. People and facility assets are also considered to the extent that they support information and technology assets.

Other groups have also made efforts to classify cyber risks into particular categories of relevance to particular industry sectors, for instance the white paper report produced by the Chief Risk Officer (CRO) Forum.[7] This group is a collection of professional risk managers from the insurance industry that focuses on developing and promoting industry best practices in risk management. A white paper report was produced by this group – "CRO Forum Concept Paper on a proposed categorization methodology for cyber risk"[8] which also aims to incorporate the standards for operational risk management reporting to undertake analysis of cyber risk. The standards it proposed are those used within industry leading database providers such as ORX[9], ORIC[10] and Schema, all of these are currently being developed to support the emergence of cyber insurance markets. The definition provided by the CRO Forum for cyber risk is:

[7] www.thecroforum.org.

[8] www.thecroforum.org/2016/06/20/concept-proposal-categorization-methodology-for-cyber-risk/.

[9] https://managingrisktogether.orx.org/.

[10] https://www.oricinternational.com/.

"*Any risks emanating from:*

- *The use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks.*
- *Physical damage that can be caused by cyber attacks.*
- *Fraud committed by misuse of data.*
- *Any liability arising from data use, storage and transfer.*
- *The availability, integrity and confidentiality of electronic information be it related to individuals, companies or governments."*

It also highlights recommendations for proposed common cyber risk categorizations based on four event type groupings which are worth to mention for consideration when categorizing these type of loss events:

- system malfunctions/issue – own system or network is malfunctioning or creating damage to third-party's systems or supplier's system not functioning, impacting own digital operations;
- data confidentiality breach – data stored in own system (managed on premise or hosted/managed by third party) has been stolen and exposed;
- data integrity/Availability – data stored in own system (managed on premise or hosted/managed by third party) have been corrupted or deleted; and
- malicious activity – misuse of a digital system to inflict harm (such as cyber bullying over social platforms or phishing attempts to then delete data) or to illicitly gain profit (such as cyber fraud).

Furthermore, the Federal Information Security Management Act of 2002 (FISMA), which applies to U.S. federal government agencies, involves a relevant working definition of cyber crime. It also provides a working definition of information security. This definition links the identified operational cyber security risks to specific examples of consequences impacting confidentiality, integrity, and availability:

"Information Security: means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide ([FISMA, 2002]):

- *integrity, which means guarding against improper information modification or destruction, and includes ensuring information non repudiation and authenticity;*
- *confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and*
- *availability, which means ensuring timely and reliable access to and use of information."*

The working definitions typically adopted in financial organizations around the globe follow definitions laid out under Basel II/III guidance documents for OpRisk management the general notion of OpRisk is defined (see BCBS (2006)) as follows: *"Operational risks are defined as those arising due to the actions of people, systems and technology failures, failed internal processes, and external events."*

In OpRisk modelling there is a collection of Level 1 and more detailed Level 2 risk categorizations provided according to business unit and event types, making up 56 risk cells (8 business lines times 7 event types) at level 1. We will mention below just the OpRisk categorizations and highlight which of these we believe are of relevance to cyber risk events according to the Basel II/III accords at event type categories of level 1 and level 2. We select in bold the categories we argue are most relevant to consideration for Cyber risk loss events.

Level 1 and Level 2 Cyber Risk Relevant Event Types:

- **internal fraud - unauthorized activity; unternal theft & fraud; system security internal willful damage;**
- **external fraud - external theft and fraud; system security external willful damage;**
- employment practices and workplace safety - employee relations; safe Workplace Environment; Employment Diversity & Discrimination;
- **clients, products & business practices - suitability, disclosure & fiduciary; improper business or market practices; product flaws; selection, sponsorship & exposure; advisory activities;**

- damage to physical assets - natural disasters; accidents & public safety; **willful damage and terrorism;**
- **business disruption and /or system failures - systems failure internal; system failure external; network unavailability;**
- **execution, delivery & process management - transaction capture, execution & maintenance; monitoring and reporting; customer intake and documentation; customer / client account management; vendors & suppliers**.

As we see from the selections we have made, we believe that the majority of OpRisk event types are applicable to some form of cyber crime loss events as proposed by the categories offered by other groups mentioned previously.

2. Cyber Risk Capital or Cyber Risk Insurance

In this section we start by discussing the current fledgling market for cyber risk insurance products and discuss the areas they are beginning to grow. We then contrast this to capital reserving under Basel II/III for mitigation of cyber risk in financial organizations. There are other studies that have also performed analysis on the insurability of cyber risk, see for instance Eling and Schnell (2016) and Biener and Wirfs (2015).

In general, we might consider that cyber insurance is protection from cyber risk. For example, data- breach insurance, a type of cyber insurance, compensates the insured against losses due to an incidence of an information leakage. Earlier studies include Gordon et al. (2003); Baer and Parkinson (2007).

There are numerous challenges facing the early development of cyber insurance which have started to be explored. Several studies examining the question of whether cyber security risk can be insured or not (such as Mukhopadhyay et al. (2013); Biener and Wirfs (2015); Shackelford (2012); Opadhyay et al. (2009)) pointed out that correlation of losses, lack of data, and information asymmetry hinder the growth of cyber risk insurance, and argued that firms still need to proactively manage and enhance cyber security due to the limitations of cyber insurance and that overpriced cyber insurance limits the growth of cyber insurance markets.

Shim et al. (2017) studied covariates and insurance costs of data breach losses in United States during 2005-2015 (published by the Identity Theft Resource Center[11]) under the frequency-severity model. They observed a weak autocorrelation in the frequency and found economic indicators such as S&P500 and VIX volatility index to be leading external covariates of data breach incidence. They also found that a frequency-conditional severity loss model explains the percentile premium for data breach insurance better than a frequency-unconditional severity model.

Romanosky (2016) examined data set of cyber incidents acquired from Advisen[12], a US-based organization that collects, integrates and resells the data to the commercial insurance industry. It was observed that the aggregate rates of cyber events and litigation show similar trends getting more frequent and potentially more expensive to organizations collecting and using personal information. However, the actual costs of these events for most firms was less than $200,000, representing only 0.4% of firm revenues, far less than other losses due to fraud, theft, corruption, or bad debt.

Eling and Wirfs (2015) applied operational risk loss distribution approach for cyber losses from the world's largest collection of publicly reported operational losses (SAS OpRisk Global data https://www.sas.com), fitting data using extreme value theory and incorporating covariates such as country, industry and company size. Their results showed that human behavior is the main source of cyber risk and that cyber risks are very different compared to other operational risks.

2.1. Exploring Cyber Risk Insurance Specifics

We begin by asking the general question:

What is cyber insurance?

An emerging class of insurance product began to appear in the 1990's and has been growing since - known as cyber insurance. The Department of Homeland Security [13] defines cyber insurance as follows. *"Cyber-security insurance is designed to mitigate*

[11] `www.idtheftcenter.org`.

[12] `http://www.advisenltd.com`.

[13] `https://www.dhs.gov/cybersecurity-insurance`.

losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cyber-security insurance market could help reduce the number of successful cyber attacks by:

- *promoting the adoption of preventative measures in return for more coverage; and*
- *encouraging the implementation of best practices by basing premiums on an insureds level of self-protection."*

Risks of this nature are typically excluded from traditional commercial general liability policies or at least are not specifically defined in traditional insurance products, leading to the emergence of cyber security insurance as a "stand alone" line of coverage. Coverage provided by cyber-insurance policies may include:

- first-party coverage against losses such as data destruction, extortion, theft, hacking, and denial of service attacks;
- liability coverage indemnifying companies for losses to others caused, for example, by errors and omissions, failure to safeguard data, or defamation; and
- other benefits including regular security-audit, post-incident public relations and investigative expenses, and criminal reward funds.

Currently, the market is in a state of flux due to uncertainty; in fact it is reported that in practice many companies are favouring forgoing available policies, due to the perceived high cost of the policies and confusion about what they cover. Furthermore, there are still several questions arising as to the efficacy of cyber- risk insurance, in the sense that creating a market may not provide sufficient coverage of pooling of risk to be solvent for insurers underwriting such large and uncertain potential losses from this source of risk.

In this regard there starts to emerge studies to question the suitability of such types of insurance product, see operational risk insurance questions in Peters et al. (2011) and specifically on cyber risk in Biener and Wirfs (2015). In particular in this second work from the University of St. Gallen, which appeared in the Geneva Papers in 2015, the authors specifically question the ability to insure cyber events.

They note that as of 2015 the annual gross premiums for cyber insurance in the United States are US$ 1.3 billion and growing 10-25% on average per year. Furthermore, in

continental Europe they claim that cyber insurance products so far are estimated to generate premiums of around US$ 192 million, but this figure is expected to reach US$ 1.1 billion in 2018. Clearly, this is still a fledgling market compared to other more mainstream lines of insurance business. For such an important and emerging risk class, which is gaining a rapidly increasing attention of banking and finance sector, one may question why these products are still slowly emerging and slowly gaining popularity.

One challenge in this insurance market is a non-standardization of nomenclature and contract specification of covered items. For instance, products and coverage tend to change rapidly, and exclusions as well as terms and definitions vary significantly between competitors. There is a reason for this flux, primarily it is currently being driven by the fact that the risks faced by corporations are often unique to its industry or even to the company itself, requiring a great deal of customization in policy writing. This will, we believe, begin to resolve as more data and studies such as the ones we present here begin to emerge highlighting aspects of cyber risk characteristics.

We provide below some examples of the core determinants insurers may consider when developing pricing of a cyber insurance policy in regard to its terms and pricing:

- company size;
- size of the customer base;
- web presence; and
- type of data collected and stored (sensitive nature of the data and commercial value).

Having said this, there are still a number of policies available on the market. For instance typical policies can include (see Biener and Wirfs (2015)) those listed below:

THIRD PARTY

- Coverage: Privacy Liability
  - disclosure of confidential information collected or handled by the firm or under its care, custody, or control (e.g., due to negligence, intentional acts, loss, theft by employees).
- *Insured Losses:*

  - legal liability (also defense and claims expenses (fines), regulatory defense costs);
  - vicarious liability (when control of information is outsourced); and
  - crisis control (e.g., cost of notifying stakeholders, investigations, forensic and public relations expenses)

- Coverage: Network Security Liability

  - unintentional insertion of computer viruses causing damage to a third party;
  - damage to systems of a third party resulting from unauthorized access of the insured;
  - disturbance of authorized access by clients;
  - misappropriation of intellectual property.

- *Insured Losses:*

  - cost resulting from reinstatement; and
  - cost resulting from legal proceeding.

- Coverage: Intellectual Property and Media Breaches

  - breach of software, trademark and media exposures (libel, etc.)

- *Insured Losses:*

  - legal liability (also defense and claims expenses (fines), regulatory defense costs).

FIRST PARTY

- Coverage: Crisis Management

  - all hostile attacks on information and technology assets.

- *Insured Losses:*

  - costs from specialized service provider to reinstate reputation; and
  - cost for notification of stakeholders and continuous monitoring (e.g., credit card usage).

- Coverage: Business Interruption Data Asset Protection
  - denial of service attack;
  - hacking;
  - information assets are changed, corrupted, or destroyed by a computer attack; and
  - damage or destruction of other intangible assets (e.g., software applications).

- *Insured Losses:*
  - costs resulting from reinstatement;
  - loss of profit;
  - cost resulting from reinstatement and replacement of data; and
  - cost resulting from reinstatement and replacement of intellectual property (e.g., software).

- Coverage: Cyber Extortion
  - extortion to release or transfer information or technology assets such as sensitive data;
  - extortion to change, damage, or destroy information or technology assets; and
  - extortion to disturb or disrupt services;

- *Insured Losses:*
  - cost of extortion payment; and
  - cost related to avoid extortion (investigative costs).

3. Some Regulatory Perspectives on Cyber Risk and Insurance

In addition to the previously discussed guidance on cyber- risk as it pertains to OpRisk, there are also other regulatory approaches being developed to tackle cyber risk related losses and risk management. For instance, in 2005 the Federal Financial Institutions Examination Council (FFIEC) developed guidelines for authentication in an Internet banking environment.[14]

[14]Guidance Document "Authentication in an Internet Banking Environment" at `https://ffiec.bankinfosecurity.com/new-ffiec-guidelines-full-text-a-3802`

The FFIEC in the US is a formal inter-agency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions.

The guidance the FFIEC established was aimed at providing a risk management framework for financial institutions offering Internet based products and services to their customers. Since, this first release there have been additional supplements also released updating the guidance according to emerging challenges and threats faced. As stated by the FFEIC:

"*The Guidance provided minimum supervisory expectations for effective authentication controls applicable to high-risk online transactions involving access to customer information or the movement of funds to other parties. The 2005 Guidance also provided that institutions should perform periodic risk assessments and adjust their control mechanisms as appropriate in response to changing internal and external threats.*"

The guidance covers both retail/consumer banking as well as business commercial banking. The minimum frequency recommended for updating of these assessments is annual and the recommended risk assessments that should be undertaken in this context include at a minimum assessment of the following:

- changes in the internal and external threat environment;
- changes in the customer base adopting electronic banking;
- changes in the customer functionality offered through electronic banking; and
- actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry.

In particular for commercial banking wire transfers, they must consider to utilize layered security protocols.

3.1. Layered Security Protocol Recommendations to Mitigate Cyber Risks

The concept of layered security as set out by the FFIEC guidance documents relates to the use of different controls at different points in a transaction process. The intended purpose of such layering is that any weakness in one control is generally compensated for by the strength of a different control. It is believed that such approaches may enhance the overall security of internet-based services and protect sensitive customer information, aid in prevention of identity theft, and reduce account takeovers. At a minimum such layered approaches should aim to undertake the assessment and reporting of anomalous activity relating to:

- initial login and authentication of customers requesting access to the institution's electronic banking system; and
- initiation of electronic transactions involving the transfer of funds to other parties.

The FFIEC recommends the following minimum list of effective controls be adopted in a layered security program[15]:

- fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- the use of dual customer authorization through different access devices;
- the use of out-of-band verification for transactions;
- the use of "positive pay", debit blocks, and other techniques to appropriately limit the transactional use of the account;
- enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows [e.g., days and times];
- internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
- policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;

[15]Source: `https://ffiec.bankinfosecurity.com/new-ffiec-guidelines-full-text-a-3802`

- enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and
- enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

Furthermore, in follow up guidance, the FFIEC also developed frameworks for how business affected by cyber crime events should respond from a business continuity perspective[16]. It also sets out business continuity expectations related to managing cyber risks. Also, the Office of the Comptroller of the currency, in the US Department of Treasury has also issued guidance advice on emerging cyber-security risks facing payments and mobile transactions could adversely affect banks. This was followed by the release by the FFIEC in their online handbook series[17], of the Business Continuity Planning Handbook as part of the Information Technology (IT) wxamination handbooks. The FFIEC states:

"*The focus of this booklet continues to be based on an enterprise-wide, process-oriented approach that considers technology, business operations, testing, and communication strategies that are critical to business continuity planning for the entire business, instead of just the information technology department.* "

In the UK there have also been a range of regulatory responses to cyber risk. For instance, the Bank of England Prudential Regulatory Authority (PRA) recently released in mid 2017 a supervisory statement directed at the insurance and reinsurance industries pertaining to directly to cyber risk and in particular Cyber insurance underwriting risks[18]. This statement followed earlier releases by the PRA which produced guidance and consultation in 2016 relating to the regulators expectations for prudent management of cyber underwriting risk.

This recent guidance of the PRA is targeted at all insurance and reinsurance industry on cyber risk for all UK non-life firms and groups within the scope of Solvency II,

[16]Source:`https://www.bankinfosecurity.com/business-continuitydisaster-recovery-c-76`

[17]`https://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/introduction.aspx`

[18]Bank of England, PRA, Supervisory Statement — SS4/17 Cyber insurance underwriting risk, July 2017 `http://www.bankofengland.co.uk/pra/Documents/publications/ss/2017/ss417.pdf`

including the Society of Lloyds and managing agents (Solvency II Firms). Furthermore, the guidance covers two types of cyber risk policy:

- affirmative cyber risk, ie insurance policies that explicitly include coverage for cyber risk; and
- non-affirmative cyber risk, ie insurance policies that do not explicitly include or exclude coverage for cyber risk . This latter type of cyber risk is sometimes referred to as 'silent' cyber risk.

This supervisory statement sets out the PRA's expectations of firms regarding cyber insurance underwriting risk, which the PRA defines as:

"*... the set of prudential risks emanating from underwriting insurance contracts that are exposed to cyber-related losses resulting from malicious acts (eg cyber attack, infection of an IT system with malicious code) and non malicious acts (eg loss of data, accidental acts or omissions) involving both tangible and intangible assets.* "

In particular in Section 2.1 of the guidance it is stated that:

"*The PRA expects that all Solvency II firms robustly assess and actively manage their insurance products with specific consideration to non-affirmative cyber risk exposures. This includes all property and casualty (P&C) covers which could give rise to cyber risk exposure from physical and non-physical damage. Such firms are expected to introduce measures that reduce the unintended exposure to this risk with a view to aligning the residual risk with the risk appetite and strategy that has been agreed by the board. To achieve this, besides making adequate capital provisions that clearly link with this risk, as they would for any other risk type, firms could consider any of the following (the list is not exhaustive):*

- *adjusting the premium to reflect the additional risk and offer explicit cover;*
- *introducing robust wording exclusions; and/or*
- *attaching specific limits of cover.*"

They further note:

"*The PRA is not a pricing regulator and does not look to design products. The short-to-medium term aim is to enhance the ability of firms to monitor, manage and mitigate*

non affirmative cyber risk and to increase contract certainty for policyholders as to the level and type of coverage they hold. "

Basically, in summary of this guidance, insurers can demonstrate compliance and best practice through four key steps:

- Review your existing insurance products and their underlying contracts, focusing on understanding exposure to non-affirmative cyber risk.
- Firms offering affirmative cyber cover should set up a clear strategy on how this risk is managed, including quantitative and qualitative risk appetite statements.
- Use cyber scenarios as a way to understand your exposure. We believe scenarios based on "near misses" are a good basis for robust portfolio stress tests.
- Demonstrate that your firm is investing in cyber knowledge and expertise (both affirmative and non-affirmative cyber).

4. Some Industry Perspectives on Cyber Risk and Regulations

A number of industry groups and organizations have also begun to explore business based approaches to tackling the growing challenges associated with cyber risk and cyber security.

With regard to layered approaches proposed as guidance by agencies such as the FFIEC, mentioned previously, there are practical risk management and business process challenges associated with developing such systems. These have recently been highlighted by several industry groups. For instance, the group RSA who provide solutions to cyber risk management and mitigation have produced a recent white paper[19]. In this report it is claimed that the research firm Gartner has demonstrated that practically cyber risk is causing significant costs to business practice. For instance, they state:

"*Worldwide cyber-security spending for 2015 topped $75 billion and in spite of this level of spending, we have seen 2000 data breaches, 700 million personal records stolen, and an average financial loss of $3.5M per incident. However, the most shocking statistic*

[19] "How can we Improve Cyber Risk Management? (Business-driven security bridges the gap between cyber security and risk management)" available at `https://www.rsa.com/en-us`.

is that on average organizations only know that they have been hacked less than 30% of the time."

Of particular interest when looking at the industry practitioners experience of cyber risk and cyber loss events is what the RSA have called the GAP. This term refers to a fundamentally different approach to assessing, diagnosing vulnerabilities and assessing impacts that is arising between the IT and security professionals in an organization and the risk management teams managing the impacts of the losses. As RSA points out in its white paper, generally it is the case that risk managers and senior executives are not so interested in the specificity of the attack type and vulnerability of particular detailed aspects of the IT system, rather they have been focusing on the cost to the business and the potential size of impacts. Conversely, the IT and security teams have not been focusing on which types of cyber breach may cause most business process disruption or lead to highest loss impacts, they rather focus on particular specificity of a systems vulnerabilities. It is in these two fundamentally different approaches to the problem and its consequences that one encounters a serious business and governance challenge when developing a cyber risk management strategy in practice. As the RSA report states:

"In most organizations today, we see a distinct Gap between business leaders and security teams, essentially a disconnect with security teams absorbed in trying to determine what a cyber incident is and how fast can they stop it while the business leaders are laser focused on only the impact to the organization. The Gap is especially poignant when an incident happens and the CEO asks, "How bad is it?" and the security team is not entirely confident they understand the scope of the threat, or how it will impact the organization. Which, as mentioned above, is really what senior management cares about."

They argue that the evolution of cyber security systems in many organizations has followed a pattern which has involved a layering of preventative tools such as:

- static, signature-based technologies like firewalls, IDS/IPS, and A/V;
- next generation firewalls, sandboxes, and other advanced threat solutions; and
- addition of security inclusion protocols to maintain one of the most important threat vectors "identity management" through technologies such as Public Key Infras-

tructures, multi-factor authentications, provisioning/deprovisioning systems, governance, and life cycle management.

The challenge with such a layering approach in practice is that it is targeted from a management perspective in terms of reactionary policies and management as new vulnerabilities are exposed or new threats emerge. From a business and risk- management perspective, this can be a challenge, as such reactionary strategies may not always be well aligned with the business processes affected. The business developments taking place outside the IT sphere, or even be at the appropriate level of the risk appetite set out by the risk- management teams, which, the RSA argues, could come at the expense of "*creation of tremendous complexity that may not even be protecting what matters most to the organisation*".

To overcome this challenge, organizations should aim to begin to align the interests of both these groups by ensuring that business initiatives integrate with security strategies from the onset. Such processes should then be regularly assessed in new emerging government and business practice environments in order to ensure all critical systems/processes/data are categorized and aligned to security.

The sentiment communicated by RSA that pertains to how different members of an organization view cyber risk and its mitigation and management is also echoed in other white papers such as the one brought out by Oliver Wyman partners Paul Mee and James Morgan[20]. In this report they also describe the fact that "*Boards of Directors and all levels of management intuitively relate to risks that are quantified in economic terms. Explaining any type of risk, opportunity, or tradeoff relative to the bottom line brings sharper focus to the debate.* "

They note that, as a consequence of the combination of communication of risk processes and events in economic terms to senior executives, as well as the expectations of regulators that losses be modelled and quantified, there has been traditionally an approach adopted

[20]Source: "Deploying a cyber risk strategy. Five Key moves beyond regulatory compliance" `http://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2017/jun/Deploying_A_Cyber_Risk_Strategy.pdf`.

to quantify in dollar terms all financial and many nonfinancial risks. In fact, institutions have developed methods for quantifying expected and unexpected losses in dollar terms as part of risk- management processes that needed to be regulation- compliant to allow for valuation of economic capital, Comprehensive Capital Analysis and Review (CCAR) and the assessment of resolution and recovery planning (business continuity planning). Furthermore, the economic quantification of such losses allows them to then be compared to key management decision criteria such as earnings and capital required to undertake certain business practices.

As noted in the Oliver Wymann report: " *Predicting losses due to Cyber is particularly difficult because it consists of a combination of direct, indirect, and reputational elements which are not easy to quantify.* " Furthermore, like RSA, the report of Oliver Wymann also argues that the governance structure needs to close, as RSA put it, the GAP between risk management from business perspective and from IT perspectives. Oliver Wymann's report then argues that this may be achieved through posing or focusing the response to cyber risk through linking its risk management strategies to cyber risk governance and the organizations risk appetite. In particular they argue that:

"*Regulators are specifically insisting on the establishment of a Cyber Risk strategy, which is typically shaped by a Cyber Risk appetite. This should represent an effective governance anchor to help address the Boards concerns about whether appropriate risks are being considered and managed effectively. Setting a risk appetite enables the Board and senior management to more deeply understand exposure to specific Cyber Risks, establish clarity on the Cyber imperatives for the organization, work out tradeoffs, and determine priorities.* "

Such views are not being ignored, for instance the recent Bank of England PRA guidance for insurers and re-insurers clearly states in section 3.2 of the guidance note[21]: " *The cyber strategy should include clearly articulated risk appetite statements with both quantitative and qualitative elements, for example defining target industries to focus on,*

[21]Bank of England, PRA, Supervisory Statement — SS4/17 Cyber insurance underwriting risk July 2017 `http://www.bankofengland.co.uk/pra/Documents/publications/ss/2017/ss417.pdf`.

strategy for managing non-affirmative cyber risk, specifying rules for line sizes, aggregate limits for industries, splits between direct and reinsurance, etc. (this list is not exhaustive)". This indicates that such industry concerns are beginning to be addressed in regulatory guidance documents, at least in the insurance sector for cyber risk insurance.

Other industry challenges faced include non-consensus or standardization of regulations or guidance when it comes to addressing, mitigating and assessing cyber risk. For instance, it was reported by Reuters[22] that the CEO of JPMorgan's corporate and investment bank is quoted as saying that it is his opinion that "*Governments need to develop global cyber security standards and increase information sharing on cyber threats...*", such sentiments are echoed by many industry groups when it comes to understanding cyber crime and cyber risk. Furthermore, he pointed out that there is at present a range of different global policies and required compliance to address cyber risk issues, which are not sufficiently standardized, in his words

> "*Global banks have to comply with a hodgepodge of cyber security standards across different countries, increasing costs and risks.... Each country has a different standard but we have a global problem ... When you go to point where you have to have different standards in every place, you put yourself in a vulnerable position.* "

Echoing this view, the Financial Stability Board, comprised of central banks, released an analysis of different countries cyber security regulations and guidelines for financial services. Their findings were that in some instances there were countries that had up to 10 different sets of rules and that these typically varied widely across jurisdictions.

These types of views serve to further highlight the already mentioned growing concerns among financial market participants and regulators about the risks cyber attacks pose to the financial systems. Apart from the fact that keeping track and managing compliance with multiple, potentially contradictory codes of regulation and guidance in different jurisdictions is a significant business cost, it also raises additional compliance concerns

[22]source: "Regulators need to develop global cyber security standards -JPM's Pinto" in Reuters Market News October 14, 2017 / 4:44 PM `https://www.reuters.com/article/ usa-iif-banks/ regulators-need-to-develop-global-cyber-security-standards-jpms-pinto-idUSL4N1MP093`.

relating to increased cyber risk vulnerabilities associated with compliance.

For instance, there have been other industry perspectives that relate the security issues industry participants may face when complying with certain emerging regulations on reporting. For instance, as part of the electronic exchange reporting requirements: EMIR, Dodd Frank, MiFID I/II, MiFIR, REMIT, Reg NMS and T2S, see an overview in Peters and Vishnia (2016), the US Securities and Exchange Commission is beginning to observe the challenges they may face in performing the emerging regulations of reporting transparency with respect to the increased vulnerability and cyber risk associated with compliance.

Recently, it was discovered that the SEC's corporate filing system had been breached. This is problematic, since the new regulations require banks, financial traders and market participants such as hedge fund to report and disclose to such regulators specific details of their trading behaviors and strategies. This information is extremely valuable to such organizations as it pertains directly to their business practices and products. If such information is reported outside the premises of the organization to a regulator, who may even have access to the physical computer code used to perform such strategies, there is a significant additional cyber risk faced by both parties, the institutions reporting to meet regulatory compliance requirements and the regulator who is now holding an industry worth of critical information in their IT system. There are serious questions relating to increased vulnerability in this regard, from cyber risk perspectives, that need to be further explored in such regulatory settings[23].

As noted in this aforementioned article, the Commodity Futures Trading Commission (CFTC) Chairman J. Christopher Giancarlo stated that he believes the SEC hack raises questions about how much proprietary data should be held by market regulators. He is quoted as saying:

> " *I'm very concerned that we don't house gratuitous market information that makes ourselves a target for commercial espionage and commercial hackers.* "

[23]Further discussion in article by Ryan Tracy on October 03, 2017 at `http://www.foxbusiness.com/features/2017/10/03/regulators-fret-about-cyber-risk-after-sec-hack.html`.

As noted in the article, such concerns could then challenge the uptake of the implementation of the SEC's consolidated audit trail rule. This rule was particularly aimed at keeping track of every trade and order in U.S. stock and option markets, as well as efforts by the CFTC to expand regulators' access to the computer code that drives automated trading strategies and bring more high-frequency traders under their oversight.

5. Conclusion

We have provided a detailed exploration of the different approaches adopted by cyber research and cyber crime agencies to classification of cyber crime loss event types. We have studied the relationship between these taxonomies and how they relate to OpRisk classifications given under Basel II.

Furthermore, we have explored cyber risk insurance and the challenges faced by insurers and re-insurers when establishing this fledgling market. In this context, we have discussed the lack of homogeneity in product design and coverage in this space that is arising from a limited access to cyber loss data and exposure data. As the data collection and availability enhances in this area of risk management and insurance, we believe there will be greater convergence to standard product types and more transparent and consistent pricing for premiums on such products. To aid in this development, we have also explore the current status of cyber risk and cyber insurance from key financial, banking and insurance regulator guidance perspectives.

We have concluded by highlighting key challenges that industry groups face when meeting certain regulations and guidance on cyber risk management. In this regard we also note the consensus that many industry groups believe there needs to be a more concerted effort to standardize the cyber risk regulation guidance which is as yet still in a state of heterogeneity between different jurisdictions, a potential real problem for organizations operating across different markets.

We have also highlighted how the layering approach to cyber security system design often specified as best practice in regulatory guidance and adopted by many firms in their cyber risk strategies, faces a challenge of disconnect. In particular, we discuss how the business managers and risk managers think of cyber risk and cyber exposures,

and consequently plan their business practice around, differs substantially in view and approach to those views often held by the IT and security teams, who often have a different approach and set of priorities to cyber risk and security approaches. It is increasingly being recognized that a coherent joint governance view and plan that covers both business practice and IT considerations of cyber security needs to be integrated more intricately into business models and practice. This ensures that projects involving significant IT components and may if facing cyber attack cause a significant business disruption are prioritized appropriately by the IT security teams, and conversely, unconsidered aspects of IT systems that could cause significant reputation losses or legal costs from a cyber exposure are carefully flagged and dealt with from both business and IT perspectives.

In addition, there are problems arising from recent regulations aimed at increasing financial reporting and transparency in certain electronic exchange market places, however, as we discuss such regulations may further enhance the cyber risk exposure that market participants and indeed the regulators may face when holding significant amounts of sensitive data on local IT systems outside of the companies private systems.

In conclusion, we have captured the current state of evolution of cyber risk classification and challenges faced when considering how to set up data collection for modelling and insurance contract design. We have also highlighted the challenges faced by industry when faced with a range of different regulatory guidance documents that are not yet standardized in their requirements or recommendations.

References

Baer, W. S. and Parkinson, A. (2007). Cyberinsurance in IT security management. *IEEE Security Privacy*, 5(3):50–56.

BCBS (June 2006). International convergence of capital measurement and capital standards: A revised framework (comprehensive version). *Basel, Switzerland: Basel Committee on Banking Supervision, Bank for International Settlements.*

Biener, C., M. E. and Wirfs, J. H. (2015). Insurability of cyber risk: an empirical analysis. *Geneva Papers on Risk and Insurance-Issues and Practice*, 40(1):131–158.

Cebula, J. L. and Young, L. R. (2010). A taxonomy of operational cyber security risks. Technical report, Carnegie Mellon University, Pittsburgh PA Software Engineering Institute.

Cruz, M. G., Peters, G. W., and Shevchenko, P. V. (2015). *Fundamental Aspects of Operational Risk and Insurance Analytics: A Handbook of Operational Risk*. John Wiley & Sons.

Eling, M. and Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *The Journal of Risk Finance*, 17(5):474–491.

Eling, M. and Wirfs, J. H. (2015). Modelling and management of cyber risk. `http://www.actuaries.org/oslo2015/presentations/IAALS-Wirfs&Eling-P.pdf`.

Gordon, L. A., Loeb, M. P., and Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3):81–85.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., and Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure it or not? *Decision Support Systems*, 56:11–26.

Opadhyay, T. B., Mookerjee, V. S., and Rao, R. C. (2009). Why IT managers dont go for cyber-insurance products. *Communications of the Acm*, 52(11):68–73.

Peters, G. W., Byrnes, A. D., and Shevchenko, P. V. (2011). Impact of insurance for operational risk: Is it worthwhile to insure or be insured for severe losses? *Insurance: Mathematics and Economics*, 48(2):287–303.

Peters, G. W. and Shevchenko, P. V. (2015). *Advances in Heavy Tailed Risk Modeling: A Handbook of Operational Risk*. John Wiley & Sons.

Peters, G. W., Shevchenko, P. V., Hassani, B., and Chapelle, A. (2016). Should the advanced measurement approach be replaced with the standardized measurement approach for operational risk? *Journal of Operational Risk*, 11(3):1–49.

Peters, G. W. and Vishnia, G. (2016). Blockchain architectures for electronic exchange reporting requirements: EMIR, Dodd Frank, MiFID I/II, MiFIR, REMIT, Reg NMS and T2S.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2):121–135.

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, 55(4):349–356.

Shevchenko, P. V. (2011). *Modelling Operational Risk Using Bayesian Inference*. Springer Science & Business Media.

Shim, H., Kim, C., and Choi, Y. H. (2017). Covariates and insurance costs of data breach risk. *working paper*.