International Journal in Management and Social Science
Volume 07 Issue 10, October 2019 ISSN: 2321-1784 Impact Factor: 6.319
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

CYBER RISK MANAGEMENT AND INSURANCE IN ZIMBABWE. A CASE OF SHORT TERM INSURANCE BROKERS IN ZIMBABWE

Samugwede,O. H,
Midlands State University, Insurance and Risk Management Department
Matsika R,
Midlands State University, Insurance and Risk Management Department
Ndlovu A. O,
Midlands State University, Tourism and Hospitality Management Department
Nyadzayo Chipochedu(Bcom)
Midlands State University

ABSTRACT

Emerging risks are hard to identify, let alone anticipate their impact. It is imperative that insurance brokers be conversant with emerging risks such as cyber risk so that they can set themselves apart from other risk management providers. The world is now a global village, thanks to the internet and other technological advancements that have taken place. Although cyber risk is prevalent in the first world, it is important to note that cyber risk is increasing in the developing countries, and Zimbabwe is no exception. Insurance brokers must therefore provide effective cyber risk management and insurance solutions to cater to the Zimbabwean client. This study assessed the current risk management and insurance solutions that brokers are providing, and whether these solutions are effective in mitigating cyber risk. The study was based on convience sampling and 11 short term insurance brokers were used. 4 reinsurance brokers were also used to provide regional expertise. All samples are registered with the Insurance and Pensions Commission. The researcher utilised interviews and questionnaires to carry out the survey. The data gathered from the survey was presented and analysed through tables, charts as well as graphs. After assessment of the findings, the research concluded that the current cyber risk management and insurance solutions being provided by insurance brokers is not effective in mitigating cyber risk. The main reasons for this was due to the complex nature of cyber risk, lack of broker expertise as well as the lack of flexibility of the regional and international risk carries. The research also recommended

that IPEC should assist in lobbying for a cyber Act so that regulations on the Zimbabwean cyber space are locations-specific and breach of these regulations can penalise offenders. The research noted that training and development of IT related courses as well as technical partnerships with regional and international brokers will assist in insurance brokers providing a bespoke cyber product offering unique to Zimbabwe.

Background of the study

The soft insurance market in the country has made competition amongst insurance brokers extremely volatile, resulting in large amounts of commission rebates being offered to clients as well as undercutting of premium rates. This means that the profits of existing business for insurance brokers is significantly declining each year, and the only solution to retain or increase profits is to obtain new business. However, the insurance market is too concentrated with high numbers of insurers and insurance brokers. The Insurance and Pensions Commission (IPEC) (2017) stated that the number of registered insurers is 20 and brokers are 32. This makes the probability of obtaining new business relatively low.

According to IPEC (2017) "the asset base for insurance brokers marginally decreased to $29.47 million for the nine months ended 30 September 2017 from the $31.15 million reported in the comparative period of 2016. This was mainly as a result of a decrease in premium receivables from $5.72 million reported at 30 September 2017 to $3.66 million recorded under the current quarter. A further decrease of $0.63 million was witnessed in cash and cash equivalents for the current quarter as compared to the same period in 2016".

The solution to the decreasing revenue of insurance brokers is to take a holistic approach to their product offering, and move away from traditional risk solutions. Until recently, there was no specific insurance policy in Zimbabwe that covered any loss or damage as a result of cyber risk. A standard property damage and business interruption policy excludes cover for loss or damage of any electronic equipment. The standard policy wording for some insurance companies is as follows:

"The policy excludes any loss or damage to a computer system, hardware, program, software, data, information repository, microchip, integrated circuit or similar devise in computer

equipment or non-computer equipment, whether the property of the Insured or not, do not in and of themselves constitute loss of/or damage unless arising out of one or more of the following perils: fire, lightning, explosion, aircraft or vehicle impact, falling objects, windstorm, hail, tornado, cyclone, hurricane, earthquake, volcano, tsunami, flood, freeze or weight of snow".

While the standard electronic equipment covers accidental loss or damage of the actual electronic equipment, it does not cover any losses as a result of cyber risks such as hacking. The fidelity guarantee policy would only respond to any system hacking as a result of fraud by employees. The above noted policies present a gap in the insurance market.

This is where emerging risks become an opportunity for some insurance brokers to gain a competitive advantage above others. In a world where people are more and more dependent on technology and the internet, the emergence of cyber risk becomes inevitable. Cyber risk is no longer a problem for the developed world only, but now affects every part of the globe, including Zimbabwe. Some African countries have gone a step further and created cyber risk laws. Zimbabwe has also created a draft Computer Crime and Cyber Crime Bill, which is yet to be enacted.

In Zimbabwe, the number of mobile smart phone users is rapidly increasing. With regards to the increase in mobile internet and data traffic in Zimbabwe, the Postal and Telecommunications Regulatory Authority of Zimbabwe (2017) stated that, "consumption of data/internet services increased by 39.1% to record 4,129.4 Terabytes from 2,968.2 Terabytes recorded in the previous quarter. With the shortage of cash in the country, most banks have resorted to online banking platforms. The recent debit card fraud cases as well as ransomware have resulted in more awareness that Zimbabwe does not live in a vacuum, but can also be affected by cyber risks. These circumstances pose an opportunity for short term insurance brokers to increase their profitability by providing risk management and insurance solutions for emerging risks such as cyber risk.

Statement of the problem

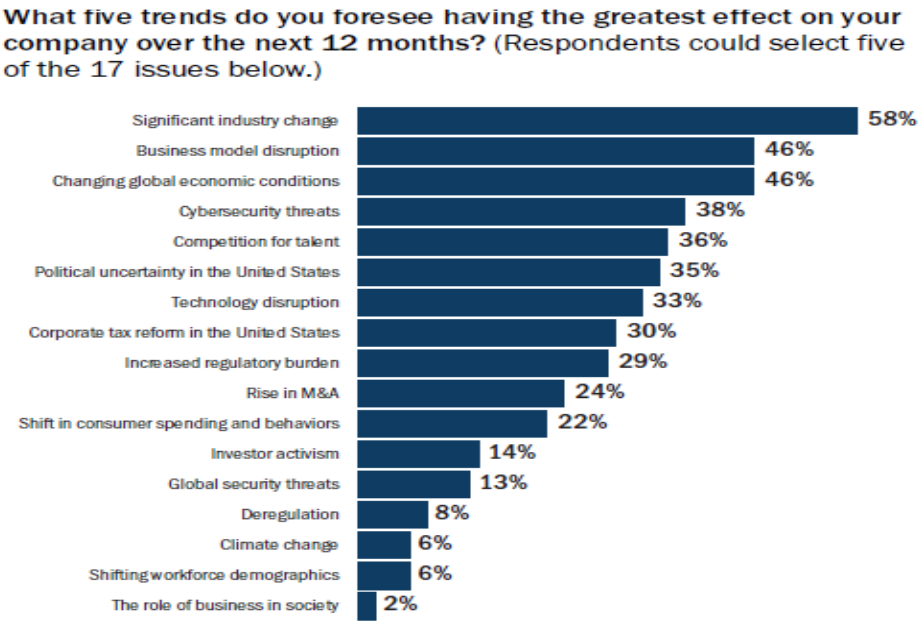
Emerging risks are never static, and the rapid changes in an economy introduces new risks leaving some industries virtually extinct. These emerging risks such as technological advancements, as well as improvements to existing technologies pose various threats that affect the existence of companies in Zimbabwe. For instance, innovations such as interactive websites as well as mobile applications have resulted in the advent of cyber risks. Although cyber risks are known to exist in Zimbabwe, there is little experience with determining the actual probability of losses resulting from these risks. However, more time must be put to understanding cyber risk, as bespoke insurance and risk solutions can be created which will bring about competitive advantage for short term insurance brokers in Zimbabwe.

Development and Trends of Cyber Risk

Almost every business entity in the world uses the internet in one form or another, from advertising, to manufacturing, to recordkeeping. The emergence of Electronic Commerce (E-commerce) has brought about many benefits in all industries, and it has also made the global markets more accessible as consumers can now access goods and services from the click of a button. According to Andam (2003), e-commerce refers to, "any form of business transaction in which the parties interact electronically rather than by physical exchanges or direct physical contact". Usually, e-commerce is carried out with the use of the internet. Although e-commerce has many benefits, it has resulted in the emergence of cyber risks that are associated with internet use. Any kind of business that transacts electronically or with the internet is prone to cyber risk. The healthcare sector for instance is prone to many cyber risks through the use of pacemakers as well as insulin pumps that can be manipulated through the internet (Gonzalez: 2018). Cyber-attacks were first realised in the developed countries over 30 years ago, with some notable cases such as the Morris Worm dating back as far as 1988. The first world has over the years experienced many disasters due to cyber risk, and the effects of cyber-attacks have become more and more serious.

Companies in the United States of America have placed cyber risk in the top 5 trends most likely to impact their performance, according to a study carried out by the National Association of Corporate Directors (2017)

Figure 2.1 Trends that have the greatest effect on companies in the USA



Source: National Association of Corporate Directors (2017)

2.1.1 The Dark Web

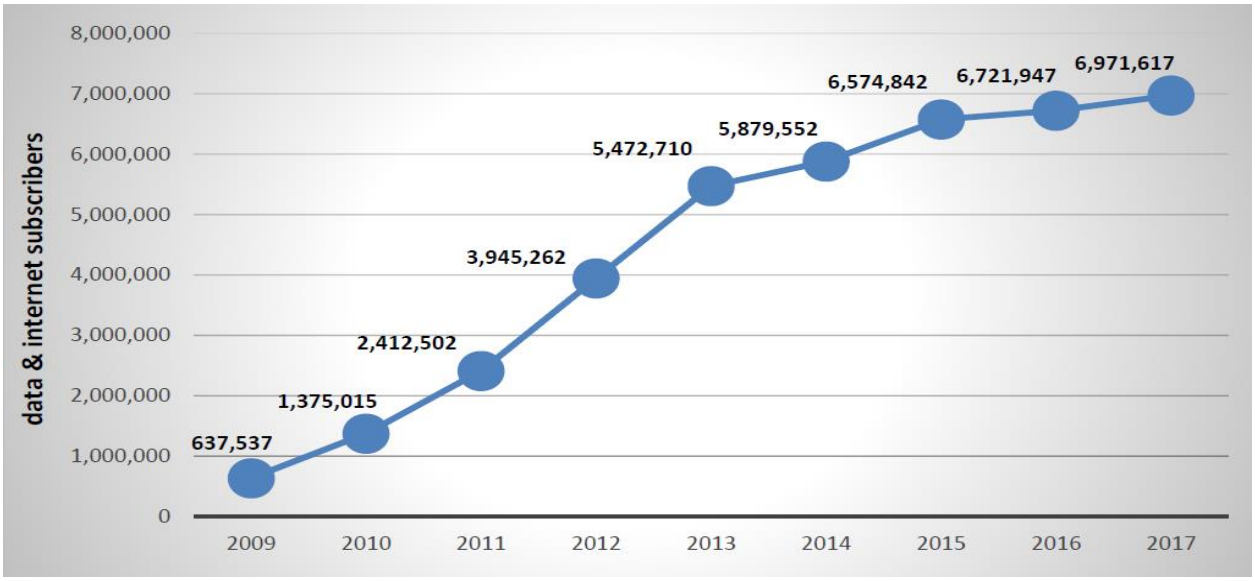
Most people in the world have been exposed to the normal web, which can be accessed through normal search engines such as Google or Firefox. However, much like outer space, the internet is a much larger dimension. According to Hoffman (2016), "the dark web exists on darknets, which are "overlay networks…they require special software to access, so they aren't normally visible or accessible to people who aren't in the know". Criminals have over the years used the dark web to participate in activities such as human trafficking, selling of drugs, etc. Hoffman (2016) also further explains that although the dark web can be used by people living in oppressive countries to access social media, it can also be used to lure unsuspecting individuals to hacking, and perpetrators will be anonymous.

Cyber Risk Development in Zimbabwe

Cyber risk has started to gain momentum in the developing world, as more and more companies are using the internet for business transactions. For instance, Zimbabwe's liquidity crisis has seen an exponential increase in the use of point of sale machines, internet banking, as well as mobile money transactions through service providers such as Ecocash or One Money. Nowadays, one only needs to log onto a bank's portal and access RTGS services instead of actually walking into a bank. Because of this, the public is now exposed to various cyber-attacks that were previously unheard of, such as card cloning.

In Zimbabwe alone, "the internet penetration rate increased by 0.8% to reach 50.8% in 2017 from 50% recorded in 2016. Fibre internet registered the highest growth in active subscriptions of 59.7% to reach 31,455 in 2017 from 19,698 recorded in 2016" (Postal and Telecommunications Regulatory Authority of Zimbabwe, 2017. POTRAZ also mentioned that there has been a significant decline in postal services due to social media platforms such as WhatsApp. The table below reflects the growth trend in data and internet subscribers in Zimbabwe:

Figure 2.1.2 Data and Internet Subscribers in Zimbabwe



Source: Postal and Telecommunications Regulatory Authority of Zimbabwe (2017)

According to POTRAZ (2017), the level of mobile money services significantly increased due to the liquidity crisis being faced in the country. POTRAZ further reported that the amount of both cash in and cash out transactions exceeded USD 1billion across all service providers in the country. These high volumes show that mobile money transactions contribute significantly to the economy, and this also brings about a new cyber risk as banks are no longer the only service providers offering financial services.

Newsday Zimbabwe (2018) reported an incident where a group of people distracted a fuel attendant in order to steal a POS machine. This has led to more and more banks in the country providing awareness advertisements on card cloning and safekeeping of bank cards. Because of these alarming trends, it is prudent for insurance broking firms in the country to provide risk management solutions and insurance for cyber risk.

Notable Cyber Attacks

There have been many infamous cases that have resulted in more awareness of the effects of cyber risks, and these cases have also influenced the type of insurance coverage available in markets, as well as risk management strategies that companies must adopt.

The Morris Worm

Bortnik (2013) studied the first recognised case of malware recorded. In 1988, a man by the name of Robert Morris created a form of malware that slowed down performance of a large number of computers in the USA to the extent that they could not function. According to Bortnik (2013), “The worm slowed thousands of systems down to a crawl by creating processes and files in temporary folders and trying to spread copies of itself”. Morris was the first man to be convicted of the crime. Etsebeth (2007) examined the effects of malware and cited the definition of malware according to Grimes (2001) as, “any software program designed to move from computer to computer and network to network to intentionally modify computer systems without the consent of the owner or operator”.

Sony Pictures Hacked

Peterson (2014) detailed the cyber breach on one of the world's biggest entertainment giants Sony Pictures. She revealed that Sony Pictures had a data breach on their servers caused by a malware. The malware is reported to have stolen tones of employee confidential and intellectual data. The reason for this cyber-attack on Sony was targeted on a movie produced by Sony called The Interview which was based on a fictitious comic storyline of an assassination attempt on the North Korean president Kim Jong Un. It is reported that North Korea had issued statements about the repercussions of releasing the movie. The data stolen was then used by the hackers to threaten leaking all the sensitive information to the public if Sony pictures proceeded to release the movie. The movie eventually never premiered. Later in November 2015 BBC reported that Sony agreed to pay USD 8 million to its employees who claimed they had suffered economic harm from the stolen personal data. Subsequent investigations of the hack report the hack technology to that used by the hacking group known as the Lazarus group.

Estonia Cyber Attack

Herzog (2011) studied the cyber-attacks that Estonia experienced in 2007. He outlined the ethnic tensions that were being experienced between the native Estonians and the Russians. The tensions resulted in denial-of-service cyber-attacks on Estonia's infrastructure and websites of all government websites and some political parties, as well as two major banks. Because Estonia was well established in electronic channels of doing business, various businesses were distracted due to this cyber-attack.

Target Data Breach

Target experienced one of the largest data breach cyber-attacks in 2003, and this resulted in them having to pay a settlement of over USD 18million to the various states affected in the United States of America, according to McCoy (2017). McCoy further explained that the attackers hacked credentials of Target to gain access to personal information such as credit card information, names, and addresses, of 41million clients. This data breach not only resulted in direct financial loss to target, but it also created bad reputation for the large retail outlet.

ABSA Bank South Africa Phishing Attack

In 2003, hackers managed to log into ABSA bank as well as two other banks and managed to transfer funds into prepaid accounts of mobile operators, and one method that was used to access the bank's account was through phishing, according to a study conducted by Van Niekerk (2017). Phishing, as defined by Jagatic et al (2005) in Lotter and Futcher (2015) is, "a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party". Phishing may occur by clicking on links found in spam messages, or even opening emails that seem to be from a legitimate source.

Cyber Threats Exposures

The above noted cases as well as many other cases that have occurred all over the world in the past years have enabled the following exposures to be identified:

Hacker attacks

Many are accustomed to thefts that are physical in nature, where a thief has to be present in order to steal or cause harm. However, cyber risk presents a more dangerous form of thief, named a hacker, who is not visible to the naked eye. Hackers are quirky programmers, capable of brilliant, unorthodox feats of machine manipulation (Berry, 2015). In other words, these hackers are geniuses when it comes to the internet and computers such that they can manipulate any program to their advantage. Companies are exposed to these hackers as they are known to have sensitive information as well as large amounts of funds.

Data Breach

As eluded earlier, e-commerce has formed the basis of many companies as it brings about many benefits. Although they provide professional advice with regards to risk exposures, insurance broking firms also have large amounts of data that they keep regarding their clients which also leaves them exposed. This data is usually kept electronically and any breach of data poses devastating consequences to the broker as privacy of consumers will be breached. Many companies are exposed to data breaches as their information will be leaked into the wrong hands. Symanovich (2017) defines a data breach as, "an incident that exposes confidential or protected

information". Many other companies that keep their confidential data electronically are also exposed to data breaches.

Virus Transmission

Hackers create what are known as computer viruses that attack both the software and hardware of a computer system, compromising its defenses. Robinson (2012) also explains that computer viruses "are destructive programs that delete or corrupt files, interfere with your computer operations and reproduce themselves to fill disk or RAM space on your computer". Although companies may have anti viruses installed, these may prove to be insufficient as viruses will continuously be updated.

Cyber Extortion and Vandalism

This form of exposure is more company or individual specific, as hackers or cyber criminals take control of specific important information and demand payment in exchange of the stolen information. This form of attack is known as ransomware. Cyber criminals who mainly operate in the dark web are rarely caught. Robinson (2016) further explains that the cyber extortionist is different from the ordinary hacker as he takes the victim's confidential information and threatens to publicly distribute it unless he is paid. Many corporations and prominent individuals are prone to this form of exposure as they are known to have enough wealth to give in to a cyber criminal's financial demands.

Some hackers form groups that terrorise companies worldwide. Some websites of large corporates have been breached and replaced by other images that do not represent the companies.

Business Interruption

The loss of profits of a firm following accidental physical damage of an asset is the normal form that is anticipated by risk managers. However, many companies are now exposed to loss of profits as a result of cyber-attacks. It is important to determine the extent to which cyber-attacks affect losses, especially with institutions such as banks, where large volumes of people use bank cards. The loss of profits can become catastrophic in nature if a bank is compromised.

Third Party Liabilities

This is probably the most important aspect of cyber exposures as liability is unlimited. Service providers can be sued for losses that have been incurred as a result of hacking. Owners of applications or websites for example may be sued for not having a secure portal. A mobile service provider for example, may engage a software engineer to provide a mobile application for use by its subscribers. If the application is hacked and losses are incurred, the software engineer may be liable for the losses if their application was found to be compromised before the hacking.

Legislation on Cyber Security

An important aspect that needs review is the current legislative frameworks that have been enacted to respond to cyber security as well as cyber threats. Internationally, the laws have differed from one continent to another. Countries such as USA have enforced compulsory law that obligates all companies to have standard cyber protection in order to protect the rights of consumers. Failure to abide by these laws results in huge fines being slammed on non-compliant entities.

Criminal laws and international treaties can only go so far in deterring and punishing those responsible for cyber-attacks and threats .Therefore, governments are updating and passing new laws to improve the security and resilience of electronic networks, systems and data (Lloyds, 2017).

Legislation in UK, USA and Schengen Countries

Marsh and McLennan (2016) outlined the different legal frameworks among the Schengen Countries, the United States of America as well as the United Kingdom. The following facts were highlighted:

1) United Kingdom: Besides telecoms companies, mandatory reporting is not required for cyber-attacks. However, serious breaches should be reported. The London Stock Exchange also mandates companies that are listed to disclose any material information that may compromise their system. Companies that are regulated by local bodies are also

obliged to report incidents that may harm their reputation. According to Ward (2016), the UK first published its paper on cyber security in 2011, and in 2016 it published the National Cyber Security Strategy, which contained 3 pillars namely, defend, detect and develop. However, this current legislation will be affected by the current European Union in the course of 2018.

2) USA: In the USA, each state has its own laws; however, national institutions such as the FBI regard cyber security as a national security issue. Most cyber criminal groups originate from USA, and USA has also experienced some of the most devastating cybersecurity breaches. It is no surprise therefore, that USA's legislation as well as risk management is more advanced than in other countries in the world. There are a number of cyber laws that have been put in place to mandate banks to disclose any attacks, as well as punish firms that have compromised computer systems. According to Fischer (2014), the Obama administration also launched various initiatives, such as appointing the first White House cybersecurity coordinator.
3) According to Marsh and McLennan, "the European Union's policy making is driven by its cyber security strategy, which outlines the following priorities for its member states
    i. Achieving cyber resilience
    ii. Drastically reducing cyber crime
    iii. Developing cyber defense policy and capabilities related to the common security and defense policy
    iv. Develop the industrial and technological resources for cyber security
    v. Establish a coherent international cyberspace policy for the European Union and promote core U values".

The European Union therefore launched Network and Information Security which is mandated to oversee the standards of cybersecurity in European Union countries.

Cyber Risk Control Measures

Various cyber risk control measures can be implemented in order to mitigate the adverse effects of cyber-attacks. Signe and Signe (2018) suggested that African businesses should adopt the following measures:

a) Design and deploy cyber resilience
b) Protect data integrity
c) Integrate cyber risk awareness into the decision process
d) Develop cyber security skills

Various leading insurance brokers over the world have adopted the above risk management frameworks in order to assist their clients in securing their private information, as well as reducing the severity of cyber risks when they do occur. Apart from the NIST and ISO 27000 certification, Aon International as well as Marsh and Mclennan Group of Companies have published a number of articles on their websites regarding the cyber risk management services they offer to their clients.

Other control measures that insurance brokers provide include training and awareness of staff, constant reviews of antiviral software, as well as insurance to cater for the losses when they occur.

Cyber Insurance as a Risk Transfer Mechanism

The role of an insurance broker is to provide solutions that mitigate risks being experienced by insureds. This means that any prudent insurance broker must anticipate the effect that emerging risks have on their clients, and being to provide solutions that reduce or even eliminate these risks. Cyber insurance is therefore a risk transfer mechanism that companies can utilize in order to mitigate the effects of cyber risks.

Policy Coverage

Cyber insurance is still an emerging risk, and there is insufficient data that has been collected to date. The availability of data on cyber risk is rather scarce. This might be due to the fact that institutions that have been compromised do not disclose incidences (Eling and Schnell, 2016). However, with time, insurers will have more data, which will enable modification of the current coverage to suit the actual risk on the ground. Lloyds as well as Zurich are some of the cyber insurance carriers in the world.

Traditional insurance policies do not offer coverage for cyber risk, and if they do, coverage is very minimal. Amos and Pettifer (2016), outlined the difference in coverage that is provided by cyber insurance, compared to traditional risks:

Figure 2.7.1 Traditional Insurance vs Cyber Insurance Coverage

Cover	Property	General Liability	MGT Liability	PI / D&O	IT Liability	Crime	Cyber Security
1st Party							
Incidence Response	✗	✗	✗	✗	✗	?	✓
Information Asset Loss	✗	✗	✗	✗	✗	?	✓
Regulatory	✗	✗	✓	✗	✗	?	✓
Cyber Extortion Expenses	✗	✗	✗	✗	✗	?	✓
Loss of Income	✗	✗	✗	✗	✗	?	?
3rd Party							
Data Privacy Liability	✗	✗	?	?	?	✗	✓
Media Liability	✗	?	?	?	?	✗	✓
Network Security Liability	✗	✗	✗	✗	?	✗	✓

✗ Not generally covered ✓ Covered ? Uncertain or varied coverage

Source: Amos, S. & Pettifer, A. (2016)

The policy coverage has been generally standard across most insurers, due to the fact that insurers rarely retain the risk, but cede a large portion to reinsurers. Below is a summary of the basic coverage:

i. Cyber Incident Response
This section covers loss or damage as a result of response costs following a breach, as well as any legal, forensic investigative as well as crisis management costs.

ii. Cyber Crime

This section covers losses which are more prevalent in Zimbabwe such as card cloning, funds transfer fraud, extortion, identity theft, as well as phishing. Card cloning is not covered in some policies, and a separate policy would need to be taken out for this cover.

iii. System Damage and Business Interruption

The costs incurred in rectifying a hacked system will be covered under this section. Also covered is loss of profit following a cyber-attack.

iv. Network Security and Privacy Liability

Following events such as malware, denial of service, identity theft, or failure to prevent unauthorised access to information stored or applications hosted on computer systems, this section will cover any third party claims that have been incurred up to the policy limit. The section will also provide for any fines or penalties that would have been incurred following the breach. International banks for instance must adhere to certain bodies and if losses occur because of a compromised system, they may face penalties from regulators.

v. Media Liability

If any liability attaches to the insured because of defamation, or infringement of intellectual property, the section will pay the costs up to the policy limit.

vi. Technology Errors and Omissions

Any loss arising out of any act, error, omission or breach of contract in the provision of technology services will be covered under this section. However, some policies do not cover this section, as it can be sought under a separate policy namely, a professional indemnity policy.

vii. Court Attendance Costs

Any legal costs that may be incurred during litigation following a cyber breach will be covered up to the specified limit in the policy.

Notable Exclusions

The following are standard exclusions that can be found in most wordings:

i. Business interruption liability for that part of any claim that constitutes actual or alleged liability to a third party, or legal costs in the defense of any claim, including customer compensation.
ii. Actual or alleged antitrust violation, restraint of trade, unfair competition, false, deceptive or unfair trade practices, violation of consumer protection laws or false or deceptive advertising.
iii. Associated companies.
iv. Betterment which results in the insured being in a better financial position or benefitting from upgraded versions of computer systems as a direct result of the event which gave rise to the claim under this policy.
v. Bodily injury and property damage.
vi. Chargebacks for any credit card company or bank, wholly or partially, reversing or preventing a payment transaction, unless specifically covered under the policy
vii. Core internet infrastructure failure arising directly from a failure, material degradation or termination of any core element of the internet, telecommunications or GPS infrastructure that results in a regional, countrywide or global outage of the internet, including a failure of the core root servers, satellite network or the IP addressing system or an individual state or non-state actor turning off all or part of the internet.
viii. Professional Liability.

Underwriting Considerations

Because cyber risks are complex in nature, the information required for cyber insurance is also relatively complex. Insurance brokers usually recommend that clients seek the assistance of their IT department when completing the proposal form. The following notable information is required:

i. Nature of business, including products and services offered
ii. Public facing URL addresses
iii. Gross revenue
iv. Geographical spread
v. Details of any unscheduled network outage that has occurred in the past eg 2years
vi. Current information security policies which have been approved by management

vii. Details of information security certifications
viii. Minimum password length restriction applied to accounts
ix. Frequency of IT environments being subjected to vulnerability or penetration testing
x. Type of data stored and details of own as well as third party data, including back up services
xi. Security system details currently in place
xii. Frequency of antivirus updates
xiii. Details of third party IT service providers
xiv. Details of documented and approved disaster recovery and business continuity plans
xv. Personnel security screening details
xvi. Claims history
xvii. Limit of liability required

RESEARCH METHODOLOGY

Kothari (2004) defines research as "…a search for knowledge. One can also define research as a scientific and systematic search for pertinent information on a specific topic". In other words, sample data that is collected should be derived from a population, and this data must be organised in such a way as to be able to be analysed, so that certain conclusions can be made regarding the data. This chapter details the methodology used to test the objectives highlighted in chapter one, as well as provide a summary for the instruments that were used in data collection. The research design, research participants, target population, sampling procedures, data collection methods and justifications of various methods and tools that were used in carrying out the research are also provided in this chapter.

Study Population

A study population forms the basis of the research as information is derived from there. According to Kumar (2011), a study population is comprised of individuals, groups and communities where information is sought. The study population is comprised of the people with whom possess the information required to carry out the research.

For the purposes of this study, the target population was all the 31 insurance brokers and 7 reinsurance brokers in the Zimbabwe insurance market (IPEC, 2019). The respondents were all in managerial positions in operations divisions in those companies, and the respondents were located in Harare. The researcher based the sample of respondents based on their contribution to the insurance market, their market share, as well as their expertise in regards to complex risks.

Non-Probability Sampling

There are different types of sampling, but the researchers focused on opportunity or convenience sampling. Cherry (2018) described that convenience sampling, "involves using participants in a study because they are convenient and available". Kothari (2004) also describes convenience sampling as deliberate in nature. According to Cohen, Manion and Morrison (2000), "quota sample strives to represent significant characteristics (strata) of the wider population; unlike stratified sampling it sets out to represent these in the proportions in which they can be found in the wider population". According to Cherry (2018), purposive sampling, "involves seeking out individuals that meet certain criteria".

The researcher carried out the study based on non-probability sampling because it selects a the samples at random, which gives a relatively equal chance of all the population to be selected. In this instance, the researcher aimed at interviewing as well as handing out questionnaires to experienced insurance brokers in supervisory or management level, who would have more expertise with regards to cyber risk.

Population Vs Sample size

Sample size is a term used to define the number of respondents included in a sample, selected from the population and it is considered as a fair representative of the entire population for that specific area of study (Norris, 2013). A sample size of more than 33% of the population is recommended to act as a representation of the population under study (Haralambos et al, 1990).Furthermore, Saunders (2016) in his study stated that 10 % of the target population is sampled when the population is above 200 and 40 % of the population is sampled when the population is below 200.The researcher adopted the idea of halarambos and holborn to come up with the sample size.

Population Vs Sample size

Population Insurance Brokers	Sample
31	11
Reinsurance Brokers 7	4

Source : primary data

Research Instruments and Data Collection

For the purposes of this study, the researcher used questionnaires as well as interviews. The use of two research instruments will enable the acquisition of accurate data from the sample size. While designing data-collection procedure, adequate safeguards against bias and unreliability must be ensured (Kothari, 2004). The use of two data collection methods ensures that data is not biased.

Primary Data Sources

According to Kothari (2004), "the primary data are those which are collected afresh and for the first time, and thus happen to be original in character". Primary data is more reliable, authentic and objective as it has not been published yet. Its validity is greater than secondary data as it has not been changed or altered by humans. Primary data is useful because there is limited published material on the subject under study and this data can be collected through the use of questionnaires or interviews. Furthermore primary data is important because it gives factual information about the outcomes of research or observation.

Questionnaires

According to Kumar (2011), "a questionnaire is a written list of questions, the answers to which are recorded by respondents. In a questionnaire respondents read the questions, interpret what is expected and then write down the answers. They are a list of closed ended and open ended questions given to respondents so as to collect information. These are mainly used to produce quantitative data and they will be distributed to various players in the industry. Forms are to be completed and returned by the respondents. The responses are gathered in a standardised way and respondents should be told why the information is being collected and how the results will be beneficial. They should be asked to reply honestly and told that if their response is negative

this is just as useful as a more positive opinion. If possible the questionnaire should also be anonymous.

Justification for the Use of Questionnaires

The use of questionnaires allowed the researcher to collect information that was relevant to the research problem. Furthermore, by utilising the email (electronic mail), questionnaires were quickly sent to most chosen respondents, and this provided the researcher with a cost-effective means to reach out and get information from the geographically spread respondents. In addition, by giving respondents ample time to complete the questionnaires, the respondents were able to think deeply about the answers, to make consultations before answering and to appraise their answers, thereby enhancing the quality of the data provided.

Interviews

Cohen, Manion and Morrison (2000) describe an interview as, "an interchange of views between two or more people on a topic of mutual interest". Interview responses are more qualitative in nature as they highly rely on experience and opinion in relation to knowledge of the respondent on the subject matter than actual information.

Justification for the Use of Interviews

Personal interviews help improve the interaction and simultaneous influence on the respondents presenting facts as they are. This gives room for probing further giving more room for detailed the responses. Emphasis will be placed on the researcher's interpretation of the question. The advantage of carrying out interviews is that data is collected immediately.

Secondary Data

The researcher made use of secondary data obtained from various newspaper articles, as well as journals to derive at the conclusions. Because cyber risk is an emerging risk, there have been few books that were published.

DATA PRESENTATION AND ANALYSIS

An Analysis of Response Rate

The researcher distributed 35 questionnaires to 11 insurance broking firms and 4 reinsurance brokers in the market, and a total of 31 questionnaires were returned successfully. In addition, the researcher carried out 8 interviews to complement the questionnaires that were distributed. The table below summarises the results of the data collection process:

Table 4.1 Response Rate of Participants

Frequency of Questionnaires/Interviews	**Questionnaires**	**Interviews**
Distributed	37	11
Returned/Conducted	31	9
Discarded	0	0
Analysed	31	9
Response Rate	**83.78%**	**81.81%**

Source: Primary Data

Work Experience of Respondents

The researcher targeted respondents who are in managerial ad supervisory positions in their organisations, and who have atleast more than 5 years' working experience in the insurance industry. The reason for selecting respondents at managerial level is to ensure accuracy of results since complex risks are dealt with by persons at higher levels. Respondents with higher working experience were selected because of the complex nature of cyber risk, and this would require respondents to have some form of exposure with regards to complex risks. The questionnaires used for instance come with a risk of non-response, which is the failure of a respondent to provide wholly or partially information required in a sample survey (Oxford Dictionary of Statistical Terms: 2003). More experienced respondents would reduce the risk of non-response, as they may be more equipped to understand the context of what is being asked of them. Below is a diagram which details the work experience of the respondents:

Data Presentation and Discussion

Prevalence of Cyber Risk in Zimbabwe

The statements relating to the above question were asked in order to justify that cyber risk is a prevalent risk in Zimbabwe which insurance brokers need to address. A series of questions were presented, and respondents were supposed to pick an answer from 1(strongly disagree) to 5 (strongly agree). The following table represents the mean number of results:

Table 4.3.1 Results for Prevalence of Cyber Risks in Zimbabwe

Statement	Mean
The company sees cyber risks as an opportunity for business development.	4.41
The company values cyber risk as an important field which brings financial value addition to its clients.	3.93
A significant proportion of both existing and new clients have been making enquiries about cyber risk.	3.59
I have been/know someone who has been a victim of a cyber-attack.	4.89
I am satisfied with the statement that cyber risk is a significant emerging risk in the Zimbabwean context.	4.97

Source: Primary Data

According to Kothari (2014), mean refers to the total number of numbers recorded divided by the number of results in a given set. The mean determines the measure of central tendency and it assists in identifying the average results in a given set of data. The formula used is as follows:

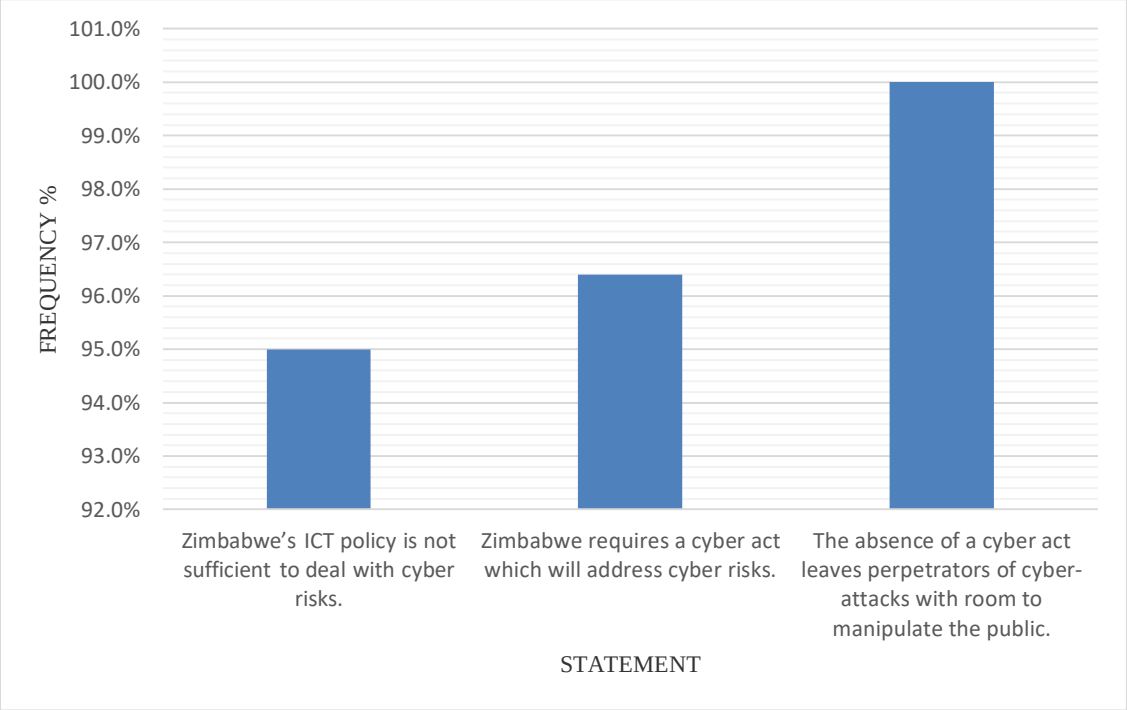
$$\frac{\text{Summation of results}}{\text{Number of results}}$$

The results above show that a significant proportion of clients that come through brokers have been making enquiries about cyber risk. A mean of 4.97 also suggests that the respondents strongly agree that cyber risk is a significant emerging risk in the country, which supports the notion that cyber risk is indeed prevalent in developing countries such as Zimbabwe. According to the Reserve Bank of Zimbabwe (2015), cybercrime has significantly contributed to the USD 1,8billion obtained criminally each year in Zimbabwe. The above results indeed support this notion as most respondents have been or know someone who has been a victim of a cyber-attack.

Importance of Cyber Legislation in Zimbabwe

The statements relating to the above question were asked to establish that lack of cyber legislation leads to gaps in the cyber risk management process. The diagram below details the relevance of cyber laws currently available in Zimbabwe:

Figure 4.3.2 Cyber Legislation in Zimbabwe



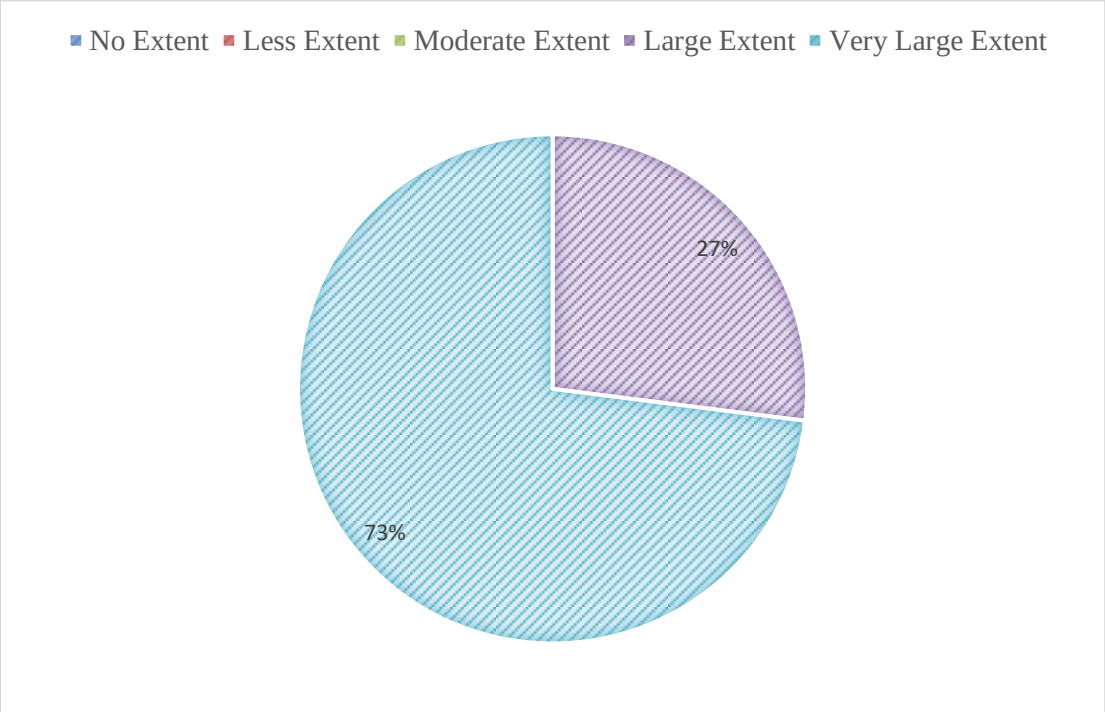
Source: Primary Data

95% of respondents agreed that Zimbabwe's ICT policy is not sufficient to respond to cybercrimes that occur in the country. Although there is a draft cyber bill, 96.5% of the respondents strongly agree that a cyber act will effectively address the cyber risks being faced in the country. All the respondents strongly agreed that without a cyber act, cybercriminals could not be answerable to their crimes as no law would be breached if there is not cyber act.

Cyber Insurance in Zimbabwe

Cyber Insurance packages in Zimbabwe are obtained regionally and internationally only
The above question was asked in order to determine the level of underwriting experience towards cyber insurance in Zimbabwe. The diagram below details the results from no extent (1) to very large extent (5) to the above statement:

Figure 4.3.4 a) Cyber Insurance in Zimbabwe

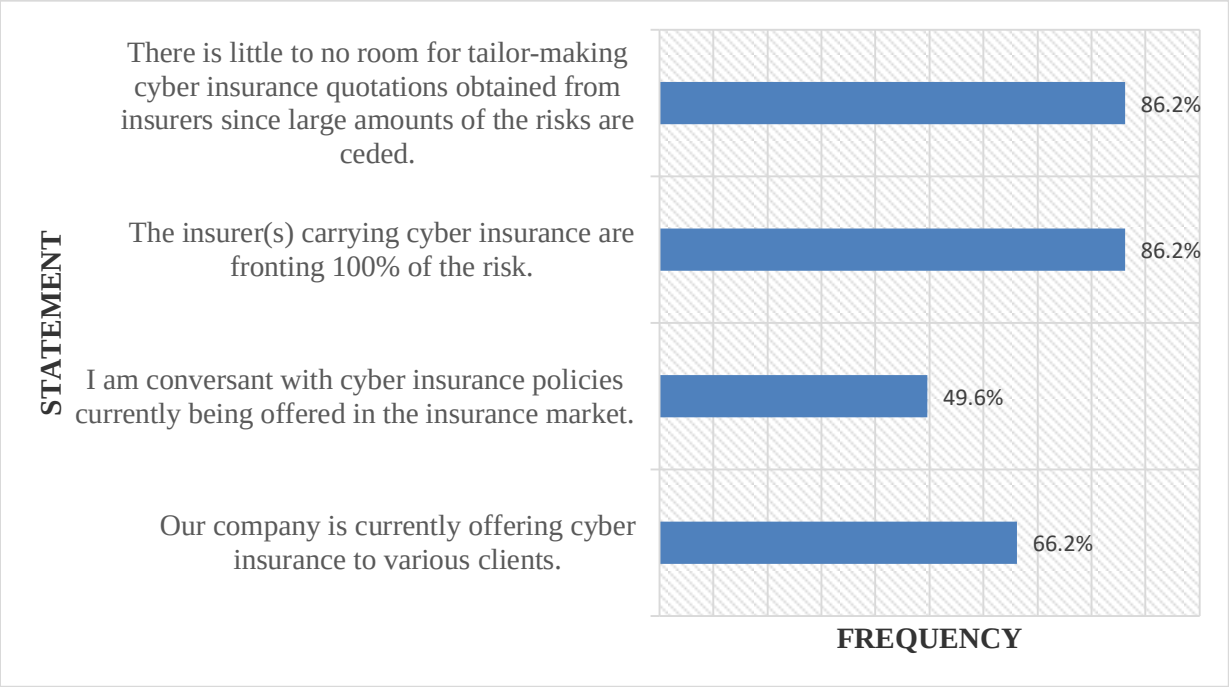


Source: Primary Data

The diagram above can support the conclusion that cyber insurance is still new to the insurance industry in Zimbabwe, and insurance brokers are heavily reliant on the expertise of international brokers, insurers as well as reinsurers.

a) Level of product knowledge and suitability of current cyber insurance to Zimbabwean market
The statements pertaining to the question above were presented to determine the level of product knowledge of insurance brokers with regards to cyber insurance. The diagram below relates to cyber insurance product knowledge as well as applicability of the product available to the local insurance market:

Figure 4.3.4 b) Cyber Insurance Product Knowledge and Relevance of Cyber Insurance Policies to Zimbabwe



Source: Primary Data

From the above diagram, it can be concluded that on average, insurance brokers in Zimbabwe are not adequately knowledgeable with cyber insurance policies. Since the insurers cede most or all of the risk, the insurance brokers cannot negotiate for increase in scope of cover or even removal of other covers to suit the actual risk being faced by their clients.

b) Recommendations on scope of cover currently being provided

The statement above was asked so that the respondents could share possible recommendations to the current cyber insurance cover that could suit the Zimbabwean context. The following recommendations were noted:

i. The local broking market should lobby for cyber legislation
ii. Brokers do not have much product knowledge. Bodies such as IBAZ and IIZ must provide training workshops on cyber risk and insurance.
iii. The current coverage being provided internationally is adequate, although the underwriting considerations required are too cumbersome.

iv. Brokers must directly interface with the external insurers which offer cyber insurance. This will reduce the chain and create room for tailor made cyber insurance products.

v. There is need for broker forums where experienced brokers train cyber insurance.

vi. Research analysts should be employed so that they develop a cyber insurance product that speaks to the Zimbabwean client.

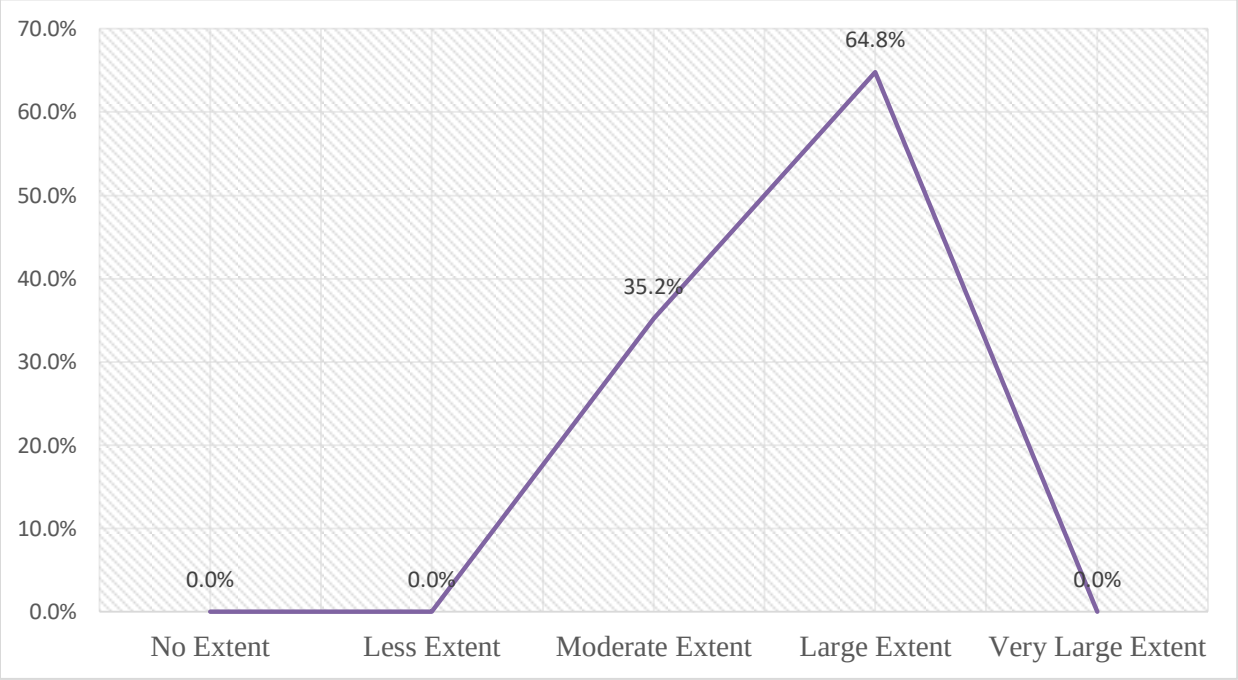
vii. Assessors with IT background should be employed to provide cyber risk models that can be implemented by clients.

4.3.5 Claims Experience on Cyber Insurance Policies

a) Cyber claims are beginning to increase

The statement relating to the above topic was established in order to determine the trends of cyber claims. The following results were obtained from the statement that although claims frequency is currently low, cyber insurance claims are beginning to increase especially in financial institutions:

Figure 4.3.5 a) Claims Experience on Cyber Insurance Policies



Source: Primary Data

The frequency of 64.8% suggests that claims are beginning to increase in financial institutions.

Lack of cyber claims data is also due to reluctance of victims to report incidents
The above topic was also presented to establish the reasons why insurance brokers do not have adequate loss history on cyber claims. The table below details the results obtained:

Table 4.3.5 Composition of Cyber Insurance Proposers and Claims Data in Zimbabwe

Statement	**Mean**
The bulk of cyber insurance proposers emanates from actual losses that proposers have experienced.	3.37
Because cyber-attacks negatively affect the reputation of an organisation, companies rarely disclose that they have been affected by cyber-attacks.	3.83
Insurers and brokers have little claims experience and data in Zimbabwe with respect to cyber insurance claims.	4.07

Source: Primary Data

From the results above, it can be concluded that the bulk of cyber insurance insureds are because of past losses that have occurred that have brought about the need for cover, unlike motor insurance where insurance brokers advertise to proposers. The mean of 3.83 on non-disclosure of losses can support the conclusion that companies would not want to be in the spotlight for cyber losses as this would damage their reputation and ward off potential customers (Javers:2013). Like other emerging risks, cyber claims data in Zimbabwe is still at its infancy.

Data Presentation and Discussion: Interviews

The researcher interviewed 8 respondents who are all in managerial positions in their organisations. Two respondents who were interviewed were from reinsurance broking firms. Because reinsurance brokers work within the regional and international insurance market, their inclusion was meant to provide more insight as to the risk management and insurance programs

that are being offered outside Zimbabwe. The following results were obtained through the interviews:

Comments on the view that insurance brokers must be knowledgeable with emerging risks such as cyber risk in Zimbabwe

All the respondents agreed with this view, as they indicated that cyber risk is slowly becoming a hot topic due to the high prevalence of card cloning as well as phishing incidents in the country. One interviewee indicated that one of the main roles of insurance brokers is to have expert knowledge about risk, and cyber risk should not be an exception.

Do you think the Zimbabwean insurance broking market is experienced enough to provide advice on cyber risk?

88% of respondents agreed that while the knowledge is there, there is little experience with technical aspects of cyber risk, such as information technology concepts as well as risk management models that fit the Zimbabwean context. All respondents indicated that there is need for industry knowledge through workshops and training programs.

CONCLUSION AND RECOMMENDATIONS

Summary of findings

From the data analysis, the researcher managed to obtain the following findings:

i. Lack of underwriting experience

There is lack of information on the extent to which losses have occurred because of cyberattacks. This makes anticipation more difficult and cyber risk management less accurate. This supports the notion that cyber risk is an emerging risk and data is still scarce, making cyber risk underwriting difficult. (Greenwald:2011).

ii. Cyber Legislation in Zimbabwe

There is no legislation available locally to deal with cybercriminals, and this makes it difficult for insurance brokers to advise clients on any legal steps they should take following a loss. There is also no cyber legislation that mandates companies to have minimum cybersecurity standards to protect members of the public.

Cyber insurance solutions being provided by short term insurance brokers in Zimbabwe and their effectiveness

i. No room for product design
Generic insurance policies are being offered in the local market, usually offering blanket perils of cover. There is no room for insurance brokers to design specialised coverage to suit the actual risk on the ground because the local insurers front the policies wholly to regional and international reinsurers.

ii. Policy coverage and availability
Insurance cover for card cloning is excluded in most cyber insurance policies, and one would need to take out a separate card cloning policy for cover to be awarded.

iii. Underwriting considerations
The underwriting considerations are cumbersome and proposal forms are difficult to understand for proposers.

iv. Premium for cyber insurance
The premium is on the higher side and the policy often comes with high deductibles. One of the reasons why premiums are high is because of a long chain of players (i.e. local broker; local insurer; local reinsurer; regional reinsurer; international reinsurer). Policy requirements for certifications also increase the total cost to the cover. This leaves brokers with no room for price bargaining.

v. Technical expertise for insurance brokers in Zimbabwe
Although cyber insurance policies are fronted, insurance brokers lack technical expertise to effectively negotiate as well as design specialised policies for their clients.

Conclusion

The research conclude that there are very few data with regards to cyber risk and insurance because it is still an emerging risk worldwide, although some countries were ahead of others in terms of mitigating cyber attacks. The researcher also noted that the current cyber insurance product being offered in Zimbabwe was too broad and too standardised for the risks that were being experienced in the market as all risks were being fronted to regional and international

(re)insurers. This resulted in insurance brokers not being able to provide cyber insurance that related to the risk exposure of each client.

Recommendations

The researcher gathered the following recommendations which could be implemented to enhance the cyber risk management and insurance solutions currently being offered by insurance brokers in Zimbabwe:

Recommendations to insurance brokers

i. Technical Partnerships
Insurance brokers must engage in technical partnerships so that they can learn from international insurance markets and find methods of adapting international cyber risk management concepts to local needs. This also improves bargaining power of insurance brokers so that they can design cyber insurance policies that speak to the actual risk of their clients.

ii. Training and Education
Because cyber risk involves ICT expertise, insurance brokers must invest in training and education for their staff so that they are well equipped to provide technical advice. This also reduces overreliance on insurers.

iii. Price reduction through technical partnerships
Technical partnerships may also reduce the pricing of cyber insurance through reducing the chain of insurance. For instance, a broker may place their cyber insurance policies with Zimnat Lion Insurance, who already have a technical partner Sanlam in South Africa.

iv. Creation of database
Insurance brokers must also create a database of cyber losses so that the industry becomes more experienced with cyber losses.

Recommendations to insurance regulatory bodies

i. Lobbying for Cyber Act
IBAZ and IPEC must lobby for a cyber act which includes minimum cyber risk management frameworks for companies, as well as penalties for cybercriminals which

include incarceration. This will reduce the cybercrimes currently being faced in the country, thereby protecting the members of the public.

ii. Training and Education
The Insurance Institute of Zimbabwe (IIZ) must provide ICT courses as well as training workshops on cyber risk so that insurance brokers are equipped with more expertise on the subject.

REFERENCES

Text Books

Andam, Z. R. (2003) E-Commerce and Business: UNDP.

Cohen, L., Manion, L. and Morrison, K. (2000) Research Methods in Education, Fifth Edition, Routledge-Falmer-Taylor and Francis Group, New York.

Head, G. L. (2009) Risk Management – Why and How: An Illustrative introduction to risk management for business executives, International Risk Management Institute: Dallas.

Kothari, C. R. (2004) Research Methodology Methods and Techniques, Second Revised Edition, New Age International (P) Limited, Publishers, New Delhi.

Kumar, R. (2011) Research Methodology- A Step-By-Step Guide for Beginners, Third Edition, SAGE Publications Ltd, London.

Journals

Berg, H. (2010) Risk Management: Procedures, Methods and Experiences, Vol 1, pp79-95.

Eling, M. and Schnell, W. (2016) "What do we know about cyber risk and cyber risk insurance?" in the Journal of Risk Finance, Vol. 17, No. 5 pp474-491 [online] https://doi.org/10.1108/JRF-09-2016-0122 accessed on 2 July 2018.

Herzog, S. (2011) Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses, Journal of Strategic Security, Vol 4, No2 [online] http://scholarcommons.usf.edu/jss/vol4/iss2/4 accessed on 6 July 2018.

Lotter, A. and Futcher, L. (2015) "A framework to assist email users in the identification of phishing attacks" in the Journal of Information and Computer Security, Vol. 23, No.4 pp370-381 [online] https://doi.org/10.1108/ICS-102014-0070 accessed on 2 July 2018.

Van Niekerk, B. (2017) "An analysis of cyber -incidents in South Africa" in The African Journal of Information and Communication (AJIC), Vol.20 pp113-132 [online] https://doi.org/10.23962/10539/23573 accessed on 12 July 2018.

Reports and Publications

Institute of Directors in Southern Africa (2009) King Code of Governance for South Africa
Institute of Risk Management (2014) Cyber Risk Resources for Practitioners: London.
Insurance and Pensions Commission (2017) "Short Term (Non-Life) Insurance Report For The Quarter Ended 30 September 2017" [online] http://ipec.co.zw/?page_id=1482 accessed on 20 June 2018.

Marsh and McLennan Group of Companies (2016) Cyber and the city: Making the UK financial and professional services sector more resilient to cyber attack, The City UK: London.

National Association of Corporate Directors (2017) Public Company Governance Survey [online] https://www.nacdonline.org/files/2017–2018%20NACD%20Public%20Company%20Governance%20Survey%20Executive%20Summary.pdf accessed on 2 July 2018.
National Institute of Standards and Technology (2018) "Framework for improving critical infrastructure cybersecurity: Version 1.1" [online] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf accessed on 18 July 2018.

Postal and Telecommunications Regulatory Authority of Zimbabwe (2017) "ABRIDGED POSTAL & TELECOMMUNICATIONS SECTOR PERFORMANCE REPORT: THIRD QUARTER 2017" [online] https://www.techzim.co.zw/zimbabwe-potraz-telecoms-reports/ accessed on 20 June 2018.

Reserve Bank of Zimbabwe (2015) "Cybercrime in Zimbabwe and Globally" [online] http://www.rbz.co.zw/assets/cybercrime-globally-and-in-zimbabwe.pdf accessed on 27 September 2018.

Articles

Amos, S. & Pettifer, A. (2016) "Insuring Cyber Risk: Concerns about Coverage" [online] https://www.actuaries.digital/2016/06/29/insuring-cyber-risk-concerns-about-coverage/ accessed on 7 July 2018.

Bonner, M. (2016) "Is the insurance market hard or soft?" [online] https://www.thebalancesmb.com/is-the-insurance-market-hard-or-soft-462561 accessed on 25 June 2018.

Bortnik, S. (2013) "Five interesting facts about the Morris worm (for its 25th anniversary)" [online] https://www.welivesecurity.com/2013/11/06/five-interesting-facts-about-the-morris-worm-for-its-25th-anniversary/ accessed on 5 July 2018.

Cherry, K. (2018) "Sample Types and Sampling Errors in Research" [online] https://www.verywellmind.com/what-is-a-sample-2795877 accessed on 24 July 2018.

Etsebeth, V. (2007) "Malware: the new legal risk", The Electronic Library, Vol. 25 Issue: 5, pp.534-542 [online] https://doi.org/10.1108/02640470710829523 accessed on 2 July 2018.

Fischer, E. A. (2014) "Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation" [online] https://fas.org/sgp/crs/natsec/R42114.pdf accessed on 5 July 2018.

Gonzalez, G. (2018) "Medical devices open Pandora's box of cyber risks" [online] https://www.businessinsurance.com/article/20181009/NEWS06/912324484/Medical-devices-cyber-security-internet-of-things-cyber-risks accessed on 10 October 2018.

Graham, A. (2017) "What is the ISO 27000 series of standards?" [online] https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards/ accessed on 12 July 2018.

Greenwald, J. (2011) "Lack of data hinders cyber risk management, underwriting" [online] https://www.businessinsurance.com/article/99999999/news070101/399999946/lack-of-data-hinders-cyber-risk-management-underwriting accessed on 7 October 2018.

Hoffman, C. (2016) "What is the dark web?" [online] https://www.howtogeek.com/275875/what-is-the-dark-web/ accessed on 20 July 2018.

Javers, E. (2013) "Cyberattacks: Why Companies Keep Quiet" [online] https://www.google.com/amp/s/www.cnbc.com/amp/id/100491610 accessed on 29 September 2018.

LeClair, J. and Keeley, G. (2015) "Cybersecurity in our digital lives" [online] http://hudsonwhitman.com/books/cybersecurity-in-our-digital-lives/ accessed on 25 June 2018.

Lloyds (2017) "Closing the gap - Insuring your business against evolving cyber threats" [online] https://www.lloyds.com/about-lloyds/what-lloyds-insures/cyber/cyber-risk-insight/closing-the-gap accessed on 24 July 2018.

Mccoy, K. (2017) "Target to pay $18.5M for 2013 data breach that affected 41 million consumers" [online] https://www.google.com/amp/s/amp.usatoday.com/amp/102063932 accessed on 20 July 2018.

Newsday Zimbabwe (19 June 2018) "CCTV sells out suspected thieves".

Peterson, A. (2014) "The Sony Pictures hack explained" [online] https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.fc46beeedd63 accessed on 14 July 2018.

Price, N. (2018) "How to build a cybersecurity risk management framework" [online] https://www.boardeffect.com/blog/cybersecurity-risk-management-framework/ accessed on 22 July 2018.

Robinson, E. (2012) "What are computer viruses?" [online] https://blog.productcentral.aol.com/2012/08/14/what-are-computer-viruses?guccounter=1 accessed on 02 July 2018.

Robinson, R. M. (2016) "The growing threat of cyber extortion" [online] https://securityintelligence.com/the-growing-threat-of-cyber-extortion/ accessed on 14 July 2018.

Symanovich, S. (2017) "What is a data breach?" [online] https://www.lifelock.com/education/data_breaches_need_to_know/ accessed on 02 July 2018.

Signe, L. and Signe, K. (2018) "Cybersecurity in Africa: Securing businesses with a local approach with global standards" [online] www.brookings.edu/blog/africa-in-focus/2018/06/04/cybersecurity-in-africa-securing-businesses-with-a-local-approach-with-global-standards/amp/ accessed on 18 September 2018.

The Oxford Dictionary of Statistical Terms (2003) "Non Response Rate" [online] https://stats.oecd.org/glossary/detail.asp?ID=3765 accessed on 12 September 2018.

Old Mutual Insurance Wording Assets Policy

Ward, C. (2016) "The UK's Cybersecurity Regulatory Landscape: An Overview" [online] https://www.hldataprotection.com/2016/12/articles/international-eu-privacy/the-uks-cybersecurity-regulatory-landscape-an-overview/ accessed on 15 July 2018.