CYBER RISK AND CYBER INSURANCE

Suraj Eswaran
Colorado State University
Fort Collins,Colorado
suraj22@colostate.edu

Prof. Yashwant K. Malaiya
Colorado State University
Fort Collins,Colorado
malaiya@cs.colostate.edu

***Abstract*—Cyber risk is a form of risk from the exposure resulting from a cyber-attack or data breach. Organizations tend to become more vulnerable to these kinds of threats due to their high reliability on computers, networks, and information in order to get along with the delivery of the services.A failure on these system will create negative impact on the processes which is not good for any organization as very few of them know that their system has been hacked.It is necessary to showcase how cyber risk is dangerous and role of cyber insurance in business organizations.Thus,this paper deals with the visualization of various views on cyber risk and its challenges that arises in insurance markets in the recent years.**

***Index Terms*—Cyber risk, Cyber risk Insurance, Risk avoidance,insurance premium,Cyber security.**

I. Introduction

Companies spend millions of dollars on security factors like firewall, anti-virus and IDS(Intrusion Detection Systems) in order to reduce security breaches from hackers.They utilize techniques like digital signature and encryption to maintain confidentiality and integrity. Cyber risk refers as any form of risk of financial crisis, damage to the organization's reputation resulting in failure of its information systems [1].For example,hackers get into organization's database for accessing the confidential information by exploiting security level vulnerabilities.An Anonymous group have caused a loss of $50,000 on Symantec Software in the year 2012 [2].Thus,cyber risk disasters could create a large impact on organizations loss towards opportunity cost.Organizations tend to be more reliable on computers, networks and information for maintain a good relationship with the customer service. In order to protect against these risk, many businesses have cyber insurance with their insurance policy. Cyber insurance is a financial policy which allows the businesses to send them funds which involves in recovery from cyber risk events.It helps in reducing financial losses of organization using payment if the premium to the insurer. The reasons for the insurance company covering the cyber risk are:

- If the confidential information has been mishandled, the standard policy would not help in restoring them.A cyber policy help in providing a coverage in recovering data with policy limits.Nearly, 2 billion records were stolen in data breaches in 2017 which costs about $225 per records [2].
- Cyber criminals tend to attack small companies as they do it for larger companies.49 percent of targets are businesses under $500 annually, according to cyber study. This is due to the fact that there are expected vulnerabilities in the case of small companies as compared to larger companies.Hackers would consider smaller companies have fewer protections as they invest less money for security aspects.Thus,cyber insurance would help in these situation regardless of company size.

Organizations know how to witness cyber risk and its consequences.But there is not any evidence of how to deal those situations and regulations in utilizing the cyber insurance.Main motive of evaluating cyber risk is to show dangerous in the present world using some statistics from previous years and analysing it with the present scenarios. Organizations maintain the cyber insurance in order to protect from the consequences, but none of the empirical studies fail to record how these regulations are functioning. Thus, it is necessary to analyse on the perspective of severity of cyber risk and regulations involved in it.This work mainly explains in detail on steps taken in detecting a risk , with its severity,role of cyber insurance with their regulations and challenges in imposing these regulations.

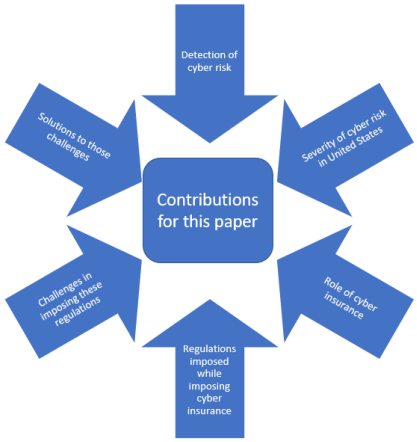

Fig. 1. Contributions and Concepts exist in this report

List of research questions were listed during this analysis:

- RQ1: How dangerous is Cyber Risk?
- RQ2: What were the several ways in handling Cyber–Risk by Insurers?

- RQ3: What are the challenges faced in insurance markets in the recent years?

Remaining paper is organized as followed: Section 2 deals with discussion of background literature as they are categorized based on modelling cyber risk and methodologies to control it with the help of cyber insurance. Section 3 involves description of findings regarding cyber risk which explains the results while performing the empirical study and section 4 concludes the study with some future enhancements and threats to validity and final section shows the references utilized for this study.

II. Related Work

Analysis and Modelling of Cyber Risk

According to Inversion Model Expert System, there has been a shift from manual to automation which tend to change from external risk to internal risks. The external threats are related to process whereas internal threats with information. From this, several aspects has been proposed in creating models with various scenarios. Kokolakis et.al [4] have utilized IT risk with the help of BPM(Business Process Modeling) which is a method of controlling the process in a phase of crisis. This approach relies on the mixture of risk analysis with business procedure , thus support Information Security Analysis and Design. Pernul et al. [5] have focused on developing a secured business process based on security requirements.
Similar work was proposed by Roehrig et al. [6] and Ribeiro et al. [7] where they proposed it against security policies. Halliday et al. [8] conducted risk analysis with high level business strategy. Whereas Rodriguez et. al. [8] elaborated the analysis of Business Process Modelling Notation with security requirements. Furthermore, there were few more analysis where they have also utilized Business Process Model, like Suh and Han [10] and Rainer et al. [11] where they have proposed at various scenarios.

Controlling the risk using Cyber Insurance

Cyber Insurance depends on the organization's exposure to cyber risk and data breaches. The market for insuring against these has been grown rapidly in the past decade. Cyber insurance has been the term utilizes first and third-party losses that results in loss due to system-based attack. Several approaches have provided an excellent elaboration of cyber insurance. Böhme and Schwartz [12] defined a unified model for cyber insurance with some structural details of the business protocol.In addition to theoretical model, Marotta et al. [13]compared various approaches of cyber insurance market and direction towards further advances in cyber insurance. Majuca et. al. [14] describes evolution of cyber insurance in 2005 which focusses on analysis of market with discussion of several problems. Woods et al. [15] determines insurance carriers by examining 14 questionnaires.
Romanosky et al. examined over recent top 100 cyber insurance policies with state insurance policies [16]. It is very difficult to find businesses without cyber insurance pricing in order to store sensitive information. Cyber Criminals will target large organization so that they can take away more money with lot of damages. Thus, it is necessary to focus on the pricing aspect of cyber insurance. Mukhopadhyay et. al. [17] developed Utility Based Preferential Pricing(UBPP) in order to help the organization, decide on the pricing aspect of cyber insurance products. Similarly, Hemantha and Tejaswini [18] utilized a scheme called Copula-based cyber-insurance model (CBCI) where they fitted a copula to the empirical values and computed the expected value. But, Ulrik Franke [19] documented the empirical study pf cyber insurance market in Sweden with 10 different insurance companies and provided an analysis for average pricing of cyber insurance.

III. Objectives

The main objectives involved in this survey paper involves:

- Providing a statistical proof of how severe is cyber risk
- Present the regulations imposed on cyber insurance by the organization as well as insurance perspective.
- To know how challenging it is while imposing regulations within the company

IV. Description of Findings

When organizations approach cyber risk,it is necessary to the kind of the cyber risk and steps to handle it.There are two different kinds of cyber risk. They are:

- Malicious cyber risk: If a cyber risk caused due to malicious attacks, then it is called malicious cyber risk. For example: Cause of unauthorized leakage data by the hackers is an example of malicious cyber risk.
- Non-Malicious cyber risk: If a cyber risk caused due to accidental attacks, then it is called non-malicious cyber risk. For example:Cause of unauthorized leakage data due to accidental usage of links or websites are an example of non-malicious cyber risk.

There are cases where both malicious and non malicious happens. Instances where systems has been affected due to intrusion when Intrusion Detection System(IDS) and Intrusion Prevention System(IPS) is down because of accidental loss.In figure 1, cyber risk is a combination of both malicious and non malicious.Thus, the intersection between them shows that any events can cause due to both malicious and non-malicious.

Based on the existing studies, there are five main factors for developing cyber risk management.For maintaining an efficient and relative cyber risk management, it is necessary to have a proper evaluation and risk control.

- Risk Identification: Identification shows the vulnerabilities due to cyber risk which causes the consequences for assets due to breaches. With regards to this, the organization need to find out risk control measures. For that, they utilize either top-down or bottom-up technique. Top-down points out the main threats from the strategic point of view whereas bottom-up tends to be featuring detailed evaluation of threats. It is advisable to utilize bottom-up technique as top-down might not identify few risks which creates correlation. Risk identification is conducted with

Fig. 2. Different kinds of risk

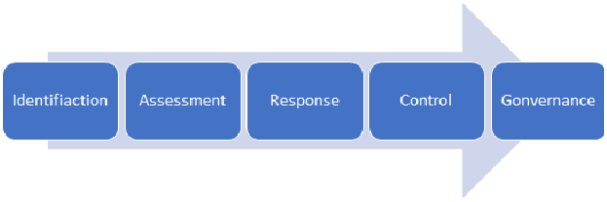

Fig. 3. Factors involving Risk Management

With higher sensitive information and information system, the implementation of organization based cyber risk management with proper response level is necessary. From the above discussion we can infer that proper IT security requirements as well as insurance policy coverage can lower the risk exposure or even loss. Organization that depend on Internet services or cloud services should look over their risk positions, in the case of crashes of website, there will be a drop in the incomes which tend to allow customers to go for different products. There will be reduction in the market value if the situation of log term cyber risk occurrence.Thus, it is necessary for an organization to get along with cyber risk management with assessment,evaluation, and improvement.Risk awareness has to be helpful in providing a good risk management system for the organization.

Fig. 4. Implemented Model for Cyber Insurance Market

the help of questionnaires regarding business activities or network security. In the case of complex risks, insurance companies utilize technical handwriting.

- Risk Assessment: The organization need to expose the risk and check whether it can be assessed or not which includes estimation of loss due to cyber risk and assessment of risk level. Along with that, the amount of long-term profit loss share will be calculated which share the majority of share in cyber risk loss.
- Risk Response:Response involves three methods to measure the response of the risk. They are avoidance, mitigation, and acceptance, which shows amount loss from the incident.
  - Avoidance: It involves elimination of activities and exposures which affects the organization.
  - Mitigation: A strategy which is utilized for reducing the adverse effects due to the cyber risks.
  - Acceptance: It is a process of choosing the option depending on the user agreed level of appropriate cyber risk.
- Control: After the identification, evaluation and processing of cyber risk , the next step would be controlling of risk. Organization need to regularly monitor their risk and improve these factors.
- Governance: Governance is needed in order to finish a complete cyber risk risk management. It focuses on organization's culture and develops awareness within all the employees, thus provides instructions on IT security.

A. RQ1: HOW DANGEROUS IS CYBER RISK?

Cyber risk has been serious issue with increase in virtual interactions during the pandemic. Due to this, there has been an increase in surface for the attacker which doubted the organization's integrity, confidentiality, and availability factors in year 2020. From various sources we can infer various facets of cyber risk.

- According to Gartner Research, there will be an increase of global information security market in the year 2022, to a range of 170.4 billion dollars [17].
- According to Symantec, one out of 36 mobile devices tend to have high risk application and one out of 13 web request causes malware [18].
- Average cost of cyber crime tend to be 14.7 million dollars which is 68 more than what we obtained in the year 2019 [19].
- Cyber risk of 2020 includes new and insecure usage of software because after the transaction from office to home there has been a high usage of new software in order to reduce the distance between the customer and consumers. But it does not guarantee that these software are secure enough and implementation of these software.
- Beginning of the corona pandemic,cyber criminals utilized this situation, and it has been reported that there were thousands of scams and malicious websites created every day which results in phishing of data.
- Processing of these sensitive data would be one of the biggest risks in 2020.

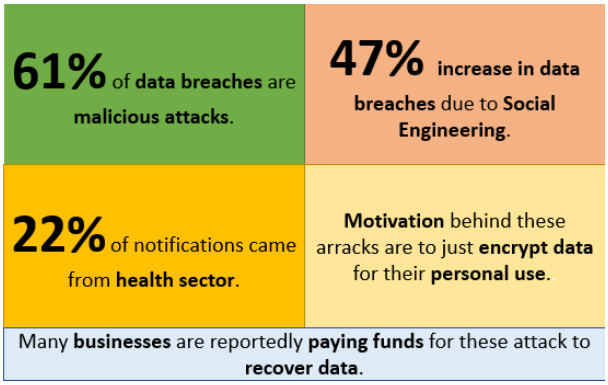

Fig. 5. Recent stats on Cyber risk-I

According to National Law Review, there has been a fact that 61 percent of the 518 total data breaches have happened due to malicious attacks,resulting in phishing, ransomware and spear phishing [23].Social engineering is an inappropriate manner of manipulation of people into performing illegal actions for handling a confidential data.So far there has been 47 percent increase in data breaches due to social engineering [24].Surprisingly, 22 percent of breaches came from health sector as patient health records can be sold about 363 dollars on the black market which is more than any piece of information from other industries [25].According to U.S Bureau of Labor Statistics,there has been report saying that 32 percent of businesses have experienced cyber attacks at least once a week [26]. Average amount of cyber attacks of businesses of all sizes is about 3846.48 dollars as compared to the previous years of about 3256.10 dollars. While average amount of cyber attacks of businesses of medium and large sizes is about 6216.34 dollars which shows lots of damages have happened in large and medium organization, which has been the limelight for hackers and cyber criminals [27]. It has evident that the potential for the cyber crime to overlap has been considerable. That is why it was termed as Internet Fraud Complaint Center(IFCC), later was renamed as IC3 for distinguishing internet fraud from cyber crime.

DATASET

For this research question, I have collected the data from Internet Crime Complain Center(IC3) [28] where its mission is to provide the public a clear view on the cyber risk and submit information to the Federal Bureau of Investigation (FBI) for any hazardous events across United States. From 2000, IC3 have been receiving lots of complains regarding cyber crimes with respect to computer intrusions economic theft and data breaches

METRICS

For this study, I have used two following metrics in order to answer the research questions.The metrics involves number of victims and victims loss amount. All these metrics are been recorded from IC3 report from 2016 to 2019.

Fig. 6. Internet Crime Complaint Center- IC3

- Number Of Victims: It is defined as number of people or organizations who have been suffering from injurious actions due to cyber criminals.
- Victim Loss Amount:It is defined as total loss that has happened due to the cyber risk.

STATE WISE SEVERITY MEASURE

Table 1 shows how different states have been affected from year 2019 to 2016 in United States of America. For four years, we can witness states like California, Texas, Florida seems to be affected the most due to internet crimes like business email compromise and other scams.From 2019 FBI data, it was evident that about $2 billion was stolen from the victims using business email attacks. After examining the data by FBI, researchers have found that Washington, California, and Ohio have become the centers for internet crimes from 2016.A team lead by Dr. Michael Crain, director of FAU's Center for Forensic Accounting, expressed that fraudsters are being more efficient at going after where the money is [29]. California tends to be listing the most affected state due to business crime and other scams. There has been an increase of 27 percent of financial loss in California from 2018 to 2019, which is about 573.9 million dollars.
Florida has been recorded the second most affected state over the past five years. Surprisingly, the average amount of loss funds has been increased from 4,700 dollars to 10,800 dollars in a span of five years.
Comparing California and Florida, Texas and Ohio has been producing the highest loss ratio even though they are less affected states.From IC3, Ohio businesses have been losing $22.6 million per hundred organizations which shows a steep increase of about $9 million.

States	2019	2018	2017	2016
Alabama	4108	4585	3865	3726
Alaska	1451	1603	1418	1259
Arizona	7795	8027	6417	6349
California	50132	49031	41974	39547
Colorado	9689	9328	7909	6847
Delaware	1062	897	759	703
Florida	27178	23984	21887	21068
Georgia	9074	9095	7007	6697
Hawaii	1396	1100	1923	6697
Idaho	1485	1513	1186	1120
Iowa	5094	1983	1533	1560
Kansas	1970	2098	1767	1923
Kentucky	3083	2813	2740	2621
Louisiana	3804	3469	3319	3002
Maine	880	832	740	770
Maryland	11709	8777	6789	8361
Massachusetts	1654	6173	5221	4888
Michigan	8249	7533	6400	6384
Minnesota	4388	4304	3619	3390
Mississippi	1654	1882	1799	1467
Missouri	5083	5508	4187	4096
Montana	967	787	737	744
Nebraska	1350	1205	1140	1028
Nevada	6831	5228	4675	4096
New Hampshire	1155	1056	1106	1126
New Jersey	9067	8440	7657	6690
New Mexico	2037	2127	1415	1702
New York	21371	18124	17662	16426
North Carolina	8223	7523	7316	6492
North Dakota	489	459	355	350
Ohio	9321	7812	8157	7052
Oklahoma	2997	2644	2809	2455
Oregon	4813	4511	3455	3947
Pennsylvania	10914	10554	11348	8265
Rhode Island	1011	1028	704	663
South Carolina	4541	3575	3687	3500
South Dakota	473	465	404	376
Tennessee	5586	5584	4779	4693
Texas	27178	25589	21852	21441
Utah	3034	3041	2260	2295
Vermont	500	525	451	440
Virginia	11674	14800	9436	8068
Washington	13095	10775	7505	6874
West Virginia	1227	1109	1085	1153
Wisconsin	6378	6621	5245	3662
Wyoming	550	497	434	432

TABLE I
NUMBER OF VICTIMS AFFECTED ACCORDING TO US STATES

While in 2018, there has been increased 32 percent within first three months in most of the states which shows there has been increase in data breaches in most of the organizations.

From the fig 8, there seems to be a similar trends even though California, Florida and Ohio have been the most affected states where that was the time where the beginning of Information Technology field has started.

Incapability of cyber authorities to catch these cyber criminals may be the reason for non mitigating in the growth of online cyber crime. As Dr. Michael Crain expressed his disappointment as it would be impossible If the cyber authorities cannot get the criminals or else they will be doing it. As years passed by,the number of victims and their loss tend to be high in states like Washington, Colorado, Illinois Georgia have some mixed trends.

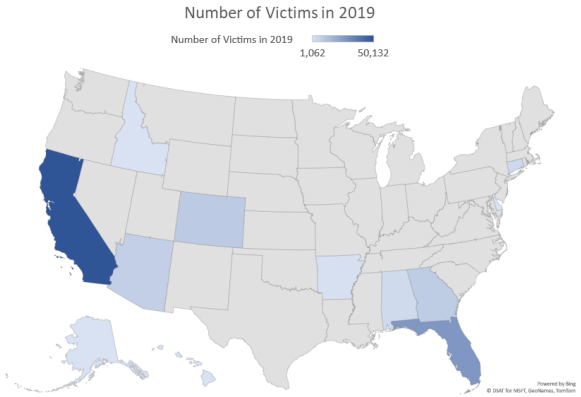

Fig. 7. Cyber risk at 2019

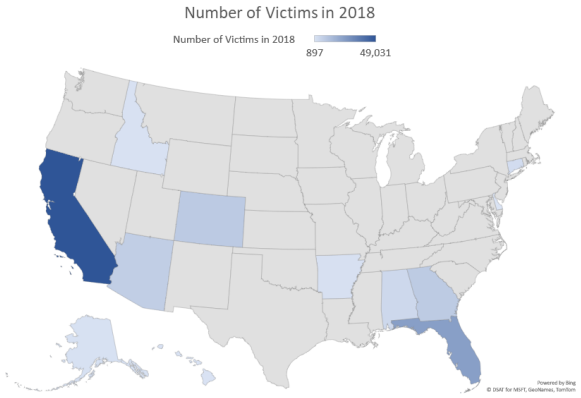

Fig. 8. Cyber risk at 2018

THREAT WISE SEVERITY MEASURE

Cyber risk authorities tend to protect these cyber threats which are caused due to various groups like corporate spies, terrorist groups , criminal organization, hacktivists and cyber criminals.Thus I have categorized list of nine fraud events that are occurring in an organizations. They are:

- Business Fraud: Business Fraud happens when a corporation falsely project themselves as a truth and dealing with illegal material fact like bankruptcy fraud and false copyrights.
- Government Fraud:Government fraud is also projecting falsely in order to project the government to its own disservice like tax evasion, welfare fraud.
- Investment Fraud: It involves the use of capital in order to create more money using income producing properties for resulting in capital gains, thus resulting in failure.
- Confidence Fraud: Confidence Fraud happens when individual or groups provide a relational trust resulting in financial loss or property loss.
- Auction Fraud: It is same as confidence fraud but does some nuisances like non-delivery of payment or illegal merchandise.

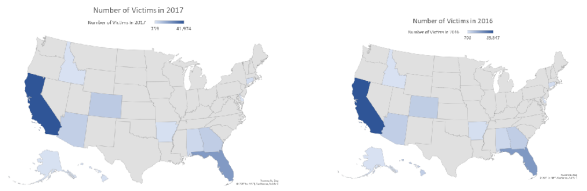

Fig. 9. Cyber risk at 2017 and 2016

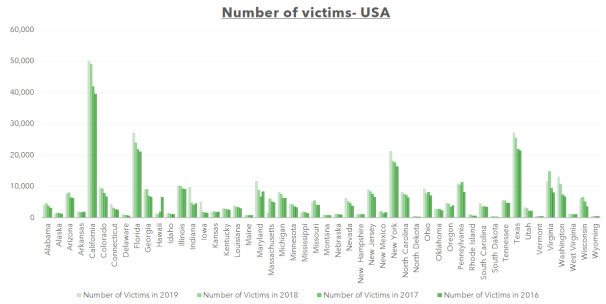

Fig. 10. Number of victims affected from 2016 to 2019

- Credit and Debit Card Fraud: Usage of credit or debit card illegally for various purposes which results in debt.
- Technology Fraud: It involves frauds due to usage of technology. According to Office of Special Investigation, technologies are utilized as a mechanism to mishandle data with the help of phishing, spear phishing and malware tactics.
- Check Fraud: Check fraud involves usage of cheques on a closed account or accounts which has insufficient funds.

I have summarized list of cyber events from 2019 to 2016 with the help of Internet Crime Complaint Center(IC3) in table 2. From the reports, there were lots of technology frauds as the dependency of computers and information system. As the dependency increases, more confidential information would exist which excites the cyber criminals to damage those system.Hence, it is necessary for organization to look over several aspects of securing data which would minimize the loss rate.

Types	2019	2018	2017	2016
Utility Fraud	1307	1394	1445	979
Government Fraud	13873	10978	9149	12344
Investment Fraud	3999	3693	3089	2197
Business Fraud	23775	20373	15690	12005
Confidence Fraud	19473	18493	15372	14546
Auction Fraud	10842	10826	10949	9619
Credit/Debit Card Fraud	14378	15210	15220	15895
Technology Fraud	114702	106379	105344	109465

TABLE II
NUMBER OF VICTIMS AFFECTED ACCORDING TO CYBER THREATS

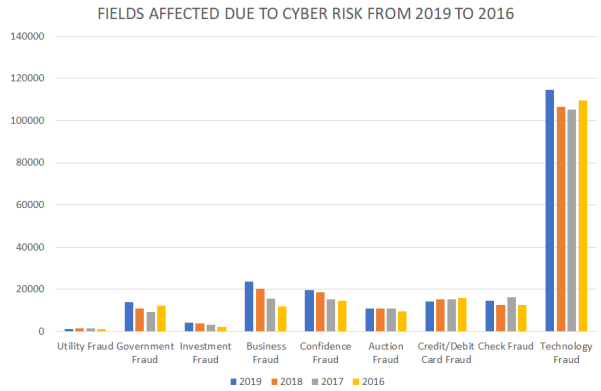

Fig. 11. Fields affected due to cyber risk from 2019 to 2016

B. RQ2:What were the several regulations in handling Cyber Risk by Insurers?

Cyber Risk Insurance is developed in such a way to reduce the losses from various cyber incidents like data breaches, or network interruptions.In order to provide a robust cyber risk insurance, it is necessary to follow:

- A method for improving the usage of preventative measures for more coverage.
- Usage of best practices by premiums in the insurer's perspective.

But the doubt arises when there is an irregularity in handling in cyber risk situations. Many companies work under the forgoing policies, which lack in efficiency of cyber-risk insurance. Based on risk loss and risk management, there are few regulations that were imposed in order to handle cyber events. Coverage includes 1st party coverage,liability coverage and other benefits includes security-audit, post- incident and criminal rewards.From a survey, annual premiums for cyber risk insurance in United States ranges from $1.5 billion to $2.5 billion [30].Thus,there is a fledgling market compared with others streamlines of insurance business.For this research,I have categorized two different approaches in order to show how regulations are imposed in various fields.

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL

FFIEC was established in March 1979, which became an act of financial institutions,reform, recovery and enforcement in 1989 for establishing an appraisal subcommittee.It is utilized as a formal inter-agency body for prescribing an uniform principles,standards and forms for financial institutions by 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) [31]. The main guidelines they follow is to provide a proper risk management framework for Internet based products to customers.The guidelines follows both retails as well as commercial businesses.

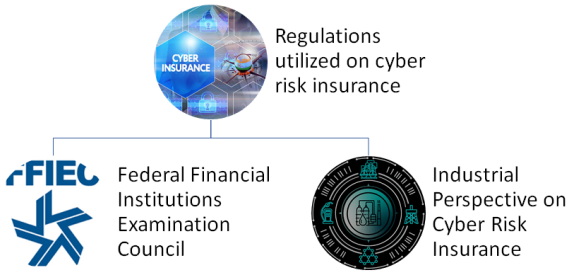

Fig. 12. Different categories of cyber insurance perspective

In 2018, FFIEC members have elaborated a joint statement in order to help financial institutions look over risk factors management and methods in considering cyber insurance policies [31].The joint statement mentioned:

- Cyber attacks are increasing exponentially and traditional general coverage may not provide the necessary effective coverage against cyber events.
- Cyber insurance may reduce financial loss that have caused due to data breaches.
- Cyber insurance may be a resource for extending risk management strategy.

It is always necessary for organizations to know the differences first-party and third party coverage and type of coverage needed for the organization. First part involves expenses like business interruption, cyber extortion and event management. Third part mentions claims regarding customers or suppliers who are facing cyber risk incident. Since cyber insurance is an upcoming field, there would be differences in methodology and other elements can change between suppliers.Secondly, cyber insurance only helps in financial risk while it is not an strategy involving risk management. Thus, the organization have to take a measure to figure out the risk management requirements in order to stick with coverage and potential payout.According to FFIEC, risk exposure changes when there will be a need for cyber insurance. So cyber insurance is not a single product that satisfies all the needs for the organization's loss [31].Every company have to work on the risk assessment when looking over cyber insurance.

But in the case of commercial banking wire transfer, it is necessary to follow layered security protocols. The concept is to provide approaches which may enhance overall security of internet-based products [31] and services. FFIEC delivers several categories for effective controls in a layered security program:

- Fraud detection and surveillance system for effective institution responses.
- Dual Customer Authorization in order to allow small business banking customers to look over certain transactions which involves second user's credentials.
- Utilization of internet protocol reputation tools for blocking those events which are tend to be fraud and forgery.
- Awareness of fraud risk and measures to deal the situation.

Industrial Perspective on Cyber Risk Insurance Regulations

There has been several industries who provides practical risk management with cyber insurance regulations. One such group named RSA helps in enabling organizations to flourish in an high risky atmosphere with some latest cyber security information. They tend to claim that a research firm Gartner has provided a result saying 700 million personal data were stolen which is about 3.5 million dollars per incident. Surprisingly, only 30 percent of the organization knows that their systems has been hacked.RSA mentioned in their report a term named GAP [32] which explained an approach to assess, diagnose vulnerabilities between IT fields and security fields.In that report,they have pointed out that risk managers and senior executives are not interested to specify the kind to attack and vulnerability according to perspective of IT fields whereas IT team and security team do not focus on type of cyber breach that leads to high loss impacts. They implied after an arguments with several organizations regarding preventative tools like:

- Signature based tools like firewall,Intrusion Detection System/Intrusion Prevention System
- Addition of several security protocols which deals with methods like Public Key Infrastructure or multi-factor authentications.

On the other hand, National Association of Insurance Commissioners(NAIC) have listed few task force in order to place regulatory framework by completing few important projects between 2015 and 2016 [33].

First project in 2015 was set up in such a way that principles would be helpful in serving the insurance regulators overall strategy in the case of cyber risk.The main motive was to protect sensitive customer details and create a protection efforts to be scaled according to the regulated entry's size and capacity.

Second project in 2015 was examined by the financial examiners to enhance data security analysis when insurance companies undergoes any sought of financial examination. Financial exam must take place at least once every five years as there would be change in schemes as per Industrial Perspective on Cyber Risk Insurance Regulations.

Third project in 2015 deals with collecting and analyzing of data regarding cyber insurance market.Many insurance companies now sell cyber insurance product to American organizations. So, insurance regulators gather information in order to understand dynamics of the market. In order to complete the third project,insurance regulators follows Cyber Insurance Coverage Supplement with annual financial statement.

Final project in 2015 involves development of road map for cyber customer protections. Road map includes rights to show

what type of personal information being collected and stored in the data base, rights to get privacy policy by the insurer,rights to receive notification within 60 days while occurring a data breach and rights to receive one year of identify protection paid by the insurers. NAIC Cyber Task Force drafted a formal cyber security model law in order to establish moderate standards for data security,investigation of the data breaches which are applicable to all insurance policies.The model law allows policies for holding their information security scheme depending on the size, complexity and scope of the events with sensitivity of customer information to be protected.

C. RQ3: What are the challenges faced in these regulations?

Regulations are needed for cyber insurance in order to keep the operations run smoothly.But there are situations where regulations itself has been an issue while purchasing with cyber insurance policies. For instance, insurance companies that are focused towards cloud services and agile development, are showing new kind of risks into the organization which may not perfectly fit existing insurance's control models and audit procedures.Traditional controls needs to get adjusted with the fast-moving agile environment which can be more complicated. Thus, my research question is based on the challenges that are faces while following these regulations by the organizations. The challenges are:

- Reactionary strategies are not designed well with affected process of the business. Insurance which follow cloud storage might not work with the traditional policies.
- According to a survey paper by Gurpreet Dhllion,about 65 percent of organizations do not follow a formal method to collect and analyze data regarding cyber insurance market [34].
- Business developments are involved outside the IT sphere which only allows to see in loss point of view rather than the information point of view. For example, any risk loss happens due to any malicious event, the IT team would look over threat perspective rather than loss rate because they focus on dealing the recovery part and not on whether the company has the sufficient funds to support.Thus, 95 percent of cyber risk happens due to misinterpretations by business team and IT team. If it continues like this, then by the year 2022, there can be huge loss of $140 billion in working on this collaboration itself.

To overcome those challenges, organizations must look over interests of both the groups by looking over business initiatives with respect to security strategies.It has to be assessed in order to ensure all the critical processes are recognized and aligned properly to security. It is also necessary to be proactive while handling cyber risk activities.Being proactive includes identifying security weaknesses and providing the necessary processes in order to identifying the threat.Proactive security tactics involves:

- Threat hunting:It is a process of searching threat through network and isolate threats in order to protect the systems.
- Staff training:Most of cyber attacks are due to human vulnerabilities due to leakage of staff credentials. Therefore,it is necessary to train all the staffs regarding securtiy precautions.
- Proactive Networking and Monitoring: It is necessary to monitor your network 24/7 for providing an instant response to the team so that they can analyse the situation.
- Ethical hacking: Google believes that ethical hacking can be a potential method for threat hunting. It can help in identifying network's weak point and perform actual with an intention of helping the company.

V. Threat to Validity

As Internet Crime Complaint Center(IC3) submits the 2020 cyber risk report at the end of the year,hence it is not possible to accurately provide data from the present scenarios. Even though, with the help of Forecast Model,it is possible to predict the present scenarios but the accuracy rate is very less.Due to less rate of accuracy,it might not be a reliable method. Along with that, there has been an increase in reliability on computer systems due to Covid-19 as some of the work have been converted to remote.So there are high possibility that hackers and cybercriminals would exploit those systems. With those information from IC3,it is possible to visualize how dangerous cyber risk has been since the development of Information Technology.

VI. Conclusion

This paper covers analysis of cyber risk and its severity in United States.For this study, I have utilized data set from Internet Crime Complaint Center(IC3) with the metrics risk loss and number of victims affected. States like California, Florida and Ohio are been mostly affected as there are hubs for Information Systems. Due to the reliability on computers, there has been spiking value in the case of technology fraud. In order to avoid those risk, it is necessary for states like California to take serious step on protecting the systems. For that companies have been exercising cyber risk insurance.
Cyber Insurance is a way of providing financial aids to businesses in order to help them in recovery. A robust cyber risk insurance requires usage of preventative measures for delivering coverage and best practices by premiums on insurer's level of self protection.It is considered as a "stand alone" line of coverage as it involves first party coverage, liability coverage and other benefits includes security-audit,and criminal rewards.Due to this, there has been an increase of 15 percent in annual gross premiums within a year.Thus, it is necessary to follow few regulations while purchasing a cyber insurance. Federal Financial Institutions Examination Council follows a guidelines so that they provide a risk management framework for Internet based products to customers.A group named RSA mentioed a GAP which elaborates an approach to diagnose vulnerabilities between IT fields and security fields.They have criticized saying that risk managers and senior executives are not interested to specify the kind to attack and vulnerability according to perspective of IT fields. Due to

this misunderstanding, about 92 percent of cyber risk happen. It can increase upto 140 billion dollars from 100 billion dollars if they do not co operate each other.

Organizations need to look over every aspects of dealing a cyber risk scenario, so that they can at least reduce the loss amount they spent. It is also necessary to be proactive so that they can study the risk and analyse it properly.Educating the employees on the insurance regulations and risk factor so that they can protect their credentials and confidential data.

VII. Future Work

The approach can be elaborated by examining with more features and creating a model in such a way that the organizations can utilize while handling cyber risk.Along with that, usage of IC3 2020 report data and utilising forecast model to identify the trends in 2021 can be successful study on cyber risk severity.

References

[1] Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. "Insurability of cyber risk: An empirical analysis." The Geneva Papers on Risk and Insurance-Issues and Practice 40.1 (2015): 131-158.

[2] Cleary, Gillian, et al. "Symantec internet security threat report." (2018).

[3] Cheng, Long, Fang Liu, and Danfeng Yao. "Enterprise data breach: causes, challenges, prevention, and future directions." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 7.5 (2017): e1211.

[4] Kokolakis, S. A., A. J. Demopoulos, and Evangelos A. Kiountouzis. "The use of business process modelling in information systems security analysis and design." Information Management Computer Security (2000).

[5] Herrmann, Gaby, and Guenther Pernul. "Towards security semantics in workflow management." Proceedings of the Thirty-First Hawaii International Conference on System Sciences. Vol. 7. IEEE, 1998.

[6] Röhrig, Susanne, and Konstantin Knorr. "Security analysis of electronic business processes." Electronic Commerce Research 4.1-2 (2004): 59-81.

[7] Ribeiro, Carlos, and Paulo Guedes. "Verifying workflow processes against organization security policies." Proceedings. IEEE 8th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE'99). IEEE, 1999.

[8] Halliday, Sharon, Karin Badenhorst, and Rossouw Von Solms. "A business approach to effective information technology risk analysis and management." Information Management Computer Security (1996).

[9] Rodríguez, Alfonso, Eduardo Fernández-Medina, and Mario Piattini. "A BPMN extension for the modeling of security requirements in business processes." IEICE transactions on information and systems 90.4 (2007): 745-752.

[10] Suh, Bomil, and Ingoo Han. "The IS risk analysis based on a business model." Information & management 41.2 (2003): 149-158.

[11] Rainer Jr, Rex Kelly, Charles A. Snyder, and Houston H. Carr. "Risk analysis for information technology." Journal of Management information systems 8.1 (1991): 129-147.

[12] Böhme, Rainer, and Galina Schwartz. "Modeling Cyber-Insurance: Towards a Unifying Framework." WEIS. 2010.

[13] Marotta, A., et al. "A survey on cyber-insurance." Technical Rep. IIT TR-17/2015. Istituto di Informatica e Telematica, Consiglio Nazionale delle Richerce, Pisa (2015).

[14] Majuca, Ruperto P., William Yurcik, and Jay P. Kesan. "The evolution of cyberinsurance." arXiv preprint cs/0601020 (2006).

[15] Woods, Daniel, et al. "Mapping the coverage of security controls in cyber insurance proposal forms." Journal of Internet Services and Applications 8.1 (2017): 8.

[16] Romanosky, Sasha, et al. "Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk?." Available at SSRN 2929137 (2017).

[17] Mukhopadhyay, Arunabha, et al. "Cyber-risk decision models: To insure IT or not?." Decision Support Systems 56 (2013): 11-26.

[18] Herath, Hemantha, and Tejaswini Herath. "Copula-based actuarial model for pricing cyber-insurance policies." Insurance markets and companies: analyses and actuarial computations 2.1 (2011): 7-20.

[19] Franke, Ulrik. "The cyber insurance market in Sweden." Computers & Security 68 (2017): 130-144.

[20] Gartner Inc. (n.d.). Forecast Analysis: Information Security, Worldwide, 2Q18 Update. Retrieved November 08, 2020, from https://www.gartner.com/en/documents/3889055

[21] Symantec Security Center. (n.d.). Retrieved November 08, 2020, from https://www.broadcom.com/support/security-center

[22] Böhme, Rainer, and Galina Schwartz. "Modeling Cyber-Insurance: Towards a Unifying Framework." WEIS. 2010.

[23] Aleroud, Ahmed, and Lina Zhou. "Phishing environments, techniques, and countermeasures: A survey." Computers & Security 68 (2017): 160-196.

[24] Workman, Michael. "A test of interventions for security threats from social engineering." Information Management & Computer Security (2008).

[25] 23, November, et al. "Hackers Selling Healthcare Data in the Black Market." Infosec Resources, 14 Oct.2020,resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[26] Cashell, Brian, et al. "The economic impact of cyber-attacks." Congressional research service documents, CRS RL32331 (Washington DC) 2 (2004).

[27] "Cost of Cyber Attacks On Businesses Large and Small-2020 Version." Solvere One, 8 Apr. 2020, www.solvereone.com/pages/cost-of-cyber-attacks-on-businesses/.

[28] Liu, Emily Yunfeng. "The effect of state characteristics and cybercrime legislation on Internet crime." (2020).

[29] Crain, Michael A., et al. Essentials of forensic accounting. John Wiley & Sons, 2019.

[30] "Overcoming Challenges to Cyber Insurance Growth." Deloitte Insights, www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html.

[31] McKay, Peter, and Colleen Seale. "FDIC (Federal Deposit Insurance Corporation)." Journal of Business & Finance Librarianship 5.3 (2000): 63-73.

[32] "RSA Cybersecurity and Digital Risk Management Solutions." RSA.com, 9 Dec. 2020, www.rsa.com/en-us.

[33] Randall, Susan. "Insurance regulation in the United States: regulatory federalism and the National Association of Insurance Commissioners." Fla. St. UL Rev. 26 (1998): 625.

[34] Dhillon, Gurpreet, ed. Information Security Management: Global Challenges in the New Millennium: Global Challenges in the New Millennium. IGI Global, 2000.