ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com
Journal DOI:10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Cyber Risk Insurance-An Indian Perspective.

Jayendra Kumar, Sharmistha Mukhopadhyay, Dr. Priti Puri
Symbiosis Centre for Information Technology, Pune India.

Manuscript Info

Manuscript History:

Received: 12 May 2016
Final Accepted: 19 June 2016
Published Online: July 2016

Key words:
Predictive analytics, Universal framework, lack of awareness.

Corresponding Author

Jayendra Kumar.

Abstract

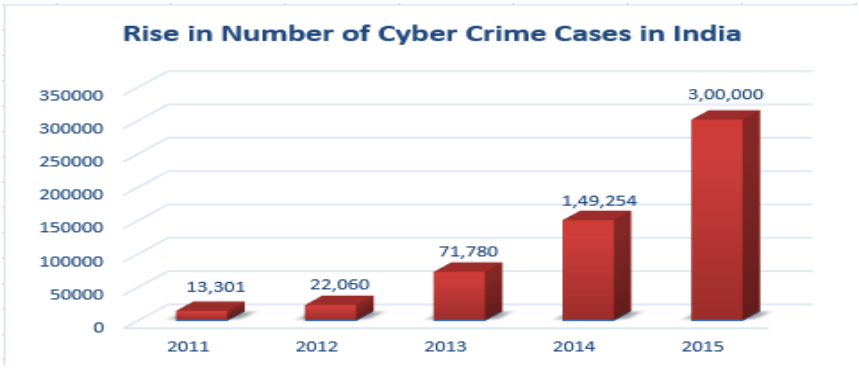
Standing in the 21st century, technology forms an integral part of our lives. With increased dependence on technology, individuals and businesses are constantly exposing them towards more cyber risks and frauds. Cyber Fraud incidents lead to significant loss in Business Value, Customer, Reputation, non-compliance, theft of Intellectual Property and Financial losses. Companies adopt to various cyber security frameworks and standards to prevent risk from cyber threats, thus, trying to mitigate the harsh impacts of a breach. Despite of adopting such security measures, no organization is 100% protected. Organizations try to mitigate or reduce the impact of risk by transferring some of the risks to Cyber Insurance Providers by purchasing Cyber Risk Insurance.

India at its present situation is lagging behind in cyber security policies and hence at a vulnerable position to the threats resulting in huge financial and reputational loss. There are very few cyber insurance companies and efficient policies in India to safeguard against these risks. Therefore via this paper, we would like to bring forward the importance of Cyber Risk policy, issues faced by the insured and the insurer and some proposed solutions to them from an Indian perspective. To conduct this research we interviewed experienced IT Industry professionals and drew an understanding and proposed solutions based on our study and their inputs.

Introduction:-

With the growth and revolution of IT, Big data, Cloud Computing, Internet of Things and Smart Cities there has been an explosion of data and newer technologies are invented every day that tend to make our life simpler. Online services such as online shopping, net banking , booking of cabs, educational services and IT services our life has become much easier but at the cost of rigorous hard work of the employees who ensure that the services run flawlessly. But as everything has its pros and cons, so does have IT. The cyber-crime rate is increasing tremendously in India. As per PwC analysis, a 173% increase in the number of crime cases reported is expected since 2010.

ASSOCHAM- Mahindra SSG Study 2015



An ASSOCHAM SSG study predicted that the number of cyber-crimes in India might reach a number of 3, 00,000 by 2015. Data breaches over the past decade have cost organizations hundreds and millions of dollars. And this leads to the rise of demand for Cyber Risk insurance. But India has been lagging in this field till date. Less than 100 such policies have been sold in India as per data collected till 2013-14. According to Rakesh Jain,CEO, Reliance General Insurance; "After some years, this policy could be among the top liability covers sold in India".

Objective of Study:-

1. To understand about Cyber-Risk Insurance (CRI)
2. State of Adoption of CRI in India
3. Coverage offered by CRI
4. The barriers to the growth of CRI in India
5. Recommending a solution to the issues faced

Methodology:-

The methodology of the research consists of interviewing experienced Industry professionals like CTO's, CISO's, CISA's, InfoSec entrepreneurs and understanding the current state of Cyber-Risk Insurance from different journals, white papers and yearly reports and come up with an understanding and proposed solutions based on our study and inputs from them.

Evolution of Cyber Risk Insurance:-

The Reserve Bank of India highlighted the need for Indian Banks to obtain Cyber Crime Insurance in its Internet Banking Guidelines of June 14, 2001 to ensure that customers are spared from phishing liabilities. The first company which issued cyber insurance in India was HDFC Ergo. Eventually Bajaj Alliance General Insurance, ICICI Lombard and Tata AIG followed suit and offered cyber insurance policies to satisfy the needs of the market then. According to KPMG Cybercrime survey report 2015, 72 percent of Indian companies faced cyber-attacks in 2015. It also indicated that only 41 percent of the Indian organizations consider cybercrime as part of the board agenda, despite being aware of the fact that cybercrime is a major threat faced by the organizations. Security managers from global businesses indicated that their companies either did not have the insurance or were unaware of its presence.

Companies in India are increasingly suffer huge losses due to rising number of cyber-attacks leading to interruption of business and loss of customer data. As part of Business Continuity Planning for the Organization, companies need to adopt Cyber-Risk Insurance as part of Risk Transference. Financial sector handling huge amount of Customer Personally Identifiable Information and financial transactions is among the high-risk targets, but most banks in India, barring a few large private lenders, do not possess cyber risk insurance.

Standing the age of digital revolution, and with the advent of IoT (Internet of Things) and Smart Cities, cyber risk will become widely prevalent. Not just IT companies, but manufacturing, healthcare, agricultural, banking firms, educational institutes, and government websites will be the targets. Therefore proper regulations and standards need to be set both for the insurers and the insurance companies to set the coverage for cyber fraud insurance and the criteria (implemented standards) based on which insurance might be provided.

Understanding the Cyber Risk Insurance Policy:-

As per KPMG Cybercrime survey report 2015, 54% of survey respondents indicated that they spend on cyber defenses in less than 5% and according to Chubb 2012 Public Company Risk Survey, 65% of the public traded companies do not purchase cyber insurance. In India the maximum cyber insurance cover provided till now is worth 300crores. "As India goes digital and e-commerce takes off, the cyber risk will increase. Therefore, there will be a higher demand for such product," said Sanjay Datta, chief of underwriting and claims, ICICI Lombard. And hence the insurance cover can be raised to 600 crores based on the requirement of the customer.

As per Dinesh Bareja, COO, Open Security Alliance, "Improvement of response to cyberattacks is not a by-product of CI;however the insurance company may insist on the need to have resilient ISMS in place. This can be considered to be a means to improve incident response." However adoption of a cyber risk insurance is not an alternative for a weak security framework. The policy is a back up to protect the company's financial loss above the threshold it can't manage. Adoption of a rigid security framework along with constant monitoring and control is needed to reduce the impact of a potential risk and premium cost of a Cyber Insurance. The existing types of covers that are provided by the Cyber Insurance companies are:

a. First Party Coverage(not comprehensive): protects against the direct expenses of the company in response to a cyber incident, which includes:

- Employee Theft Coverage
- Premises Coverage
- Transit Coverage
- Computer Fraud Coverage
- Depositor's Forgery Coverage
- Forensic Investigation
- Business Interruption
- Computer Data Loss and restoration
- Extortion

b. Third Party Coverage (not comprehensive): protects against the expenses incurred by the third parties on occurrence of a cyber incident. This includes:

- Litigation and Regulatory
- Regulatory Response
- Notification Costs
- Crisis management
- Credit Monitoring
- Media Liability
- Privacy Liability

According to Niranjan Reddy, CTO, Netconclave Systems, "Basically, IT assets are any company-owned information, system or hardware that is used in the course of business activities. The coverageof IT assets under Cyber Risk Insurance must include:

Network Security Liability:

Uniqueness here is both first-party costs & third-party liabilities are covered.Third-party damages as a result of denial of access of data, costs related to data on third-party systems and costs related to theft of such data. It also applies if a firm holding trade secrets or patent applications for a client, and that information is accessed due to failure of security.

Media Liability Cover:-

Claims such as infringement of intellectual property, copyright/trademark infringement are covered. Due to presence of Internet in businesses today, technology companies will be able to migrate into media component in a Cyber policy. Third-party damages covered can include specific defacement of website.

Data Breach/Privacy Crisis Management Cover:-

Expenses related to the management of an incident covering the Forensic investigation, the remediation, data subject notification, public relation expenses, legal costs, court attendance and regulatory fines.

Extortion Liability Cover:-
Typically, losses due to a threat of extortion, professional fees related to dealing with the extortion."

The Pitfalls:-

Pitfalls are there for both insurer and the insured. The Insurer cannot bear all the burden of a cyber insurance since the loss has multi-facets. They keep check points through the premium and scope. Also an Insurer cannot fulfill its obligation when the insured is not complying with the mandated security framework.

The Insurers land into lot of trouble when the claim is involving third part loses where risk accumulation happens. The Insurer cannot estimate losses accurately as the nature of loss is a chain reaction. The Liability of stake holders like cloud storage vendors, Voluntary Payment by the Insured, Ransomware are still grey areas of Cyber risk Insurance. Obviously a ship cannot be insured when it's going for war, and a company cannot be covered from all possible attacks. A lot of debates do happen on what needs to be covered and what cannot be covered.
On the other side companies which are enrolling themselves for the cyber risk insurance should get all the coverage points explicitly stated and not assume coverage which are not stated. There are grey areas which are uncovered under Cyber Fraud Insurance such as – "Voluntary payment" where the user is tricked into cash transfer through social engineering/phishing activities .Unless the Insured stress this requirement in scope, it will not be covered by the Insurer.

Some of the major pitfalls faced by the Insurance providers are:-

- Lack of a Privacy Law in India
- Risks faced by the firms are unique to the particular sector or industry in which they operate
- Lack of historical data
- Difficulty to predict probability of occurrence and impact of the risk
- Having to customize policy covers and premiums for each industry
- Lack of predefined standards, metrics of cyber risk insurance
- Difficulty in calculating premiums based on the impact of the risk

Barriers for CRI in India:-

Cyber Risk Insurance landed in Indian market only around 2012 and the companies that offered this product had very few clients and had very few competitors. By this time the US cyber risk Insurance market was blooming with cybercrimes hitting headlines almost every day. The Regulators became watch full and strict laws were imposed but in India Cyber risk Insurance is still seen additional expense that has no returns. The product is still at a nascent phase in India, companies are tentative but the growing threat landscape has forced them to look into Cyber risk Insurance. We have listed few major barrier for CRI:

- Cost burden in adopting a cyber insurance cover
- Underlying complexity of calculating premium, assessment of third Party loses, detecting fraudulent claims
- Lack of awareness on the need of cyber risk insurance
- Ambiguity over the scope and coverage of policies
- Varying premiums for covers by different insurance providers
- Absence of a single comprehensive insurance cover (presence of multiple covers and policies by different insurers)

According to the Mahesh Balan, Director-Qadit Systems and Solutions "As there is no statutory requirement currently in India for many of the segments in Cyber risk insurance, hence the market is limited. Moreover, the implementation of the law - especially ensuring compliance of data privacy - is very weak and hence the market for CLI is not flourishing in India".

InsurancePremium:-

Insurance companies are aware of the danger of providing cover for an organisation that is inconsistent with security practices that can cost heavy loss. So the amount of premium is an indicator of how well the company is compliant with the security standards and how much it is prone to attack. Generally policy covers are tailor made and the premium varies according the risk handled. There is no established framework to calculate the premium and is mostly decided by the underwriter's judgement skills.Some key factors drive pricing of cyber insurance policies are:

- The insured's industry
- Geographic spread of operations
- Scope & Limits sought by insured
- Security and privacy controls
- Claims and loss experience
- Handling Customer Information

Cyber risk insurance caries a high premium and hence becomes unaffordable by Small and Medium Businesses. A company seeking insurance in India has to pay around 12-18 lakhs yearly premium to get a cover of 10crores, and around 2.4-3 crores yearly premium for a coverage of 300crores. SMBs do not possess a strong security frameworks and because of the cost constraint in cyber risk insurances, they prefer adopting and strengthening their security framework instead of going in for a cyber security insurance. But they can still become easy targets for cybercriminals as there are no fool-proof security practices available. There are inevitable losses when the company is being hacked and customers PII is being leaked in this scenario.Cyber Insurance gives a chance for the company to survive this debacle with minimum loss.

According to Dinesh Bareja "The second issue is the extent of adoption of the security frameworks by SMB companies which is still very nascent. In India, SMBs have yet to adopt security practices that can provide them with the first level of assurance or risk management and there is still a great need to understand the big risk they face from cyber threats. My view is that SMBs largely think that the worst that can happen is a virus attack and that they are well protected because they will (usually) have some anti-virus in place.

I believe that SMEs should adopt CI as it will provide the quickest risk management action that they can come up with. Whether the insurance company will be able to provide an economical premium in the absence of any information security implementation."

Lack of awareness:-

The major barrier for CRI is the lack of awareness. Companies do think that instead of purchasing a costly Insurance cover that does not provide you visible returns it is wiser to invest that money in hardening the security controls. But even a country like US where the security practices are much more matured are facing cybercrime at an alarming rate.

According toVijay, Director- Qadit Systems and Solutions, "There is absolute lack of awareness about Cyber Insurance coverage in India. The barriers are there from both insurer and insured. Insurer do not have a suitable product that is well advertised. For insured, they have rarely associated costs/damages with cyber incidents, and unless there is awareness that cyber incidents can cause financial loss they may not look at insurance. Traditionally also Indian businesses have not associated value to information assets. A cash box with Rupees 100 will be kept under lock and key whereas a computer with much greater value will be kept open without adequate protection." The underlying truth is that criminals are getting smarter and they are inventing new methods to hack which are hard to crack. So it is always better to be prepared for the D-day which may not be far from today. The companies have to understand this reality before it is too late. Many examples are out there showing how a single attack has led to the complete shutdown of big MNC's. Not just outside attacks, lack of awareness and proper training of data privacy and access rights amongst the employees of an Indian MNC had led to a US based healthcare management system provider slap a rigorous compensation of $940 million, leading to a significant financial loss for the company and reputational loss as well as for the other Indian companies.

The privacy laws are more comprehensive and strictly practiced in western countries whereas in India the people are not even aware of the importance of their PII. Lack of a Privacy Law in India being a major disadvantage. Personal Information are more easily available and they are not maintained according to the mandated standards in small & medium scale organization and soon India may become an easy target.

Solution:-

Calculation of premium and detecting the fraudulent claims has been the biggest challenge for the cyber risk insurance companies. Solution to these problems are not simple. Though the product flourished a decade ago there is no significant growth in terms of establishing a strong metrics. The solution that is suggested may not bring drastic

changes immediately but it can improve the system continuously and the desired outcome may be reached in the coming years.

Developing a Universal Framework:-
At present there is no framework or regulation regarding Cyber Risk Insurance. Developed cyber market such as US and Europe should initiate steps in creating a common framework that provide the metrics for calculating premium, policy cover value and losses. This will help the Cyber Insurance market to flourish in developing countries that lack standards and metrics. Anonymity is the biggest barrier and with the development of such metrics the customer's confidence on the product will improve and the market will flourish. As per Dinesh Bareja"CI market in western markets is still maturing and India is slowly following the lead. Indian companies (insurance buyers and sellers) are yet to localize the requirement or the product for Indian business scene"**.**

Predictive analytics for Premium calculation & Claim Management:-
Predictive modeling is a process whereby statistical and analyticaltechniques are used toidentify patterns that are then used to develop models to predict the likelihood of future events based on data from past.Predictive analytics help significantly in following spheres:

- Risk Assessment
- Recognition of Potentially Fraudulent Claims
- Premium calculation by Intelligent data interpretation
- Identification of Potentially High Value Losses(Outliers)
- Advanced behavioural analytics
- Allocation of Resources based on the priority
- Reducing claim cycle life time-improving customer satisfaction
- Predicting industries/organizations possessing potential threats
- Identifying IT assets under risk
- Identifying Attack Methodology

Fraudulent claims recognition at the initial stage may save a huge expense for the CRI companies. The fraud claims comprise of furnishing false evidence, claiming for uncovered assets etc. The system receives basic inputs from the claim, it starts comparing with previous sample records. It gives estimates based on the previous sample and if the quoted amount drastically varies from the system estimate, it segregate the claim and alerts the officer for allocation resource for separate attention.

An important application of Predictive analytics is the identification of those claim at an initial stage that can cause high financial loss. The claim that has the potential of causing high financial loss are identified and segregated based on the inputs provided by the insured. Resource will be allocated to review the impact assessment and the progress of the policy will be closely monitored .A typical example of such scenario is the Third part data theft involving PII-Personally Identifiable Information where the loss can have a cascading loss. Claim professional will find this as a great aid as it becomes very tedious to determine these outliers at the initial stage. The use of analytics in claims management will eventually become standard operating procedure as some experts believe. Perhapsfuture technological advances will bring this belief closer to reality.

In premium calculation the previous cases will be compared and the process of premium calculation will be automated with risk assessment reports will be given as input .This reduces the human errors in calculating premium but the final decision will be taken by the underwriter's team. Here technology is used only in assisting the accuracy of the underwriter's decision. But getting actuarial data is not an easy task as the market is in its early stage with the samples available being limited the accuracy of the analytics will be becomes debatable. But this condition will only improve with the market growing and soon predictive analytics will become an essential tool for an insurance company.

Future of CRI:-

There is a steady increase in the number of policy sold in India, the market will only improve with the cybercrime rate increasing exponentially .The government may mandate strict laws regarding handling of PII and the countermeasures for data theft. But the important question is that will government mandate CRI for companies handling sensitive data.

As per Vijay, "Laws are difficult to be implemented in India due to jurisdictional issues. Indian organizations don't associate a financial value to cyber incidents".Whereas Dinesh Bareja says "From my knowledge there is no statutory requirement for CI at present though this has been mentioned in certain regulatory documents as a recommended practice. However, in the near future CI will be the choice and regulatory authority may make this mandatory. This can be done only if the Insurance offering(s) for CI are created in a manner which will be well aligned to the business needs."

A lot of debates are going around this with some saying it is unfair on small and medium scale companies who can't afford the cost of CRI and at the same time some argue that instead of a blanket mandate sector wise implementation would be the ideal approach as an example Health care and Financial institution are the most vulnerable compared to other sectors in handling PII and cybercrimes.
There is a big opportunity for the Insurance companies to capitalize and the product will soon become a main agenda in board room discussions. The industries which are high targets of cybercrime as per KPMG's cybercrime survey in India 2015 is given below.

Conclusion:-

Though Cyber Risk Insurance looks inapplicable to many organization at present but it may soon become indispensable .The role of statutory bodies will be the key, when they take tough steps towards to PII leak, the organization will be forced to take cover. The government may mandate at least third party CRI cover for organization dealing PII as it can save the collateral damage of a cybercrime which looks more of a day to day happening.

As per Niranjan Reddy "The need for cyber insurance policy will create a need for the organization to create a robust cyber security infrastructure to meet with the clauses imposed by the insurance company. This will not only improve cyber security in general but also improve the response of these organizations to cyber-attacks.On an event of a cyber-attack the organization will carry on a cyber insurance claim, a key role in a cyber insurance claim is Incident Response. An Incident Response program that is well built and regularly tested becomes an integral component of a risk management plan. Every claim for the cyber-attack will require a thorough forensic investigation; depending on how the investigation is performed the attack can either be a minor or a major breach that is completely covered by the insurance."

Acknowledgement:-

We would like to extend our gratitude and acknowledgement towards Mr. Dinesh O Bareja, COO of Open Security Alliance and Pyramid Cyber Security. Mr. Bareja has over 23 years of work and business experience and is an Advisor in Indian InfoSec Consortium and also leads the Indian Honeynet Project.He was alsoassociated with the Cyber Defense Research Centre (Jharkhand Police) as Cyber Surveillance Advisor,

We would like to extend our gratitude and acknowledgement towards Mr. Niranjan Reddy, Founder and CTO at Netconclave Systems. Mr. Reddy is an Information Security Evangelist with more than 10+ years of experience in this domain. IT Security Trainings, VA/PT,Security,Network & Web Application Penetration Testing.Cyber Crime Investigations,Corporate Investigations. IS0 27001 Consulting.

We would like to extend our gratitude and acknowledgement towards Mr.B. Mahesh Balan, CISA, DISA, ACA, Certified Ethical Hacker,Grad. CWA, BS7799 Lead Auditor, Director at Qadit Systems and Solutions. Mahesh has 20 years of professional experience in the areas of Audit, Finance and Information technology. Rank holder in both intermediate and final CA examinations. Over 8 years of IT Security Consulting, 4 years of audit and finance experience and 5 years of systems and control design experience.

We would like to extend our gratitude and acknowledgement towards Mr. V.Vijayakumar, CISA, DISA, ACA, Certified Ethical Hacker, AICWA, LCS, BS7799 Lead Auditor, Director at Qadit Systems and Solutions. Vijay has 18 years of professional experience in the areas of Audit, Finance and Information technology. Rank holder in both intermediate and final CA examinations. Over 8 years of IT Security Consulting experience and 6 years of systems and control design experience.

References:-

1. William Lentz,Gen Re, Predictive Modeling-An Overview of Analytics in Claims Management
2. GeetikaSood (2015), Comparative Analysis Of Cyber Privacy Law In India And In The United States Of America
3. CostisToregas and Nicolas Zahn (January 2014), Insurance for Cyber Attacks: The Issue of Setting Premiums in Context
4. Inotes: Newsletter from Insurance Broking House (December 2014), Issue#51
5. Latham & Watkins (2014), Cyber Insurance: A Last Line of Defense When Technology Fails
6. Robert P. Hartwig, Claire Wilkinson (October 2015), Cyber Risk:Threat and opportunity
7. Stephane Hurtaud, Thierry Flamand, Laurent de la Vaissiere, AfafHounka (February 2015), Cyber Insurance as one element of Cyber Risk Management Strategy
8. Capgemini POV- Using_Insurance_to_Mitigate_Cybercrime_Risk
9. KPMG Cyber Crime Survey Report 2015,(November 2015)
10. Ranjan Pal, Pan Hui, LeanaGolubchik, Konstantinos Psounis (2014), Will Cyber Insurance Improve Network Security? A Market Analysis.
11. Assocham-Mahindra SSG study on cybercrime (2015).

Appendix A:-

We have conducted a qualitative Risk Assessment trying to identify the risks and the uncertainties existing in the Indian marketplace leading to a poor growth of Cyber Risk Insurance companies in India. If some of these risks are mitigated, Cyber Risk Insurance market will flourish in India in near future.

Risk Assessment of Cyber Risk Insurance						
S. No	**Vulnerability**	**Risk Summary**	**Risk Likelihood Rating**	**Risk Impact Rating**	**Overall Risk Rating**	**Recommendations**
1	Policy loop-holes	If the policy frame work is not clearly defined it could result in a loss where a client is paying to an insurer for a resource which is not covered or an insurance company will land up in law suit for not providing claim cost	Moderate	High	High	Policy frame work has to be prepared by underwriters with industry experience. Policy loop holes have to collaborate with established players.
2	Lack of techniques to quantify assets	IT assets are both physical and virtual. Quantifying the value of a data becomes very difficult. Insurer may benefit out of claim more than his acquired loss if the assets are over estimated. If underestimated the client will suffer a loss in a claim	High	High	High	Quantifying techniques have to be developed globally. There is no guideline to quantify assets at present. The governing bodies has to establish standards for quantification.
3	Ambiguity in policy exclusions	Exclusions such as terrorist attack, natural calamities, Cloud data leak etc. may be poorly defined	Medium	Medium	Medium	Policy exclusions should not be generalized instead be appropriately mentioned. Client should be aware of all these exclusions before signing the policy
4	Lack of global metrics	The product is in nascent phase and there are no global metrics developed. This leads to client feeling insecure with product price and purpose.	Low	Low	Low	Established markets like US and Europe should initiate steps to frame global metrics.
5	Lack of accurate techniques for	Accessing the loss after the security incident is complicated as the data can be	High	High	High	Impact Assessment standards have to be developed and assessment

	impact assessment	geographically spread and may cause cumulative loss which cannot be assessed accurately, companies are unaware of the impact that they might face in occurrence of a cyber incident				should be done byexperienced professionals with knowledge on cybercrime
6	Financial constraint – High Premium	Inability to bear the complete cost of cyber insurance by Small and medium enterprises might lead to lesser penetration in the market.	High	High	High	Cyber insurance companies should maintain a scope of covering one or more IT resources only of the company which they consider is risk prone.
7	Lack Of Knowledge on cybercrimes	Knowledge of Cybercrime and their mode of operations are important for both the insured and the insurer.	Medium	Medium	Medium	Continuous tracking and analysis of the crimes and their preventive techniques is required to come up with a proper assessment.