ISSN: 2349 - 4891

International
Journal of Recent Research and Applied Studies
(Multidisciplinary Open Access Refereed e-Journal)

The role of cyber security in micro insurance sector

Archa. S. Nair[1] and j.s.sudhir[2]

[1]Research Scholar, Department of Commerce, Iqbal college peringammala, University of Kerala, Thiruvanthapuram

[2]Associate professor, Department of commerce, Iqbal college peringammala

Received 15st March 2021, Accepted 1st April 2021

Abstract

Personally identifiable information is a precious asset at the heart of every insurance databases and relentlessly sought after by cyber criminals. Insurers have an obligation to customers, intermediaries, and regulators to safeguards this valuable data and meet the compliance requirements outlined by the Financial Services Authority and the Personal Card Industry (PCI) Data Security Standard. To help you address security vulnerabilities and regulatory requirements with your data rest, in use, or in transit, our audit controls identify where the data is, whether it's sensitive, and if it's adequately encrypted or otherwise protected. For example, you can regularly scan employee's laptops, query all instances of personally identifiable information and act to eliminate exposure and risk.

Keywords: **micro insurance, cyber security, cyber criminals, Insurers, risk, protection.**

Introduction

Cyber security insurance, also called cyber liability insurance or cyber insurance is a contract that an entity can purchase to help reduce the financial risks associated with doing business online. In exchange for a monthly or quarterly fee, the insurance policy transfers some of the risk to the insurer.Cyber security insurance is a new and emerging industry. Companies that purchase cyber security insurance today are considered early adopters. Cyber security policies can change from one month to the next, given the dynamic and fluctuating nature of the associated cyber associated cyber- risks. Unlike well-established insurance plans, underwriters of cyber security insurance policies have limited data to formulate risk models to determine insurance policy coverage, rates and premiums.

Statement of the problem

The loss, compromise or theft of electronic data can have a negative impact on a business, including the loss of customers and revenue.

Correspondence
Archa. S. Nair
Research Scholar, Department of Commerce, Iqbal college peringammala, University of Kerala, Thiruvanthapuram

Business may be liable for damages stemming from the theft of third party data. Cyber liability coverage is important to protect businesses against the risk of cyber events, including those associated with terrorism. Cyber-risk coverage can assist in the timely remediation of cyber-attacks and incidents.

Significance of the study

Cyber security insurance policies are sold by many of the same suppliers that provide related business insurance, such as E & O insurance, business liability insurance and commercial property insurance. Most policies include first- party coverage, which applies to losses that directly impact a company, and third-party coverage, which applies to losses suffered by others from a cyber-event or incident, based on their business relationship with that company. Cyber insurance policies help cover the financial losses that result from cyber events and incidents. In addition, cyber- risk coverage helps with the costs associated with remediation, including payment for the legal assistance, investigators, crisis communicators and customer credits or refunds.

Objectives of the study

1. To determine the relationship between cyber security and micro insurance companies in Kerala

ISSN: 2349 – 4891

Literature Review

1. Dunn-Cavelty (2010, p.363) defines Cyber- security as "both about the insecurity created through cyberspace and about technical and non-technical practices of making it (more) secure. This definition attempt to present that cyber security is not merely a technical issue, which always associated with computer science, cryptography or information technology, as with many cyber security related research that have been discussed in recent years
2. Dewar (2014) explains that" the goal of cyber security to enable operations in cyber space free from the risks of physical or digital harm (p.18). How country perceive the accumulation of interplays within securitization elements in cyber security issue and the attribution problem makes their cyber security strategy policy are different each other.

Methodology

The study is qualitative in nature. The source of data is secondary. The method of data collection is review from secondary sources.

Cyber insurance

Businesses that creates, store and manage electronic data online, such as customer contacts, customer sales, PII and credit card numbers, can benefits from cyber insurance. In addition, e-commerce businesses can benefit from cyber insurance, since downtime related to cyber incidents can cause a loss in sales and customers. Similarly, any business that store customer information on a websites can benefit from the liability coverage that cyber insurance policies provide.

What is covered and not covered by cyber insurance

In the United States, most major insurance companies offer customers cyber security insurance policy options. Depending on the price and type of policy, the customer can expect to be covered for extra expenditure resulting from the physical destruction or theft of information technology (IT) assets. Such expenditure typically include costs associated with the following:

1. meeting extortion demands from a ransom ware attack
2. notifying customers when a security breach has occurred
3. paying legal fees levied as result of privacy violations
4. hiring computer forensics experts to recover compromised data
5. restoring identities of customers who PII was compromised
6. recovering data that has been altered or stolen and
7. Repairing or replacing damaged or compromised computer systems.

Many cyber security policies exclude preventable security issues caused by humans, such as poor configuration management or the careless mishandling of digital assets. Other issues excluded by cyber security policies include the following:

*. Preexisting or prior breaches or cyber events, such as incidents that occurred before the policy was purchased;

*. Cyber events initiated and caused by employees or insiders;

*. Infrastructure failures not caused by a purposeful cyber-attack;

*. failure to correct a known vulnerability, such as a company that knows that a vulnerability exists, fails to address it and is then compromised from that vulnerability and

*. The cost to improve technology system, including security hardening in systems or applications.

Micro insurance

Micro insurance looks to aid poor families by offering insurance plans tailored to their needs. Because the coverage value is lower than a usual insurance plan, the insured people pay considerably smaller premiums. An important financial service. Expect good management practices

- properly designed data bases
- Regular review results
- Data managed as valuable resource

Micro insurance companies in Kerala

A group micro term insurance product with return of 50% premium on maturity

- affordable insurance coverage
- flexibility of coverage amount
- Return of premium at maturity

The SBI Life-Shakti plan offers-

1. Security-cover your members and safeguard their families in case of an eventually
2. Reliability – through return of 50%of premiums paid at maturity
3. Flexibility – to choose the sum assured according to your members needs
4. Affordability- with reasonable premiums

Conclusion

Our paper presents an analytical framework for organizations to optimize their cyber security and micro insurance program. Analytical models are employed to quantify the effects of security investments in addressing cyber threat, vulnerability and impact, respectively, on the remaining annual loss expectancy. The paper proposes cyber insurance product innovation, by offering itemized cyber insurance coverage, risk management services and risk sharing thorough insurance pools. Global insurance companies, law firms, and uniquely positioned to help facilitate international coordination between the private sector law enforcement agencies.

Reference

1. Dunn-Cavelty (2010, p.363) managing interdepend information security risks: cyber insurance, managed security services, and risk pooling arrangements30(1)(2013)pp.123-152

ISSN: 2349 – 4891

2. Dewar (2014) The Best Cyber security Investment you can make Is better Training , Harvard Business Review, May 16,2017

3. Gordon et al.2003 L.A. Gordon, P.L. Martin, T.Sohali" A framework for using insurance for cyber- risk management Comms ACM,46(3)(2003),pp.81-85

Please cite this article as: **Archa. S. Nair and j.s.sudhir** (2021). **The role of cyber security in micro insurance sector** *International Journal of Recent Research and Applied Studies*, 8, 4(4), 35-37.