World Journal of Research and Review (WJRR)
ISSN:2455-3956, Volume-4, Issue-6, June 2017 Pages 61-64

Perspective and Growth of Cyber Insurance

Manveet Singh, CA Arvinder Pal Singh Arora

Abstract— **Many organisations believe that their current insurance policies would cover them against cyber breaches too, but that is not the case. Various kinds of policies like for general liability, property, or even casualty policy, do not cover the risk of a cyber attack. Cyber crime is growing, due to low risk of being caught and high returns from breaching & accessing intellectual property and more from the network. No type of company is free from cyber crime. In 2014 alone, 60% of small companies and 81% of large companies saw a cyber breach onto their network. Average damage of a breach to a large company is $5.9 million (□ 37.65 crore), and $410,000 (□ 2.60 crore) toa small company. Insurers are keeping a tight check on their cyber risk exposure using pricing strategies and offered terms and conditions, but this makes their clients question value of the policies they hold. The insurers and reinsurers need respond and offer a solution to the opportunity they have in front of them.**

Index Terms— **Cyber Insurance, Cyber Security, Cyber Crime, Cyber sustainability, Insurance.**

I. Introduction

Cyber Insurance is a young industry, such that its products and services are still not very well defined. It is only about 20 years old.

It is an insurance product, offered by specialised insurance companies to protect business from Internet-based risks and risks related to Information Technology infrastructure and activities.

Cyber Insurance covers losses of 2 categories.

- **First-Party losses** are accrued losses to the firm that got breached.
- **Third-Party losses** are costs suffered by related third parties – customer or partners – due to cyber breach.

Cyber Insurance is a huge market but a largely untapped opportunity by insurers and reinsurers. PwC estimates annual gross writer premiums would triple by 2020, from currently around $2.5 billion to $7.5 billion. Many insurers would have a chance to take advantage of the rare opportunity to secure higher margins in a soft market.

Some companies might believe that Cyber Insurance is a replacement for robust IT infrastructure and security, but it is not. Cyber Insurance only helps a business in mitigating the impact of different cyber incidents.

Manveet Singh, Assistant Professor, Commerce, Sri Guru Nanak DevKhalsa College, University of Delhi, India,
CA Arvinder Pal Singh Arora, Associate Professor, Commerce, Sri Guru Nanak DevKhalsa College, University of Delhi, Delhi, India,

II. Risks from a Cyber Attack

When a cyber attack happens on a company, the following could occur as a result:

1. Critical data is lost
2. Loss of trade secrets/confidential information
3. Breach of contract
4. Website downtime
5. Business interruption
6. Theft
7. Network security liability
8. Customers may be lost and business interrupted
9. Loss of IP/trade secrets
10. Intellectual Property damage

Other than these direct damages, some indirect damages a Company faces due to a Cyber attack are:

- Loss of reputation
- Notification costs and other response costs; i.e. forensic IT
- Regulatory actions and associated fines and penalties
- Profits impacted/value of shares may fall
- Product recall
- Directors' and officers' liability
- Damages to be paid due to loss of customer data
- Extortion

In a survey powered by Ponemon Institute, 71% consumers surveyed by Edelman, said they would leave an organization after a data breach.

Data protection regimes differ all over the world, as governments are moving towards tougher rules to ensure cyber security. US legislation has become tougher and European Union is reviewing its data protection laws for a harmonised regime. Hong Kong, Australia and Singapore already have new data protection laws in place.

III. Role of Insurance

Cyber Insurance is not a replacement for cyber security measures. Just like property insurance covers property risk but you would still install sprinklers to mitigate losses due to fire and fire alarms to take action in time, similarly is the case with cyber risk. After purchasing Cyber Insurance, you cannot just ignore IT security, you need to be prepared to provide protection against the worst.

Cyber Insurance alone is not enough protection, and cannot replace a company's current portfolio of security products, services and processes in place. It needs to be considered as an important part of company's overall security strategy.

The technological aspect, operational aspect and insurance aspect go hand-in-hand to avoid any losses.

Cyber Insurance provides specific coverage for damages and costs incurred due to cyber attacks.Even though it offers many benefits, only a fraction of companies avail such insurances. But this is changing and experts expect rising demand in coming years.

A. *Security Strategy*

Cyber crimes cost the global economy on an average more than $400 billion annually. While a conservative estimate puts it at $375 billion, but it could really be $575 billion annually. Even the most conservative number is more than total GDP of many countries of the world.

The number is going to increase with every year. PwC saw an increase in detected information security events by 38% between 2014 and 2015. As companies become aware of cyber risk, 73% companies have placed it as a top-10 business risk, yet they underestimate the real risk and cost of such a crime.

In its Cyber Impact Report, Ponemon Institute found that no company was discriminated for cyber incident, even though the financial loss they incurred due to it was different. A large company suffered an average financial loss of $5.9 million; a medium company suffered around $1.3 million while a small company incurred an average loss of $410,000 for a cyber attack. According to an estimate by Mandiant, a cybersecurityfirm puts the cost of several high-profile breaches of retail companies in 2014 at $1 billion each. In the same year, companies around the world faced 100,000 security incidents per day.

The prospect of a catastrophic cyber loss seems more likely now. An attack leading to huge loss of data or BI, would inevitably damage reputation of the company and then possibly put the corporation out of business.

Even a cyber incident involving an energy or utility company could lead to significant outage, damage to property and even loss of life. At the same time, if countries were to wage a cyber war against each other, it could disrupt Internet services around the world. Thus the governments need to take interest in protecting critical infrastructure, be involved in cyber security, resulting in greater level of scrutiny.

B. *Insurance Process*

The process to get Cyber Insurance is quite complex, and fraught with various pitfalls. The process involves securing a policy, filing claims and annually renewing the policy. Going through the process is valuable to a company over & above just getting insurance against cyber attacks. It forces the company to hold important conversations with all the relevant stakeholders about overall cyber risk stance, risk appetite, cyber threat profile, and current IT security approach. Given these conversations happen amongst at least company's Board of Directors, CEO, CISO, CTO amongst others, the company can decide how much it can take on and what risk they want to be covered by an insurance agency.

Due to its complex process, it sometimes requires involvement from an external agency for its expertise and also to broker on their behalf with the underwriter from Cyber Insurance providing company.

C. *BenefitsOf Cyber Insurance*

Financial resiliency: If a company suffers a breach, it will be able to mitigate insured aspects of loss and also recover insured out-of-pocket losses.

Stronger public security stance: By following the cyber insurance placement process, a company creates a record of actively managing cyber risk. This would bring them in line with 2011 directive issued by The U.S. Securities and Exchange Commission about the need for businesses to disclose their financial position on cyber risk and insurance.

Streamlined contracts: Cyber Insurance helps in contracting with third parties, as they know their data will be protected if anything goes wrong. When a business regularly does business where it accesses, processes or stores protected information like personal health information (PHI) or personally identifiable information (PII), risk of data loss is inherent, but Cyber Insurance gives peace of mind to contracting parties that their data would be safe.

D. *ProblemsWith Cyber Insurance*

Insurance companies are still wary of cyber attacks. Some simply don't want to cover it, while other have limits set lower than what the clients seek, making a match really difficult. Some insurers have imposed restrictive conditions such as 100% updated security patch in IT systems, or state-of-the-art data encryption, which are difficult for any business small or large to maintain. Due to the restrictions on claims, imposed limits, high cost of coverage, and tight attaching terms and conditions, companies end up questioning real value provided by Cyber Insurance.

The problem for insurer is that Cyber Insurance is nothing like other risks. Public information on scale and financial impact of cyber attacks is very limited. The fact that cyber threats are very rapidly changing and proliferating doesn't help the insurers. As seen in case of many companies, cyber security breaches might only come to light after several months, as they remain undetected. This causes the losses to be accumulated and compounded.

E. *Cyber Insurance Trends*

- Cyber insurance market is expected to be worth more than $20 billion by 2025
- Currently data protection risks and liability dominate the market, but over the next decade demand for business interruption cover will grow.
- Financial institutions, transport, utility, telecommunications and energy sectors will lead the widening demand for insurance cover.

- Standalone insurance products would become the norm for liability cover and coverage via traditional policies would be decreased.
- Cyber Insurance market will see diversification and volume. Insurers specialised in certain sectors will segment the market.
- Businesses will need to be educated on exposure to cyber incidents better and attain more knowledge of underwriting for Cyber Insurance policy.
- Businesses will increasingly have to focus on supply chain cyber risk, as they will incrementally be exposed to them.
- Third party experts will become increasingly important in event of a cyber security incident, to mitigate losses they would be as indispensable as speedy response to the incident.
- Governments will have to collaborate with businesses and insurers to protect critical infrastructure in case of catastrophic cyber loss.

IV. Cyber Insurance coverage

A. *Commonly Covered Incidents*

Forensics: This is the cost involved in cyber forensics, of investigating and analysing an attack. A specialised third party often does this.

Notification expense: Certain laws require a breached entity to notify customers, partners and suppliers if they have been impacted by the breach. Even when law doesn't explicitly require it, many firms do so to manage their brand and business relationships during and after the breach.

Public relations: Extensive communications with the press and the business community might be required, to announce about the breach.

Business interruption: If systems or data are unavailable due to an attack, and business is disrupted, the loss incurred can be covered. This is generally the highest expense — in 2014 organizations suffered an average of $204 million in business interruption costs due to cyber attacks.

Credit monitoring: It is becoming standard for companies that have been breached to offer consumers credit-monitoring services to protect them from any subsequent identity threat or financial fraud.

Breach coaching: A breach coach is a high-level response coordinator, working with technical experts to isolate affected data, notify customers, retain necessary forensics professionals and manage crisis communications. A breach coach is often the first responder to an incident and helps the company triage the response to a breach.

Legal costs: These can be hefty, as lawsuits filed against breached companies only add to all the business losses. Hiring legal experts and settling the lawsuits can add up to tens of millions of dollars.

Regulatory fines: If any violation of regulations such as the Health Information Portability and Accountability Act (HIPAA) or Payment Card Industry (PCI) rules occurs, your organization may be fined.

B. *Commonly Uncovered Incidents*

A lot of incidents that cause direct loss to businesses are still uncovered. Due to ambiguity in the industry on what should cyber insurance cover and what it should not, theft of intellectual property and remediation of a breach are still not covered. The industry hasn't still standardized its offerings to the companies.

V. Growth of Cyber Insurance

There are many reasons that would lead to growth of Cyber Insurance in the coming years, making it a substantial offering by insurers.

- Legislations dealing with data protection will toughen globally.
- Lawmakers are expected to introduce significant fines for data breaches.
- Industrial control systems are highly vulnerable, which poses significant threat.
- Frequency and severity of cyber crime incidents, including data breaches is being driven by an increase in interconnectivity of devices and commercialization of the crimes.
- As more systems move online, Business Interruption (BI) costs incurred could be equal to, or exceed, losses incurred due to a breach.
- Intellectual property theft and cyber-extortion risk potential increasing.
- There is still no silver bullet solution for cyber security.

VI. Cyber Insurance Landscape of tomorrow

Developments in technology and how they are used are going to drive the cyber risk landscape in the future.Increasing usage of mobile devices, like smartphones & tablets, smartwatches, wearables connecting to Internet are set to increase threats of cyber risk and possibility of cyber incidents. As *Internet of Things* comes of age, and technology to connect with Internet is embedded in devices around our homes in domestic appliances, lighting systems, entertainment systems, etc., a cyber incident would have a snowball effect on all connected devices.Once smart cars come on the road, cyber risk would pose a dilemma even to people on road. No networked device would be safe from such an incident.

"Predictions suggest that a trillion devices will be connected by 2020, which could lead to a significant increase in cyber vulnerability," says Rishi Baviskar, Senior Cyber Risk Consultant, AGCS

Internet of Things will make cyber security a bigger issue. For example, in 2014, as part of competition, Chinese students hacked a Tesla Motors electric car, and remotely controlled its locks, headlights, horn and skylight, while the car was still in motion. Incidentally, recently around 1000 Internet connected smart household appliances, like fridges, televisions and microwaves, were hacked and used in a botnet attack to send spam-emails. Attacks like these have underwriters exercising their mind for Cyber Insurance.

As more devices connect, *Internet of Things*, they would bring increased potential for physical losses in addition to data breaches. Increasing use of mobile wallets for financial transactions make wallet holders' bank information highly vulnerable to attacks.

VII. Conclusion

As companies become more aware of broader cyber risks, like impact of business interruption and regulatory changes, it would propel rapid growth of Cyber Insurance around the globe. On the other hand, as more everyday devices become technology driven, new risks will emerge.

Weaknesses like overreliance on third parties or "human factor" need to be identified along with the risks. Employees can cause, either advertently or inadvertently, loss of privacy event or a large IT security event. Even though the best-designed internal control system might not be able to prevent them, but businesses need to adopt a 'think-tank' approach to tackling risk, and create a culture of cyber security. This is possible when different stakeholders share knowledge, implement a crisis/breach response plan and test it thoroughly.

No company can be 100% secure from cyber risks, even after best internal controls in place. This makes cyber insurance to be considered as an integral part of company's active security strategy. This should include inputs from all levels of offices, Board of Directors, CEO, CISO, CIO, CFO, IT leadership, risk management team and legal experts.

The trend and need for securing Cyber Insurance is undeniable, and the best approach is not a standard insurance package to be availed. Each company should follow a thorough process to secure coverage that will ensure cover for most likely cyber risks they face.

VIII. Scope for Further Research

Availing Cyber Insurance is a very complex process. It involves, a cyber security team, evaluation of risks to the business; a specialized broker to evaluate company's risk and to broker a deal with Cyber Insurance underwriters. Furtherresearch into understanding and explaining the process to avail Cyber Insurance, comparison of various insurers, their offerings vs. what the industry needs is required for all sizes of companies.

References

[1] Center for Strategic and International Studies. (2014). Net Losses: Estimating the Global Cost of Cybercrime. United States: McAcfee

[2] Dobie, G. (2015). A Guide to Cyber Risk. Allianz Global Corporate & Speciality. September 2015

[3] Edelman Privacy Risk Index. Edelman. November 2012

[4] FireEye. (2016). Cyber Insurance: A Growing Imperative.

[5] Friedman, S., Thomas A. Deloitte Center for Financial Services. (2017). Demystifying cyber insurance coverage: Clearing obstacles in a problematic growth market. Deloitte University Press.

[6] Ishaq, S. K. (2016). Cyberinsurance: Value Generator or Cost Burden? ISACA Journal. Volume 5, 25-31

[7] O'Hearn, S. et.al. (2015). Insurance 2020 & beyond: Reaping the dividends of cyber resilience. PricewaterhouseCoopers.

[8] Ponemon Institute. (2015). 2015 Global Cyber Impact Report. Aon Risk Services.

[9] Speech by John Nelson, Lloyd's Chairman, at the AAMGA, 28 May 2015. https://www.lloyds.com/lloyds/press-centre/speeches/2015/05/vision-2025-and-aamga