inotes Newsletter from India's Leading Insurance Broking House
July 2017

Summary

Issue # 54

Message from the Editor

Dear Readers

It is with great pleasure that I present to you the latest edition of *i-notes*.

Our focus for this edition is on the very dynamic and increasingly complicated cyber risk exposure. With the lifeline of any economy being the financial sector of the country, we have focused our attention for this issue on the impact that Cyber Risk exposure has on the banking and financial industry of India.

The Reserve Bank of India has reported 16,468 instances of financial cyber-crime in the year 2015-16. According to the National Crime Records Bureau 11,592 cases of cyber-crime were registered in India leading to 8,121 arrests in the year 2015-16. The recent attacks of WannaCry and Petya ransomware / malware have also impacted various government departments and brought to surface the increasing vulnerabilities that we are exposed to. We have worked towards giving you a quick insight into what the risk exposures are and the extent of damages that it can cause. We have also highlighted how cyber insurance can play a significant role in reducing the burden on the balance sheet of the organization. I would like to thank Mr Kiran Lokhande from Bajaj Allianz General Insurance Company Limited, for sharing his views and thoughts on this topic with us.

Coming to the Insurance Industry, as always the industry has been seeing it's share of changes with the Agriculture sector growing at over 200%. With almost 9 new reinsurers setting up offices in India, the Indian Insurance Industry is becoming a more exciting market to be part of as it now opens a whole new world of opportunities for all stakeholders.

I do hope you enjoy our latest edition of i-notes and would welcome your feedback and suggestions on what you would like to read in our coming editions of the newsletter.

With regards,

Deepali A Rao
Editor - *i-notes*

Cyber Crime & Cyber Insurance

Introduction

Almost half the world population are connected to the internet today. When one observes the speed with which the online movement is catching on, it is only surprising to note that there is still over 51% of the population still to be connected. However, it is only a matter a time when that becomes a reality. The number of Internet users in India alone is expected to reach approx. 465 million by June 2017, up 4-8% from 432 million in December 2016, a report from the Internet and Mobile Association of India and market research firm IMRB International said. The report suggests that the overall Internet penetration in India is at 31% currently.

The Internet or the Online way of life is not limited to technology freaks; in fact, those who don't opt for the online mode of payments / shopping / reading... or in short living, are considered a freak...at least in urban India. The wave of smartphones has acted as a catalyst to this tremendous internet growth and rural India is also very quickly adapting to the internet way of life. The Digital India movement is another strong catalyst in this growth story.

With the increasing dependence on Internet, there is also an equal increase in the victimization of internet users.Hacking, Phishing, Malware and spyware are some of the common cybercrimes that people are exposed to. While the victims are the end users of the internet, the onus of preventing victimization is that of the service provider. Cyber-Crime is being considered a serious threat to the nation's economic growth as maximum instances of the same are being observed in financial institutions. With programs for financial inclusion, digitisation of the economy and increased use of smartphones, online transactions are already quite popular among the urban Indian population. In recent months, with the SMAC format (social, mobile, analytics and cloud) driving innovation in the banking sector, the security imperative is even more compelling with regard to preventing data theft and checking financial fraud. An increasing number of users of online services leads to an increased risk of cyber-crime.

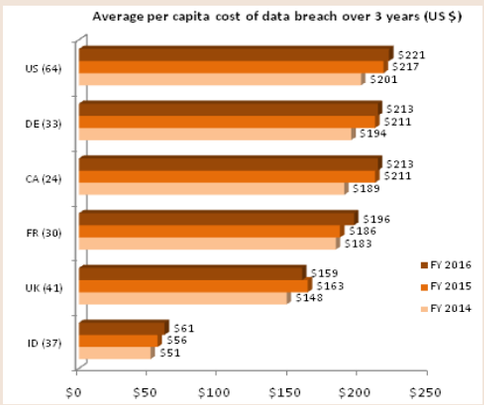
In addition to the financial fall out of cyber-crime, organizations also need to deal with the damage caused to their brand image and their market reputations due to these events. Not to mention the regulatory fall out depending on which jurisdictions the organizations are operating out of. Most countries insist on mandatory notification of data breach to the regulators as well as to all end customers whose information may have been compromised. All of this leads to a huge load on the balance sheet of the organization. The fear of having their vulnerabilities exposed to the market at large has made many organizations withhold information regarding minor data breaches or cyber-crime events. However, knowledge sharing within the industry, awareness campaigns by regulatory and government bodies & peer group experience has increased awareness in the industry & has helped to address this fear to some extent. Corporates now are geared towards having enhanced security features as well as having well-crafted cyber response plans in place to help manage and mitigate this risk. However, have they adequately addressed their risk transfer options?

(Contd... 02)

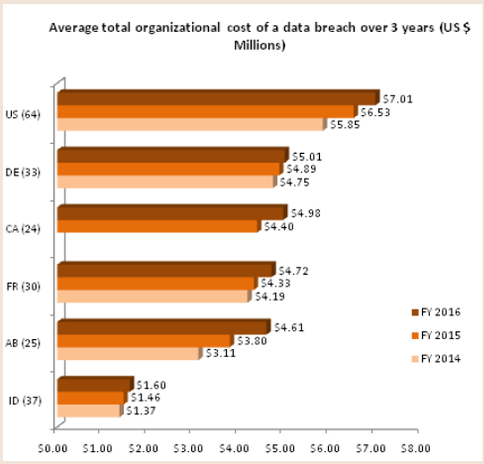
Statistics – Cyber-crime – World Vs. India

Before proceeding further on Cyber risk management, let us look at some key statistics on the financial impact that cyber-crime incidents have had worldwide. While the Ponemon Institute have analyzed information across a wide range of countries, we are giving you information specifically of where India stands Vis-à-vis the top five countries globally facing the maximum impact of cyber-crime.

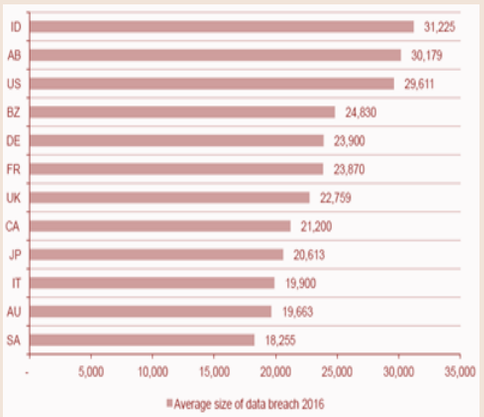
The average per capita cost of data breach over 3 years (Measured in US$)*



The average total organizational cost of a data breach over three years(Measured in US$ millions)*



The average number of breached records by country*

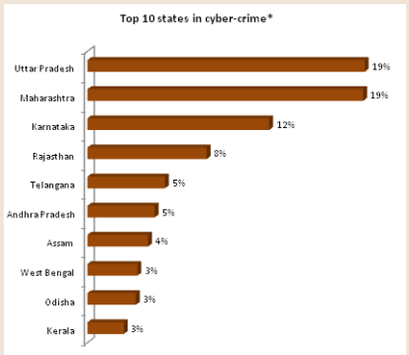


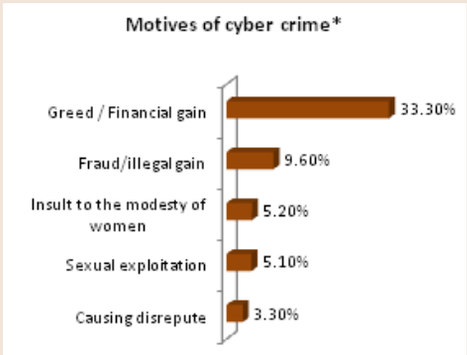
Source: 2016 Cost of Data Breach Study:Global Analysis by Ponemon Institute

Statistics -Cyber-Crime in India*

Cyber Crime Statistics				
	Under IT Act	Under Indian Penal Code (IPC)	Under Special & Local Law (SLL)	Total
2014	7,201	2,272	149	9,622
2015	8,045	3,422	125	11,592

- Cases of cyber-crimes (IT Act + IPC sections + SLL crimes) have increased by 20.5% in 2015 vis-a-vis 2014.
- Out of the total cases reported under IPC relating to cyber-crimes, majority of cases during 2015 were reported under Cheating (65.9%).
- Under IT Act, majority of cases reported in 2015 were under computer related offences (under sections 66 to 66E) accounting for 81.6% (6,567 cases) of total cases under IT Act during 2015.
- During 2015, 33.2% of cyber-crime cases reported were for greed/financial gain (3,855 cases) followed by fraud/illegal gain with 9.6% (1,119 cases) and insult to the modesty of women with 5.2% (606 cases).





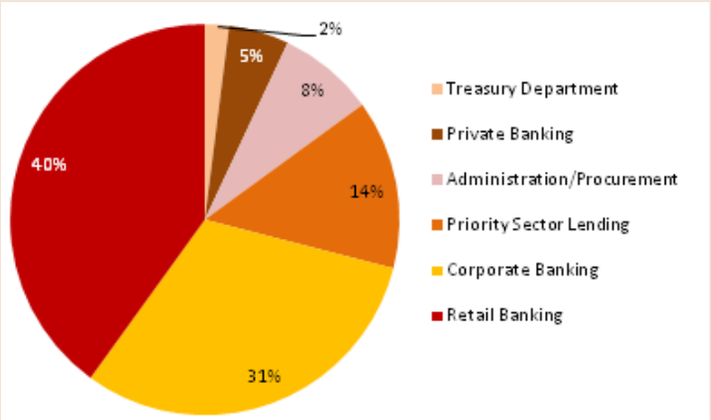
Source: National Crime Records Bureau

Cyber-Crime & Financial Institutions

Financial institutions are ripe for cyber-attacks because of the breadth of personal and business data embedded within their networks as well as financial information.Over the past few years, the global cybercrime landscape has changed dramatically, with criminals employing more sophisticated technology and greater knowledge of cyber security. India has also been a target of such cyber-attacks.

Important observations from Reports by Deloitte, PwC and KPMG on cyber-crime and frauds in the financial services sector including banks:

Instances of cyber-crimes observed in certain banking functions*



The exponential growth in digital payments in India and the push towards a cashless economy has renewed focus on the need to strengthen financial cybersecurity. Banks and financial institutions are extremely vulnerable to various forms of cyber-attacks and online frauds. India has steadily moved up the ranking for countries with the highest number of financial Trojan infections over the past three years. At least ***40% of Banking, Financial Services and Insurance ('BSFI') businesses*** have been attacked at least once.

(Contd... 04)

Interview - *Insurer*

In this issue, we speak to **Mr. Kiran Lokhande,** Head, (Liability Underwriting), Bajaj Allianz General Insurance Company Ltd., on his views on 'Cyber risks and insurance'.

What are the new cyber-risks that have emerged in the recent years and how has the insurance industry responded to them?

The cyber risks have been evolving every year and the preparedness of various Industries and Insurance companies is also getting revamped with every new situation. The latest risk is extortion and ransomware and the recent example of a large scale impact has been Wannacry.

What is the key difference between a commercial crime and Cyber insurance policy? What are the available options for 'Cyber insurance' in the market?

A commercial Crime Policy and a Cyber Data Protection Insurance policy are two different policy forms. The Market understands few difference between the two coverages.We have highlighted the purchase of both these policies together as Cyber data Breach exposures could be only to specific Industries. The Insurance Industry is actually promoting a combination of Professional Indemnity, Commercial Crime and Cyber to offer a full proof coverage of all risk elements.

What according to you are the biggest barriers to an organization's purchase of cyber insurance?

- Non Identification of need to buy such a policy
- As per client the IT framework and IT security policies are strong and sufficient
- No losses seen by clients which has harmed their balance sheet

What are the key recommendations you would give organizations considering the purchase of cyber insurance?

- Review policy wordings of the Cyber product
- Buy basic limits the first time and keep enhancing on every renewal
- Check for sub limits within coverage
- Review deductibles for business interruption

What does the future of cyber risk insurance look like?

Cyber Insurance shall be a new age product which will be useful for all business sectors due to digitization initiatives worldwide. A far as the policy form is concerned it will evolve with time and shall be a flagship product within Liability Insurance space

"Views expressed herein are purely personal and do not reflect the views of the Company"

Some Common Cyber Security Threats

- Botnets: Software robots/'bots' are used to create an army of infected computers (known as 'zombies') that are remotely controlled by them
- Denial of Services (DoS): a machine or network resource is made unavailable to its intended users
- Distributed Denial of Services (DDoS): A malicious user gets a network of zombie computers to sabotage a specific website or server
- Distributed Reflection Denial of Service Attack (DrDoS): A reflection of distributed services and disabling the target system connected to a network
- Data Theft: information is illegally copied
- Data alteration / destruction: making unauthorized modifications to code/data, attacking its integrity
- Hacking: Gaining unauthorized access to the computer
- Malware: Injecting malicious software such as viruses, worms, Trojan horses, spyware and adware
- Ransomware: Restricting access to your computer/ your files & demand payment for the restriction to be removed
- Phishing: using electronic communication to lure individuals to divulge sensitive information
- Spoofing: used in conjunction with phishing to steal the information
- Pharming: user is directed to a malicious and illegitimate website by redirecting the legitimate URL
- Small businesses should buy cyber insurance
- Asia: Most companies in region lack cyber insurance before WannaCry attack

A ***six-fold increase in credit and debit card fraud cases*** has been reported in the same period. In addition to core banking, additional services like e-banking, ATM and retail banking are also increasingly vulnerable to cybercrime. ***Mobile frauds are also expected to grow to 60-65% in 2017***, which is especially alarming because 40-45% of financial transactions are being conducted on mobile devices today.[1]

Cyber-attack - Financial institutions - Global Examples

- June 2017 – 'Petya Ransomware Attack' – affected 65+ countries
- May 2017 'Wannacry Ransomware attack' – affected 74+ countries including India
- 2016-Bangladesh Bank attack - $951 million
- The 2016 SWIFT Hack - $81 million loss
- 2015 – The Carbanak Gang Robbery attack – Russia and Ukraine - $1 billion
- The 2014 JP Morgan Data Breach - affected millions of people and 7 million businesses—a total of 83 million customers

Cyber-attack-Indian banking sector- (past year):

- June 2016- the SWIFT systems of 4 Indian banks were targeted
- October 2016- the largest data breach in the country- 32 lakh debit cards-cyber-malware attack
- Early 2017- Hackers infiltrated the systems of 3 government-owned banks
- Wannacry Ransomware attack.

The top 51 banks in India have lost INR 485 crore from April 2013 to November 2016, finance ministry data showed. Of this, 56% was lost due to net-banking thefts and card cloning. As per estimates, there are at least 15 ransomware attacks per hour in India and one in three Indians fall prey to it.[2] A total of 39,730 cybercrime incidents were reported in India during the first 10 months of 2016, as against 44,679 and 49,455 cases observed during the years 2014 and 2015, respectively, according to an Assocham-PwC joint study.

The need for increased focus on cybersecurity in banks follows not only domestic incidents but global developments as well.

Cyber-crime and Insurance

According to a recent study by Gartner Inc. the IT Spend by the Indian banking and security firms is expected to reach almost USD 8.9 Billion in 2017 which is a 9.7% increase over last year. While this is certainly encouraging news for consumers, there is another key spend area which needs focus to ensure that organizations can get back to their feet within the minimum possible time frame in the worst-case scenario of a cyber-crime incident. In this section, we have focused on one of the key risk transfer solutions for the increasing risk exposure to financial institutions due to cyber-attacks i.e. Cyber Insurance. In order

to clearly articulate the effectiveness of the insurance product we are taking a step back to clearly understand what really a cyber-crime entails and when does the insurance policy truly become essential to have.

Cybercrime refers to any illegal activity that involves a computer/network-connected device; these are typically categorized into: crimes in which the computer system is the target (hacking), crimes in which the computer is used as a weapon (Dos), and crimes in which the computer is used as an accessory to a crime (storing of illegal data).

Cyber-crimes result in huge monetary losses which are incurred not only by the customer but also by the financial institution ultimately leading to economic losses to the nation. Non-monetary cyber-crime occurs when viruses /malware are created and distributed on other computers and/ or confidential information is posted on internet. The most common are phishing and pharming.

Threats to financial institutions include two types of cyber-crime:

- ***'Cyber- dependent'*** crimes such as pharming, phishing, spoofing, hacking, Denial of Services (DoS)/ Distributed Denial of Services (DDoS) / Distributed Reflection Denial of Services (DRDoS) attacks which are not possible without the use of the internet.
- **Cyber-enabled** (or 'cyber-assisted') crimes which are 'traditional' crimes – such as fraud, robbery and extortion – which are facilitated and made easier by technology but would still take place if the technology were not available.

  Financial institutions need to have strategies in place that allow them to respond to and understand both these types of threat. Information which is available online is highly susceptible to be attacked by cyber criminals and due to risk concentration. Thus, operational risks which were historically frequency losses are now turning into severity events.

  This change in risk events have a direct impact on the insurance products available to cover the same. Where previously insurance products were largely used for protecting frequency events, we now have an insurance product which can also protect severity events.

Constraints in the available standard policies are:

- Commercial General Liability: The policy does not provide cover for loss/damage to electronic data. Losses associated with unauthorized access by third parties are also excluded.
- Crime Insurance: Provides coverage for loss of money, securities, stock or other property caused by infidelity of employees and third parties

20 Eye-Opening Cybercrime Statistics

Cost of a Data Breach

1. The global cost of cybercrime will reach $2 trillion by 2019, a threefold increase from the 2015 estimate of $500 billion.
2. The cybercrime cost figure above may be the tip of the iceberg. According to "The Global Risks Report 2016," from the World Economic Forum, a significant portion of cybercrime goes undetected. This is particularly true in the case of industrial espionage and the heist of proprietary secrets, because illicit access to sensitive or confidential documents and data is hard to detect.
3. According to the Identity Theft Resource Center's (ITRC) "ITRC Data Breach Report," more than 29 million records were exposed in 858 publicized breaches across sectors including financial, government, health care and education.
4. According to the Ponemon Institute's "2016 Cost of Data Breach Study: Global Analysis," which queried 383 organizations that suffered at least one breach in 2016, the average cost per breach was $4 million. That figure rose to $7 million in the U.S.
5. The same study found that the cost per record stolen averages $158 globally, but tops $220 in the U.S.
6. Due to the intensity of compliance and regulations, the costs per breach to organizations in the health care and financial services sectors top all other industry groups, according to the Ponemon study.
7. The financial hit resulting from theft of trade secrets ranges from 1 percent to 3 percent of an entire nation's gross domestic product (GDP), according to IDG's "Global State of Information Security Survey 2016." The cost ranges from $749 billion to $2.2 trillion annually.
8. Last year, IDG detected 38% more cybersecurity incidents than the year prior.
9. 48% of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest.

SMB Struggles

1. Small and midsized organizations (SMBs), defined as those with 100 to 1,000 employees, are hardly immune to cybercrime — actually quite to the contrary. According to Keeper Security's "The State of SMB Cybersecurity" report, a staggering 50% of small and midsized organizations reported suffering at least one cyber-attack in the last 12 months.

Cyber Crime & Cyber Insurance .... Contd. # 3

- Errors & Omissions: It protects for financial losses resulting from a failure of service delivery only. Trigger has to be a loss to a third party; first party losses are excluded.
- Property Insurance: covers tangible property wherein a loss must be caused by a physical peril. Data is neither a tangible property nor caused by a physical peril, hence not covered. Moreover, a technology failure need not necessarily cause a physical damage to property which is a pre-requisite for coverage under the policy.

There are policies available which have an exclusive section dealing with crime committed using electronic equipment or the internet. The most common one is the Bankers indemnity policy which has a specific section in the coverage which deals with "Computer crime coverage". There is also an exclusive cyber insurance policy which is available in the market today. While there are some overlaps in coverage, there are significant differences which make the cyber Insurance cover more reliable and robust to cater to the growing menace of cyber-crime.

The computer crime insurance gives more weightage to the first party loss. This means the said policy would get triggered if the insured business experiences a financial loss because of computer systems or networks being compromised, receipt of fraudulent transfer instructions or any other similar event. Financial loss caused directly as a result of third-party computer crimes are covered, such as the hacking of the Insured's network or systems, the planting of a virus designed to illegally transfer funds out of an account as well as the loss

[1]*https://ccgnludelhi.wordpress.com/2017/02/08/cybersecurity-in-the-financial-sector-an-overview/*
[2]*http://tech.economictimes.indiatimes.com/news/internet/rbi-tries-to-close-gaps-in-cybersecurity-of-state-owned-banks/56727413*

(Contd... 05)

2. The average cost of a data breach involving theft of assets totaled $879,582 for these SMBs. They spent another $955,429 to restore normal business in the wake of successful attacks.
3. For these SMBs, 60% of employees use the exact same password for everything they access. Meanwhile, 63% of confirmed data breaches leverage a weak, default or stolen password.

Cybersecurity Spending & Resources

1. In 2016, 62% of organizations used managed security services for at least part of their cybercrime defenses, according to PwC's "The Global State of Information Security" report.
2. Just half of the global organizations PwC surveyed reported that they already use advanced big data analytics to model for and identify threats. Meanwhile, machine learning techniques are adding significant muscle to fraud detection and application security efforts.
3. Global spending to combat cybercrime will top $80 billion this year, with organizations increasingly focusing on detection and response because taking preventive approaches have not been successful in blocking malicious attacks.
4. Spending on cyber insurance has swelled, primarily in the U.S., from $1 billion two years ago to $2.5 billion in 2016. Experts expect dramatic growth in the next five years as the insurance concept spreads globally.

Preparedness and Response

1. Only 38% of organizations surveyed for ISACA's "2015 Global Cybersecurity Status Report" believed they were prepared to meet the onslaught of sophisticated cybercrime.
2. Of the 1,000 IT leaders polled for Invincea's "2016 Cyberthreat Defense Report," three-quarters reported that their networks had been breached in the last year, and 62% said they expect to suffer a successful cyberattack at some point this year.
3. Phishing is a well-known cybercrime technique that involves defrauding an online account user by posing as a legitimate entity. According to the Verizon DBIR, 30% of phishing emails are actually opened, and 12% of those targeted click on the infecting link or attachment.
4. An Osterman Research survey of 540 organizations in North America, the U.K. and Germany revealed that nearly half had sustained ransomware attacks in the last year.

Source: securityintelligence.com

Cyber Crime & Cyber Insurance .... Contd. # 4

of electronic data and information. However, first party expenses relating risk mitigation and evaluation are not covered.

A Cyber Insurance policy provides the right mix of First party losses, expenses and third-party liability coverage; making the policy more cost effective and comprehensive to the insured.

Cyber Insurance

Cyber insurance as a product is only 2 decades old. The product offerings have been undergoing constant variations in order to keep up with the changing risk environment. Fundamentally, cyber insurance is an insurance product used to protect businesses from Internet-based risks and, more generally, from risks related to information technology infrastructure and activities. Covered losses today fall into two categories: First-party losses & Third-party losses. It is designed to protect organizations against a wide range of first and third party related losses occurring out of cyber exposures associated with e-business, internet, networks and information assets.

A Cyber Insurance has its roots in the 'Errors and Omission Policy'. It helps an organization to mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach. Though a Cyber Insurance cannot protect the organization from cybercrime, it can keep the business on stable financial footing when a significant breach occurs.

(Contd... 06)

Small businesses should buy cyber insurance

Source: The Times of India

Small businesses are, finally, waking up to the threat posed by cyber-attacks. After the WannaCry ransomware incident, they are turning to cyber liability insurance to safeguard themselves against this risk. Earlier, these businesses only insured physical assets. But now they are realising the worth of their data, an intangible yet perhaps the most crucial asset. If data gets stolen or destroyed in a cyber-attack, it can cause great harm, both to the business and to its customers. The latter could even sue the firm for the damage they have suffered.

Asia: Most companies in region lack cyber insurance before WannaCry attack

Source: The Asia Insurance Review

Many companies outside the United States may lack cover WannaCry computer-system attack, leaving them potentially with millions of dollars of losses because there has been relatively little take-up of cyber insurance, reported Reuters citing insurers.Cybersecurity experts said the spread of the virus which locked up more than 200,000 computers in more than 150 countries - had slowed, but the respite might only be brief. The overall cost of getting businesses going again could run into the billions of dollars, with companies in Europe, including Russia, and Asia particularly vulnerable.Nearly 9 out 10 cyber insurance policies in the world are in the US, according to Mr Kevin Kalinich, global head of Aon's cyber risk practice. The annual premium market stands at US$2.5-$3 billion.The biggest reason for the larger penetration in the US, said Mr Bob Parisi, US cyber product leader for insurance broker Marsh, "is that the US has been living with state breach notification laws for the past 10 years."

No insurance cover for using pirated, outdated software

Source: The Times of India

Chennai: With more than 50% companies in India using archaic versions of Windows XP operating system, it makes them vulnerable to cyber-attacks like WannaCry — the fallouts of which will not be covered by insurance. However, even if the company is using original software, such attacks might not be covered unless a separate add-on cyber insurance cover is bought. This type of insurance normally is reinsured because the extent of loss cannot be ascertained.Insurance companies say takers for cyber insurance in India are predominantly banks, other financial sector entities, IT companies, pharma and auto manufacturers.

This year, slew of insurance IPOs await investors

Source: Money Control

The insurance sector, which otherwise has been a quiet participant in the initial public offering (IPO) of companies, will have about three new listed entities by the end of this financial year. ICICI Prudential Life Insurance was the first listed insurance company in the country, being listed in 2016.While the initial plan was to have insurance companies list on the stock

News Titbits

exchanges once they complete ten years in business, not all insurance companies were in favour of this. Hence, this was not made mandatory for insurers unlike in the banking sector where listing is compulsory across different categories of banks.As per regulatory norms, an insurer will have to post profits for three consecutive years and be in operation for atleast 10 years for it to get permission to list.New India Assurance and General Insurance Corporation of India (GIC Re) will be the first set of non-life insurers to bring out their IPO in this financial year. The initial process of the IPO has already begun among the insurers who expect the process to be completed in the next 6-8 months.

Insurance sector will adjust to GST rate

Source: The New Indian Express

IRDAI chairman T S Vijayan has said that though the newly introduced goods and services tax (GST) has raised the tax rate for the insurance sector to 18%, the sector will adjust to it."GST of 18% is levied on the insurance sector, which is a hike from the earlier rate of 15 per cent tax on insurance products. Though the higher GST rate would increase the burden, insurance industry will adjust to the new GST and will keep growing," he said.

Fire insurance premium may go up from July 1

Source: The Hindu Business Line

From 1st July 2017, fire insurance premium may go up since the IRDA is trying to check the insurance players from deep discounting in premium to gain market share. A new set of burning cost 'referral' rates from the Insurance Information Bureau is going to be applicable from July 1 and that could see premium going up substantially in several 'occupancies'. "But the changes being introduced could impact differently on each occupancies on insurance companies," said Mr. KB Vijay Srinivas, Chairman and GM of Assocham's insurance council. "Our new set of reference rates for fire will be applicable from July 1 but these are not compulsory on insurance companies," said Mr. Kunnel ,CEO of Insurance Information Bureau.

Crop insurance sees 288% growth in business in FY17

Source: Money Control

Crop insurance business, driven by the government-backed Pradhan Mantri Fasal Bima Yojana (PMFBY) saw a 288% growth in premiums for the financial year ended March 2017 (FY17).The segment saw premiums of INR 20,611 crore in FY17 as compared to INR 5,310 crore collected In FY16.The crop insurance had a market share of 5.5% in FY16 that grew to 16.1% in FY17.Privately held insurers collected premiums of INR 9,865 crore in the crop segment while PSU insurers collected INR 3,683 crore. Agriculture Insurance Corporation of India (AIC) collected INR 7,064 crore in FY17.The PMFBY scheme will see further growth this year as the government has announced a higher Budget allocation of INR 9,000 crore for the scheme. For FY17, the allocation was INR 5,500 crore.

Cyber Crime & Cyber Insurance .... Contd. # 5

A common policy framework is as follows:

Cyber Liability Coverage	First Party Expenses	Regulatory Costs
- Loss or breach of client data	- Business Interruption	- Cost of investigation
- Privacy breach	- Restoration & Response Costs	- Administrative fines & penalties
- Defense cost & settlement costs	- Monitoring & Mitigation Costs	- Legal Expenses

Some insurers may offer ***business interruption, extortion, multi-media liability*** etc. as optional covers.

Different organizations have varying needs, thus cyber insurance policies can be customized to include any or all of the above coverage. Cyber insurance is still evolving as is cyber risk. Organizations tend to not report the complete details and impact of the breaches as they fear it would damage the trust of customers. Sometimes the lack of reporting is purely out of ignorance about the gravity of the situation as well as the available remedial measures. This acts as a huge constraint to the underwriters resulting in them having access to limited data on which to determine the accurate financial impact of attacks.

As businesses wake up to the need to reduce their risk, the experts expect the global cyber insurance market to grow from $2.5 billion today to $5 billion in annual premiums by 2018 and at least $7.5 billion by the end of the decade.[3]

Conclusion

Cyber- attacks could be in different forms and no organization today can escape it. Earlier (cyber) threats were of nuisance value, now they are disruptive and may become destructive. Crisis response and recovery strategies will have to step up along with the increased digital footprint. Security awareness of all the stakeholders will be a vital pillar. However, the pertinent point related to 'Cyber Attack' is how will an Organisation respond; not if a cyber-breach happens, but when a cyber-breach happens. Therefore, companies must have an up to date and effective incident response program in place. More sophisticated the technology, more sophisticated is the methodology of breach / attack. Organizations implementing new technology will need to have a breach response system in place which is five steps ahead of the technology itself!

As experts say, Cyber risks can only be combated through proper risk mitigation and risk transfer strategies, it can never be completely eliminated as there is a huge gap between the nature of new threats and the capabilities available to detect and monitor / stop attacks. Although IT security can provide a preventive measure against cyber-crime, it is impossible to ensure complete protection, hence preparing for the threat makes a huge difference. In the battle against cybercrime, companies should use a combination of technology for risk management and insurance for risk transfer.

Cyber insurance can be an extremely valuable asset in an organization's strategy to address and mitigate cyber security, data privacy and other related losses. However, the lack of standardized policy language presents a challenge to the customer in choosing the right product and that is where the insurance broker plays a key role by partnering with the organization to assist, help and structure a comprehensive program.

[3] *PricewaterhouseCoopers. Cyber insurance market set to reach $7.5 billion by 2020.*

News Titbits

DHFL General Insurance to start operations soon

Source: The Business Standard

DHFL General Insurance has received a certificate of registration from the IRDAI and will start its business operations soon.The venture is founded by the investment company, Wadhawan Global Capital (WGC), whose flagship brand is Dewan Housing Finance (DHFL), a listed entity.Mr Kapil Wadhawan, Chairman of WGC and DHFL General Insurance, said that WGC businesses have established a leadership presence across financial services that range from home loans, project finance, SME lending, education loans, mutual funds, and asset management to life insurance."Our general insurance venture would help us in our commitment to offer protection and mitigate the economic effects of illness, accidents, death, disability and disasters," he said.DHFL General Insurance, which is a 100% owned subsidiary of WGC, was incorporated on 5 July 2016. It is the 31st nonlife insurer in the country.

Report Card - MAY 2017

Gross premium underwritten by non- life industry for and up to the month of May, 2017* **(INR crores)**

INSURER	MAY		Growth over the Same Period of Previous Year (%)	APRIL - MAY		Growth over the Same Period of Previous Year (%)
	2017	2016		2017	2016	
New India	1,476	1,232	19.8%	3,647	3,158	15.5%
United India	1,313	1,069	22.8%	2,647	2,471	7.1%
National	1,282	1,165	10.0%	2,569	2,321	10.7%
ICICI-Lombard	949	828	14.6%	2,147	1,939	10.7%
Oriental	799	785	1.8%	1,813	1,786	1.5%
Bajaj Allianz	536	462	16.0%	1,298	1,063	22.1%
HDFC ERGO General	381	239	59.4%	1,141	612	86.4%
Tata-AIG	352	237	48.5%	928	682	36.1%
Reliance General	322	225	43.1%	832	617	34.9%
IFFCO-Tokio	351	381	-7.9%	798	801	-0.4%
Cholamandalam	281	208	35.1%	582	408	42.7%
SBI General	167	157	6.4%	465	351	32.5%
Royal Sundaram	202	178	13.5%	452	382	18.3%
Star Health & Allied	224	160	40.0%	425	303	40.1%
Future Generali	135	135		359	335	7.4%
Shriram General	164	145	13.1%	299	266	12.6%
Bharti AXA General	109	114	-4.4%	217	236	-7.8%
ECGC	98	95	3.2%	184	172	7.1%
Universal Sompo	84	76	10.5%	178	151	17.7%
Apollo MUNICH	85	70	21.4%	161	132	22.1%
Religare	65	43	51.2%	152	105	44.0%
Liberty	61	41	48.8%	149	103	44.5%
Max BUPA	55	40	37.5%	104	80	29.4%
Magma HDI	34	33	3.0%	72	62	17.0%
Aditya Birla Health	5			50		
Cigna TTK	20	15	33.3%	38	26	46.7%
HDFC General (L&T General)	16	44	-63.6%	38	100	-62.1%
AIC	23	83	-72.3%	24	122	-80.2%
Kotak Mahindra	12	4	200.0%	21	6	271.6%
Raheja QBE	5	4	25.0%	10	8	27.7%
PRIVATE TOTAL	**4,615**	**3,839**	**20.2%**	**10,916**	**8,767**	**24.5%**
PUBLIC TOTAL	**4,991**	**4,429**	**12.7%**	**10,884**	**10,030**	**8.5%**
GRAND TOTAL	**9,606**	**8,268**	**16.2%**	**21,800**	**18,797**	**16.0%**

Source: IRDAI

Observations: April –May 2017

- The non-life industry has registered a growth rate of 16% with total premium of INR 21,800 crores upto May 2017 vis-à-vis INR 18,797 crores upto May 2016. The PSU insurers secured INR 10,884 crore, while private players secured about INR 10,916 crore.
- The PSU's have registered a growth rate of 8.5% during the period April-May 2017 vis-à-vis 13% for the same period last year while the private players have registered a growth rate of 24.5% during this period compared to last year's 17.7%.
- The major contributors for the performance during the period April-May 2017 have been: HDFC ERGO with an accretion of INR 529 crores, New India with an accretion of INR 490 crores, National with an accretion of INR 248 crores, TATA-AIG with an accretion of INR 246 crores & Bajaj Allianz with an accretion of INR 235 crores.
- In terms of growth %: HDFC ERGO registered a remarkable growth of 86.4% followed by Cigna TTK @46.7%, Liberty Videocon @ 44.5%, Religare @ 44%, and Cholamandalam @ 42.7%.
- The private players (including stand-alone health insurers) have increased their market share collectively from 46.6% in May 2016 to 50.1% in May 2017 while the PSU's (including specialized insurers) have decreased their market share collectively from 53.4% to 49.9% during the same period.

News Titbits

Acko gets in-principle regulatory nod to start general insurance business

Source: Money Control

Acko General Insurance has received in-principle regulatory clearance to launch a general insurance business in India. The company has received the initial R1 licence and has filed for the second-stage R2 licence with the IRDAI.Acko, set up by Coverfox co-founder Varun Dua, has also raised US$30 million in seed finance, in one of the largest seed rounds for a start-up in India. Coverfox is an online insurance brokerage.Acko will operate as an independent general insurance company with its entire operations offered through the digital platform. It will create products and deliver opportunities in areas where there are gaps such as personalised insurance products based on user consumption behaviour.

Nine reinsurers to set up operation in India, invest nearly $800 million

Source: The Indian Express

Two prominent global reinsurers, SCOR and Axa Re of France, have initiated the process of setting up operations in the country, joining seven other multinational players for a pie in the reinsurance segment. 7 global players — Swiss RE, Munich Re, Hannover Re, Lloyd's, XL Catlin, RGA and Gen Re — have already received approvals from IRDAI. The nine companies are expected to pump in close to Rs 5000 crore to set up their operations. While SCOR, the fifth largest global reinsurer has already started its operations, Axa Re which is for the first setting up branch operations outside its headquarters in Paris, is expecting its final approval from the IRDAI shortly.

Sagarmala to give boost to marine insurance sector: Experts

Source: The Business Standard

The Centre's Sagarmala project will provide a huge boost to the country's marine insurance sector, according to experts from the industry. The prime objective of the project, approved by the Union Cabinet in March 2015, is to promote port-led direct and indirect development and provide infrastructure to transport goods to and from ports quickly and cost-effectively.New India Assurance Chairman and MD G Srinivasan said huge marine insurance opportunities exist in the country given its long coastline, focus on infrastructure development and boom in industrial production and exports.R Chandrasekaran, Secretary General, General Insurance Council, said the Sagarmala initiative has come at a right time as the country is looking at developing its shipping and port infrastructure.The project will bring the latest in marine insurance practices and training methodologies in India and help augment the talent in the insurance industry, he added.

Series of Panel discussion- "Is Group Mediclaim Dying? The writing's on the wall"

A Panel Discussion for the corporate sector– India Insure in association with NHRD

*In mid-June, India Insure co-hosted a series of Panel Discussion on 'Is Group Mediclaim Dying?' in Mumbai and New Delhi along with **NHRD**. The discussion was moderated by Dr. Pallabh Bandopadhyay, a Leadership Architect, Career Coach, Change & Transition Specialist from HR Plus.*

A glimpse from the panel discussion at New Delhi: L to R:
Ms. Neera Saxena – DGM (Health & Misc. Tech.) The New India Assurance Co.
Ms. Amrita Das – AVP, Total Reward & Performance Mgmt. HCL Technologies
Mr. Biplob Banerjee-Exec. VP (HR & CSR), Jubilant Foodworks Ltd;
Mr. Sandeep Tyagi – Director (HR), Samsung Electronics
Mr. Tapan Singhel, MD &CEO, Bajaj Allianz General Insurance Co.
Mr. Vippin Chandra – Director, India Insure

A glimpse from the panel discussion at Mumbai:

Mr. Gaurav Timble, Lead - Rewards and Global Mobility, Deloitte

Ms. Susmita Mukherjee, GM, The Oriental Insurance Company

Dr. PallabhBandopadhyay, Career Coach, Change & Transition Specialist, HR Plus

Mr. Prem Singh, President - Global Human Resources, Wockhardt

Mr. Madhur Jain, Vice-President - Procurement, Citibank

Mr. V. Ramakrishna, Chairman, India Insure

Key Takeaways:

- There is a need for a change and all stakeholders have to do their bit.
- There is a need for a regulator who will be responsible for regulating hospitals as most believed that there are leakages in the system.
- Preventive measures like wellness and other elements need to be considered by the Insured.

Disclaimer

Contact us

India Insure Risk Management & Insurance Broking Services P Ltd.

Ahmedabad	402, Aryan Work Space, St. Xaviers College corner Road, off C.G.Road, Navrangpura, Ahmedabad - 380009. Ph: 079 - 65152255 / 56 Contact: Mr. B. Rajesh email: rajesh.b@indiainsure.com	**Kolkata**	1st Floor, 197, Sarat Bose Road, Kolkata – 700029. Ph: 033-64602097 / 98 Contact: Mr. P. C. Shaw email: pcshaw@indiainsure.com
Bangalore	# 302, 3rd Floor, Gold Towers, Residency Road, Bangalore - 560025. Ph : 080 -41128056/57 Fax - 080-41128597 Contact: Mr. Janardhan Shenoy email: janardhan.h@indiainsure.com	**Mumbai**	**Branch & Corporate Office :** Unit 2, 2nd Floor, Swagat Building, Shraddhanand Road, Vile Parle (E), Mumbai – 400 057 Ph: 022-26104051 / 52 Contact: Mr. Arindam Ghosh email: arindam.ghosh@indiainsure.com
Chennai	Building No.824, Bhandari Towers, 1st Floor, E.V.R. Periyar Road, Kilpauk, Chennai – 600 010. Ph: 044-45566521 Contact: Mr. V. G. Dhanasekaran email: dhanasekaran.vg@indiainsure.com	**New Delhi**	404, Mansarover Building, Nehru Place, New Delhi – 110 019. Ph : 011-41050081 / 82 Contact: Mr. Manikant email: mani.kant@indiainsure.com
Hyderabad	# 405, Archana Arcade, St John's Road, Secunderabad - 500025. Ph: 040-27822990 / 91 Fax: 040-27822993 Contact: Mr. B N Prasad email: bn.prasad@indiainsure.com	**Pune**	Rachana Trade Estates, Offfice No. 5, Law College Road, Main Chowk, Erandwane, Pune - 411004 Ph: 020-25444448 Contact: Mr. Sudhir Kulkarni email: sudhir.kulkarni@indiainsure.com