
inotes Newsletter from India's Leading Insurance Broking House
December 2014

Summary


- Cyber Attacks - not "if" but "when"
- India Insure - Cyber Risk Survey 2014
- Interview - Mr. Harsh Kothari, DSP Blackrock & Mr. Sanjay Datta, ICICI Lombard GIC Ltd.


Issue # 51

## Message from the Editor

Dear Readers

I derive great pleasure in presenting this issue of *i-notes* to our ardent readers.

The devastating floods in Jammu and Kashmir in September and the Cyclone Hudhud that ravaged Eastern India in October have taken a heavy toll on the profitability of non-life insurers with claim payments in excess of INR 4000 Crores. In the aftermath of these catastrophes, expectations are that the industry may want to take a relook at the nat-cat insurance premiums.

On the brighter side, the Indian Insurance Industry has come out with flying colors in Asia's Insurance Industry. Out of a total of 15 categories contested at the 18th Asia Insurance Industry Awards, five were won by players in the Indian Insurance Domain. We offer our congratulations to the winners.

Professional Hackers and Cyber Terrorists have been working overtime to develop various techniques for deployment in Cyber-attacks and a variety of ways to administer them to damage or destroy computer-based information of individuals or on a broader scale infrastructures and establishments. In this scenario, organisations need to build up capabilities for anticipating attacks which are serious, and at times, catastrophic and paving inroads into critical corporate information.

Apart from building up organisational resilience to Cyber-attacks, it will also be prudent for organisations to obtain Cyber Insurance. In this issue, we are carrying an article which elaborates on cyber-attacks and also provides insights into proper structuring of cyber insurance.

Our team had conducted a Survey among a select list of corporates in diverse industries to understand their perception about Cyber Risks. Excerpts from the Survey are being published in this issue for the benefit of our viewers.

Our editorial team had interviewed Mr. Harsh Kothari, Sr. Vice President - Finance & Operations, DSP Blackrock Mutual Fund and Mr. Sanjay Datta, Chief - Underwriting & Claims of ICICI Lombard General Insurance Company. Their views are captured in the Interview Section of this issue.

With regards,

**V G Dhanasekaran**
Editor - ***i-notes***

## Cyber Attacks - not *"if"* but *"when"*

- *21 July 2014: Cyber frauds cost India $870 million in 2013 - Moneylife*
- *24 April 2014: 69% of targeted cyber attacks in India on large companies: Symantec - Economic Times*
- *10 October 2014: Indian companies concerned about cyber attacks - Hindu Business Line*
- *15 September 2014: Data theft threat sees rise in cyber security insurance policies - Financial Express*

### Introduction

Cyber attacks are on the rise with unprecedented frequency, sophistication and scale. They are pervasive across industries and borders. Seemingly, not a week goes by without a reference to cyber risk hitting the mainstream press. In fact, for the first time in the seven year series of the World Economic Forum's Global Risk Reports, "cyber attack" was named one of the five most likely global risks facing business leaders and governments in 2012. With the trend of e-business and online communication catching up, companies are exposing themselves to increased risks of cyber attacks including hacking, malware, cyber terrorism, fraud and identity theft. Cyber attackers can disrupt critical infrastructures such as stock markets / power infrastructure; air traffic control systems; carry out identity theft and financial fraud; steal corporate information, state and military secrets. Anyone can take advantage of vulnerabilities in any system connected to the Internet and attack it from anywhere in the world without being identified. As the Internet and new technologies grow, so do their vulnerabilities.

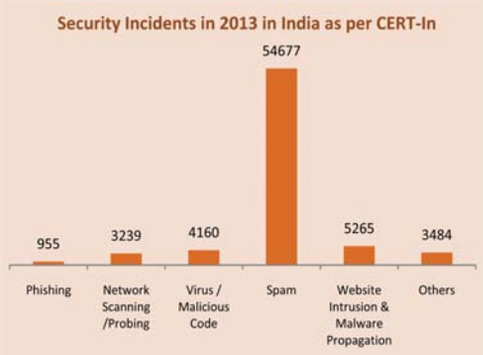
Data is one of the most important assets of a business and with hackers stealing tens of millions of customer details in recent months, firms across the globe are pushing network security beyond the IT department to the board room. According to Symantec's ISTR Report, the total number of data breaches in 2013 was 62 percent greater than in 2012 with 253 total breaches. The complexity of these attacks is also increasing - eight breaches in 2013 each exposed greater than 10 million identities. The likelihood is that the number of breaches reported represents only the tip of the iceberg and there are massive number of small data breaches that go undetected and unreported mainly in countries like India where cyber regulation is not so stringent.


(Contd... 02)

## Cyber Attacks .... Contd. # 1

The 2013 Cost of Data Breach Study, which the Ponemon Institute conducted for IT security provider Symantec, states that " the average global cost of a data breach has gone upto $136 a record in 2012, up $6 from in 2011". The study, says human errors and system problems caused about two-thirds of data breaches, and that contributed to the worldwide increase in costs. Malicious or criminal attacks are most often the cause of data breach globally. Over 37 percent of incidents involved a malicious or criminal attack, 35 percent concerned a negligent employee or contractor (human factor), and 29 percent involved system glitches that includes both IT and business process failures.

The annual report of Indian Computer Emergency Response Team (CERT-In) reveals that they have handled more than 71000 cyber security incidents in 2013 as depicted in the graph.




In 2013, around 2050 people were booked under the IT Act in India and most of the cyber crimes were intended for economic forgery and sexual harassment. In 2013, India ranked fourth in the world by the volume of phishing attacks - which try and trick a user into revealing passwords for official or personal accounts as a way to steal information — and was the most targeted country in Asia Pacific, according to a report by security provider RSA.

### The Impact

The impact of a cyber crime can be classified into many components:

- Loss of sensitive business information
- Loss of intellectual property & trade secrets
- Lost productivity and lost sales including Business Interruption
- Costs for restoration of business
- Irreversible damage to the Corporate Reputation
- Regulator penalties
- Shareholder outcry and litigation
- Class action lawsuits
- Professional Indemnity claims
- Loss of customer trust

Cyber attacks cause an impact on not only the brand value and revenue of the companies but more severely impact the trust of the customers involved due to the loss of sensitive information. Data security breaches can severely impact a company's bottom line.

### What data is at risk?

Cyber criminals target information that can be quickly turned into cash with minimal effort, for example:

- Personally identifiable information (PII)
  - May include any combination of the following: names, addresses, credit card data, phone numbers, age, sex, political affiliation, marital status, fingerprints, blood type, education, employment history, employment, date of birth, financial information, tax information, disability information and zip codes
- Government ID numbers
- Medical records
- Payment card data including account numbers and passwords
- Intellectual Property

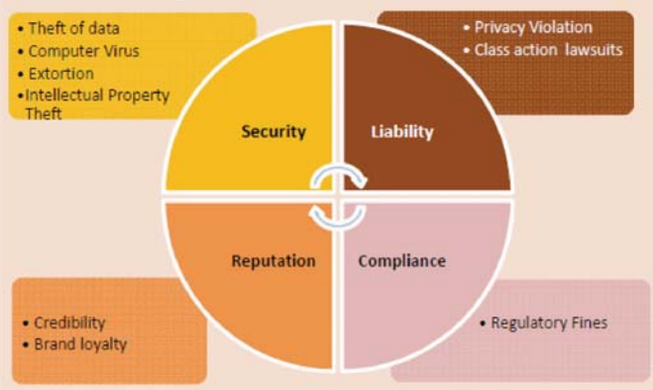
*"There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again."*

Former FBI Director Robert Mueller (2012)

After two monster breaches at large email marketing firms, the definition of Personally Identifiable Information (PII) has got broader and email addresses are now arguably considered PII.

Experts opine that the majority of breaches result from opportunistic attacks rather than organized criminal groups. However, breaches can just as easily happen through lost or mishandled files, unintentional security breaches or illegal behaviour by employees.

### Dimensions of Cyber Risks




*"It is no longer a question of a nation protecting its own security; it is a question of the global community protecting itself."*

Kapil Sibal, Minister for Communications and Information Technology, India (2012)

### Recent regulatory and legal changes

Recent regulation in many countries including US, Germany, France, Australia have imposed stringent reporting requirements as well as penalties for a data breach. Failure to comply and provide privacy and security controls could result in penalties ranging from large fines to jail terms. For example, the US Securities & Exchange Commission (SEC) guidance released in October 2011 indicated that a computer breach should be viewed as a potential material event requiring disclosure regardless of whether the breach involved release of confidential data or not.

While corporates must be mindful of the relevant laws in their own country, when it comes to cyber crimes, borders can become meaningless. If the personal details of a customer who lives outside your country are compromised, your business could be subject to the laws of the customers' country.

### Cyber Security - Legal Framework India

To cater to the cyber security issues, India has implemented IT Act 2000, revised IT (Amendment) Act 2008 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and released the National Cyber Security Policy 2013. Different types of cyber crimes have been described as offences under Chapter IX of the IT Act. Several crimes like hacking, phishing, data theft, identity theft, denial of service, spreading of virus, source code theft, sending lewd SMS/MMS/Email, pornography and disclosure of information by organizations have been looked in detail.

As per the Rules 2011, every "body corporate" that "collects, receives, possess, stores, deals or handles" any information including sensitive personal data and information is required to provide a privacy policy for handling or dealing with such information. The term 'sensitive personal data and information' has been comprehensively defined and includes information relating to financial information, passwords, biometric information and call data records. The Rules impose wide ranging obligations on a corporate regarding usage, collection and transfer of personal information and implementation of reasonable security practices.

But legal experts opine that at present, the Rules construct an incomplete regime that does not adequately protect privacy and for this reason, falls short of internationally accepted

(Contd... 05)

# Interview - *Corporate & Insurer*

Cyber-insurance is relatively new, but it's becoming a critical element of most enterprises' risk management framework. The interview of Mr. Harsh Kothari, Sr. Vice President - Finance & Operations of DSP Blackrock captures his thoughts on how cyber risks and related liabilities are increasing for organizations. The second interview of Mr. Sanjay Datta, Chief-Underwriting & Claims, ICICI Lombard GIC Ltd. delves into issues concerning the cyber insurance market, explaining risks, coverage and pricing trends.

**Mr. Harsh Kothari,** Sr. Vice President - Finance & Operations, DSP Blackrock

To what extent are cyber risks and related liabilities increasing for organizations? How vulnerable are organizations to cyber attacks?

We feel cyber risks have increased many fold in last three years. In our view most of the organizations are vulnerable to cyber attacks.

How would you rate the awareness among Indian corporates on cyber risks and cyber insurance policies? Are Indian organizations fine tuned to the all pervasive cyber risks? Is there a gap on the awareness front?

On awareness amongst Indian corporate on cyber risks and cyber insurance, we think on a scale 1 to 10, it could be 3; it has just started off (beyond IT firms). We feel, a large population of corporate needs deeper understanding on cyber risks, of course the degree of risks will differ for each of them.

What according to you needs to be done to improve the awareness levels of cyber risk?

Industry forums, Insurance companies and insurance advisors need to take the lead in educating (workshops, single pager leaflets) corporates on the various cyber risks they are exposed to and equally important are recent trends in terms of kind of damage; it can cause to the organization.

At what point in time did the Cyber Insurance policy become part of your insurance program and why?

The day management decided to embark on building the online business, it triggered the thought process. Off late, if one notice there are many articles on reporting of cyber attacks, which reflects the risks are increasing with each passing day and they are getting wider in terms of nature of damage it can do and the financial loss it can cause.

Can you please advise our readers on the points to be kept in mind when an organization is purchasing cyber insurance?

Understand the various cyber risks associated in their business and mirror them in terms of the coverage offered by insurance companies.

Do you believe that the Cyber insurance policy available today is aligned to completely meet your requirement? If no, what are the areas of improvement you would look for?

To a large extent yes, we would like to see a crime policy and cybercrime to converge, to avoid any ambiguity from coverage perspective and of course, the commercials, we expect the commercials to become more economical as the market grows.

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

**Mr. Sanjay Datta,** Chief-Underwriting & Claims, ICICI Lombard GIC Ltd.

To what extent are cyber risks and related liabilities increasing for organizations? How vulnerable are organizations to cyber attacks?

In today's data-driven world, every organization irrespective of its size, industry, profile is vulnerable to cyber risk. The question is not 'what if my organization will suffer a breach,' but when. Hackers have defaced Indian websites of government departments and organisations, they have targeted ecommerce sites for ransom, banks have witnessed cyber losses of more than INR 130 cr in three years, cyber risk is no longer a theoretical concept, it's a reality.

According to a recent study conducted by PricewaterhouseCoopers (PwC), the total number of security incidents detected in India was over 1 million last year, which translates to 2,800 attacks per day. These numbers do not represent the incidents which are not reported and have occurred while organizations were unaware of the attack.

Increasingly companies are taking measures to protect themselves. While their technology platforms become more robust, it's just that one little episode that creates havoc - one stolen laptop, one misplaced mobile, one successful hacker, one malicious code or one lost paper record of customer data. And it is this one event that can adversely affect business strategy, its execution and can create enormous financial and reputational consequence for businesses.

How does the market in India fare on the cyber insurance front? Are Indian organizations fine tuned to the all pervasive cyber risks? Is there a gap on the awareness front?

As the horror stories continue to make news, the 'It will never happen to us....' thought is fast disappearing and cyber risk is bringing in fear, uncertainty and concern in boardrooms. Organisations are realizing that Cyber risk is a matter of concern for the risk managers, in-house lawyers, finance, board and not just the IT team. Organisations are now trying to understanding the threat as well as the tools and techniques available to address them proactively, rather being reactive to the risk.

In terms of availability, cyber insurance policy is currently being offered by only three companies. Insurance Companies are witnessing a spurt in enquiries and requests for quotation from companies. The market size in terms of policy count is currently a two digit number but is growing fast.

Insurance is a key part of managing cyber risk. What are the biggest barriers to an organization's purchase of cyber insurance?

Indian Cyber laws are at a fairly nascent stage. Besides, insurance continues to be a 'push' product and 'cost cutting' is high on priority for almost all corporate. These have been the biggest barriers in the proliferation of Cyber market. Developed markets on the other hand e.g. the US have their own privacy breach notification laws and the associated regulatory penalties. Besides they are a litigious society and the regulators are very active. This has led to the US market being world's largest Cyber Insurance policy market.

What considerations should organizations make when evaluating cyber insurance coverage including policy provisions and exclusions?

Following are some points that organisation's should address while buying cyber insurance

- The most important factor to bear in mind is that cyber insurance isn't a means to compensate for weaknesses in an IT security program.
- Although called 'Cyber Insurance', the policy is not an answer to all cyber issues that the organisation faces. The policy offers a specific cover, which is mentioned in the 'Insuring Clause'.
- The list of exclusions can make one wonder, what cover exists in cyber insurance. Develop practical scenarios of cyber exposures to determine if the policy responds to such situations.
- Companies that outsource their IT and other services to third party need to have a firm handle on the third parties' IT controls in addition to their own. Also, the third party needs to be insured under the company's cyber policy.

(Contd... 04)

## Interview .... Contd. # 3

- Companies should have a retroactive coverage for losses that arise from undiscovered breaches that have occurred before a policy purchase.

How would you describe pricing trends for cyber insurance?

Pricing is influenced by many factors namely the size of the company, industry, customer data, loss history, probable loss etc. A very rough estimate would be premiums starting with US $10,000 for US$ 1 million in coverage.

The IT Act in India does not specify the need for any mandatory notification either to the regulator or the affected parties in case of a data breach. Will this 'no-legal obligation' cause organizations to be lax in their approach to data security?

Many of Indian corporate have global footprint, foreign shareholders, customers in various countries etc. Their business contracts require them to address the data protection issues. Corporate (and their number is increasing by the day) have sizeable IT budgets, are investing in IT resources, buying latest network logging and security analytics products.

We read that NASSCOM is in the process of drafting legislation to amend the country's existing Information Technology Act of 2000, with the intention of bringing the data protection regime up to the standard required by the US and the EU. The Indian laws will sooner than later adopt the best practices of the overseas markets.

What changes and developments do you expect to see in cyber insurance over the coming years?

The Cyber policy in its current form covers 'data breaches'. Cyber-related industrial espionage is another concern which typically targets a particular company i.e. malicious attacks on transportation companies, health care equipment, industrial controls, utility companies which can lead to bodily injury and property damage exposures. Covers that can provide insurance for such risks would evolve in the coming years.

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

## News Titbits

**Insurance firms may take Rs 2,400-crore hit due to Hudhud**

*Source : Economic Times*

USA-based catastrophe modelling firm AIR Worldwide has estimated that insurance companies may take a hit of around Rs 2,400 crore due to Cyclone Hudhud which recently battered Andhra Pradesh and Odisha coasts. AIR Worldwide's insured loss estimates assume that an insurance penetration of three per cent for residential lines, 20% for commercial, and 30% for industrial segments.

**Indian insurance sector needs capital infusion of Rs 50,000 crore: IRDA**

*Source : ibef.org*

IRDA said the Indian insurance sector needs capital infusion of Rs. 50,000 crore to expand reach, maintain a healthy capital base and improve solvency standards.

# Report Card - November 2014

**Gross premium underwritten by non life industry for and up to the month of November 2014* (Rs. In crores)**

| INSURER | NOVEMBER | | Growth of November 2014 over November 2013 | CUMULATIVE UPTO NOVEMBER | | % of Growth Upto November 2014 over the period Upto November 2013 |
|---|---|---|---|---|---|---|
| | 2014-15 | 2013-14 | | 2014-15 | 2013-14 | |
| Private Sector | 2563 | 2358 | 8.70% | 22843 | 20903 | 9.30% |
| Public Sector | 3147 | 2732 | 15.20% | 27830 | 25051 | 11.10% |
| Stand-alone Health Insurers | 212 | 158 | 34.40% | 1578 | 1229 | 28.30% |
| Specialized Insurers | 195 | 297 | -34.30% | 2709 | 3123 | -13.30% |
| **Grand Total** | **6117** | **5545** | **10.30%** | **54960** | **50307** | **9.20%** |

**Source : General Insurance Council*

- The non-life industry has registered a growth rate of 9.2% up to the month of Nov 2014. Total premium collected by general insurers up to the month of Nov 2014 is Rs. 54960 crores vis-à-vis Rs. 50307 crores last year.
- The PSU's have registered a growth rate of 11.1% during the period April - Nov 2014 while the private players have registered a growth rate of 9.3% during this period.
- The stand-alone health insurers have registered a stupendous growth of 28.3% during the same period while the specialized insurers (ECGC & AIC) have registered a de-growth of (13.3%).

## News Titbits

**Insurers companies settle Rs 300-crore claims in Kashmir**

*Source : Economic Times*

Insurance companies are busy settling claims in Kashmir, and have so far given out close to Rs 300 crore to people and businesses affected by devastating floods recently. "We have settled nearly 3,500 of around 6,000 claims that we have received, surveyed and paid," said Aijaz A Khan, regional head at Bajaj Allianz, a private insurer.

**Aditya Birla Group announces joint venture with South African firm MMI Holdings Limited**

*Source : Economic Times*

Aditya Birla Group has announced a joint venture with a South African insurance giant to enter India's huge health insurance market. ABG's financial services division has signed a MOU with MMI Holdings Limited, in which the South African company will hold 26% stake, which will be upped to 49% once India's regulatory regime allows this. The transaction is subjected to execution of the respective legal agreements and obtaining the required regulatory approvals, MMI said.

**IRDA to look into price undercutting in group health insurance segment**

*Source : Business Standard*

Speaking at a summit organised by the National Insurance Academy, M Ramaprasad, member (non-life), IRDA, said that IRDA will look into the group-health space, which constitutes 55% of the health segment; retail health makes up the rest. Claims in group health are much higher than in the retail side of the business, he said, adding the high claims, 100% at one point, was a matter of concern. The IRDA is looking into this matter and will look at having higher capital requirements or solvency rates for those insurance companies that quote unviable prices.

**Insurers face mega claim for Bathinda Refinery fire**

*Source : Economic Times*

Insurance companies including New India Assurance, General Insurance Corporation are staring at a hit of Rs 650 crore from a fire that broke out at Mittal-Hindustan Petroleum refinery in Bathinda. The refinery was insured for Rs 7,500 crore under mega risk policy.

data protection standards. Though the Act provides certain kind of protection, more effective mandatory provisions are required to be implemented to protect, preserve and promote cyber security in India.

**Do I have to report loss of data?**

The provisions of the Indian IT Act do not mandate reporting the loss of data either to the regulator or the affected individuals. However, notification can be provided

- As a matter of contract
- Obligations to customers
- Obligations to counterparties / supply chain
- Obligations to investors / stakeholders
- As a matter of reputation management

### The need for Cyber Insurance

In the wake of numerous recent data breaches, much has been talked on cyber liability insurance. As per experts, Cyber risks can never be completely eliminated as there is a stunning gap between the nature of new threats and the capabilities available to detect and monitor / stop attacks. The rising tide of cybercrime can only be combated through proper risk mitigation and risk transfer strategies. For this reason, more and more organizations are assessing insurance options as part of their approach to risk management to ensure they have the most appropriate cover available.

Cyber-insurance is relatively new, at least when compared to other types of property and liability insurance, but it's becoming a critical element of most organizations' risk management framework.

### Gaps in traditional policies

**Commercial General Liability** policies often do not provide cover for loss/damage to electronic data. The triggers are bodily injury, property damage, personal injury and advertising injury. Losses associated with unauthorized access by third parties are also excluded.

**Electronic Equipment** policies typically limit coverage to damage to and/or loss of electronic equipment resulting from an insured peril. Even coverage under 'External data media' limits coverage to the cost of restoring the damaged or corrupted data.

**Crime policy** covers loss of money, securities or other property (e.g. stock) caused by the dishonesty of employees and third parties.

**Professional indemnity** policies only extend as far as the professional service description allows and generally do not provide coverage for cyber exposures. Also very limited cover is provided for first party expense.

Typically companies operating in the IT/ITES sector opt for the below extensions under their Professional Indemnity policy which provides cyber coverage to some extent:

- Unauthorized access, denial of service and Breach of confidentiality (i.e. third party liability)
- Cyber Extension (first party expenses)

However, understanding how insurance applies to cyber risk is becoming increasingly important as traditional policies may leave gaps for cyber liability.

### What is Cyber Insurance?

Cyber insurance is designed to protect organizations' against a wide range of first and third party liability occurring out of cyber exposures associated with e-business, internet, networks and information assets.

There are three fundamental coverages in a cyber insurance policy which may vary between insurers

| THIRD PARTY LIABILITY | FIRST PARTY EXPENSE | REGULATORY |
|---|---|---|
| COVERS LIABILITY FOR<br>• Loss or breach of client data<br>• Privacy Breach<br>• Includes defense & settlement costs | COVERS<br>• Business Interruption (BI) loss<br>• Restoration costs and response costs following a data breach<br>• Including investigation, public relations, customer notification, credit monitoring, extortion costs etc. | COVERS<br>• The costs to investigate, defend, and settle data administrative fines and penalties that may be assessed by a regulator. |

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

All policies are different but typically include cover for a range of First Party risk exposures and Third Party liability exposures. Different organizations have varying needs, thus cyber insurance policies can be customized to include any or all of the above coverage. Coverage is on a world-wide basis.

### Basis of Premium Calculation

Pricing methodology seems to vary by insurer, however it is commonly based upon a blend of

- No. of records held and the type of records kept
  - Personally Identifiable Information
- Sector / Industry classification
- Revenue of the firm
- Organization's approach to Security
  - Security in place to mitigate or prevent data breaches
  - Privacy policy
  - Point of sale technology
  - IT budget dedicated to cyber security

The annual premium for a Rs 10 crore cover is around Rs. 15-20 lakh and Rs. 25-35 lakh for a Rs 25 crore cover.

### Who needs Cyber Insurance?

Companies who should consider purchasing cyber insurance are those who:

- Store personal and confidential information of customers
- Store proprietary company information
- Generate revenue over the Internet
- Share confidential data with third party service providers
- Have a website and publish dynamic content on the Internet
- Store information on a cloud

Cybercrime is not limited to any specific industry though Defense, utilities, energy and financial services remain the top industries globally suffering from cybercrime in terms of annual cost. In India, the uptake of cyber insurance is more among financial institutions, banks and health care providers. Even though the scenario in India does not call for notifying the regulator/customer, the financial institutions will need to incur huge costs on investigation, rectification and restoration of the data breach which is covered under the cyber policy.

### Examples of Publically Reported Data Breaches

**Sony:** Hacktivists ("Anonymous") breach Sony's network, compromise the PII of over 100 million Sony users, and render several crucial components of the Sony network inoperable for days. Sony publicly estimated the total costs in connection with the breach to be approximately $175 million.

**SAIC:** Loss of a computer back-up tape compromised the protected health information and social security numbers, of 4.9 million active military personnel, veterans, and their families.

(Contd... 06)

## Cyber Attacks.... Contd. # 5

**Wiley Rein LLP**: Advanced persistent threat suspected to have originated from Ukraine or China compromised D.C. based business litigation firm and extracted gigabytes of client and employee data.

**Domino's Pizza**: Hackers held Domino's Pizza to ransom after stealing more than 650,000 passwords from its customers in France and Belgium. The group, known as Rex Mundi, said in a post to dpaste.de it had gained access to a vulnerable customer database shared by the pizza firm's European headquarters. It had demanded 30,000 euros (£23,890) from the firm or it will begin publishing the details online.

**ADOBE**: Adobe Systems announced the discovery of a "sophisticated attack" on its network in October 2013 causing exposure of personal information including names, passwords, encrypted credit and debit card numbers of almost 3 million customers. In the months that followed the size of the breach grew to involve as many as 150 million people. Thieves also stole Adobe source code which may enable exploitation of weaknesses in product security. Class action filed in CA Federal Court on November 11, 2013, Halpain v. Adobe Systems, Inc., alleging failure to adequately protect PII, misrepresentation of security capabilities and failure to provide timely breach notification.

**Target**

- Between 27 Nov. and 15 Dec. 2014, attackers used malware to infect point-of-sale registers that stole credit and debit card data. Intruders also set up a control server within Target's internal network as a central repository for collected data.
- Potentially Affected Data of up to 70 million individuals and it included Names, Mailing Addresses, Phone Numbers, Email Addresses, Credit Card / Debit Card data,
- Credibility / Brand Loyalty affected
- NY Attorney General investigation
- Pending Class Action Lawsuits

**Some Indian Cases**

1. A Pune based businessman was allegedly duped of Rs 6.7 lakh after an unidentified man hacked into his email account and sent an email to two of his banks to transfer money.
2. The cyber crime cell of city crime branch has arrested a Delhi resident for alleged involvement in siphoning of lakhs of rupees from the bank account of a Sion businessman. The businessman's firm lost Rs 15.58 lakh from its account last year.
3. Some ex employees of BPO arm of MPhasis Ltd MsourcE, defrauded US Customers of Citi Bank to the tune of Rs. 1.5 crores. An investigation by the bank traced the money to several bank accounts in Pune where it had been transferred electronically.
4. Mumbai police have arrested a student of Second Year Engineering College for duping a Payment Gateway. The accused initially opened a website supposedly to carry out business of web designing. He opened an account with a payment gateway situated in Mumbai under false credentials. He then started browsing the web, specially various chat rooms and Newsgroups to obtain the credit card numbers. He then became his own client and started making payments to his own account using the credit card numbers he obtained from the net of foreign nationals.
5. Using the Sony sambandh website, an order was placed for a Sony Colour Television set and a cordless head phone using the credit card number of an American national which the accused gained while working at a call centre in Noida.

**Conclusion**

As the ubiquity of the Internet continues to transform the way we conduct our business and personal lives with an ever-growing dependence on data and systems; it has also made us more susceptible to 'hi- tech crime'. Considering that we now live in a connected world, the era of insulation is almost over!

Clearly cybercrime has emerged as a serious threat to organizations across the globe and India has had its share of incidences. Most breaches today go unnoticed until long after they occur and the damage has been done. Businesses must take a proactive approach to tackling cyber security rather than waiting for a breach to occur and then acting on it.

Although IT security can provide a preventive measure against cybercrime, it is impossible to ensure complete protection; hence preparing for the threat makes a huge difference. In the battle against cyber crime, companies should use a combination of technology for prevention and insurance for mitigation.

Cyber insurance can be an extremely valuable asset in an organization's strategy to address and mitigate cyber security, data privacy and other risks. But the lack of standardized policy language presents a challenge to the customer in choosing the right product and that's definitely where a broker can add value.

## The India Insure Story

India Insure was conceptualized way before the liberalization of the insurance sector in India. The company is the brainchild of 4 professionals who came in from diverse backgrounds with a dream and a sense of conviction to do something different. Sensing the huge opportunity that existed in the insurance industry post-liberalization; the idea to create a world-class insurance broking firm emerged.

Insurance broking operations commenced in India, in the year, 2003 and India Insure acquired the first insurance broking license in the country, a historical statistic now, but a proud moment for Team India Insure then.

Many milestones have been achieved during this exciting odyssey which began in 1999. From its humble beginnings, India Insure has grown to be a leading provider of insurance & risk management solutions and services, handling the insurance portfolios of around 300 corporates across 9 offices with a headcount of over 100 employees. And with that same pioneering spirit with which it started, India Insure is still expanding and innovating.

Team India Insure stands united by a single, driving passion: *to continue to create value for our customers.*

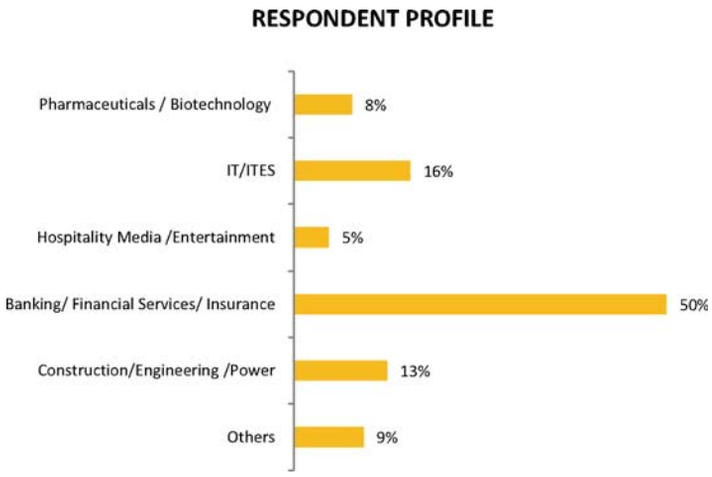
## News Titbits

**Magma HDI General Insurance turns profitable in seven quarters**

*Source : Business Standard*

Magma HDI General Insurance Company has turned profitable in the seventh quarter of its existence beating its own guidance of achieving break-even in the fourth quarter of this financial year. The insurer, which commenced business in October, 2012, made a net profit of Rs 1.7 crore in April-June period.

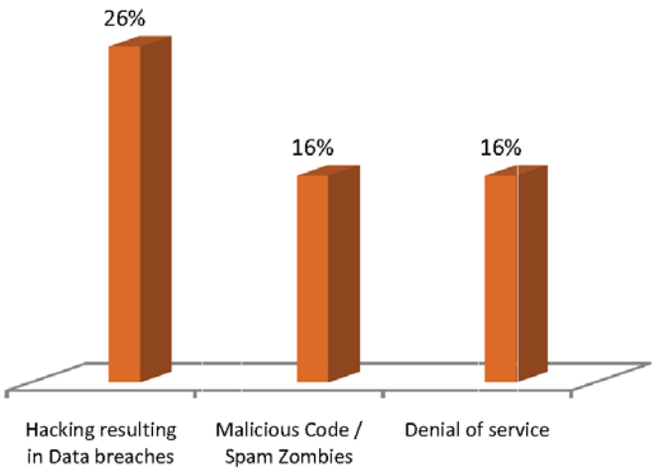
# India Insure - Cyber Risk Survey 2014




**97%**

of managers agree that Cyber risk represents a significant business risk for their company.

## Top 3 forms of cyber threats facing your organization




Hacking followed by Malicious code & Denial of Service attacks have been ranked the top 3 forms of cyber threats facing the respondents.

Malware or Malicious Software refers to programs such as viruses and worms that try to exploit computer systems or networks leading to business disruption, leakage of sensitive data, or unauthorized access to system resources.

Denial-of-Service (DOS) Attack refers to making a computer resource unavailable to its intended users or preventing it from functioning efficiently.

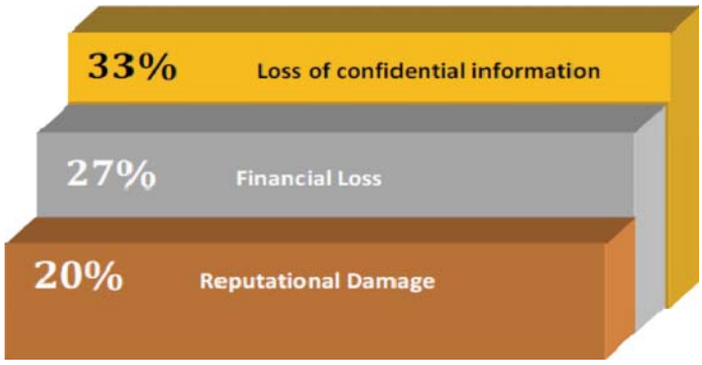
**75%**

of respondents say that they have not been subject to a cyber attack in the past 3 years.

**80%**

of managers say that concern about cyber security has increased in the past 12 months.

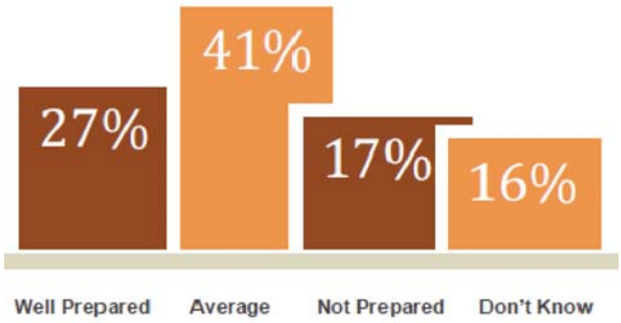
## The single biggest impact of a cyber attack on your organization



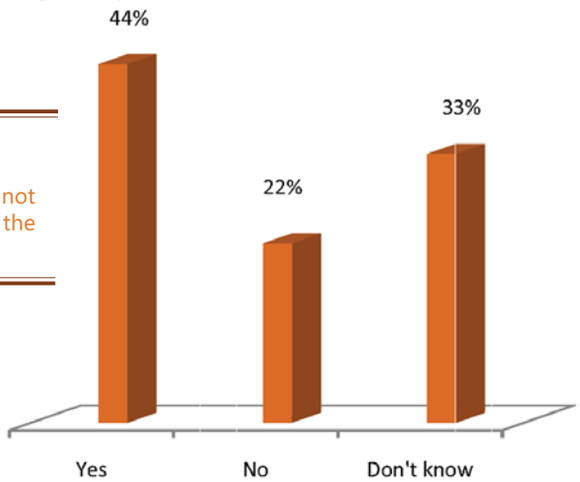

'Loss of confidential information' from a cyber attack is the top concern at 33% followed by 'Financial loss' at 27%.

20% of the respondents are worried about the damage that a cyber attack can cause on their firm's reputation.

## How prepared is your organization to tackle any risks arising from cyber crime?




## Does your organization have a formalized plan outlining policies & procedures for reporting and responding to cyber events?




44% of respondents say that their organization has a formalized plan outlining policies & procedures for reporting and responding to cyber events.

However, it's surprising to note that 33% of respondents were unaware of whether or not their organization has such plan in place.

# Cyber - Risk & Remedy

*A series of Workshop by – India Insure in association with Clyde & Co and Classis Law*

'Cyber' – a word which has become part of our everyday lives and is considered to be a representation of the modern way of life, is also a word which leaves many in the corporate world with sleepless nights. To create awareness about this topic, India Insure organized series of workshop in 3 major cities of India viz. Mumbai, Delhi & Bangalore in July this year; which was well attended by Corporate India.


**Key speakers at the event:**
Mr. Sakate Khaitan - Classis Law, Mr. Kevin Haas - Clyde & Co, Mr. Manoj A.S. - TATA AIG General Insurance, Ms. Deepika Mathur - HDFC ERGO General Insurance, Ms. Anita Pandita- ICICI Lombard, Ms. Deepali Rao - India Insure


The workshop furnished insight for organizations trying to evaluate their cyber risks as well as for those considering the purchase of cyber-insurance.

The year 2013 has come to be known as the year of "Mega Data Breach" as per the Symantec - Internet Security Threat Report 2014. Over 552 Million identities have been exposed in the last year alone with over 10 Mln identities being exposed by only 10 breaches. The statistics gets even scarier when one hears of India being the most likely country to have a data breach.

India Insure has made a small attempt in trying to bring to light the various Risks and Remedies that are currently associated with Cyber threat.


## 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: P. Srinivas Rao email: srinivas.rao@indiainsure.com | **Pune** | Rachana Trade Estates, Offfice No. 5, Law College Road, Main Chowk, Erandwane, Pune - 411004 Ph: 91-9823010457 Contact: Mr. Bhalachandra Bodas email: bodas.b@indiainsure.com |