BIMTECH

PGDM (Insurance Business) - 2014-16

Sub: Global Perspectives in Insurance

(INS-504)

Trimester – V End – Term Examination: December 2015

[Time Allowed: 2.30 Hours] **[Max Marks: 50]**

Roll No: _____

Instruction: Students are required to write their Roll No. on the question paper. Writing anything other than the Roll No. will be treated as **unfair means.** For rough work, please use answer sheet.

Note: ***- Please be brief and relevant in your answers.***
- Section C is compulsory.

Section-A

[There are 5 Questions in this section. Attempt any 3 Questions. Each Question carries 5 marks.]

[3x5=15 Marks]

[A1]
(a) Discuss briefly the three major "global environmental risks" resulting from human activities and related broad risk mitigation measures for these risks. **[4]**

(b) What, very briefly, does "2°C" mean, in the light of the recent discussions in the International Climate Summit in Paris? **[1]**

[A2] Viewed globally, the insurance industry faces significant "disruptors". Relate 5 of such disruptors to the "concerns" felt by insurers. **[5]**

[A3] Critically examine the likelihood and implications of the three major global financial risks (a) large scale cyber attacks (b) massive incident of data fraud/theft and (c) massive misuse of new era technologies like 3D printing and artificial intelligence. **[5]**

[A4]
(a) Discuss the salient features of the mass tort (class action) suits in liability claims especially in U.S. **[3]**

(b) The Govt. of India has filed a class action suit against Maggi in the Consumer Court. Briefly, examine the implications of this step. **[2]**

[A5]
(a) Discuss why the London insurance market is considered unique as compared to other international markets. **[3]**

(b) What, in your view, are the implications of the proposed commencement of operations of the Lloyds group in India? **[2]**

P. T. O.

BIMTECH
BIRLA INSTITUTE

Roll. No. _____

Section-B

[Note: Answer any 2 out of the 3 Questions given below. Each Question carries 10 marks]

[2x10=20 Marks]

[B1] Critically examine the corporate governance liability law in the U.S. especially in the context of business judgment, fiduciary duty of due care and fiduciary duty of loyalty. **[10]**

[B2]
(a) Discuss the major risks associated with nuclear power generation and the future of nuclear power in general.

[6]

(b) What, in your view, are the important issues and risks of nuclear power generation in India. **[4]**

[B3]
(a) Discuss the issues most relevant to the identification of political risks and their measurement. **[7]**

(b) List three political risks factors relevant to India from the point of view of a foreign insurance company wanting to start operations in India. **[3]**

BIMTECH

SECTION – C
COMPULSORY CASE STUDY
CYBER RISK INSURANCE

[Total Marks – 15]

Important: Answer the Questions given at the end.

1. The Cyber threat to the private sector

In late April 2011, one of the biggest data breaches in corporate history took place. Hackers penetrated Sony's PlayStation and Online Entertainment services and reportedly made off with 102 million customers' names, addresses, user names and passwords and possibly their debit and credit card numbers (Tsukayama, 2011). In total the attacks may cost Sony between $1 billion and $2 billion directly, and likely even more indirectly due to the reputational harm to Sony, (Nakashima & Robertson, 2011). These figures should not be surprising, given that data breaches have reportedly. cost U.S. companies on average $20.4 per lost consumer record as of 2009 (Betterley Risk Research, 2010), and because the attacks on Sony were just the latest in a string of data breaches affecting firms around the world. Epsilon and its customers, including JPMorgan Chase, Verizon, Best Buy, Target, Marriott, and Hilton. Lockheed Martin. The International Monetary Fund. Sega. Citigroup. All of these- and more-were hit by cyber attacks in just 3 months, from April to June 2011. And that followed on the heels of RSA's high-profile breach in March 2011 (Aspan, 2011; Goldman, 2011; Wolf & Maclean, 2011). The T.J. Maxx data theft, though, remains among the costliest attacks to date, resulting in 45 million credit and debit card numbers being stolen. A $9.75 million settlement followed, along with promises to invest in enhanced cybersecurity (Greenemeier, 2007).

Cybersecurity is increasingly on the minds of managers as cyber attacks now regularly cost firms millions in direct and indirect losses, to say nothing of the implicit costs of decreased future revenues and potential legal liability (Ishiguro, Tanaka, Matsuura, & Murase, 2006). Much of the potential risk surrounding e-commerce, however, is nothing new. Copyright infringement and defamation, for example, often occur through mediums other than the Internet. The differences here are the scale of the problem, the involvement of state and non-state actors, and the potential for collateral damage (National Counterintelligence Executive, 2011). Over 90% of respondents to a survey by the Ponemon Institute (2011) reported experiencing a cyber at- tack during the last year, costing on average more than $2 million per organization. Such attacks have been shown to negatively impact the stock prices of targeted firms, though this effect has lessened somewhat with increased media attention to breaches post-September 11, 2001 (Gordon, Loeb, & Zhou, 2011).

At-risk firms have been turning to cyber risk insurance to mitigate the cyber threat and any resulting legal liability from data breaches. For example, in the wake of the cyber attacks on Sony, a brewing legal battle pits Zurich American Insurance Company against Sony over the question of responsibility for the data breaches (Zurich American Insurance Company vs. Sony Corporation of America, 2011). Zurich claims that it should be absolved of any liability in the more than 55 putative class-action lawsuits being filed against Sony in the United States, and another three in Canada. Sony expects to spend more than $180 million on breach-related costs, including litigation, in 2011

alone (Vijayan, 2011). Given this state of affairs, how useful is cyber risk insurance? Does it really protect companies, or is it true that "there aren't many success stories where cyber insurance [has played] a significant role in reducing the costs of incidents" (Vijayan, 2011)? Ultimately, does cyber risk insurance make firms less proactive in enhancing cybersecurity, thus increasing the likelihood of data breaches?

I argue that firms must adopt a proactive strategy to manage cyber attacks for their own competitive well being, as well as to help secure critical national infrastructure. Cyber risk insurance then may be a part of an overall risk mitigation strategy, but over-reliance puts both corporate intellectual property and consumer records at risk.

2. Cyber attacks and the bottom line

To address a problem, at least two variables are required: a clear definition of the problem itself and a shared, reliable way of attaching value to it.

Consensus on what constitutes a cyber attack has been slow to emerge, while assessing the data is difficult for at least two main reasons. First, no entity is demanding, and few are asking, for. relevant data. Second, firms rarely feel compelled to voluntarily compile, organize, and transmit data about breaches: strategic management incentives are misaligned to report cyber attacks. For example, estimated losses to the malicious Conficker worm vary widely-between$200 million and $9 billion-in part because its costs are distributed and many of its victims are unknown As ZDNet reports, in a perfect world, compromised enterprises would confess their losses; but "in the real world, a Conficker infected international com pany would try to stay beneath the radar if it can"(Danchev, 2009). Thus, given those caveats, any conclusions about the nature and extent of the cyber threat must be critically analyzed.

From 2000 to 2008, the number of organizations reporting a cyber attack ranged from 43% to 70%(Richardson, 2008). In 2011, fully 80% of 200 surveyed IT executives reported they had detected one or more attacks (McAfee, 2010). Identity theft alone costs consumers more than $5 billion per year and firms another $48 billion, increasing 21% in 2008 (FTC, 2011). In all, hundreds of millions of personal records have been exposed in hundreds of incidents. A single incident involving the theft of a laptop owned by the Veterans Administration led to the loss of 26 million social security numbers of retired and active duty military personnel, resulting in a class action lawsuit claiming more than $26.5 billion in damages (Evers, 2006). In another incident, the Commerce Department managed to misplace more than 1,100 laptops, including 250 from the Census Bureau in 2006; of these, only 107 were fully encrypted (Sipress, 2006). Besides identity theft, fraud is also a significant problem, with more than 600,000 complaints and over $1.B billion in claims in 2008.

How do all of the costs impact the bottom line? According to the Ponemon Institute (2012 - a privacy and information management firm-the average data breach cost just over $6.75 million in the United States, though figures range widely from $234,000 up to $31 million. One recent study by Symantec (2010) found a combined average cost due to cyber attacks of $2 million annually for all businesses, and $2.B million for large businesses. Though figures may vary, it's clear cyber attacks nave the potential to impact the bottom

BIMTECH
BIRLA INSTITUTE OF MANAGEMENT TECHNOLOGY

lines of firms of all sizes. For example, an article in the Los Angeles Times described how Village View Escrow Inc. - a small escrow and title company- suffered a cyber attack that cost the firm $465,000 (Zwahlen, 2011). According t Symantec's June 2010 5MB Information Protection Survey, which includes responses from 2,152 businesses with 10 to 499 employees, 73% of small and mid-sized business were hit by cyber attacks from May 2009 to 2010.

Thus, there is a basic misunderstanding in some firms about the extent to which cyber risk is part of enterprise risk. Indeed, only one-third of board members from the Carnegie Mellon survey reported that their boards regularly reviewed incident reports, along with data controls and policies. There are exceptions, though, to the prevailing ignorance surrounding the prevalence and cost associated with cyber attacks. Security Magazine (2010), for example, benchmarks spending on security as part of a 'Security 500' group, reporting that spending on security in 2010 either increased or remained flat in 82% of firms surveyed. However, this figure includes physical security and drug and alcohol testing along with a number of other responsibilities.

Commentators have been calling insurance a key part of the cyber security solution for years, and there is some evidence that it is catching on despite the continuing difficulty of assessing risk and calculating premiums (Willis, 2010). In the best case, these policies could help quantify risk and help shield proactive firms from the fallout of cyber attacks. In the worst case, they could contribute to a more reactive focus maintaining the suboptimal cyber security status quo. In order to assess which scenario is more likely and how to ensure that cyber risk insurance becomes an effective tool for firms seeking to manage risk, it is necessary to investigate how cyber risk insurance has evolved and what the major roadblocks are to its continued adoption

Policies range in what types of cyber incidents are covered. Plans can include post-breach response costs such as hiring computer forensic experts and arranging for credit monitoring services. Business interruption insurance, providing compensation for time lost to cyber attacks, is common as well. There is also the possibility of purchasing different types of insurance for different types of cyber attacks. The market in cyber risk insurance is still developing, with options of first-party insurance involving a policy that applies to oneself or property, covering instances of trade secret theft or extortion; and third-party risk, which is protection against the actions of another, as in the case of cyber attacks. Geography plays an important role, too, in what insurance options are available to firms. More policies are available in the United States, for example, than even other advanced markets such as Canada due to differing insurance premium bases (Drounin, 2004).

How are cyber risk insurance plans priced? Calculating insurance premiums is no simple matter, and as a result many insurance companies limit their coverage options. A long history of actuarial data is needed for these calculations. That is often not possible, given the relative youth of the Internet and the lack of incentives for effective information sharing; as such, calculations based on limited data are oftentimes skewed. One issue is adverse selection, in which firms that have been hit by a cyber attack are more likely to purchase insurance. Another is that firms having a high degree of exposure or history of attacks are more likely to seek coverage. Insurance companies deal with this uncertainty in their calculations by requiring information security audits, the virtual equivalent of the physical exam required for health

insurance coverage. A number of factors are gauged; for example, insurance firm J.S. Wurzler adds a surcharge to firms using Microsoft NT (Gordon et al., 2011). Even after a successful audit, insurance companies may worry about firms' behavior when insulated from risk. This can be addressed through monetary incentives such as deductions for firms that avoid bad behaviors, analogous to a safe driving discount, or premium reductions for firms that enhance their cybersecurity.

Relying on cyber risk insurance, alone, to manage the threat is an insufficient response to a growing problem. Firms can, and must, do more to mitigate their enterprise risk. Consider how a small dry cleaning business in a difficult Detroit neighborhood handles street crime. Insurance is likely part of its strategy, but so is investing in better locks and security cameras to catch intruders. Due to the limitations of cyber risk insurance, firms need to proactively enhance their cybersecurity and protect data through investing in the virtual equivalent of padlocks and security cameras, including intrusion detection capabilities, patching software holes quickly, encrypting important data, and air gapping vital systems (i.e., disconnecting them from the public Internet).

*****

Questions to be answered:

(1) Should cyber risk be treated as part of enterprise risk? If not, why not? Are there specific advantages in taking cyber risk cover? **[6 Marks]**

(2) To reduce corporate risk, what measures should companies initiate and later build on? **[5 Marks]**

(3) In general, what has been the financial implications of cyber attacks on firms? **[4 Marks]**

[Total: 15 Marks]