

What are the Cyber Risk Liability Exposures or E-Business Risk Exposures?

75% of organizations polled did not carry insurance against Cybersecurity Risks according to Computer Security Institute in 2005.

Every quarter second a file is stolen containing information that, if used, could compromise an individual's identity.

An identity is stolen about every three (3) minutes, resulting in an average loss of \$3,000.

Theft of intellectual property (IP) has seen, and will continue to see, double digit growth. (Please note that IP theft undermines our economy, our competitiveness, and in many cases our National Security.)

The Pentagon is cyber attacked three (3) million times a day. It has been reported that 27 terabytes of data was stolen from Depart of Defense (DOD) last year (2007).

There are approximately 10,000 Distributed Denial of Service attacks daily on e-commerce platforms.

On average there are about 200 new computers viruses every month that are launched.

Cyber exposures include website breaches which cause both first party and third party damages as indicated by the Computer Security Institute.

- 1) 40% of all websites have been hacked into during 2007.
- 2) 56% of them did not know that they were hacked.
- 3) Only 34% of them admitted it to the public.

Cyber exposures include hacking into other operating systems of companies and not just the website operation.

- 1) It is estimated that for every one computer break-in reported there are 400 other break-ins that are not reported.
- 2) In 2007, it is estimated that business around the world lost close to \$278,000,000,000 due to hackers.
- 3) 377 Leading Internet Company's were hacked during 2007.
- 4) 56% of all hacking into computers is caused by internal security violations.

Loss Analysis of e-business activity from the 2007
Computer Security Institute Survey

- 1) 95% of respondents reported that the most frequent point of attack was through the website.
- 2) 56% of respondents reported unauthorized use of computer systems.
- 3) 56% of respondents reported that unauthorized access was created by insiders.
- 4) 91% of respondents reported financial losses due to electronic attacks for their e-business activities.

Firewalls will prevent the breaches of websites and other essential computer programs?

- 1) 97% of websites have firewalls in place, yet 65% of them reported system penetration from outside and this has increased for the third year in a row. (Computer Security Institute/FBI 2007)
- 2) 80% of corporate computers host at least one instance of unwanted software such as Adware, Spyware, Trojan Horses, and Hacker Tools.
- 3) It is estimated that every PC averages 27 pieces of spyware which is a 19% increase just in the past quarter. (Network Computing Magazine Sept. 22, 2006)
- 4) Over 52,400,000 credit card numbers were stolen by hackers in 2007.
 - a) Card systems, Atlanta, GA - 13,900,000
 - b) United Parcel Service - 3,900,000
 - c) Citi Financial - 3,900,000
 - d) Bank of America - 1,200,000
 - e) Time Warner - 600,000
 - f) Cost to reissue and stolen credit card is on average \$125 per card. You do the math on the exposure
- 5) Approximately 9% of all websites sales transactions are stolen credit cards.
- 6) Average legal expense to recover stolen intellectual property through breaches to the website or other computer programs is estimated at \$250,000 per incident.