Managing E-Commerce Risks

Manoj Kumar, Chartered Insurer
ACII (UK), CPCU (USA), ARe (USA), ARM (USA), FIII (India). MBA
Email: manoj@einsuranceprofessional.com

E-Commerce and Risk Management

- E-Commerce is the delivery of information, products, services or payments via telephone lines, computer networks or any other electronic means.
- Types of risks – Business Risk & Accidental Risk (Accidental loss & Business loss)
- Risk Management is the process of making and implementing decisions that will minimize the adverse effects of accidental and business losses on an organization.

Organization of the Presentation

- Magnitude of the problem
- Identification of Risks
- Case Specifics
- Some Examples
- Treatment of the Risk
  - Risk Control
  - Risk Financing
- Trends
- Recommendations

Magnitude of the Problem

- 600 Million users
- Absence of a uniform law
- No credible loss data, undetected for long
- ‘Love Bug’ – 45 Mio computers, $15 Bio in losses, 20 countries
- FBI Survey
  - $266 Mio loss due to cyber crime
  - Breach of security in 7 out of 10 systems in US
  - 74% acknowledged financial losses
  - Over $30 Bio is lost per year due to electronic fraud

Magnitude of the Problem

- In 1999, about 2 Mio credit card fraud in Europe alone
- 67% of Fortune 500 companies have been hacked. Average losses between $250,000 to $500,000. Examples include Microsoft, Amazon, eBay, Buy.com, Yahoo, CNN, Etrade
- E-commerce transactions has grown from $200 Bio in 1999 to $700 Bio in 2000 and is likely to exceed $1 Trio by the close of 2001.

Risk Identification

First Party Risks

- Property Risks
- Business Interruption

Third Party Risks

- Legal Liability

First Party Risks (1)

- Physical damage to host computer and network equipment – theft, destruction, alteration
- Breaches of security by employees, former employees or contract professionals - easier
- Hacking by outsiders
- Destruction of computer network due to viruses, e.g., Melissa, Love Bug, etc.
- Destruction of credit card and related information leading to lost sales

First Party Risks (2)

- DOS / DDOS – Distributed Denial of Service Attack – CNN, Ebay, Yahoo
- Lost new E-Commerce customers due to various forms of disruptions - Valuations will be affected
- Theft of intellectual property, trade secrets and other confidential information stored on computer networks
- Computer Fraud
- Extortion – CD Universe

First Party Risks (3)

- Programming errors
- Cost of litigating against those who have infringed on company intellectual property
- Cost to restore damaged Web site / network
- Cost to repair or upgrade security systems / firewalls after the breach of a security
- Business Interruption & Loss of Reputation
- Extra expenses arising out of disruptions to intranets and Extranets

Third Party Risks (1)

- Misuse of credit card numbers or credit history information of customers
- Transmission of computer viruses
- Infringement of Copyright, trademark & patent
- Piracy, misappropriation or other intellectual property violations
- Defamation – libel (written) and slander (oral)
- Advertising injury including false or misleading advertising

Third Party Risks (2)

- Legal liability for the content of emails
- Cyber Squatting - Madonna
- Meta Tag Abuse – Playboy in 1997
- Public disclosure of private facts
- Hacker access to wrongful information e.g., Pair Gain on Bloomberg; and failure to remove this information promptly
- Defence Costs

Case Specifics

- Service Providers - ISPs
- Hosts, Infrastructure Providers
- Solution Providers
- Developers
- Content Providers
- Software Tool Providers
- Advertisers
- Publishers – NY Times
- Users – Website Owners

Some Examples (1)

Defamation

Norwich Union reached a Pound 450,000 out-of-court settlement with Western Provident Association after Emails suggesting that W.P. was under investigation by DTI were found circulating at NU.

Some Examples (2)

Hacking & Fraud

A disgruntled computer hacker took revenge on the creator of an IT security by changing his bank details and making it impossible for him to sell his house to get a mortgage

The hacker added 6 default notices of non-payment and a County Court judgement to the victim's financial records

Some Examples (3)

Viruses (1)

An Email virus called Melissa (in March 1999) brought almost 60 major companies in the USA to a halt as well as affecting thousands more throughout world.

One victim was the Governor of North Dakota, who sent a list of pornographic sites to confused constituents and party donors

Some Examples (4)

Viruses (2) - April 1999

- Allied communications during the Balkan conflict were hit by viruses. The US defence department stated that all base to base email between US marine units world-wide had been silenced by Melissa.
- NATO's web site was hit by a cyber attack by Papa, Melissa’s more pernicious cousin

Treatment of Risk

- Risk Control
  - Avoidance
  - Loss Prevention
  - Loss Reduction
  - Segregation or Duplication
  - Contractual Transfer of Risk
- Risk Financing
  - Retention
  - Transfer of Risk (Contractual Transfer, Insurance)

Risk Control

1. Copying data onto backup sources
2. Duplication of hardware & software
3. Firewall
4. Virus detection software
5. VPN – Virtual Private Networking
6. Access Control & User Identification
7. Physical Security Audits
8. Email Policy – Content Security
9. Training & Education

Risk Financing

- Contractual Transfer of Risks
- Cyber Insurance
  - Availability
  - Pricing
  - Non-standard
  - Non-traditional
  - Jurisdiction
  - Security Audit
  - Valuation

Recent Trends

- Formation of IT-ISAC in Feb. 2000 (Information Sharing & Analysis Centre) – 19 Companies including IBM, Microsoft, Cisco and others
- Domain Registration
  - Earlier only Network Solutions Inc.
  - Now Internet Corporation for Assigned Names & Numbers - ICANN
  - Uniform Domain Name Dispute Resolution Policy by ICANN
- WAP & SMS – Increased Risks

Recommendations

- A top down view driven by high level business security
- Alignment with organization's overall risk and security policy
- Security & Risk Management to be seen as "people" problem, not just a technology issue
- Identify dangers internally as well as externally
- Consider unintentional danger as well as malicious and planned attack

Thank You !