Chapter IV
E-Risk Insurance Product Design: A Copula Based Bayesian Belief Network Model

Arunabha Mukhopadhyay
Indian Institute of Management Lucknow, India

Samir Chatterjee
Claremont Graduate University, India

Debashis Saha
Indian Institute of Management Calcutta, India

Ambuj Mahanti
Indian Institute of Management Calcutta, India

Samir K. Sadhukhan
Indian Institute of Management Calcutta, India

ABSTRACT

An online business organization spends millions of dollars on firewalls, anti-virus, intrusion detection systems, digital signature, and encryption, to ensure minimal security breach. Nonetheless, a new virus or a clever hacker can easily compromise these deterrents, resulting in losses to the tune of millions of dollars annually. To minimize the financial loss, we propose that online businesses should invest in e-risk insurance products as a complementary alternative, above the network security appliances. In this work, we develop a Copula aided Bayesian Belief Network (CBBN) model, to assist insurance companies to design e-insurance products. The CBBN model does an e-vulnerability assessment (e-VA) and e-risk quantification (e-RQ). We first draw a casual diagram (BBN) stating the probable reason for security failure in an organization. We assume the marginal distributions for each of the nodes of the
E-risk Insurance Product Design

**INTRODUCTION**

E-risk is defined as the possibility of a malicious electronic event, whose occurrence causes loss to e-business. These consist of (i) comprise of network security components (such as firewall, proxy servers, anti virus), (ii) the compromise of the organization web server, and incorrect or indecent material posted on the web site (commonly called graffiti), (iii) service providers (i.e., Application Service Provider (ASP) or Internet Service Provider (ISP)) failing, (iv) identity theft (i.e., confidential customer information is hacked from an organizational database; example, pin numbers of credit cards from a bank), (v) attacks by disgruntled employees, (vi) cyber-extortion, (vii) Denial of Service (DoS) by making malicious calls to the router, (viii) attack by wireless devices (such as PDAs, mobile phones etc). CSI/FBI 2004 report (Gordon, Loeb, Lucyshyn & Richardson, 2004) states that the most vital e-risk in USA is virus attack (loss of $55 Million). It is followed by DoS attack (loss of $26 Million), and theft of proprietary information (loss of $11 Million).

Organizations spend millions annually for deployment of sophisticated technical defenses (such as encryption, access control and firewalls) (Gordon, & Loeb, 2002) and intrusion detection systems to guard against malicious attacks. CSI/FBI report (Gordon et al., 2004) states most organizations in USA have deterrents such as (i) antivirus software (99%), (ii) firewalls (98%), (iii) proxy servers (71%), and (iv) intrusion detection systems (68%). Yet security breaches are very common.

Anderson (2001) opines that the chance of a clever hacker breaking into the system is much higher than the chance that the CTO would detect it. This can be sustained with the following example. Assume there are \( n \) vulnerabilities in an organizational network. In a given period of time, the hacker needs to find only one as opposed to the CTO who has to be aware of all the \( n \) vulnerabilities to protect the system from malicious attacks. Thus, it is a win–win situation always for the intruder. Schneier (2001) notes, that a new virus can easily comprise the perimeter security devices, as there is no signature available in the anti-virus engine to track it down. The CSI/FBI report (Gordon et al., 2004) corroborates this fact, as loss due to virus attack in USA alone was $55 Million in 2004.

To supplement the existing security measures and to reduce the monetary loss, an effective alternative mechanism is insuring (Gordon, Loeb, & Sohail, 2003; Grzebiel, 2002; Mukhopadhyay, Chatterjee, Saha, Mohanti 2005a; Mukhopadhyay, Chatterjee, Saha, Mohanti, Chakrabarti and Podder, 2005b, 2005c; Mukhopadhyay, Chatterjee, Saha, Mohanti, and Sadhukhan,2006; Mukhopadhyay 2007, Mukhopadhyay, Chatterjee, Saha, Mohanti, Roy and Sadhukhan,2007a; Mukhopadhyay, Chakrabari Saha, Mohanti 2007b) against these risks. This would help reduce the financial burden on the organizations, as the insurance company would indemnify the loss. In effect, the organizations risk is being passed on to another party at the cost of a premium. This reduces the companies concern about “self insuring” (i.e., keeping aside huge amount for contingency purposes). This, in turn, is a good corporate strategy,