Decision Support Systems 56 (2013) 11–26

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Cyber-risk decision models: To insure IT or not?☆

Arunabha Mukhopadhyay [a,*], Samir Chatterjee [b], Debashis Saha [c], Ambuj Mahanti [c], Samir K. Sadhukhan [c]

[a] Indian Institute of Management Lucknow, India
[b] Claremont Graduate University, United States
[c] Indian Institute of Management Calcutta, India

ARTICLE INFO

Article history:
Received 17 April 2011
Received in revised form 20 November 2012
Accepted 23 April 2013
Available online 14 May 2013

Keywords:
Security breach
Cyber-risk
Cyber-insurance
Copula
Bayesian Belief Network
Premium
Utility models

ABSTRACT

Security breaches adversely impact profit margins, market capitalization and brand image of an organization. Global organizations resort to the use of technological devices to reduce the frequency of a security breach. To minimize the impact of financial losses from security breaches, we advocate the use of cyber-insurance products. This paper proposes models to help firms decide on the utility of cyber-insurance products and to what extent they can use them. In this paper, we propose a Copula-aided Bayesian Belief Network (CBBN) for cyber-vulnerability assessment (C-VA), and expected loss computation. Taking these as an input and using the concepts of collective risk modeling theory, we also compute the premium that a cyber risk insurer can charge to indemnify cyber losses. Further, to assist cyber risk insurers and to effectively design products, we propose a utility based preferential pricing (UBPP) model. UBPP takes into account risk profiles and wealth of the prospective insured firm before proposing the premium.

1. Introduction

Organizations invest millions of dollars on perimeter security applications such as firewalls, anti-virus and intrusion detection systems to minimize security breaches from attack such as hacking, phishing, and spamming [41,58]. Nonetheless, a new virus or a clever hacker can easily compromise these detection systems, resulting in millions of dollar losses annually. Organizations also use digital signature and encryption to ensure confidentiality (C) and integrity (I) of their transferred data. Yet, eavesdropping and man-in-the middle (M-n-M) attacks are common. Use of stringent technology policies is enforced [5,30–33,41] by organizations to authenticate and authorize individuals to access data. Organizations also plan to ensure availability (A) of online resources for customers and employees 24 × 7/365 days. This helps promote ecommerce activities and in turn leads to growth of the top lines for the organizations. C–I–A triad forms the backbone of an organization's security framework.

Cyber-risk is defined as the risk involved with a malicious electronic event that causes disruption of business and monetary loss [17,80,83]. For example, hackers and disgruntled employees exploit both the security and application level vulnerabilities and can break into organizational databases and gather confidential customer information (such as credit card pin numbers). In 2012, a hacker group, Anonymous, had also tried a cyber extortion attack of $50,000 on Symantec software and also declared its malicious plans to disrupt the power supply system in the USA through a cyber attack on the power grid in the near future [42]. Cyber-risk disasters have a direct impact on the bottom line of an organization, in terms of loss of opportunity cost. The organization's brand equity and market capitalization too are adversely impacted by these risks [70,73,79].

Cyber-insurance products are a viable complementary method for a firm, after investing in perimeter and core security appliances, to cope with security breaches in e-commerce [12–14,67,68,71,79,82,107]. Cyber-insurance is outsourcing of low frequency, high impact risk. It helps to reduce the financial losses of e-business organizations, by payment of the premium to a cyber risk insurer. An insurance company would cover cyber-risk because (i) the probability of the event(s), i.e., breakdown of network, Distributed Denial of Service (DDoS) or a virus attack is relatively small; (ii) a large number of similar risks are available for pooling and for reduction in the variance of experience; (iii) any loss involved is financially large and organizations have substantial "insurable interests" to reduce, (iv) the risks/losses of network

☆ Our previous version accepted in conferences:

* Corresponding author at: Indian Institute of Management Lucknow, Prabandh Nagar, Off Sitapur Road, Lucknow-226013, Uttar Pradesh, India. Tel.: +91 522 2736 646.
E-mail addresses: arunabha@iiml.ac.in, mukhopadhyay.arunabha@gmail.com (A. Mukhopadhyay).

0167-9236/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dss.2013.04.004

failure or DDoS are different from that of any other type of general insurance product (i.e., Property, Liability, Financial loss, Fixed Benefit) [85]; (v) the insurer can accept such a risk as it is quantifiable and also an upper limit of possible liability can be fixed; (vi) the insurer can assume that moral hazard would mostly be absent. A cyber security breach insured firm is differentiated from its competitors in terms of its information security management system (ISMS). This works to the company's advantage as it is more secure with respect to its competitors. This in turn helps in creating a sense of trust in the minds of its customers and suppliers. This helps to increase top lines of the firm. Thus ISMS helps and serves as strategic positioning for the firm. Subsequently, the growth of ecommerce helps to reduce operational expenses too and this provides a greater economic value for the organization [33,40,41,47,57,58]. This makes a strong case for a firm to insure its cyber risk to minimize its uncertain losses.

The novel contribution of this paper is twofold, first we develop a Copula based Bayesian Belief Network (CBBN) model for assessing and quantifying the cyber-risk of an online business organization. The CBBN model outputs the (i) cyber-risk vulnerability assessment (C-VA) report indicating the probable source of vulnerability/security breach, (ii) the loss expectancy report arising for the security breach, and (iii) premium value to be charged by the insurer based on collective risk model. This study is of prime importance to the CTO as they can spot the vulnerabilities in the corporate network, for the business manager to understand the financial implication arising due to the security breach, and for the CFO to decide on insuring IT assets against cyber risk. The inputs to CBBN are a directed acyclic graph (DAG) illustrating the factors (i.e., technological and business) that lead to a security breach, the log data of IT security appliances, type of organization, IT security budgets, financials and a correlation matrix for the DAG [70,73].

Second, we develop a utility based preferential pricing (UBPP) model for cyber-insurance products. The UBPP is integral to the e-risk insurer as it computes the premium to be paid by each insured firm based on the loss expectancy computed by CBBN, risk profile (i.e., averse, neutral and seeker) and financials. The UBPP model will help cyber-insurers design differentiated cyber-insurance products for a competitive advantage.

Our paper is the first attempt to provide a decision model that aids both the insurer and insured in effectively deciding on cyber insurance products as a mitigation tool against cyber disasters. Mukhopadhyay et al. [70] explored the viability of cyber insurance as a complementary tool to minimize the loss arising from a security breach. They computed gross premium for some scenarios. Mukhopadhyay et al. [68,70] demonstrated the use of cyber insurance as a tool to mitigate cyber risk. They also demonstrated how e-risk could be divided in a beneficial manner to assist multiple insurers. In doing so, Mukhopadhyay et al. proposed a Copula based model for computing e-risk [70]. This paper is different from other papers as it takes into account correlated cyber risk [12–15,20,79,80], and we have (i) restricted our study to the firm level cyber risk and (ii) used the concepts of copula to model correlated risks associated with for cyber security breach. Copula is suited for this study as we wish to capture the interdependent risks for modeling the expected loss associated with an online attack. We have used the process approach [61,93] to generate a directed acyclic graph (DAG) that illustrates the probable reasons (i.e., technological and business) for IT security breach in an organization. This forms the basis of our proposed CBBN model. Our paper is different from Herath and Herath [46], as we have used Gaussian Copula to model correlated risk as opposed to Archimedean Copulas (i.e., Clayton and Gumbel Copulas) used by them. Based on data collection and expert opinion, we have modeled each node of the causal diagram as normal distribution and aggregated the data using the Gaussian Copula. We also use, for the first time, the UBPP model to customize the premium structure, which helps in customization of the product. It would make good business sense for an insurer to provide customized products to attract the cyber insurance customers.

This paper has eight sections. Section 2 outlines the related literature. Section 3 discusses our cyber-risk vulnerability assessment (C-VA) model development, the reasons for choice of the constructs and the mathematical formulation of the problem. In Section 4, we introduce the basics of Bayesian Belief Networks (BBN) and Copula and explain how they have been used in our C-VA model. This section also has the C-VA and cyber-risk quantification algorithm. Section 5, has the methodology for the premium computation using collective risk modeling concepts. Real-life scenarios of vulnerability assessment, premium computation, and cyber-insurance product design are also evaluated in this section. Sensitivity analysis of our C-VA model is also carried out here. Section 6 discusses our proposed utility based preferential pricing (UBPP) utility model for premium computation for risk neutral, risk averse and constant risk averse firms seeking cyber insurance. Section 7 lists our contributions in this paper, vis-à-vis the related work in IT risk and cyber-insurance domain. Section 8 concludes the paper.

2. Literature review

In this section we review related work on (i) process approaches used to model and quantify IT/operational risk [3,6,10,19,25,35,50,54,60,70,73,77,81,89,93] and (ii) models to mitigate correlated risk using cyber insurance [11,13,14,79,80,89,107].

2.1. Process approach for quantifying operational risk

The process approach focuses on the chain of activities that comprise an operation or transaction to find out the exact risk for each process [18,26,28,53,86,88,95].

2.1.1. Process approach for quantifying operational risk

Basel II defines operational risk (OR) as the “risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”. OR "includes legal risk, but excludes strategic and reputational risk” [102,103]. Systems failure is a source of OR and can lead to information security risks [10]. Basel II accord and Sarbanes–Oxley (SOX) mandate quantification of operational risk (OR) [27] and propose the use of process approach for the same [93]. Broadly, there are two process methods for quantifying operational risk (OR), such as (i) top–down and (ii) bottom–up [62]. Bottom–up method measures operational risk for each business line/unit and aggregates it for in an organization [24]. Weiß and Winkelmann have proposed a bottom–up approach the using semantic business process modeling language (SBPML) for conceptualizing operational risk for a bank [102,103]. Standardized Approach (SA) and Advanced Management Approach (AMA) are mostly used by bottom–up methods [24]. AMA proposes the use of (i) process approach, (ii) factor approach [45,101], and (iii) actuarial approach to quantify operational risk.

2.1.2. Process approach for quantifying IT risk

The commonly used Process Approach techniques for IT risk assessment are: (i) causal networks, (ii) Bayesian Belief Networks (BBN) and (iii) fuzzy logic [93]. As early as 1988, the *Inversion Model Expert System* study noted that as systems shifted from manual to automation, the associated risks changed from external (i.e., sabotage and espionage) to internal (i.e., integrity and fraud) threats. In automated systems, the external attacks are more on the processes and the internal threats are directed to data. The output of this expert system was a set of recommendations of security safeguards against threats [6]. Lederman investigated the adverse impact to patient's health if an information systems failure occurred in a healthcare unit [63,64] using process modeling technique. Becker et al. and Strecker et al. used concepts of design science research

Table 1
Summary of the key concepts used for modeling operational risk using BPM.

Concepts	Strecker et al. (2011)	Weiß et al. (2011)	Becker et al. (2009) and Frank et al. (2011)	Salmela (2007)	Lederman (2004, 2005)	Kokolakis et al. (2000)	Inversion Model (1988)
Method	MEMO	SBPML	Design science	Action Research	BPM technique	BPM approach	Process model
Unit of research	–	Bank	Bank	Bank	Health care	–	–
Organizational parameters	Y	Y	Y	Y	Y	Y	–
Technological parameters	Y	Y	Y	Y	Y	Y	Y
Compliance	Y	Y	Y	–	–	–	–

methodology (DSRM) to propose a conceptual process modeling method for risk assessment [9,96]. Kokolakis et al. made a strong case for modeling IT risk by using the concepts of business process modeling (BPM). They opined that any of the commonly used business process modeling (BPM) techniques (such as IDEF, System dynamics, Process maps, Action Workflow, ARMA, Responsibilities analysis, Business transactions, HC Petri nets etc.) can be effectively used to propose security policies for an organization in terms of roles, activities, agents and their responsibilities [61]. Salmela uses the concepts of BPM and Action Research (AR) to modeled business loss for a Nordic bank due to non-availability of information required for making decisions by its credit card department [88]. Strecker et al. proposed a RiskM model using Multiple-Perspective Enterprise Modeling (MEMO) techniques for IT risk identification and analysis by taking into account risks encountered by the organizational hierarchy (i.e., IT operations, Business Process and Strategic Management units [36,96]). They assumed that interdependence exists between risk factors, IT assets and the environment [106]. They captured the concepts of correlated risk using the semantics, AND/OR. The inputs to the process model also included (i) organizational context, (ii) organizational levels, (iii) qualitative description for risk quantification [22], (iv) compliance to standards and regulations like COBIT, HIPAA and GLB [104] and (v) multiple phases from IT risk identification to risk analysis. Table 1 summarizes the key concepts used in literature to model operational risk using BPM.

Causal networks is graphical relationship between the output and input variables for a given scenario/system. *Bayesian Belief Network* (BBN) [49,54] enables reasoning under uncertainty and combines the advantages of an intuitive visual representation with a sound mathematical basis of Bayesian probability. In 1988 Bayesian Decision Support System (BDSS) was developed by using statistical techniques to quantify IT risk [81]. The inputs to BDSS included (i) identification of the asset and impact in case of damage, (ii) mapping of threat to vulnerability, (iii) exposure distribution and the frequency of occurrence of the event. BDSS outputs (i) the risk distribution for each of the threats, (ii) the viability of the safeguards to be included for reducing vulnerability of the system and (iii) a technical analysis report providing detailed information of the security elements to be adopted [6,81]. Livermore Risk Analysis Methodology (LRAM) was developed in 1987 [43]. It featured the following (i) used Bayesian theory for analysis of security controls, (ii) computed the loss potential indicator (LPI), as the product of maximum potential loss (MPL) times the control failure probability. LPI was used to identify the threats that exceeded the organization's risk threshold, and (iii) cost–benefit ratio (CBR) was used to decide on the nature of controls to be implemented [43]. The main criticism of this model was that it lacked a holistic organizational view of controls [6].

Fuzzy logic is used when some of the inputs are vague, or have subjective judgments associated with them [60,77]. Smith and Eloff propose Risk Management in Health Care—using cognitive fuzzy techniques (RiMaHCoF) based on the business process model operational in a hospital. RiMaHCoF focuses on confidentiality of data. The study identified the critical patient route in a hospital and assigned risk values for each phase along a specific patient route [88,92]. In 1978, a fuzzy logic based model called Securtae [50] was developed. The inputs to this model included subjective/linguistic values for the triplet <vulnerable IT resources, threats, security features installed>. The output from Securtae was ratings for security elements [6,47,50]. Table 2 summarizes the key concepts used in literature to model IT risk using business process approach.

2.2. Cyber risk insurance and actuarial approach

Cyber risk can be broadly classified into (i) concepts of risk transfer & market dynamics, (ii) pricing of products and (iii) legal implications of cyber-risk insurance.

2.2.1. Cyber risk transfer

Majuca et al. [67] traced the evolution of cyber insurance market. Böhme [16], computed premium, using the utility theory, for both independent and correlated risk scenarios respectively, assuming dominant and alternative platforms [15]. Bohme and Schwartz [14] proposed a framework for risk reallocation. Cyber-risk was dependent on network environment (nodes), which are controlled by agents, who extract utility from the network. Using this framework, Bohme and Schwartz [14] studied the existing models that have been proposed for modeling cyber-insurance [13]. Yurcik [107] observed that organizations may either (i) transfer their risk to an insurance company or (ii) assume the risk internally via self-insurance. They noted that the insurers face the following problems: (1) not enough data and audit procedures to quantify risk and loss potential; (2) a small market base to pool risk; (3) cyber attacks by terrorist; and (4) acceptability of insurance by technology companies. Cyber insurance, then, is a viable option if: (1) insurance companies take a proactive interest; (2) reduce insurance premiums; and (3) pressurize software companies to deliver "safe" products to the market demand or assume liabilities with valid warranties [107]. Shetty et al. [90] demonstrated that competitive cyber insurers in a market do not improve cyber security.

2.2.2. Pricing of cyber-insurance products

Böhme and Kataria [13] proposed a two-tier approach for cyber-risk modeling. Technical, managerial and policy choices form a part of the two-tier model. Tier I addressed the correlation of cyber-risks within a firm (i.e. correlated failure of multiple systems on its internal network)

Table 2
Summary of the key concepts used for modeling IT risk using process model.

Key concept	BDSS	LRAM	Securtae	RiMaHCoF
Classification of IS asset	Y	–	Y	–
Mapping of threat to vulnerability	Y	Y	Y	–
Security controls & appliances	–	Y	Y	–
Quantification of impact analysis	Y	Y	Y	Y
Technique	Bayesian	Bayesian	Fuzzy logic	Fuzzy logic
Level of risk acceptance capability	Y	–	–	–
Recommendations				
1. Safeguards for reducing vulnerability	Y	–	–	–
2. Ratings for security elements	–	–	–	Y

Table 3
Summary of the key concepts used in cyber risk insurance literature.

Concepts	Bohme et al. (2005, 2006, 2010)	Ogut et al. (2005, 2010)	Yurcik et al. (2005)	Shetty et al. (2009)	Kesan et al. (2005)	Bolot and LeLarge (2008)	Herath et al. (2011)	Mukhopadhyay et al. (2006)
Correlated risk	Y	Y	–	–	Y		Y	Y
Premium	Y	Y	–	–	–	Y	Y	Y
Legislation	–	Y	–	–	Y	–	–	–
Organizational parameters	Y	–	–	–	–	–	–	Y
Market	Y	–	–	Y	Y	–	–	–
Technique	Utility theory	Utility theory	–	–	–	–	Copula	Copula
Recommends								
a. IT security	Y	Y	Y	–	Y	–	–	Y
b. Transfer risk	Y	Y	Y	Y	Y	Y	Y	Y

[12,15]. This influences the firm's decision to seek insurance. Tier II included the correlation in risk at a global level (i.e. correlation across independent firms in an insurer's portfolio) and this influenced the insurers' decisions about premium computation [11]. Ogut and Menon [79] concluded that the interdependency of cyber-risk leads firms to invest less than the socially optimal levels in IT security technologies and instead buy insurance coverage. Insurers are also not keen in absorbing large risks since the insured is investing less on security. As a consequence, the insurance premium is high [79]. Bolot and LeLarge [11] concluded that firms do not invest in self protection due to the presence of network effects and discriminatory insurance pricing by insurers. Herath and Herath [46] investigated cyber-insurance pricing from an actuarial approach using the Clayton and Gumbel Copulas. They adopted an empirical approach using Archimedean Copulas that is different from the process/utility based approaches used by Bohme [15], Böhme and Kataria [13], Mukhopadhyay et al. [70], Bolot and LeLarge [11], and Öğüt et al. [80].

2.2.3. Cyber risk insurance and legislation

Öğüt et al. [80] studied the impact of government intervention and public policy on correlated cyber security risk [80]. Kesan and Majuca [58] studied the cyber insurance industry, in terms of cyber liability legislation. They observed that a proper cyber insurance market will need (i) higher security investment, by firms and (ii) best practices to be followed by firms in terms of risk management and IT security. This will result in higher overall societal welfare [58]. Table 3 summarizes the key concepts used in cyber risk insurance literature.

Review of related work on (i) IT risk and (ii) operational risk management shows that Strecker et al., Salmela, Becker et al., and Weiß and Winkelmann [9,88,96,102,103] have proposed various process models to identify, assess and quantify cyber-risk. The process approach is effective, as it can clearly model the processes that are operative in an organization. It is easy to find the points of failure from a causal model [93]. Review of cyber insurance literature shows that (i) transfer of cyber risk has been accepted as a complementary tool to minimize losses arising from IT security breaches, (ii) differential premium for organizations. In this context our paper too proposes to (i) quantify cyber risk associated with ecommerce transactions for a firm using our C-VA model and (ii) also to provide help to insurers in developing cyber insurance products using our UBPP model.

3. Our cyber-vulnerability assessment (C-VA) model for an organization

Based on the literature survey our C-VA model assumes that a security failure in an organization may occur either due to (i) technological and/or (ii) business/organizational reasons. This is in contrast to most of the studies in IT risk assessment which have been focused primarily on IT assets, threats and vulnerability [84] alone. Few studies have also taken into account strategy and business parameters along with technical security appliances [65] to model security failure.

3.1. Technological approach

We also take into account principles of (a) ISMS as documented by BS7799[1] [16], (b) COBIT[2] [23], and (c) Telecommunications Network Management (TNM) principles, i.e., FCAPS,[3] [66], to formulate our C-VA model as illustrated in Fig. 1. Our C-VA model also takes into account that cyber-risks are correlated [20,30,31,96]. The technological approach is aimed at ensuring that the C–I–A triad is implemented effectively in an organization.

3.1.1. Access control using perimeter security elements

To ensure that users, services and applications have the required rights to access online data and to deter malicious intruders and to ensure C–I–A, keeping in line with FCAPS, BS7799 and COBIT framework [4], organizations deploy (i) application level, (ii) host level and (iii) network level. Yet a smart hacker may simultaneously expose multiple vulnerabilities in the perimeter security elements to compromise [38] a system, through probe packet or DDoS attack.

The commonly used security technologies by organizations are: (i) packet filtering or proxy firewalls placed at the perimeter to prevent unauthorized packets leaving or entering the militarized zone (MZ). Host level firewalls are also deployed to prevent data flow from specific hosts; (ii) network based IDS placed after the firewall and before the internal network of an organization, either use signature based or statistical anomaly based techniques to detect and prevent malicious intruders from compromising data; (iii) anti-virus software scans the virus signature database to check if any malicious virus is attempting to break in and; (iv) Remote Authentication Dial in User Service (RADIUS) server is deployed to ensure that unauthorized users do not anonymously access remote information assets [100].

3.1.2. Security policy

Security policy consists of multiple policy statements which maps onto controls from BS7799/ISO 27000/COBIT. These controls are implemented by procedures [4]. The security policy of an organization, lays down the *technology policy* implementation rules for the perimeter security elements such as: (i) keeping ports open in the

[1] (i) Security Policy, (ii) Organizational Security, (iii) Asset Classification, (iv) Personnel Security, (v) Physical Security, (vi) Communications and Operations Management, (vii) access control, (viii) System Development and Maintenance, (ix) Business Continuity Management and (x) Compliance.

[2] IT controls to ensure IT Governance in an organization by ensuring proper (i) alignment of business requirements with IT, (ii) IT process, effectiveness and (iii) IT resource utilization. IT processes are broadly divided into 4 broad domains, 34 subprocesses and 236 control activities.

[3] Focuses on five functional management issues in a network, namely Fault (F), Configuration (C), Accounting (A), Performance (P) and Security (S).

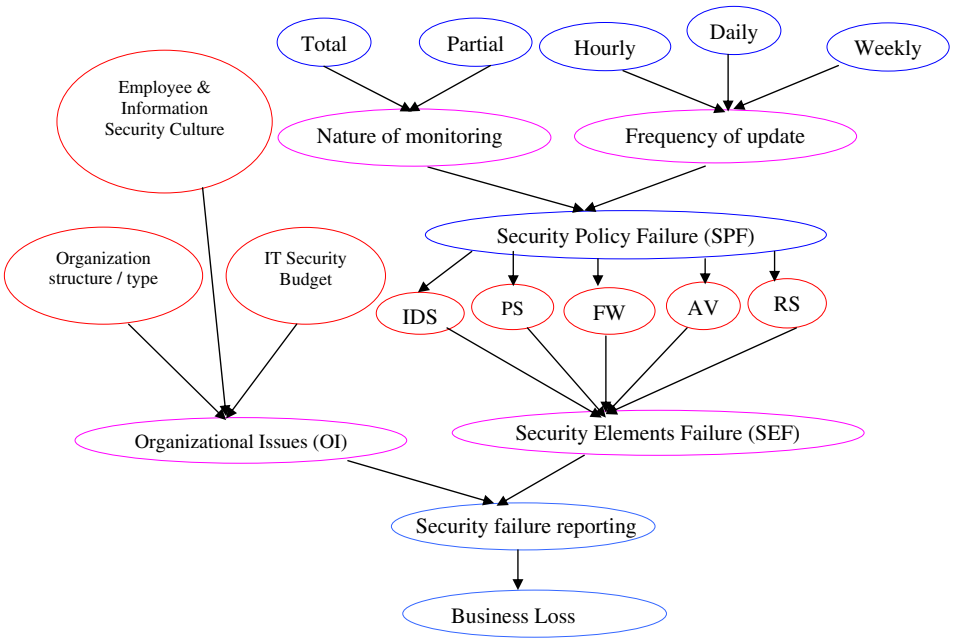

Fig. 1. Our C-VA model [IDS = Intrusion Detection System; PS = Proxy Server; FW = Firewall; AV = Anti-Virus; RS = RADIUS Server].

firewall, (ii) granting of user privileges and access control rights, and (iii) authenticating users correctly.

3.1.3. Monitoring and review

BS7799 and COBIT 4.1 mandate the frequent monitoring and review of the information security controls implemented in an organization [51]. According to the Plan–Do–Control–Act-(PDCA) cycle followed by ISMS [23], it is of utmost importance that the security policies be reviewed and updated regularly. For instance, the type and number of ports left open in a firewall (FW) should be scanned daily. The signatures in the anti-virus engine (AV) and IDS need to be updated regularly. The authentication rules in the RADIUS server (RS) also need to be updated frequently. Monitoring of log files and audit trails of perimeter security elements is also of utmost importance, according to the FCAPS model [66]. The increased frequency of update (i.e., hourly, daily or weekly basis), and nature of monitoring/review (partial or total) increase the efficiency of the security policy [23].

3.2. Socio-organizational issues

Socio-organizations should be taken into account while modeling security, since the security solution is "not with technology, but with the organization itself" [33]. Along with people–process–technology (P–P–T), organization design/strategy plays a crucial role in determining the effectiveness of the information security policy in an organization. The organization structure interacts with the P–P–T triad and determines the (i) culture, (ii) IT Architecture and (iii) the governance structure of an organization [59].

3.2.1. Organization structure/type

The effectiveness of information security is dependent on the organization structure [29,33,48,65,88,96]. Depending on whether the IT security management team reports to the CIO directly or indirectly [55], the effectiveness of IT security may vary. Formalized technological models and approach such as Bell La Padula and Denning model, work well in hierarchical centralized organizations (such as military) as opposed to flat, networked organizations [29].

3.2.2. IT security budget

Investment in IT security is a strategic decision and judicious spending on it should be done based on cost–benefit analysis to ensure that the risks are mitigated adequately [41,55]. Gordon and Loeb [108] proposed a risk adjusted Net Present Value (NPV) method for budgeting of IT security resources. Kolkowska and Dhillon [62] opined that a clear understanding of power relationship in an organization is critical for proper implementation of information security policy and also compliance [62]. Investment in IT security in some organizations is thought as cost center and with no direct return on security investment (ROSI) [8,17,40].

3.2.3. Employee & information security culture

Employees are potential internal threat to information security implementation in organizations [98]. Niekerk and Solms [78] have modeled internal threat, using management and economic theories and concluded that an effective information security culture is required for effective implementation of security in an organization. It follows that protection of data is possible efficiently if employees and organization adhere to a stringent informational security culture [78]. Awareness among employees about security is one of the important parameters of information security culture. This ensures proper monitoring of perimeter security elements in an organization [96,98].

3.3. Business loss due to security failure

It is has been noted that a security failure in organization could lead to IT resources malfunctioning and this is in turn leads to business loss [29,33,38,47,70,88,105]. We summarize in Table 4 the variables used in our C-VA model and their support from literature. Fig. 1 illustrates our causal diagram for the C-VA model.

3.4. C-VA model: the mathematical formulation

The directed acyclic graph (DAG), illustrated in Fig. 1, consists of 20 nodes or variables (i.e., X_1, X_2…, X_{20}) and multiple arcs. The arcs indicate causal relationships between the variables. Each X_i (i.e., technological parameters) is a random variable and represents

Table 4
Summary of the variables used and their sources.

Variables of C-VA model	ISMS frameworks			Other security papers
	COBIT	FCAPS	BS7799	
(A) Business loss	Y	–	Y	Gordon et al. (2009), Westerman et. al. (2007), Salmela (2007), Hinz (2005), Dhillon et al. (2001, 2006), Mukhopadhyay et al. (2006)
(B) Security failure reporting	Y	Y	Y	Gordon et al. (2009)
(C) Security element failure (SEF)				
(1). Security elements: (a) IDS (b) PS (c) FW (d) AV (e) RS	Y	Y	Y	Venter et al. (2003), Dhillon et al. (2001)
(2). Security policy failure (SPF)	Y		Y	Barnard et al. (2000)
(3). Frequency of update	Y	Y	–	–
(4). Nature of monitoring	Y	Y	–	–
(D) Organizational issues (OI)				Segecv et al. (1998), Dhillon (2006), Kiely (2006), Benzel (2006)
(i). IT security budget	Y	–	–	Gordon and Loeb (2002), Baskerville and Portugal (2003), Cavusoglu et al. (2004), Johnson, Gordon et al. (2006), Goetz (2007), Kolkowska et al. (2012)
(ii). Employee & information security culture	Y	–	Y	Thomson et al. (2006), Neikerk et al. (2010), Strecker et al. (2011)
(iii). Organization structure/type	Y	–	Y	Loch et al. (1992), Hitchings (1996), Armstrong (1999), Dhillon (2001, 2003), Dhillon et al. (2001), Dhillon et al. (2006), Salmela (2007), Johnson, Goetz (2007), Strecker et al. (2011)

an uncertain event and is depicted as a probability table/belief associated with it. The marginal data or prior probability is assimilated from log files present in perimeter security appliances. Each node, X_i (i.e., technological parameters), has 7 states each (very low, low, low-medium, medium, high-medium, high, very high). The organizational variables are discrete ordinal variables. Let the union of all nodes (i.e., $U = \{X_1, X_2, \ldots, X_{20}\}$) be described as the universe (U). If a security breach event (E_i) is observed with certainty, we then designate the parent node (i.e., causes) as S_E (or evidence set) and the child nodes (i.e., effects) as S_Q (or query set). The correlation (ρ) among the nodes, $X_1, X_2, \ldots, X_{20}$ is represented by the variance–covariance matrix, R. Interested readers may refer to [70] for details of the model construction and implementation. Our C-VA tool detects the weakest link based on the posterior probability computation done by Eq. (1).

$$\begin{aligned} &\textit{Find} \quad Rank(E_i) \\ &\textit{where}, \quad E_i = P(S_Q|S_E);\ \textit{for a given } R \textit{ matrix} \\ &S_Q,\ S_E \textit{ are probablity densities } f_i(x_i) \textit{ or cumulative distribution } F_i(x_i)). \\ &\textit{Subject to}: \quad S_E, S_Q \in U;\ U = \{X_1,\ X_2 \ldots,\ X_{20}\} \\ &0 \le \rho\left(X_i, X_j\right) \le 1, \text{ when an arc exists between } S_Q \text{ and } S_E \text{ nodes} \\ &\rho\left(X_i, X_j\right) = 0, \text{ Otherwise} \end{aligned} \tag{1}$$

For all practical purposes, it is assumed that the set of S_Q or S_E is disjoint.

Example. A CTO observes a security breach in an organization due to a SEF failure and wishes to determine the point of vulnerability that caused it, as shown in Table 5.

4. Methodology & data

In the following sub-sections we first discuss the basics of BBN, the advantages of using BBN for modeling cyber-security risk, and limitations. We then discuss the basics of Copula and use the same in our C-VA model. We also provide the C-VA algorithm here. In Section 4.7, we describe the data points used to validate our C-VA model.

Table 5
Vulnerability assessment.

Event	Details	S_Q	S_E
E_1	P (Firewall = moderate| SEF = moderate)	Firewall	Techno failure
E_2	P (Antivirus = moderate| SEF = moderate)	Antivirus	Techno failure

4.1. Bayesian Belief Network (BBN)

We chose to use BBN [54,94] as it enables reasoning under uncertainty and combine the advantages of an intuitive visual representation with a sound mathematical basis of Bayesian probability. We decided to start investigating the IT security breach study, as shown in Fig. 1, by using the belief values provided by experts about the parameter, θ, about any node X_i, and improving it as more information becomes available through experiments. Use of BBN is motivated by the fact that it has the ability to train itself based on observed data. BBN also can take into account dependence/correlation among the variables.

The root node(s) of a DAG have marginal probability tables, while the child nodes have conditional probability tables associated with them. For computing the conditional probability for a given (S_Q, S_E) pair as shown in Eq. (1), we take into account the concept of independence [87] based on the DAG. The full joint probability of these n random variables is joint distribution; this is defined as a product of conditional probabilities for every node-parent combination as shown in Eq. (2).

$$\begin{aligned} &P(S_Q \mid S_E) = \frac{P(S_Q \cup S_E)}{P(S_E)} \\ &P(S_Q \cup S_E) = \prod_{i=1}^{n} P(X_i|\text{Parents}(X_i)) \\ &S_Q, S_E \in U \text{ and } U = \{X_1, X_2 \ldots, X_n\} \\ &\text{Note}: \ S_Q \text{ is equivalent to prior belief about a paramter, } \theta \end{aligned} \tag{2}$$

For example:

Event	Details	$P(S_Q\|S_E)$
E_1	P (Firewall = moderate|SEF = moderate)	= P(SEF|FW,AV) * P(FW|SPF) * P(AV|SPF) * P(SPF)
E_2	P (Antivirus = moderate|SEF = moderate)	= P(SEF|FW,AV) * P(AV|SPF) * P(FW|SPF) * P(SPF)

There are two techniques such as (i) top–down (or causal inference) and (ii) bottom–up (or diagnostic) to solve Eq. (1). S_Q comprises child nodes (i.e., effects) and S_E represents parent nodes (i.e., causes); in turn this is called a *causal or top down inference*. In a *diagnostic or bottom up inference* technique, S_Q comprises parent nodes (i.e., causes) and S_E comprises child nodes (i.e., effects).

4.2. Limitations of BBN based C-VA model

The main drawbacks of the BBN based C-VA are as follows. Firstly, specification of the conditional probability tables is time and space

```
Procedure C-VA ( )
        Input:   Number_of_nodes, DAG, Risk_amount, OV, k
        Input:   Mean, Variance, Marginals_for_nodes Set ,Inference ,Evidence Set,
Observed Set
        Output : Risk_frequency, Expected_loss, Premium  /* Array*/
         For i = 1 to Number_of_nodes            /* Generate (prior) marginals */
            Node_cdf(i) = Populate_Node_cdf ( i, mean(i), variance( i))
            Node_pdf(i) =  Populate_Node_pdf( i, mean(i), variance( i))
        End For
          R= Generate_correlation ( DAG)
          JDF=Generate_ JDF (R, Node )
          MD= Generate_ Marginal(JDF, Marginals_for_nodes Set)
          Risk_frequency= Frequency_of_failure (JDF,MD, Inference ,Evidence Set,
Observed Set)
          Expected_loss=Loss_calculation (Risk_frequency, Risk_amount)
          Variance_of_loss= Variance _calculation (Risk_frequency, Risk_amount)
          Premium = Premium_calculate (Expected_loss, Variance ,OV, k )
End  C-VA
```

```
Function Populate_Node_cdf ( i, mean(i), variance( i))
        Return Node_cdf (i)          /* Prior distribution for a node generated */
End Populate_Node_cdf
```

```
Function Populate_Node_pdf ( i, mean(i), variance( i))
        Return Node_pdf (i)          /* Prior distribution for a node generated */
End Populate_Node_pdf
```

```
Function Generate_correlation (DAG)
    For i = 1 to Number_of_nodes
        For j = i+1 to Number_of_nodes
            R (i, j)=Correlation (Node_pdf (i), Node_pdf (j))
        End For
    End For
    Modify matrix R using DAG using concepts of Independence
    Return R
End Generate_correlation
```

```
Function Generate_ JDF(R,Node)
For each Node and State combination
                Compute JDF
                    /*JDF (Node (1)  Node (n))  = Node_pdf (i) * ……..*
Node_pdf (n)
                    *Copula (Node_cdf (i) ,…….Node_cdf (n)) */
Return JDF
End Generate_ JDF
```

Fig. 2. C-VA algorithm.

```
Function Generate_Conditional(JDF, Marginals_for_nodes Set)
                Compute MD
                    /*MD=∑JDF (Node (1) … Node (n))  for the given Node and
state*/
                Return MD
End Generate_ Marginal
```

```
Function Frequency_of_failure (JDF,MD, Inference ,Evidence Set, Observed Set )
        If (Inference = "Causal Inference")        /*  P(Observed Set | Evidence Set) */
            Risk_frequency= JDF/ MD          /* Posterior Distribution generated */
        Else          /* Diagnostic inference   i.e.,  P(Evidence Set |Observed Set ) */
            Risk_frequency = JDF/ MD…    ./* Posterior Distribution generated */
        End if
        Return Risk_frequency
End Frequency_of_failure
```

Fig. 2 (*continued*).

consuming. If the number of nodes or variables for a DAG is large, then the number of joint probability values to be enumerated would be exponentially large. For example, in case of the DAG shown in Fig. 1, there are 20 variables, each having 7 states, the size of the joint probability would be 20^7, or 1280 million. This would make *probabilistic inference* computationally very costly and time consuming. Secondly, the probability distribution associated to each node can only be a normal distribution. To overcome the above limitations we propose to use the concepts of Copula to make our C-VA model more robust. There are no restrictions on the choice of marginal distributions [70,73]. A brief introduction about Copula is discussed in the following section.

4.3. Concepts of Copula

Copula is a function, which allows us to combine univariate distributions to obtain a joint distribution with a particular dependence structure. In our C-VA model as shown in Fig. 1, there are 20 random variables (RV) i.e., X_1, X_2, ..., X_{20}. Each RV has a marginal cumulative distribution function (CDFs) such as $F_1(x_1)$, $F_2(x_2)$, ..., $F_{20}(x_{20})$, respectively. We are interested to compute the joint cumulative distribution i.e., $F(x_1,x_2, \ldots, x_{20})$. According to Sklar's Theorem it follows a joint cumulative distribution (F), which can be written as a function of marginals, as shown in Eq. (3) [91].

$$F(x_1, x_2, \ldots\ldots\ldots\ldots, x_{20}) = C[F_1(x_1), F_2(x_2), \ldots\ldots\ldots, F_{20}(x_{20})] \tag{3}$$

where $C(u_1,u_2\ldots\ldots\ldots\ldots u_{20})$ is a joint distribution function with uniform marginals [21,75,76].

In our C-VA model each F_i is continuous, so the function C (i.e., Copula) is unique. Given that F_i and C are differentiable, the joint density $f(x_1, x_2, \ldots, x_{20})$ can be written as:

$$f(x_1, x_2, \ldots, x_{20}) = f_1(x_1)\ldots\ldots \times f_{20}(x_{20}) \times c[F_1(x_1), F_2(x_2), \ldots\ldots\ldots, F_{20}(x_{20})] \tag{4}$$

where $f_i(x_i)$ is the density corresponding to the cumulative distribution function $F_i(x_i)$ and c is the Copula density [21,75,76].

From Eq. (4), it is clear that the Copula density (c) encodes information about dependence among X_is. Hence, c is called the dependence function. Thus, in short, in this case a Copula is a probability distribution on a 20 dimensional unit cube $[0, 1]^{20}$ for which every marginal distribution is uniform on the interval [0,1].

4.3.1. Correlation measurement

The correlation among the random variables of our C-VA model, is captured in pairs, using measures of dependence or association. Two common measures are Spearman (ρ) and Kendall (τ) correlation coefficients. The correlation matrix so obtained is termed R*. The final R* matrix is obtained by using the transformations $r_{ij} = \sin(\Pi\tau_{ij} / 2)$ and $r_{ij} = \sin(\Pi\rho_{ij} / 6)$, respectively, for Kendall and Spearman [21,75,76]. The correlation matrix (R*) is for our C-VA model obtained from the data and domain experts.

4.4. Gaussian Copula based C-VA model

Broadly speaking, there are two types of Copula, such as Gaussian and Archimedean (such as Clayton, Frank and Gumbel) [21,34,75,76]. In this study we have used Gaussian Copula aided C-VA for risk assessment and quantification since (i) there exists a linear correlation among the nodes of the DAG and (ii) based on expert opinion, we have arrived at the fact that for each individual IT risks follow a normal distribution. The Gaussian Copula aggregates multiple normal distributions for determining the vulnerability. Gumbel Copula is used to combine extreme distributions. Archimedean and t-copulas are used to combine distributions, which have dependence in the tail [21,34,75,76]. Incorporating the R matrix and assuming a multivariate normal density $\phi^{(20)}(y_1,., y_{20}|R^*)$ Eq. (4) can be rewritten as follows [21]:

$$\phi^{(20)}(y_1, \ldots\ldots\ldots, y_{20}|R^*) = \phi_1(y_1) \ldots\ldots\ldots\ldots \times \phi_{20}(y_{20}) \times c_{20}[\Phi(y_1), \ldots\ldots\ldots \Phi y_{20})|R^*] \tag{5}$$

here, Φ and ϕ denote univariate standard normal distribution respectively. We derive the Gaussian Copula formula for our C-VA model [21] as follows:

$$c[\Phi(y_1), \ldots\ldots\ldots \Phi y_{20}))] = \frac{\phi^{(n)}(y_1, \ldots\ldots\ldots, y_{20}|R^*)}{\phi_1(y_1) \ldots\ldots\ldots\ldots \times \phi_{20}(y_{20})}$$

$$c[\Phi(y_1), \ldots\ldots\ldots \Phi y_{20}))] = \frac{\dfrac{e^{\left\{-\frac{1}{2}y \times R^{-1} \times y^T\right\}}}{\sqrt{2 * 20 \times |R^*|}}}{\dfrac{e^{\left\{-\frac{1}{2}y \times I \times y^T\right\}}}{\left(\sqrt{2 * 20}\right)^{20}}} = \frac{e^{\left\{-\frac{1}{2}y \times \left(R^{-1} - I\right) \times y^T\right\}}}{|R^*|^{1/2}}. \tag{6}$$

Details can be found in [21]. In summary it can be stated, as shown in Fig. 4, that the inputs needed for our C-VA are: (i) causal diagram; (ii) marginal distributions (such as Beta, Gamma, Poisson, Log-normal) for each node (iii) the correlation matrix (R), which describes the dependence among the marginal's; and (iv) choice of Copula function. The output is the vulnerability assessment table (Table 8).

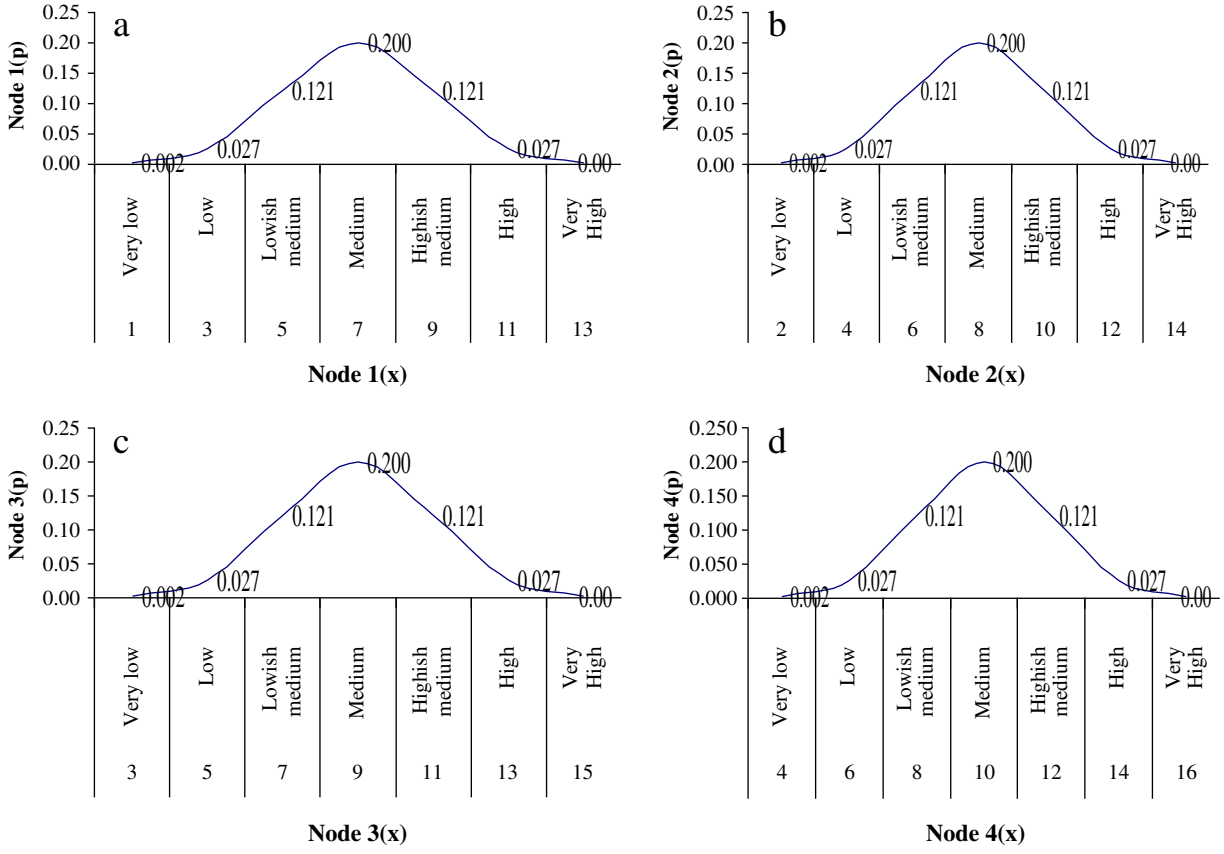

Fig. 3. Prior belief.

4.5. CBBN based C-VA algorithm

The algorithm is given in Fig. 2. It has 6 functions, as shown below:

(i) Node_cdf ( ),
(ii) Node_pdf( ),
(iii) Generate_correlation( ),
(iv) Generate_ JDF( ),
(v) Generate_ Conditional( ),
(vi) Frequency_of_failure( ).

Based on the DAG supplied by the user, the functions Node_cdf( ) and Node_pdf( ) populate the nodes. The inputs to the function are the number of nodes, the DAG and the mean and variance for each of the nodes. The output results in marginal probability density and distribution functions (i.e., pdf and cdf) for each of the nodes. Each continuous variable has 7 states (very low, low, low-medium, medium, high-medium, high, very high). The Generate_correlation( ) function takes the above populated nodes as input and generates the correlation matrix (R) from the nodes. The R matrix is modified using the DAG supplied by the user based on domain knowledge provided by experts. If there are no arcs between two nodes of the DAG, then the correlation for that pair is set to zero. The Generate_JDF( ) function takes the R matrix and the node distributions (pdf and cdf) and creates a joint distribution. Then, based on the requirement of the user, the marginal distributions are computed by the function Generate_Marginal( ). The inputs are the joint distribution function and the set of nodes for which the marginal distribution is needed. Frequency_of_failure( ) computes the probability of a security breach for a set of observed and evidence nodes. Frequency_of_failure( ) uses the joint distribution function and the marginal distribution as inputs.

4.6. Complexity analysis of CBBN based C-VA algorithm

The CBBN based C-VA algorithm requires a non-polynomial number of probability computations. There are n BBN nodes, each having m states each. The function Generate_JDF( ) generates an m^n celled joint distribution table. Generate_Marginal( ) generates for n nodes, thus 2^{n-2} determines conditional distributions. For example for 18 nodes, 2^{18} distributions are generated. Frequency_of_failure( ) takes each cell from the joint distribution table and divides it by the corresponding marginal distribution to compute the conditional probability (i.e., the posterior distribution). The computation is shown in Fig. 2.

4.7. Data for our C-VA model validation

However, to show as a proof of concept we have kept ourselves restricted to 4 nodes only (SPF, FW, AV and SEF) in this study. We have collected log data of perimeter security elements [43], from a premier business management school in India, for a period of two years, and computed their averages. On analysis we note that each of the 4 nodes follows normal distribution. Fig. 3a–d shows the prior belief distributions (i.e., probability density function (pdf)) of the nodes SPF, FW, AV and SEF. The x-axis represents the range of values for each of the nodes (i.e., x_i) and the y-axis represents the probability (i.e., p_i) of event occurrence. The values of the x-axis stretch to 3 times the standard deviation on either side of the mean. In Fig. 3a, the x-axis indicates the technology policy failure occurring over a month. We note that 7 failures occur on average, with a variance of 2 failures. Each point plotted on the x axis represents the mean of each of these ranges. For example, the range 3 to 5 depicts very low failure. The mean failure for the range is 4. For example, the probability value corresponding to 10 is 0.1995. This indicates that there is 20% chance of 10 failures occurring in a month. Table 6 illustrates the prior belief for each node in terms of: (i) distribution type, (ii) parameters (μ, σ), (iii) ranges and (iv) expectation of the loss amount distribution for each of the nodes as Binomial (1000, 0.2). Table 7 depicts the correlation matrix, R, among the nodes. In this study, we assume the loss distribution with mean (E (L_i)) of 200 and a variance (V (L_i)) of 160.

Table 6
Prior marginal beliefs and loss distribution.

Causal Variable	Failure distribution				Loss distribution
	Distribution	Failure parameters	Range	States	Parameters
SPF	Normal	$\mu = 7; \sigma = 2$	[1–13]	7	Binomial (1000, 0.2)
Firewall failure	Normal	$\mu = 8; \sigma = 2$	[2–14]	7	Binomial (1000, 0.2)
Anti-virus failure	Normal	$\mu = 9; \sigma = 2$	[3–15]	7	Binomial (1000, 0.2)
SEF	Normal	$\mu = 10; \sigma = 2$	[4–16]	7	Binomial (1000, 0.2)

Table 7
Correlation matrix (Rho).

	SPF	Firewall failure	Anti-virus failure	SEF
SPF	1.0			
Firewall failure	0.0	1.0		
Anti-virus failure	0.1	0.1	1.0	
SEF	0.0	0.0	0.1	1.0

5. CBBN based C-VA: results

The output of the C-VA is as follows: (i) vulnerability assessment report and (ii) expected cyber-risk value at each of the nodes of the DAG supplied to the model.

5.1. Vulnerability assessment report

We started our study with the belief that the probability of moderate firewall failure and antivirus leading to an IT security breach was 0.20 respectively. We next used our CBBN based C-VA model to compute the vulnerability of the firewall. The posterior probability computation by the Frequency_of_failure( ) module of the C_VA procedure reports the probability of vulnerability for the firewall as 0.50 and that of anti-virus as 0.38. Table 8 ranks the malicious events, based on the C-VA model shown in Eq. (1). It thus follows that the firewall is the weakest link, which malicious attackers will use to break into the organization network.

Fig. 4a–b shows the comparison between the posterior and prior distributions for the events.

5.2. Cyber-risk quantification

Using the Collective Risk Model [52], we construct the combined distribution of the loss, E (S_i) by assuming both the frequency of the

Table 8
Vulnerability assessment report.

Event	Details	Prior belief	Posterior belief
E_1	P (Firewall = moderate| SEF = moderate)	0.20	0.49
E_2	P (Antivirus = moderate| SEF = moderate)	0.20	0.38

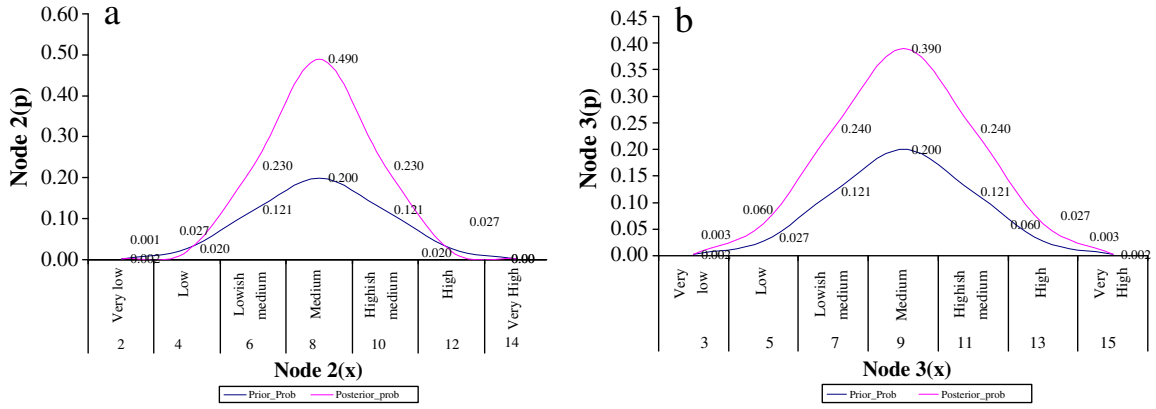

Fig. 4. Prior and posterior probability distributions of the events.

attack, E (N_i) and the associated loss, E (L_i) as stochastic variables. The central tendencies of the combined loss distribution, E (S_i), are defined in Eq. (7).

$$E(S_i) = E(N_i) * E(L_i) Var(S_i) = E(N_i) * Var(L_i) + \{E(L_i)\}^2 * Var(N_i) \quad (7)$$

The basic inputs for cyber-risk quantification are the C-VA report and the expected loss distribution at each node. The output is the expected loss due to cyber-risk; this is represented in terms of the mean and variance. We denote the frequency of failure as E (N_i) as per Eq. (7). In this study, we assume the expectation of the loss amount distribution for each of the nodes to be of the form Binomial (1000, 0.2). Table 9 illustrates the expected loss or claim severity (i.e., E (S_i)) and its variance (i.e., Var (S_i)) as obtained using Eq. (1).

5.3. Cyber-risk insurance product characteristics

We propose a cyber risk insurance product that has provisions of indemnifying the first and third party perils related to cyber risks such as (i) business interruption due to failure of software or hardware or virus attack or DDoS or (ii) loss to a third party due to virus-infected mail sent to them or due to downloading of a document or clicking on a hyperlink on a website. We assume that the claim distributions are short-tailed. The first party claims for cyber disasters will be reported immediately and be settled. While the third party claims (e.g. a virus in a mail attachment) would take a slightly longer time to settle. The product will have an exclusion policy that no compensation will be paid to the insured for any and all instances of self-inflicted loss, accessing insecure websites, acts of terrorism and/or improper self-protection.

Currently, the maximum coverage provided to e-businesses, by an insurer, is only $200 million [1,2,69,81,82]. Only after more data is collated about cyber disasters by insurance companies, risk analysts and the government on a regular basis can the claim distributions be updated. Similar practice has been followed by other insurance business such as (i) life and marine insurance, (ii) motor car insurance and (iii) home insurance. Cyber insurers should initially go to market with products that have limited chance of exposure, small claim amounts to be indemnified and with limited product traits. Ideally they should launch them in small geographic spread/markets too.

Table 9
Cyber-risk computation.

Event	Details	Probability	E(S)	Var(S)
E_1	P (Firewall = moderate| SEF = moderate)	0.49	1600	81,280
E_2	P (Antivirus = moderate| SEF = moderate)	0.38	1800	81,440

5.4. Premium fixation

Based on the expected loss arrived at in Eq. (9), the premium (Pr_i) at each node is defined as the expected loss E (S_i) multiplied by the quantity of the overhead loading (OV) plus the variance ($V(S_i)_i$) multiplied by the contingency loading (k) [52]. The premium (Pr_i) is arrived at by using Eq. (8):

$$Pr_i = (1 + OV)^* E(S_i) + k^* \sqrt{Var(S_i)} \quad (8)$$

where OV is the loading factor and k is the contingency loading.

The loading factor is provided to account for the profit and other related administrative charges. The contingency loading (k) accounts for any variation from the mean. Fig. 5 illustrates the risk and premium computation modules. The inputs to this module are risk-frequency and risk-amount generated from the CBBN based C-VA algorithm (Fig. 4). Loss_calculation( ) provides the expected amount of loss due to a security breach, occurring at a node. The inputs are the frequency of failure for the node and the associated loss distribution. Premium_calculate( ) combines the expected amount of loss and the overhead (OV) and contingency (k) loading as inputs and determines the premium as output.

We arrive at the premium by using Eq. (10). We will now illustrate the model using the following example. We assume an expense loading of 10% of the risk premium and a contingency loading (k) of 10% of standard deviation, for premium calculation. Table 10 illustrates the results.

5.5. Sensitivity analysis of CBBN based C-VA model

The aim of a sensitivity analysis is to estimate the rate of change in the output of a model with respect to changes in model inputs. Such knowledge is important for: (i) evaluating the applicability of the model, (ii) determining parameters for which it is important to have more accurate values, and (iii) understanding the behavior of the system being modeled.

For this study we change the following inputs, namely marginal distributions of the nodes, by changing the mean and variances; correlation matrix (R). We follow the subsequent methodology: (i) change the mean of a node by 5% in a gradient of 1%, while the other nodes were kept constant; (ii) change the mean of each of the nodes in graduations of 1%, to a maximum of 5%. We then run the CBBN based C-VA model, which finds that there are no significant changes noted in the posterior distributions.

```
Function Loss_calculation(Risk_frequency, Risk_amount)
        Expected loss = Risk_frequency * Risk_amount
        Return Expected loss
End Loss_calculation
```

```
Function Variance_calculation(Risk_frequency, Risk_amount)
        Compute Variance
        Return Variance
End Variance_calculation
```

```
Function Premium_calculate(Expected loss, OV )
        Premium = Expected loss *( 1+ OV) + k* √Variance
        Return Premium
End Premium_ calculate
```

Fig. 5. Module for risk and premium computation.

6. Utility based preferential pricing (UBPP) model for cyber insurers

We propose a process model [26,96,102,103] for facilitating decision making by CTOs whether to transfer the cyber-risk or to manage it in-house. Let us assume that the CTO of an e-commerce organization wishes to decide whether he should opt for cyber-insurance to mitigate the financial losses that could arise due to a malicious DDoS. Using our C-VA model the CTO is aware of the fact that the DDoS attack could arise due to vulnerabilities in the: (i) firewall, or (ii) anti-virus, or (iii) both. She is also aware that the DDoS may never materialize (i.e., the firewall and the anti-virus resist the attack). The probability of each of the malicious events is P_i (i.e., a, b, ¢ and d). He has also computed the cyber-risk for his organization using the C-VA model. If the CTO has insured, there is cash outflow of the premium (Pr) and an inflow of $XDoS_i$ (i = type of security element compromised) amount as indemnification. While, if the CTO is uninsured there occurs a direct loss of $XDoS_i$ amount. An insured organization would lose Pr amount if no event occurs. The CTO is weighing her options to buy cyber-insurance vis-à-vis handling cyber-risk in-house. In Fig. 6 we illustrate the possible scenarios that could lead to a DDoS and also the resulting financial impact to an organization.

6.1. UBPP model: the mathematical formulation

Our UBPP model shown in Eq. (9) computes the premium, Pr_i for a cyber insurer based on the following assumptions: (i) the probability of each of the malicious events is β_i and $\left(\sum_{i=1}^{n}\beta_i = 1\right)$; (ii) the online revenue earned by the organization is R; (iii) the expected utility for the insured ($EU_{insured}$) is greater than the expected utility of the uninsured ($EU_{uninsured}$) [56,99]. The occurrence of a malicious event due to any of the vulnerabilities getting exposed leads to a loss of $XDoS_i$ (where $i = 1, \ldots, 4$) amount. If insured the loss is indemnified by the insurer, else not. The utility (or reduction in wealth/revenues) for the ith event for the insured and the uninsured organization is denoted by EU_i (where $i = 1,2$).

$$
\begin{aligned}
&\textit{Find } Pr_i\\
&\textit{Subject to}: EU_{insured} \geq EU_{uninsured}\\
&EU_{insured} = \sum_{i=1}^{n\_events} \beta_i \times UI_i\\
&EU_{uninsured} = \sum_{i=1}^{n\_events} \beta_i \times UNI_i\\
&UI_i = (W - Pr - \chi \times (XDoS_i + XDoS_i)); \chi = 1 \text{ if event occurs}\\
&\qquad\qquad \chi = 0 \text{ otherwise}\\
&UNI_i = (W - \chi \times XDOS_i); \chi = 1 \text{ if event occurs}\\
&\qquad\qquad \chi = 0 \text{ otherwise}
\end{aligned}
\tag{9}
$$

where UI_i and UN_i can take any function form, such as linear, quadratic etc.

A rational decision maker would only insure the e-business, if the utility arising from insurance is greater or equal to the utility obtained from non-insuring. Using this basic premise of utility theory [56,99], our UBPP models, the expected premium (Pr) to be charged from the insured firm. Eqs. (10) and (11) respectively illustrate the expected utility [35] of insured ($EU_{Insured}$) and non-insured ($EU_{Not\ Insured}$) organizations.

$$
\begin{aligned}
EU_{Insured} = {} & a*EU(R - Pr - XDoS_{FW} + XDoS_{FW}) + b*EU(R - Pr - XDoS_{AV} + XDoS_{AV})\\
& + ¢*EU(R - Pr - XDoS_B + XDoS_B) + d*EU(R - Pr)
\end{aligned}
\tag{10}
$$

$$
EU_{Not\ Insured} = a * EU(R - X_{FW}) + b*EU(R - X_{AV}) + ¢*EU(R - X_B) + d*EU(R) \tag{11}
$$

Table 10
The basic premium amount for each event.

Event	Details	Probability	E(S)	Var(S)	Premium ($)
E_1	P (Firewall = moderate|SEF = moderate)	0.49	1600	81,280	$1789
E_2	P (Antivirus = moderate|SEF = moderate)	0.38	1800	81,440	$2089

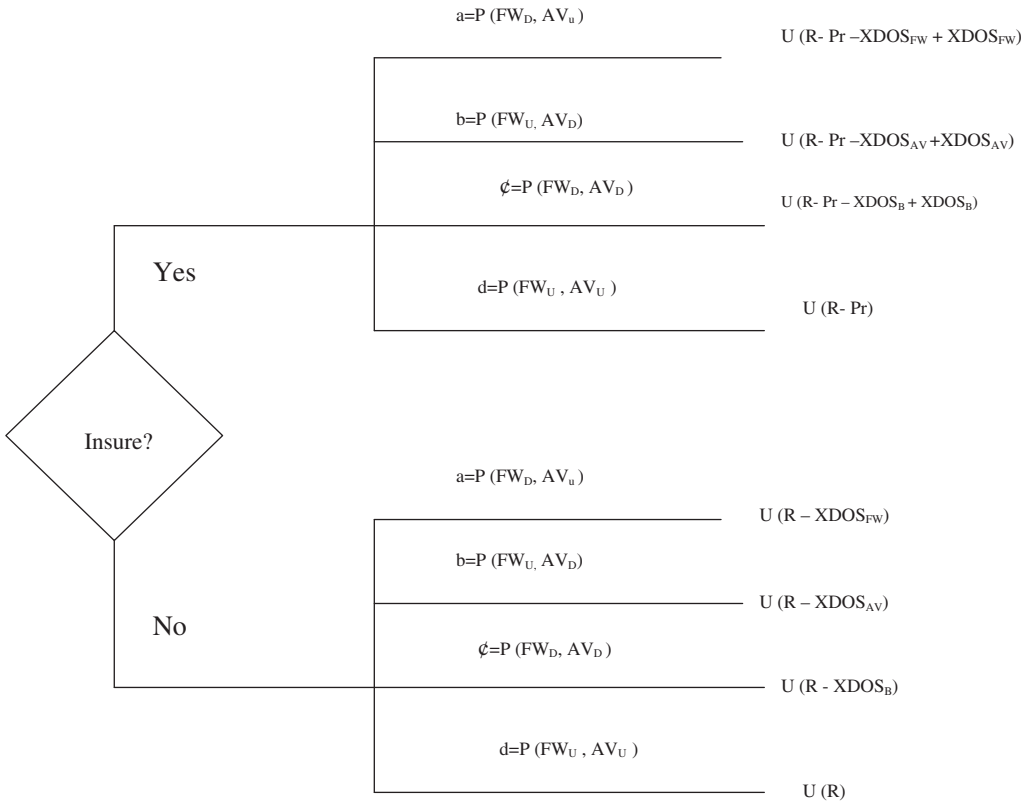

Fig. 6. Decision tree of utility payoffs for insuring vis-à-vis not insuring cyber-risk [$XDOS_{FW}$ = loss due to Firewall failure; $XDOS_{AV}$ = loss due to Anti-virus failure; $XDOS_B$ = loss due to both Firewall and Anti-virus failure; a + b + ¢ + d = 1; U = up; D = down].

6.2. Risk and premium calculation

Each organization has its own risk profile (such as neutral, risk averse and constant risk averse) based on its revenue, growth plans and other financial traits. The risk profile of the firm is denoted by a unique utility function. Our UBPP model aims to compute the risk premium for companies based on its risk profiles.

6.2.1. Risk neutral

Let us assume that the organization is risk neutral, with utility function U (R) = R [56,99]. The utility functions of the insured and not insured are illustrated in Eqs. (12) and (13).

$$EU_{Insured} = R * (a + b + ¢ + d) - Pr * (a + b + ¢ + d) \quad (12)$$

$$EU_{Not\ Insured} = R * (a + b + ¢ + d) - a * XDoS_{FW} - bXDoS_{AV} - ¢XDoS_B \quad (13)$$

It is a basic assumption that the expected utility of an insured organization is greater than that of a not insured organization (i.e., Eq. (14)) because the former gets indemnified for all losses in case of a contingency.

$$EU_{Insured} \geq EU_{Not\ Insured} \quad (14)$$

In this case, a risk neutral organization would insure, if Eq. (14) holds. The premium of a risk neutral organization is given by Eq. (15).

$$R*(a + b + ¢ + d) - Pr*(a + b + ¢ + d) \geq R*(a + b + ¢ + d) - a*XDoS_{FW} - bXDoS_{AV} - ¢XDoS_B 0 \leq Pr \leq a*XDoS_{FW} + bXDoS_{AV} + ¢XDoS_B \quad (15)$$

A risk neutral online business organization insures, if the premium value lies between zero and the organizations' expected loss.

6.2.2. Risk averse

If the organization is risk averse, we assume the utility functions [56,72,99] as shown in Eq. (16).

$$U(R) = \begin{cases} R; & If\ \ Insured \\ E(R) - 0.5 * K * XDoS_i^2; & If\ \ not\ \ insured \end{cases} \quad (16)$$

Here the expected loss ($XDoS_i$) is a stochastic variable. This indicates that the organization is trying to keep the loss as close as possible to the expected loss. The utility of the insured and not insured user is illustrated in Eqs. (17) and (18) respectively. Using Eq. (10) and the utility function in Eq. (16), we get the expected utility of the insured user as:

$$EU_{Insured} = R - Pr. \quad (17)$$

Using Eq. (10) and the utility function, we get the expected utility of the uninsured organization as:

$$(R - Pr) \geq \left(R - a*XDoS_{FW} - b*XDoS_{AV} - ¢*XDoS_B - \frac{a*K}{2} * XDoS_{FW}^2 - \frac{b*K}{2} * XDoS_{AV}^2 - \frac{¢*K}{2} * XDoS_B^2 \right) Pr \leq a*XDoS_{FW} + b*XDoS_{AV} + ¢*XDoS_B + \frac{K}{2} \left[a*XDoS2_{FW}^2 + b*XDoS_{AV}^2 + ¢*XDoS_B^2 \right]. \quad (18)$$

Table 11
Risk premium vis-à-vis risk profile for a DDoS attack.

C-VA model					UBPP model	
Failure probability		Loss amount ($)		Expected loss ($)	Risk profile	Risk premium ($)
a = P (FW_D, AV_u)	0.6	$XDoS_{FW}$	6000	5500	Neutral	5500
b = P (FW_U, AV_D)	0.2	$XDoS_{AV}$	8000		Constant risk averse	10,275
¢ = P (FW_D, AV_D)	0.1	$XDoS_B$	3000		Risk averse	20,000
d = P (FW_U, AV_U)	0.1	–	0		–	–
a = P (FW_D, AV_u)	0.1	$XDoS_{FW}$	6000	3100	Neutral	3100
b = P (FW_U, AV_D)	0.2	$XDoS_{AV}$	8000		Constant risk averse	10,968
¢ = P (FW_D, AV_D)	0.3	$XDoS_B$	3000		Risk averse	33,100
d = P (FW_U, AV_U)	0.4	–	0		–	–
a = P (FW_D, AV_u)	0.01	$XDoS_{FW}$	6000	1160	Neutral	1160
b = P (FW_U, AV_D)	0.10	$XDoS_{AV}$	8000		Constant risk averse	7554
¢ = P (FW_D, AV_D)	0.10	$XDoS_B$	3000		Risk averse	18,270
d = P (FW_U, AV_U)	0.79	–	0		–	–
a = P (FW_D, AV_u)	0.1	$XDoS_{FW}$	6000	5500	Neutral	5500
b = P (FW_U, AV_D)	0.5	$XDoS_{AV}$	8000		Constant risk averse	10,498
¢ = P (FW_D, AV_D)	0.3	$XDoS_B$	3000		Risk averse	43,600
d = P (FW_U, AV_U)	0.1	–	0		–	–

As Eq. (14) also holds in this case, the premium of a risk averse organization is given by Eq. (19).

$$(R-\Pr)\geq\left(R-a^{*}XDoS_{FW}-b^{*}XDoS_{AV}-¢^{*}XDoS_{B}-\frac{a^{*}K}{2}{*}XDoS^{2}-\frac{b*K}{2}{*}XDoS_{AV}^{2}-\frac{¢^{*}K}{2}{*}XDoS_{B}^{2}\right)\Pr\leq a^{*}XDoS_{FW}+b^{*}XDoS_{AV}+¢^{*}XDoS_{B}+\frac{K}{2}\left[a^{*}XDoS_{FW}^{2}+b^{*}XDoS_{AV}^{2}+¢^{*}XDoS_{B}^{2}\right]. \quad (19)$$

As evident from Eq. (19), if the variance from the expected loss is high then a risk averse organization should expect to pay a higher premium.

6.2.3. Constant risk averse

If the organization is risk averse with a utility function $U(R) = 1 - e^{(-R/1000)}$. According to Pratt–Arrow's measure, a utility function is constant if $-U''(R)/U'(R)$ is constant [56]. The utilities of the insured and not insured organization are illustrated in Eqs. (20) and (21) respectively. Using Eq. (16) and the utility function, we get the expected utility of the insured organization as:

$$Eu_{Insured} = \left(1-e^{\frac{-(R-\Pr)}{1000}}\right). \quad (20)$$

Using Eq. (11) and the utility function, we get the expected utility of the uninsured organization as

$$Eu_{Not\ \ Insured} = 1-e^{\frac{-R}{1000}}*\left[a^{*}e^{\frac{XDoS_{FW}}{1000}}+b^{*}e^{\frac{XDoS_{AV}}{1000}}+¢e^{\frac{XDoS_{B}}{1000}}+d\right]. \quad (21)$$

Eq. (14) also holds in this case. The premium of a constant risk averse organization is given by Eq. (22).

$$\left(1-e^{\frac{-(R-\Pr)}{1000}}\right) \geq 1-e^{\frac{-R}{1000}}*\left[a^{*}e^{\frac{XDoS_{FW}}{1000}}+b^{*}e^{\frac{XDoS_{AV}}{1000}}+¢^{*}e^{\frac{XDoS_{B}}{1000}}+d\right]$$
$$\Pr\leq 1000^{*}\left[\ln\left(a^{*}e^{\frac{XDoS_{FW}}{1000}}+b^{*}e^{\frac{XDoS_{AV}}{1000}}+¢^{*}e^{\frac{XDoS_{B}}{1000}}+d\right)\right]. \quad (22)$$

Example. Assume that the organization that faced a DDoS has online revenues of $5 billion. The CEO has to decide in consultation with the CSO whether or not to opt for the insurance policy. In Table 11, we consider four scenarios with probabilities (a, b, ¢ and d) that can lead to a DDoS and derive the expected loss using the C-VA model and risk premium for three different user risk profiles: (i) neutral, (ii) risk averse and (iii) constant risk averse using the UBPP model.

It is evident from Table 6 that the risk neutral organization would invest in the cyber-insurance policy only if the risk premium is equal to the expected loss. The risk averse organizations would be ready to pay a markup to opt for cyber-insurance because they prefer to transfer the risk to the insurer rather than handling it themselves. In all the four cases in Table 6, it is observed that risk averse and constant risk averse organizations should expect to pay higher premiums. In this context it can be concluded that the cyber-risk insurance products once introduced would find maximum popularity among risk averse online business organizations. It also shows that cyber-risk insurers need to skillfully design their products to attract various types of users and varying risk profiles.

7. Discussion

Organizations globally invest a lot in IT security budget [40] to minimize the loss arising due to a security breach. This helps to reduce the probability of attack. But, the impact of malicious attack causes serious implications to the top lines and bottom lines of an organization. Minimizing the information security breach loss is as important for the top executives as any other business risk arising due to operational activity [10,23,37,104,105]. Geer et al. in their study highlight that a risk management strategy has to be followed by organizations. Organizations should also comply with regulations such as Basel II Capital Accord, Gramm–Leach–Bliley (GLB) Act, HIPPA and SOX in the terms of risk management and accountability [37]. COBIT and operational risk mitigation principles clearly mandate that a IT security risk management should comprise of risk identification, risk assessment and risk mitigation [23,93]. In this study we propose a process model for vulnerability assessment (i.e., C-VA model). We attribute the reasons for a security failure in an organization to (i) technological and (ii) organizational parameters. Our C-VA model is different from the process models proposed by Strecker et al., Salmela, Weiß and Winkelmann, 2011, as we have used the principles of FCAPS and BS7799 to model our solution [88,96,102,103]. Our C-VA model can be applied to any organization to assess risk, based on the log files retrieved from security appliances. Our C-VA model takes quantitative log data from perimeter and core security appliances as the basic input (i.e., marginal probability distributions). This provides subjective perception about cyber risk [22]. We have also taken into account that threats to organizational information assets are interdependent or correlated as security

appliances have related vulnerabilities [20]. To identify the vulnerabilities in the security appliances and in the organizational network we use the concepts of probabilistic inference [54]. Our study is in contrast to Chen et al., where the author uses the concept of queuing theory to quantify the vulnerability matrix [20]. We use concepts of Copula to effectively compute the posterior probability for the nodes of the C-VA model as shown in Eq. (1). Our paper is different from Herath and Herath [46], as we have used Gaussian Copula to model correlated risk as opposed to Archimedean Copulas (i.e., Clayton and Gumbel Copulas) used by them. We have modeled each node of the causal diagram as normal distribution and aggregated the data using the Gaussian Copula. The CTO or a CSO needs to choose the evidence and query nodes respectively as described in Eq. (1) to identify vulnerabilities in a corporate network. The vulnerability analysis report generated can be used to prioritize the strategies to pro-actively minimize the organizational losses. The CTO or CSO effectively updates the (i) security architecture, (ii) the security policy, (iii) organizational IT infrastructure, (iv) IT Budget, and (v) the security culture of the organization [23] to ensure proper C–I–A of organizational data.

We then input loss amount distribution for each node of the C-VA model, based on expert opinion. We use Collective Risk modeling techniques as proposed in General Insurance literature to compute the expected loss, by taking into account the likelihood of breach and impact as stochastic variables respectively [52]. This is an advanced expected loss computation technique as compared to Courtney [25]. From a business manager's perspective this study is of immense importance as it provides them insight about the quantum of loss an organization may face due to a particular threat arising due to a vulnerability being exposed. Based on it they may decide on strategies for the organization to mitigate the IT related contingency. Many organizations today invest in cyber-insurance [1,7,13–15,39,44,70,72,74,79,85,97] to minimize the loss arising due to IT security breach.

We then propose our UBPP model that helps insurers to customize premium and cyber-risk insurance schemes for the insured based on its revenues and risk taking ability. Our UBPP model helps insurers to propose attractive preferential premium for the prospective insured firms. A proper premium helps to attract customers and also to ensure that the cyber-risk insurance companies do not default. Using the collective risk modeling [52] along with overhead and contingency loading we arrive at the premium. Our UBPP model for premium is an improvement on Kahane et al.'s work on quantification of risk of backup pools, disaster recovery, and default risk [56]. Our UBPP is also different from Bohme et al. (2005) utility based model for arriving at premium for correlated cyber risk [15]. The premium value arrived using UBPP helps the business manager (especially the top management) to decide on the proportion of cyber risk to be managed in house (using technological solution) vis-à-vis buying cyber risk insurance [73]. We also provide guidelines to insurers to adequately design their cyber insurance products in terms of (i) coverage, (ii) exclusion policy, and (iii) scheme types.

From an academic prospective, our research made the following important contributions in terms of proposing: (i) CBBN based C-VA, (ii) CBBN based model for cyber-risk quantification, (iii) premium computation for cyber-risk insurance products using the concepts of Collective Risk Model; and (iv) UBPP model for preferential premium computation for customers (i.e., e-business) with varying risk profiles and wealth, using the concepts of utility modeling.

8. Conclusion

Cyber-risk insurance products help organizations in reducing the losses from cyber-risk. The use of cyber risk insurance will better help e-commerce and online organizations to promote e-transactions as the potential loss from security breaches would now be indemnified by cyber risk insurers. As more and more companies begin to adopt cyber-risk insurance products the trust in the minds of customers will increase. This will positively impact the top lines of a company too. This will also help induce cyber insurers to create more attractive products for firms.

In the beginning we posed a question: should we insure IT or not. Based on our detailed presentation, we have not only identified the many reasons that organizations should acquire cyber-insurance but we have also shown the financial trade-offs and benefits of getting cyber-insurance. We hope that our work will inspire other researchers to come up with new designs of cyber insurance products.

References

[1] T. Bandyopadhyay, V.S. Mookerjee, R.C. Rao, Why it managers don't go for cyber-insurance products, Communications of the ACM 52 (11) (2009) 68–73.
[2] T. Bandyopadhyay, V.S. Mookerjee, R.C. Rao, A model to analyze the unfulfilled promise of cyber insurance: the impact of secondary loss, Working Paper, 2010, (http://www.utdallas.edu/~rrao/CyberBMR%5B1%5D.pdf).
[3] H. Barki, S. Rivard, J. Talbot, Toward an assessment of software development risk, Journal of Management Information Systems 10 (2) (1993) 203–225.
[4] L. Barnard, R.V. Solms, A formalized approach to effective selection and evaluation of information security controls, Computer & Security 19 (2) (2000).
[5] R.L. Baskerville, Designing Information Systems Security, Wiley, Chichester, U.K., 1988
[6] R.L. Baskerville, Information systems security design methods: implication for information systems development, ACM Computing Surveys 25 (4) (1993) 375–414.
[7] R.L. Baskerville, Strategic information Security Risk Management, Information Security, Policy, Processes and Practices, in: W.D. Straub, S. Goodman, R.L. Baskerville (Eds.) , 2008.
[8] R.L. Baskerville, V. Portougal, A possibility theory framework for security evaluation in national infrastructure protection, Journal of Database Management 14 (2) (2003) 1–13.
[9] J. Becker, B. Weiß, A. Winkelmann, Developing a business process modeling language for the banking sector—a design science approach, Proceedings of the 15th Americas Conference on Information Systems, San Francisco, 2009.
[10] B. Blakley, E. McDermott, D. Geer, B. Blakley, E. McDermott, D. Geer, Information security is information risk management, Proceedings of the workshop on New security paradigms (NSPW '01), ACM, New York, NY, USA, 2001, pp. 97–104.
[11] J. Bolot, M. LeLarge, Cyber insurance as an incentive for internet security, Workshop on the Economics of Information Security, Hanover, NH, 2008.
[12] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of Internet security breach announcements on market value: capital market reaction for breached firms and Internet security developers, International Journal of Electronic Commerce 9 (1) (2004) 69–105.
[13] R. Böhme, G. Kataria, Models and measures for correlation in cyber-insurance, Workshop on the Economics of Information Security (WEIS) University of Cambridge, UK, 2006, June.
[14] R. Bohme, G. Schwartz, Modeling cyber-insurance: towards a unifying framework, Workshop on the Economics of Information Security (WEIS), Harvard, 2010, June.
[15] R. Bohme, Security metrics and security investment models, in: I. Echizen, N. Ku-nihiro, R. Sasaki (Eds.) Advances in Information and Computer Security (IWSEC 2010), LNCS 6434, Springer-Verlag, Berlin Heidelberg, 2010, pp. 10–24.
[16] R. Böhme, Cyber-insurance revisited, Workshop on the Economics of Information Security (WEIS), Harvard, 2005.
[17] British Standards Institute, BS 7799: Code of Practice for Information Security Management (CoP). PD0003, United Kingdom, 1993.
[18] D. Cernauskas, A. Tarantino, Operational risk management with process control and business process modeling, The Journal of Operational Risk 4 (2) (2009) 1–22.
[19] A.S. Chernobai, S.T. Rachev, Frank J. Fabozzi, Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis, Wiley Publishing, 2007.
[20] P. Chen, G. Kataria, R. Krishnan, Correlated failures, diversification, and information security risk management, MIS Quarterly 35 (2) (2011) 397–422.
[21] T.R. Cleman, T. Reilly, Correlations and copulas for decision and risk analysis, Management Science 45 (2) (1999) 28–224.
[22] T.R. Cleman, R.L. Winkler, Combining probability distributions from experts in risk analysis, Risk Analysis 19 (2) (1999) 187–203.
[23] Control Objectives for Information and Related Technologies (COBIT), 3rd ed. IT Governance Institute, USA, 2000.
[24] C. Cornalba, P. Giudici, Statistical models for operational risk management, Physica A 338 (2004) 166–172.
[25] R. Courtney, Security Risk Assessment in Electronic Data Processing, AFIPS, Arlington, USA, 1977, pp. 97–104.
[26] B. Curtis, M.I. Kellner, J. Over, Process modeling, Communications of the ACM 35 (9) (1992) 75–90.
[27] M. Damianides, Sarbanes–Oxley and IT governance: new guidance on IT control and compliance, Information Systems Management 22 (1) (2005) 77–85.
[28] D.I. Dickstein, R.H. Flast, No Excuses: A Business Process Approach to Managing Operational Risk, John Willey & Sons Inc., Hoboken, New Jersey, 2009.

[29] G. Dhillon, J. Backhouse, Current directions in IS security research: towards socio-organizational perspectives, Info Systems of Journal 11 (2) (2001) 127–153.
[30] G. Dhillon, Managing Information System Security, Macmillan Press Ltd., London, 1997.
[31] G. Dhillon, Realizing benefits of an information security program, Business Process Management 10 (3) (2004) 260–261.
[32] G. Dhillon, J. Backhouse, Information system security management in the new millennium, Communications of the ACM 43 (7) (2000) 125–127.
[33] G. Dhillon, G. Torkzadeh, Value focused assessment of information system security in organizations, Information Systems Journal 16 (3) (2006).
[34] M. Dorey, P. Joubert, Modeling Copulas: An Overview, The Staple Inn Actuarial Society, 2005.
[35] K. Dutta, J. Perry, A tale of tails: an empirical analysis of loss distribution models for estimating operational risk capital, Working paper No.06-13, Federal Reserve Bank of Boston, 2011.
[36] U. Frank, Multi-perspective enterprise modeling (MEMO): conceptual framework and modeling languages, Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS), IEEE Computer Society Washington, DC, USA, Honolulu, HI, 2002, pp. 72–82.
[37] D. Geer Jr., K.S. Hoo, A. Jaquith, Information security: why the future belongs to the quants, IEEE Security and Privacy 1 (4) (2003) 24–32.
[38] L.A. Gordon, M.P. Loeb, W. Lucyshyn, R. Richardson, CSI/FBI Computer Crime and Security Survey, 2009. (GoCSI.com).
[39] L.A. Gordon, M.P. Loeb, T. Sohail, A framework for using insurance for cyber-risk management, Communications of the ACM 46 (3) (2003) 81.
[40] L.A. Gordon, M.P. Loeb, The economics of information security investment, ACM Transactions on Information and System Security 5 (4) (2002, Nov) 438–457.
[41] L.A. Gordon, M.P. Loeb, Return on information security investments, myths vs realities, Strategic Finance 84 (5) (2002) 26–31.
[42] S. Gorman, Alert on Hacker Power Play: U.S. Official Signals Growing Concern Over Anonymous Group's Capabilities, http://online.wsj.com/article_email/SB10001424052970204059804577229390105521090-lMyQjAxMTAyMDIwMDEyNDAyWj.html 2012.
[43] S. Guarrao, Principles and procedures of the LRAM approach to information systems risk analysis and management, Computers & Security 6 (6) (1987) 493–504.
[44] T. Grzebiela, Insurability of electronic commerce risks, Proceedings of the Hawaii International Conference on System Sciences, USA, 35, 2002.
[45] J.F. Hair Jr., William C. Black, Barry J. Babin, Rolph E. Anderson, Multivariate Data, Analysis, 7/E, 2010.
[46] H. Herath, T. Herath, Copula Based Actuarial Model for Pricing Cyber, Insurance Policies Insurance Markets and Companies: Analyses and Actuarial Computations, 2, 2011.
[47] J.D. Hinz, High severity information technology risks in finance, Paper Presented at the Hawaii International Conference on System Sciences, Hawaii, USA, 2005.
[48] J. Hitchings, The need for a new approach to information security, Proceedings of the 10th International Conference on Information Security (IFIP Sec '94), Curacao, NA, 2002.
[49] J. Hiwatashi, H. Ashida, Advancing operational risk management using Japanese banking experiences, Bank of Japan, Audit Office Working Paper No. 00-1, 2002, February.
[50] L. Hoffman, E. Michelman, D. Clements, SECURATE—security evaluation and analysis using fuzzy metrics, 1978. 531–540.
[51] K. Hone, J.H.P. Eloff, Information security policy—what do international information standards say? Computer & Security 21 (5) (2002) 402–409.
[52] B.I. Hossack, J. Pollard, B. Zehnwirth, Introduction to Statistics with Applications to General Insurance, Cambridge University Press, 1983.
[53] A.K. Jallow, B. Majeed, K. Vergidis, A. Tiwari, R. Roy, Operational risk analysis in business processes, BT Technology Journal 1 (2007).
[54] F.V. Jensen, Bayesian Networks and Decision Diagrams, Springer, 2001.
[55] M.E. Jonson, E. Gortz, Embedding information security into organization, Security & Privacy 5 (3) (2007) 16–24.
[56] Y. Kahane, S. Neumann, S.C. Taperio, Computer backup pools, disaster recovery, and default risk, Communications of the ACM 31 (1) (1988) 78–83.
[57] J.P. Kesan, P.M. Ruperto, J.Y. Willam, The economic case for cyberinsurance, Working Paper Series No. Paper No. LE04-004, Illinois Law and Economics, 2004.
[58] J.P. Kesan, R. Majuca, Cyberinsurance as a market-based solution to the problem of cybersecurity: a case study, Fourth Workshop on the Economics of Information Security (WEIS), Harvard, 2005.
[59] L. Kiely, T.V. Benzel, Systemic security management, Security & Privacy (2006).
[60] G.J. Klir, Bo Yuan, Fuzzy Sets and Fuzzy Logic: Theory and Applications, Phi Learning Pvt Ltd., 2009
[61] S.A. Kokolakis, A.J. Demopoulos, E.A. Kiountouzis, The use of business process modelling in information systems security analysis and design, Information Management & Computer Security 8 (3) (2000) 107–116.
[62] E. Kolkowska, G. Dhillon, Organizational power and information security rule compliance, Computers & Security 33 (2013) 3–11.
[63] R. Lederman, Adverse events in hospitals: the contribution of poor information systems, European Conference on Information Systems, (Turku, Finland), 2004.
[64] R. Lederman, Managing hospital databases: can large hospitals really protect patient data? Health Informatics 11 (3) (2005) 201–210.
[65] K.D. Loch, H. Carr, M.E. Warketin, Threats to information systems: today's reality, yesterday's understanding, MIS Quarterly 16 (2) (1992) 173–186.
[66] M.3400 TMN Management Functions, International Telecommunications Union, 1997.
[67] R.P. Majuca, W. Yurcik, J.P. Kesan, The Evolution of Cyber Insurance, 2005. (Available at: http://arxiv.org/ftp/cs/papers/0601/0601020.pdf (http://arxiv.org/ftp/cs/papers/0601/0601020.pdf), Accessed on September 19, 2005).
[68] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, B.B. Chakrabarti, A.K. Podder, Security breach losses in e-commerce through insurance, Paper Presented at the Proceedings of 4th Security Conference, Las Vegas, Nevada, 2005.
[69] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, A.K. Podder, e-Risk: a case for insurance, Paper Presented at the Proceedings of the Conference on Information Systems and Technology, New Delhi, India, 2005.
[70] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, S.K. Sadhukhan, e-Risk management with insurance: a framework using copula aided Bayesian belief networks, Paper Presented at the Hawaii International Conference on system sciences, Hawaii, USA, 2006.
[71] A. Mukhopadhyay, S. Chatterjee, D. Saha, A. Mahanti, R. Roy, S.K. Sadhukhan, Insuring big losses due to security breaches through insurance: a business model, Proceedings of the Hawaii International Conference on System Sciences, 40, IEEE Computer Society Washington, DC, USA, 2007.
[72] A. Mukhopadhyay, B.B. Chakrabarti, D. Saha, A. Mahanti, e-Risk management through self-insurance: an option model, Proceedings of the Hawaii International Conference on System Sciences, 40, IEEE Computer Society Washington, DC, USA, 2007.
[73] A. Mukhopadhyay, A Novel Framework for Mitigating e-Risk Through Insurance. , Phd Thesis IIM, Calcutta, 2007.
[74] A. Mukhopadhyay, D. Saha, A. Mahanti, A.K. Podder, Insurance for cyber-risk: a utility model. Decision, Journal of IIM Calcutta 32 (1) (2005) 153–170.
[75] R.B. Nelsen, Copulas characterization, correlation and counterexamples, Mathematics Magazine 68 (1995) 193–198.
[76] R.B. Nelsen, An Introduction to Copulas, Springer-Verlag, New York, Inc., 1999
[77] E.W.T. Ngai, F.K.T. Wat, Fuzzy decision support system for risk analysis in e-commerce development, Decision Support Systems 40 (2005) 235–255.
[78] J.F.V. Niekerk, R.V. Solms, Information security culture: a management perspective, Computers & Security (2010).
[79] H. Ogut, N. Menon, Cyber insurance and IT security investment: impact of interdependent risk, Fourth Workshop on the Economics of Information Security (WEIS), Harvard, 2005.
[80] H. Öğüt, S. Raghunathan, N. Menon, Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection, Risk Analysis 31 (3) (2011) 497–512 (2010).
[81] W. Ozeir, Risk quantification problems and Bayesian Decision Support System solutions, 1988. 229–234.
[82] D. Pauli, M. Crawford, Cyber insurance, what's that 2006. Available at http://www.cso.com.au/article/10744/cyber_insurance_what 2006.
[83] L. Ponemon, National survey on the detection and prevention of data security breaches. Available at http://www.csoonline.com/features/ponemon/ponemon102306.html 2006.
[84] R.K. Rainer, C.A. Synder, H.H. Carr, Risk analysis for information technology, Journal of Management Information Systems 8 (1) (1991) 129–147.
[85] G.E. Rejda, Principles of Risk Management and Insurance, 10th edition Pearson Publication, 2010.
[86] B. Di Renzo, M. Hillairet, M. Picard, A. Rifaut, C. Bernard, D. Hagen, P. Maar, D. Reinard, Operational risk management in financial institutions: process assessment in concordance with Basel II, Software Process: Improvement and Practice 12 (4) (2007) 321–330.
[87] S.J. Russell, Artificial Intelligence: A Modern Approach, Pearson, 2010.
[88] H. Salmela, Analyzing business losses caused by information systems risk: a business process analysis approach, Journal of Information Technology 23 (3) (2008) 185–202.
[89] R. Schmidt, K. Lyytinen, M. Keil, P. Cule, Identifying software project risks: an international Delphi study, Journal of Management Information Systems 17 (4) (2001, March) 5–36.
[90] N. Shetty, G. Schwartz, M. Felegyhazi, J. Walrand, Competitive cyber-insurance and internet security, Workshop on the Economics of Information Security, London, 2009.
[91] Sklar, Fonctions de Repartition a n Dimensions et Leurs Marges, 8, Publications del'Institut Statistique de l' Universiate de Paris, 1959, pp. 229–231.
[92] E. Smith, J.H.P. Eloff, A prototype for assessing information technology risks in health care, Computers & Security 21 (2) (2002) 266–284.
[93] C. Smithson, S. Paul, C. Smithson, S. Paul, Quantifying operational risk, Risk (2004) 57–59.
[94] J.R. Staker, Use of Bayesian Belief Networks in the Analysis of Information System Network Risk, Commonwealth of Australia, 1999.
[95] J. Sterman, Business Dynamics, Tata McGraw Hill Education Private Limited, 2010.
[96] S. Strecker, D. Heise, U. Frank, RiskM: a multi-perspective modeling method for IT risk assessment, Information Systems Frontiers 13 (2011) 595–611.
[97] G.S. Smith, Recognizing and preparing loss estimates from cyber-attacks, Information Systems Security 12 (6) (2004) 46–58.
[98] K. Thomson, R.v. Solms, L. Louw, Cultivating an organizational information security culture, Computer Fraud & Security 10 (2006) 7–11.
[99] H.R. Varian, Intermediate Economics, A Modern Approach, W W Norton Publication, 1999.
[100] H.S. Venter, J.H.P. Eloff, A taxonomy for information security technologies, Computers & Security 22 (4) (May 2003) 299–307.
[101] J. Wang, A. Chaudhury, H.R. Rao, A value-at-risk approach to information security investment, Information Systems Research 19 (1) (2008) 106–120.

[102] B. Weiß, A. Winkelmann, A metamodel based perspective on the adaptation of a process modeling language to the financial sector, Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, USA, 2011.
[103] B. Weiß, A. Winkelmann, Developing a process oriented notation for modeling operational risks—a conceptual meta model approach to operational risk management in knowledge intensive business process within the financial industry, Proceedings of the 44th Hawaii International Conference on System Sciences, Koloa, USA, 2011.
[104] P. Weill, J.W. Ross, IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, 2004.
[105] G. Westerman, R. Hunter, IT Risk: Turning Business Threats into Competitive Advantage, Harvard Business School Press, Cambridge, 2007.
[106] L. Willcocks, H. Margetts, Risk assessment and information systems, European Journal of Information Systems 3 (2) (1994) 127–138.
[107] W. Yurcik, Cyber insurance: a market solution to the internet security market failure, Workshop on the Economics of Information Security (WEIS), Berkeley, 2002.
[108] L.A. Gordon, M.P. Loeb, Budgeting Process for Information Security Expenditures, Communications of the ACM, 2006.

Arunabha Mukhopadhyay, **Ph.D.** is an Associate Professor of Information Technology & Systems Area at Indian Institute of Management Lucknow (IIM Lucknow). His research interests include IT Risk Management, Quantifying IT Risk, Cyber-risk insurance, IT Governance, IT Audit, Network Security, Healthcare IT, Network Science, Data mining, e-governance and Telecom Management. He has co-supervised 3 doctoral theses and published around 40 papers in various referred journals and conferences including *JIPS*, *IJISCM*, *Decision*, *IIMB Review*, *CSI-C*, *HICSS*, *AMCIS*, *Pre-ICIS workshops*, *GITMA*, *CISTM*, *ICEG* etc. He is the recipient of the *Best Teacher in Information Technology Management* in 2013 and 2011, by Star-DNA group B-School Award and 19th Dewang Mehta Business School Award, in India respectively. He is a Member of *IEEE*, *AIS*, *ISACA*, *DSI*, *ITS*, *IFIP WG 11.1* and a Life Member of Computer Society of India (CSI), Telemedicine Society of India (TSI), Indian Insurance Institute (III), Actuarial Society of India (ASI), All India Management Association (AIMA), System Dynamics Society of India (SDSI) and, Operations Research Society of India (ORSI). He has obtained his Ph.D. and Post Graduate Diploma in Business Management (PGDBM) from the Indian Institute of Management Calcutta (IIM Calcutta), in the area of Management Information Systems. He was awarded the *Infosys scholarship* during his Ph.D.

Samir Chatterjee, Ph.D. is a Professor and Fletcher Jones Chair of Technology, Management & Design in the Center for Information Systems & Technology at Claremont Graduate University. He is a technology designer, a healthcare IT strategist, and Founding Director of the Network Convergence Laboratory at Claremont Graduate University, California. His current research includes network security, persuasive technology and software design that support health behavior change. He has published over 100 articles in refereed conferences and journals including *IEEE Network*, *IEEE J. on Selected Areas in Communications*, *Communications of the ACM*, *Computer Networks*, *Journal of MIS*, *Decision Support Systems*, *Journal of American Medical Informatics Association (JAMIA)*, *Telemedicine & e-Health Journal*, *Information Systems Frontiers*, *Computer Communication*, *IEEE IT Professional*, *ACM CCR*, *Communications of AIS*, *Journal of Internet Technology* etc. He is an AE for MISQ and Health Systems Journal. His recent book titled "Design Research in Information Systems: Theory and Practice" published by Springer in May 2010 has become a seminal resource in Information Systems design field. He has managed as principal investigator over $2.6 million of grants from agencies such as NSF, and numerous private foundations and corporations.

Debashis Saha received the B.E. (Hons) degree from Jadavpur University, Kolkata, India, and the M.Tech. and Ph.D. degrees from the Indian Institute of Technology (IIT), Kharagpur, all in electronics and telecommunication engineering. He is currently a Full Professor with the MIS and Computer Science Group, Indian Institute of Management (IIM) Calcutta. Previously, he was with Computer Science & Engg Dept, Jadavpur University. His research interests include pervasive communication and computing, wireless networking and mobile computing, WDM optical networking, e-commerce, ICT for development and network economics. He has co-supervised 14 doctoral theses and published about 270 research papers in various conferences and journals, and directed four funded projects on networking. He has coauthored several book chapters, a monograph and five books including *Networking Infrastructure for Pervasive Computing: Enabling Technologies and Systems* (Norwell, MA: Kluwer, 2002) and *Location Management and Routing in Mobile Wireless Networks* (Boston, MA: Artech House, 2003). He is the Co-Editor-in-Chief of the International Journal of Business Data Communications & Networking (IJBDCN), had served on the editorial board of three international journals, member of the organizing/program committee of several international conferences, and is a regular reviewer of several international journals. Dr. Saha was the recipient of the prestigious *Career Award for Young Teachers* from AICTE, Government of India, and is a SERC Visiting Fellow with the Department of Science and Technology (DST), Government of India. He is a Fellow of West Bengal Academy of Science and Technology (WAST), Senior Life Member of Computer Society of India, Senior Member of IEEE, a member of ACM, a member of AIS, and a member of the International Federation of Information Processing (IFIP) Working Groups 6.8 and 6.10. He was the co-Vice-Chair of IEEE Calcutta Section (2010–2011) and was the founder chair of Calcutta Chapter of IEEE Communications Society (2003–2008) which won the 'Best Chapter of the World' award in 2008.

Dr. Ambuj Mahanti, D.Sc., is a professor at the MIS Group in IIM Calcutta for about three decades. He has been a UN Fellow on number of occasions and has taught in the University of Maryland at College Park, USA for several years. He has published widely in noted international journals and guided numerous theses on management and technology. He has also widely consulted and conducted many high-level training programs. He has served as the Dean (planning and administration) at IIM Calcutta. His current interests include heuristics, business intelligence, cloud computing, social networking and ontology based information security and compliance systems.

Samir K Sadhukhan received his M.Sc. degree in Applied Mathematics from Calcutta University (India), M.Tech. degree in Computer Science from Indian Statistical Institute (India) and MBA degree from Jadavpur University (India). Presently, he is associated with Indian Institute of Management Calcutta as Senior Systems Analyst. His research interests include algorithms in heuristic search, Network security, Mobile and Wireless network planning.