Inf Syst Front (2019) 21:997–1018
https://doi.org/10.1007/s10796-017-9808-5

Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance

Arunabha Mukhopadhyay[1] · Samir Chatterjee[2] · Kallol K. Bagchi[3] · Peteer J. Kirs[3] · Girja K. Shukla[4]

Published online: 17 November 2017

Abstract Malicious external attackers commonly use cyber threats (such as virus attacks, denial-of-service (DoS) attacks, financial fraud, system penetration, and theft of proprietary information), while internal attackers resort to unauthorized access to compromise the confidentiality, integrity, and availability (CIA) of the data of individuals, organizations, and nations. This results in an opportunity cost, a loss of market capitalization, and a loss of brand equity for organizations. Organizations and nations spend a substantial portion of their information technology (IT) budgets on IT security (such as perimeter and core security technologies). Yet, security breaches are common. In this paper, we propose a cyber-risk assessment and mitigation (CRAM) framework to (i) estimate the probability of an attack using generalized linear models (GLM), namely logit and probit, and validate the same using Computer Security Institute–Federal Bureau of Investigation (CSI–FBI) time series data, (ii) predict security technology required to reduce the probability of attack to a given level in the next year, (iii) use gamma and exponential distribution to best approximate the average loss data for each malicious attack, (iv) calculate the expected loss due to cyber-attacks using collective risk modeling, (v) compute the net premium to be charged by cyber insurers to indemnify losses from a cyber-attack, and (vi) propose either cyber insurance or self-insurance, or self-protection, as a strategy for organizations to minimize losses.

Keywords Cyber-risk quantification · IS security · Security breach · E-commerce · Logit and probit models · Cyber insurance · Self-insurance

1 Introduction

Cyber risk arises from an external attacker or an internal disgruntled employee (Bulgurcu et al. 2010) compromising a computer database or network (Moore 2005) or from transactions on the Internet (Mann 1998). These attacks spread more quickly than other crimes and cause monetary losses, as well as impacting the opportunity cost (OC), market capitalization (MC), and brand image of the breached entity (Campbell et al. 2003; Cavusoglu et al. 2004; Dash 2011; Hartwig and Wilkinson 2014). Based on Computer Security Institute–Federal Bureau of Investigation (CSI–FBI) data from 1997 to 2010, in this paper we identify the six most common types of cyberattacks: virus attacks (V), denial-of-service (DoS) attacks, financial fraud (FF), system penetration (SP), theft of proprietary information (TPI), and unauthorized access (UA). Table 1 lists some notable cyberattacks chronologically from 2007 to 2017, indicating the attackers (if known), the attack details, the victim, and the attack costs, and associates them with the attack types described above. We chose attacks

✉ Arunabha Mukhopadhyay
arunabha@iiml.ac.in

Samir Chatterjee
samir.chatterjee@cgu.edu

Kallol K. Bagchi
kbagchi@utep.edu

Peteer J. Kirs
pkirs@utep.edu

Girja K. Shukla
gkshukla78@gmail.com

[1] Indian Institute of Management Lucknow, Lucknow, UP, India

[2] Claremont Graduate University, Claremont, CA, USA

[3] University of Texas at El Paso, El Paso, TX, USA

[4] Lucknow, UP, India

Table 1 Security breaches due to cyber-attacks (2007–2017)

Sector	Year	Attacker	Attack details	Attacked	Type	Loss ($M)
Bank	2017	Unknown	All files inaccessible	Banks, ATM	V*	ND
	2013	Unknown	Change limit of credit cards	Banks	FF	45
	2008	3 individuals	Cloned credit card	2100 ATMs (FBI, 2009)	FF	9
Corporate	2013	Unknown	38 M user records	Adobe (Newman 2013)	TPI	152
	2013	Vietnamese	Identity theft (200 M)	Experian (Finkle et al., 2014)	TPI	ND
	2012	Anonymous	Cyber extortion	Symantec (Times of India, 2013)	FF	0.5
	2011	LulzSec	70 M credit card info	Sony PlayStation	FF	170
	2008	Unknown	Loss of proprietary info	ConocoPhillips	TPI	ND
	2007	Unknown	Graffiti attack	Microsoft	SP	ND
Health	2017	Unknown	All files inaccessible	National Health service	V*	ND
	2014	Chinese	4.5 M health records (McCann 2014)	Tennessee hospital	TPI	ND
	2009	Unknown	32,000 patient records	WellPoint	TPI	0.3
E-com	2014	Russian	1.2 B username	0.4 M email & social media	TPI	ND
	2014	Unknown	145 M Passwords	e-bay (Keily, 2014)	TPI	ND
	2009	Unknown	DNS flooding (Techflash, 2009)	Amazon, Walmart	DoS	ND
	2008	Chinese	10 M customer info	e-bay Korean	TPI	ND
Government	2012	Anonymous	sabotage power system	US Govt (Gorman 2012)	SP	ND
	2011	LulzSec	CIA website	CIA	SP	ND
	2010	WikiLeaks	Classified info leaked	US Defense dept	TPI	ND
	2008	Unknown	56,000 attacks	US Defense dept	TPI	ND
	2008	Russian	Shutdown servers	Georgian Govt (New York Times 2008)	DoS	ND
	2007	Unknown	Graffiti attack (New York Times 2007)	Estonian Govt	SP	ND

ND, not determinable; V*, ransom ware

perpetrated against Banking, Financial Services, and Insurance (BFSI), healthcare, and e-retail industries, as well as government agencies. External hackers tend to resort to the use of V, DoS, FF, SP, and TPI, while disgruntled employees typically resort to UA of organizational databases (Austin and Darby 2003; Gordon et al. 2009). It is evident from Table 1 that most attacks are external; FF, TPI, and SP attacks are increasing; and V and DoS attacks are the least common and have decreased over the years.

Various agencies have undertaken studies to ascertain the impact of losses from cyberattacks. A Federal Trade Commission report found that 8.3 million US citizens had been victims of identity theft in 2005 (Identity Theft Center 2007). A 2007 CSI–FBI report states that the total amount of loss suffered due to malicious attacks was $67 million. In 2009, the number of complaints submitted to the Internet Crime Complaint Center increased by 22% over 2008, and the total loss from all referred cases was $560 million, with a median dollar loss of $575—an increase of 112% from 2008 (Bureau of Justice Assistance 2009). In 2013, India alone reported a $38 billion loss in national income due to cybercrimes (Times of India 2013).

To minimize the frequency of malicious attacks, chief technology officers (CTOs) generally invest a portion of their information technology (IT) budget in IT security. This includes investment in perimeter security elements (such as firewalls, antivirus, intrusion detection systems [IDS], proxy servers, and Remote Authentication Dial-In User Service [RADIUS] servers), IT auditing, and business continuity processes and disaster recovery (BCP/DR). This helps ensure that the confidentiality–integrity–availability (CIA) triad is enforced for information systems, and breaches are minimized (Mukhopadhyay et al. 2013b). Organizations and governments have also implemented stricter IT governance measures, which mandate that effective management, policies, controls, and procedures are in place to ensure that information systems support organizations' objectives, control access to IT assets, and minimize IT-related risk. Effective IT governance is a core component of compliance and corporate governance programs (Solms 2005) to ensure an efficient enterprise risk management process (Miccolis 2000). Organizations try to ensure compliance with stringent mandatory procedures laid down in the Sarbanes–Oxley Act, Gramm–Leach–Bliley Act, and the Health Insurance Portability Insurance and Accountability Act. Noncompliance with such regulations leads to legal suits and hefty compensation payments from organizations to the victims of security breaches (Alhazmi et al. 2007). Most organizations follow an information security management system (ISMS) to design, implement, monitor, maintain, and improve information security and install processes to effectively carry out information risk management (Blakley et al. 2001).

In this paper, we propose cyber insurance (CI) as a viable complementary tool that organizations can use to hedge against cyber risk (CR) after investing in perimeter security and BCP/DR, establishing stringent security and audit policies, and demonstrating regulatory compliance (Bandyopadhyay et al. 2009; Majuca et al. 2005; Meland et al. 2015; Reid and Stephen 2001; Schroeder 2014; Shedden et al. 2010; Smith and Eloff 2002). CI can help reduce the financial burden on organizations, as insurers would indemnify losses (Bandyopadhyay and Mookerjee 2017; Baskerville 1993; Calandro et al. 2014). In effect, with IC, an organization's risk is being passed on to the insurer on payment of a fixed premium. This reduces the organization's concern about "self-insuring" (SI; i.e., keeping large amounts of money aside for contingency purposes). This, in turn, is a good corporate strategy, as large amounts of funds are not locked away for contingency purposes in the case of security breaches (Calandro et al. 2014; Mukhopadhyay et al. 2013b). CI is generally considered most effective in cases when "losses are common enough to be of concern but not frequent enough to be routine" (Cutler and Zeckhauser 2003), such as CR. Sometimes, long legal battles deter organizations from opting for CI (McLeod 2015).

The motivation of our study stems from the fact that information security breaches have a far-reaching impact on the top and bottom lines of organizations. To minimize the impact of such attacks, it is necessary to implement ISMS (Solms 2005). ISMS stress that top management should assess the risk of security breaches (Baskerville 2008; Dhillon and Backhouse 2000) a priori, then decide how much of their IT budgets to spend on technology and financial instruments, such as insurance (Gordon et al. 2003). This is of utmost importance for the banking industry, as Basel II norms mandate the quantification of operational risk and the allocation of capital for such risk (Di et al. 2007; Smithson and Song 2004). Fang et al. (Fang et al. 2014) have also noted that information security (IS) management minimizes to operational risk.

The contribution of this paper is six-fold, as our proposed cyber-risk assessment and mitigation (CRAM) framework does the following: estimates the probability of six types of cyber-attacks using a generalized linear model (GLM; e.g., logit and probit), estimates the loss distribution for each attack, computes the expected loss due to each of these attacks using a collective risk model, determines the premium that the cyber insurers would charge an organization for each of these attacks, classifies the losses due to each of these attacks into four classes using a 2 × 2 matrix based on the probability and severity of attacks, and recommends mitigation strategies (i.e., self-protection, SI, or CI) for each type of attack. For our analysis, we used time series data (1997–2010) published by the CSI–FBI (Gordon et al. 2009).

Our work differs from that of Bagchi et al. (Bagchi and Udo 2003), who proposed a Gompertz model for predicting the growth of malicious attacks based on the parameters of the number of attacks and preventive efforts to reduce attacks on a yearly basis. We argue that linear stochastic models such as logit and probit might be preferred choices, as cyberattacks can be associated with probabilities, and the number of attacks in a given year is independent of previous attacks. We model each attack type separately, as the trends of each differ over time.

Our proposed CRAM framework is a quantitative model for estimating the probability of a cyber-attack and the expected resulting loss to business. This paper aims to address a gap in literature by proposing a cyber-risk assessment model and mitigation of risk through cyber-risk insurance. When computing the probability of an attack, we have taken into consideration the fact that there is a lag of a year between the security technologies implemented and the number of attacks reported. We have also modeled the proportion of security elements to be implemented by an organization if it intends to minimize security breaches to a particular level.

This paper also contributes to practice by providing CTOs information on the probable trend of malicious attacks over time, as well as on how to develop organizational policies for deterrence and security, BCP/DR, investments in security technology, IT audits, and compliance all based on attack trends. Our CRAM model should help CEOs decide on the proportion of CR to be outsourced for CI based on premium estimations.

This paper has 8 sections. Section 2 provides an overview of previous literature related to CR management. Section 3 discusses some types of attacks commonly used by intruders and disgruntled employees to compromise organizational databases. In Section 4, we propose a four-stage logit- and probit-based CRAM framework and list the research topics to be addressed. Section 5 describes the data set used for validating our CRAM framework. Section 6 presents our findings, which we discuss in Section 7 before concluding in Section 8.

2 Literature Review

In this section, we chronologically follow the methods and techniques used from 1970 to the present to assess, quantify, and mitigate risks arising from IS security breaches. Broadly, we classify these methods into five classes: traditional methods, qualitative and behavioral methods, quantitative methods, hybrid methods, and CR insurance models. Traditional and quantitative methods have been applied since the 1970s, while qualitative methods appeared in early 1980s, hybrid approaches appeared in the late 1980s, and multiple studies were published in the 1990s using social, behavioral, and organizational aspects to assess IT security risks. Quantitative approaches rely on rigorous mathematical modeling involving probability theory or fuzzy theory to arrive at a CR value. Qualitative approaches typically depend on questionnaires and organizational surveys to determine the impact of failed security measures or successful intrusions. Hybrid approaches capture subjective parameters though questionnaires and use mathematical techniques to arrive at a final risk estimation. Table 2 lists the popular models for each category.

2.1 Traditional Methods

These approaches are based on the development of *formal methods* and the *evaluation criteria*. Formal methods focus on developing an analytical basis for the design, specification, realization, implementation, and evaluation of security systems. The objective is to build mathematical proofs related to IS security issues. Examples of formal methods developed include those by Bell La Padula (BLPM) (Bell 1974), Biba (BM) (Biba 1977), Clarkson-Wilson (CWM) (Clark and Wilson 1988), and Jueneman (JM) (Jueneman 1989). Evaluation criteria evaluate the strengths and weaknesses of information systems that are developed (Baskerville 1993). Table 3 critically compares formal and evaluation method models.

2.2 Qualitative Methods & Behavioral Models

Parker's computer security program (PCSP) (Baskerville 1993) takes into account (i) social and human factors (such as motives, acts, sources of threats) associated with (ii) assets classification based on (iii) threats. The output is a risk-assessment matrix (Baskerville 1993). The Smith–Lim approach (SLA) (Smith and Lim 1984) takes into account three generic threats (natural hazard, direct human, indirect human) and four generic targets or assets (facility, hardware, software, documents). The output is a vulnerability-assessment matrix indicating the impact of risk arising from two parameters: vulnerability (i.e., absence of safeguards) and impact (i.e., severity of impact). For example, a very high vulnerability and a very low impact imply low risk for an organization (Baskerville 1993). The CCTA (Britain's Central Computer and Telecommunication Agency) Risk Analysis and Management Method (CRAMM) (CCTA 1991) consists of three stages: assets identification, grouping of assets based on vulnerabilities, and evaluating existing organizational controls. The model's output is a set of recommendations for improving an organization's information security and safety measures. The main criticism of the model is that it produces highly technical reports with little focus on social and human factors (Baskerville 1993). The RITE model explores social issues, such as the responsibility (R) of different roles, integrity (I) of employees, trust (T), and ethicality (E) coupled with technology issues, to provide a holistic picture of the vulnerability and risk perceptions in an organization (Dhillon and Backhouse 2000). The value fo-

Table 2 Models to quantify IT risk

Qualitative & behavioral	Quantitative			Hybrid
	Probability	Fuzzy Logic	Expert system	
PCSP (Baskerville 1993)	Risk analysis, (Courtney 1977)	Securtae (Hoffman et al., 1978)	–	RISKPAC (Baskerville 1993)
CRAMM (CCTA, 1991)	LRAM, (Guarrao 1987)	RiMaHCoF (Smith and Eloff, 2002)	–	–
SLA (Smith and Lim 1984)	BDSS, (Ozier 1989)	–	–	–
VFA (Dhillon and Backhouse 2006)	(Böhme 2005; Böhme and Kataria 2006)	–	IMES (Baskerville 1993)	–
RITE (Dhillon and Backhouse 2000)	Ogut et al., 2011 Öğüt 2005	–	–	–
EEPS (Straub and Welke 1998)	Herath et al. 2011	–	–	–
–	CBBN for c-VA (Mukhopadhyay et al., 2007b)	–	–	–

Table 3 Formal and evaluation models

Models	Formal methods				Evaluation criteria		
	BLPM	BM	CWM	JM	TCSEC	ITSEC	CC
Common name	–	–	–	–	Orange book	–	ISO 15408
Location	USA	USA	USA	USA	USA	EU	USA, UK
Unit of evaluation							
Users	Y	Y	Y	Y	–	–	–
Processors	Y	Y	Y	Y	–	–	–
Data	Y	Y	Y	Y	–	–	–
OS	–	–	–	–	–	–	Y
Network	–	–	–	–	–	–	Y
Application	–	–	–	–	–	–	Y
Classified Info	–	–	–	–	Y	Y	–
Basis							
C	Y	–	Y	Y	Y	Y	Y
I	–	Y	Y	–	–	Y	Y
A	–	–	–	–	–		Y
Base model	–	–	–	–	BLPM	CWM	–
Security levels	–	–	–	–	6	6	7
Beneficiaries							
Military	Y	Y	–	–	Y	Y	Y
Business	–	–	Y	Y	–	Y	Y

cused approach (VFA) for IS security was based on data collected through in-depth interviews of IT managers of various organizations. It was found that social, human, and interpersonal issues also contribute to IS security, and it is important to consider them in a proper risk assessment strategy (Dhillon and Backhouse 2006). End-to-end planning solutions (EEPS) for risk mitigation associated with IT (Straub and Welke 1998) comprise four stages: recognizing security problems; defining managerial perceptions; taking mitigation strategies, such as deterrence–prevention–detection–remedies; and finding a viable strategy for implementing security based on a cost–benefit analysis. Deterrence is the ideal strategy for organizations. Comparative studies of these models are shown in Table 4.

2.3 Quantitative Methods

A risk analysis model developed by Courtney (1977) posited that expected loss is the frequency of the impact times the loss associated with each impact (Courtney 1977). Other techniques, such as Bayesian analysis (Ozier 1989), Copula (Cleman and Reilly 1999), artificial intelligence–based expert systems, and utility theory, have been used to quantify risk. The use of stochastic models, such as Bayesian belief networks (BBN), is common. They start with a priori beliefs regarding the incidence of malicious attacks (Jensen 1996) and modify them as more data are obtained. The outcomes of this approach are loss estimation, vulnerability assessment, threat assessment, current control~~s~~ evaluation, and security solution proposals. A comparison of quantitative techniques and intended outputs is shown in Table 5.

2.4 Hybrid Models

Hybrid models use a combination of qualitative and quantitative techniques. Data collected through questionnaires are used in mathematical models. RiskPAC (Baskerville 1993) relies on data from managers about their business, IS security, IT risks, IT audits, and BCP/DR. It is based on utility theory, uses qualitative techniques for estimating security (i.e., linguistic variables, as in fuzzy sets), and uses Courtney's model (Baskerville 1993; Courtney 1977) to estimate expected loss. The basic drawbacks are its limited capability to model changes in organizational issues and its inability to provide a mechanism that contrasts the viability of multiple security strategies (Baskerville 1993).

Table 4 Comparative analysis of qualitative techniques

Parameters	PCSP	SLA	CRAMM	EEPS	RITE	VFA
Identification and valuation of assets	Y	–	Y	–	–	–
Vulnerability impact analysis	–	Y	Y	–	–	–
Identification of threats and impact	Y	Y	–	–	–	–
Risk assessment	Y	–	–	–	–	–
Risk analysis				Y	–	–
Planning for security	Y	–	–	Y	–	–
Security safeguards	Y	–	–	Y	–	–
Evaluate the existing controls	–	–	Y	Y	–	–
Mitigation strategy	–	–	–	Y	–	–
Employee R-I-T-E	–	–	–	–	Y	–
Values of employee regarding IS security	–	–	–	–	–	Y

2.5 Cyber-Risk Insurance Models

CI (Baer and Parkinson 2007; Gordon et al. 2003)is an effective hedge against CR (Böhme and Kataria 2006; New York Times 2008). It is an effective supplement to existing security measures and helps to reduce the impact of a loss from a cyber-attack (Gordon et al. 2003; Grzebiela 2002; Schneier 2000). Table 6 compares the available CI approaches based on method (qualitative, quantitative), models used (copula, utility, process), basis (interdependent risk), input variables (social, technology, legal, and market issues), and output (premium value). Bandyopadhyay and Mookerjee 2017, propose the use of cyber insurance contracts to manage residual cyber risk.

Table 5 Comparative analysis of quantitative techniques

Models		A	B	C	D	E	F	G	H	I
Method	Bayesian	–	–	Y	Y	–	–	–	–	Y
	Copula	–	–	–	–	–	–	–	Y	Y
	Expert system		–	–	–	Y	–	–	–	–
	Fuzzy logic	Y	Y	–	–	–	–	–	–	–
	Utility theory	–	–	–	–	–	Y	Y	–	–
Output	Loss estimation		–	Y	Y	–	–	–	Y	Y
	Vulnerability assessment	Y	–	–	Y	–	–	–	–	Y
	Threat identify	–	–	Y	Y	Y	–	–	–	–
	Security measures	–	–		Y	Y	–	–	–	Y
	Controls	–	–	Y	–	–	–	–	–	–

A, Securtae (Hoffman et al., 1978); B, RiMaHCoF (Smith and Eloff, 2002); C, LRAM (Guarrao 1987); D, BDSS (Ozier 1989); E, IMES (Baskerville 1993); F, (Böhme 2005; Böhme and Kataria 2006); G, Ogut et al., 2011, Öğüt 2005 (Mukhopadhyay et al. 2013b), H, Herath et al. 2011, I, CBBN for c-VA (Mukhopadhyay et al. 2007b)

3 Malicious Cyberattacks

Figure 1 illustrates the trend of six malicious cyber-attacks experienced by organizations between 1997 and 2010 based on CSI–FBI survey data. From the diagram, it is evident that attacks increase and decrease in cycles of approximately three years; all attacks are currently in decline; and year-by-year the number of attacks follows no particular trend.

3.1 Virus Attack

The use of a virus by malicious users is common. These viruses replicate on computers and either erase important files or slow down the functioning of the system. They can affect both a company and an individual user. A Trojan worm captures keystrokes from an unsuspecting user's computer and passes it to a rogue website. This makes all critical user information, such as passwords and social security numbers, available to the attacker. The attacker can then execute an identity theft or a cyber-extortion attack. A worm attack can even lead to a distributed denial of service (DDoS) attack. Initially, a worm compromises a large number of computers, spreads across multiple locations, and uses them to attack the target. In most cases, the new virus or a Trojan worm gets through the perimeter security as antivirus engines do not contain all the latest signatures (Schneier 2000). Attacks by viruses and Trojan worms affect the confidentiality and availability of data. This results in loss of OC, MC, and brand equity.

3.2 DoS Attack

DoS attacks flood a router with malicious requests and shut out real customers from accessing services (Austin and Darby 2003). The techniques used are smurfing (i.e., the attacker

Table 6 Comparative analysis of cyber-insurance methods

Authors	Method		Models used			Basis	Input variable				Output
	Qualitative	Quantitaive	Copula	Utility	Process	Interdenpendent risk	Orgn /social issuses	Tech issuses	Legal	Market	Premium
1	–	Y	–	Y	–		–	Y	–	Y	Y
2	–	Y	–	Y	–	Y	Y	Y	–	Y	Y
3	Y	–	–	–	–		–	Y	–	–	Y
4	–	Y	–	Y	–	Y	–	Y	–	–	Y
5	Y	–	–	–	–	–	–	Y	–	–	–
6	–	–			Y	–	–	Y	–	–	–
7	Y	–	–	–	–	–	–	Y	–	Y	–
8	Y	–	–	–	–	Y	–	Y	Y	Y	–
9	–	Y	Y	–	–	Y	–	Y	–	–	Y
10	–	Y	Y	–	–	Y	Y	Y	–	–	Y

1: Bandopadhyay 2017; 2: Bohme 2005; 3: Bolot 2008; 4: Ogut 2005; 5: Yurcik 2002; 6: Salmela 2008; 7: Shetty 2009; 8: Kesan 2005; 9: Herath 2011; 10: Mukhopadhyay 2013a

replaces the destination address of the ping packets with the victim's address), fraggling (i.e., the attacker sends a spoofed User Datagram Protocol [UDP] packets), pinging (i.e., a multitude of ping requests are sent directly to the victim), and SYN flooding (i.e., the attacker creates numerous half-open Transmission Control Protocol [TCP] sessions by sending the SYN requests but never sending the acknowledgement [ACK]). To affect a large scale DDoS, the attacker distributes zombie software through the Internet so that partial or full control of the infected computer system can be gained. A DoS causes immense losses to e-business organizations, and DoS attacks have been inflicted on such sites as Amazon and eBay.

3.3 Financial Fraud

The Banking Financial Services and Insurance (BFSI) sector provides a range of financial products and services to organizations that are vulnerable to online financial fraud. According to the Basel II Accord, organizations should focus on credit risk, market risk, and operational risk. Losses due to operational risk arise due to inadequate or failed internal processes (i.e., deficiency in the existing process or procedure), people (i.e., intentional violation of internal policies by employees), systems (i.e., unintentional breakdown in of systems or technology), and external events (i.e., natural or man-made events or third-party actions) (Smithson and Song 2004). The Basel II Accord also proposes that all financial organizations keep a capital charge aside for unexpected operational risk (Fang et al. 2014; Harmantzis 2003). The Barings Bank incident provides an illustrative example of operational risk: Nicholas Lesson, a derivatives broker, caused the collapse of Barings Bank, the United Kingdom's oldest investment bank; he subverted internal processes by participating in both fraudulent, unauthorized speculative trading and booking the proceeds to accounts (Dhillon and Moores 2001).

3.4 System Penetration

External attackers can also compromise an organization's IT resources, such as Web servers kept in the

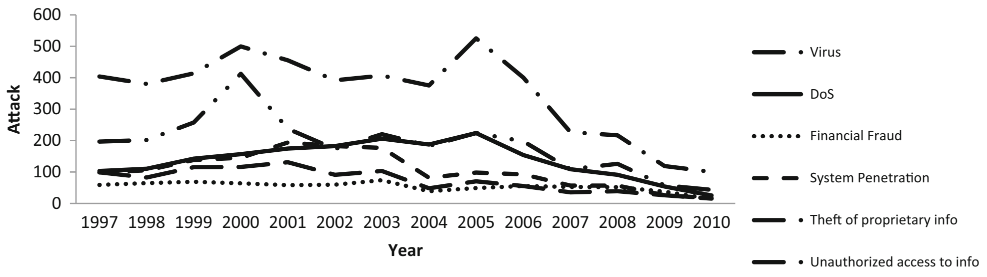


Fig. 1 Attack trends from 1997 to 2010 [Source CSI-FBI data]

demilitarized zone (DMZ), and execute a graffiti attack. Malware such as spyware and adware may compromise an organizational database, and combination attacks such as DoS, graffiti and identity theft can also be used to gain penetration (Austin and Darby 2003).

3.5 Theft of Proprietary Information

In an identity theft, the attacker uses techniques such as hacking, phishing, and pharming to obtain critical personal data (e.g., social security number, date of birth, mother's maiden name), or financial information (e.g., PIN numbers) or passwords, and uses the information to gain entry to bank accounts or for other financial gain.

Phishing is an approach for gaining information by duping the user. Types of phishing techniques commonly used are brand spoofing (the attacker replicates the webpage of a popular website), domain spoofing (the actual domain name is replaced by different one; e.g., aol.com is replaced by aol.whatever.com), homograph spoofing (the domain name of the spoofed Web page is incrementally changed, (e.g., a01.com instead of aol.com), international domain names (IDN) spoofing (exploits browser vulnerabilities), spear phishing (attacker sends e-mails posing as an authentic sender), puddle phishing (the attack is restricted to small companies), and phone phishing (make fraudulent phone calls, to con people into divulging their sensitive information) (Biswas and Mukhopadhyay 2017). In a pharming attack, the phishers hack the Domain Name Servers (DNS) and then change the DNS resolution table so that, on resolution of an IP address, the user is led to a rogue website. The target group here is financial organizations instead of customers.

3.6 Unauthorized Access

Organizational security policies are developed by top management and intended to be followed by all employees to prevent unauthorized access. Data access and authorization controls are carefully implemented and rigidly enforced, and all employees are made aware of the rules. This ensures strict ownership of information in the organization but requires constant monitoring. However, if a local security breach should occur, the consent of top management might be needed. This could result in time wasted in a time of urgency. If appropriate authority is not given to the operating staff, it is possible that delay could lead to a more severe attack or that an underappreciated employee could become an internal hacker (Bolot and LeLarge 2008).

4 CRAM Framework

From the literature review on operational risk, enterprise IT risk management, and compliance standards (such as BS7799, CoBIT) it is evident that the identification and subsequent quantification of vulnerabilities, threats, and cyber risks (Geer et al. 2003; Kahane et al. 1988; Di et al. 2007; Schneier 2000) are of great importance for developing mitigation strategies (Gordon et al. 2003).

We propose a four-stage framework for CRAM as shown in Fig. 2. Stages 1 through 4 of the CRAM model relate to cyber-risk (CR) assessment (Baskerville 1993; Biswas et al. 2016; Das et al. 2013; Mukhopadhyay et al. 2013a, b, Solms 2005), while stages 5 and 6 relate to mitigation strategies (MS) (i.e., technology and financial) that will help in cyber-risk sharing (Böhme and Schwartz 2010; Kesan et al. 2004; Kesan and Majuca 2005; Ogut and Menon 2005). Stage 1 of the CRAM model estimates of the probability of attack (p_t) over time using best fit GLM (McCullagh and Nelder 1989), taking to account past attacks (Y_t) and the security technology (Sec_{t-1}) implemented. Stage 2 computes the security investment (Sec_t) required to minimize the probability of attack (p_t). Stage 3 models the loss distribution due to a cyber-attack using gamma and exponential distribution. Stage 4 computes the expected loss, E (S_i), due to each attack over time using the concept of "collective risk" (Hossack et al. 1983). Stage 5 computes the expected premium (Pr_i) to be charged by an insurer for each type of attack. Our model should help CTOs quantify the probability (p_t) of an occurrence of cyber intrusion and plan their information security budgets and policies based on the frequency (p_t) at which breaches might occur (Mukhopadhyay et al. 2013b). Stage 6 provides a cyber-risk mitigation strategy (i.e., self-protection, SI, or CI) for CTOs, depending on the expected loss (i.e., low frequency, low severity; low frequency, high severity; high frequency, low severity; and high frequency, high severity). Table 7 lists the notation for model parameters and decision variables of CRAM.

4.1 CR Assessment

In the following subsections we will discuss the mathematical formulation of the stages 1 through 4 for the CR assessment of each of the six attack types.

4.1.1 Estimation of the Probability of Cyber-Attacks Over Time

CTOs invest around 5% to 10% of their budgets on IT security (Austin and Darby 2003; Gordon and Loeb 2002). We assume that each of the N_t respondents interviewed by CSI–FBI from

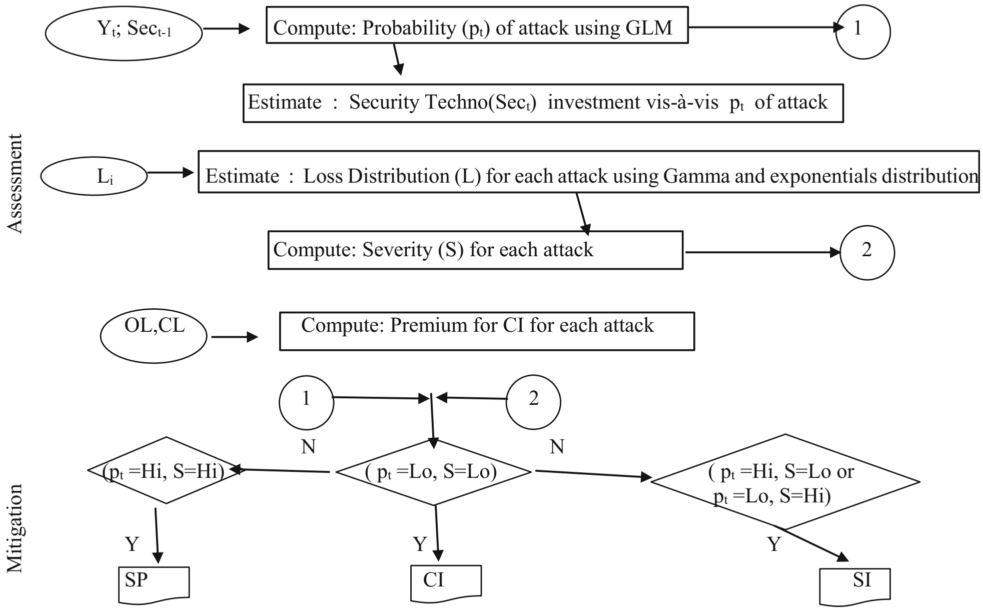

Assessment
Y_t; Sec_{t-1}
Compute: Probability (p_t) of attack using GLM
1
Estimate : Security Techno(Sec_t) investment vis-à-vis p_t of attack
L_i
Estimate : Loss Distribution (L) for each attack using Gamma and exponentials distribution
Compute: Severity (S) for each attack
2
OL,CL
Compute: Premium for CI for each attack
1
2
Mitigation
N
N
(p_t =Hi, S=Hi)
(p_t =Lo, S=Lo)
(p_t =Hi, S=Lo or p_t =Lo, S=Hi)
Y
Y
Y
SP
CI
SI

Fig. 2 CRAM framework. Y_t = Attack frequency; Sec_{t-1} = Security Technology; L_i = Loss; OL = Overhead Loading; CL = Contingency loading

Table 7 Notation for model parameters and decision variables

t	Time (i.e., year)
N_t	Total respondents
N_t - Y_t	Respondents who were not attacked in the t^{th} year.
$Y_t = 1$	Respondents who experienced a cyber-attack
$Y_t = 0$	Respondents who did not experience an attack
Y_t	Binomial Distribution,
p_t	Probability of cyber-attack estimated using exponential function (i.e., cumulative logistic and normal distributions)
1-p_t	Probability of no cyber-attack
Sec_{t-1}	Security technology deployed in the year t-1
t^2	Time (i.e., year) for the non-linear model
Z_1	Linear predictor [i.e., $-(\beta_0+ \beta_1 t + \beta_2 \text{ Sec}_{t-1})$]
Z_2	Linear predictor (i.e., $-(\beta_0+ \beta_1 t + \beta_1 t^2 + \beta_2 \text{ Sec}_{t-1})$]
G	Link function (i.e., Logit and Probit)
Φ	Normal cumulative density function
M_i	Models (i = 1,2,3,4)
E(S_i)	Expected loss or severity for each attack type (i = 1,2,3,4,5,6)
E (Y_i),	Expected number of attacks for each attack type (i = 1,2,3,4,5,6)
E (L_i)	Expected average loss for each attack type (i = 1,2,3,4,5,6)
Pr_i	Premium for each attack type (i = 1,2,3,4,5,6)
OV	Overhead loading
k	Contingency loading
Var(S_i)	Variance of the Severity for each attack type (i = 1,2,3,4,5,6)
Var(L_i)	Variance of the average loss for each attack type (i = 1,2,3,4,5,6)
MS	Mitigation strategy
SeP	Self -protection
CI	Cyber-risk insurance
SI	Self-Insurance

1997 to 2010 had implemented perimeter security technology and ensured compliance with Payment Card Industry Data Security Standards (PCI DSS) or BS7799 for the t^{th} year (Sec_t). This includes the use of a secure network with proper firewalls, use of strong passwords, encryption of stored data, frequent updating of anti-virus programs, use of secure and healthy applications, monitoring of access controls (AC), use of unique IDs, network monitoring and testing, frequent auditing, the creation of effective security processes, and the updating of security and data policies (Austin and Darby 2003; Gordon et al. 2003).

Yet, Y_t out of N_t respondents interviewed in year t reported that they had experienced a cyber-attack, while $N_t - Y_t$ respondents reported that they were not attacked in t^{th} year. So, Y_t follows a binomial distribution and can have two states (i.e., attacked, $Y_t = 1$, or not attacked, $Y_t = 0$) with a probability of p_t and (1-p_t), respectively, as shown in Eq. (1). We propose four models (M1, M2, M3, and M4) to estimate the probability of attack in year t (p_t), which is a function of time, t, and the security technology deployed in year t-1 (Sec_{t-1}). In two cases (M1 and M3), we assume that the explanatory variables, t and Sec_{t-1}, follow a linear equation, Z_1. While in the other two cases (M2 and M4), we assume the explanatory variables t^2 and Sec_{t-1}, and they form the linear predictor $Z_{2.}$ In all four models, we assume a lag of a year between the security technology deployments, Sec_{t-1}, and the number of users impacted, Y_t.

We chose GLM (McCullagh and Nelder 1989) for our CRAM to estimate the trends of attacks (Y_t) over the years from 1997 to 2010, as Y_t is a discrete random variable and can have only two states (i.e., $Y_t = 1$ or $Y_t = 0$), and it follows the binomial distribution; attack data (Y_t) follows a non-linear trend, and the homogeneity of variances is missing. The link function (G) (i.e., logit and probit) approximates the probability (p_t) of a malicious attack by using an exponential function (i.e., cumulative logistic and normal distributions) that maps each attack frequency (p_t) to the range [0, 1] that is, $0 < p < 1$, even though the linear predictor, Z_i, can take any value in the range from $[-\infty,\infty]$.The parameters $\boldsymbol{\beta}$ of the GLM are estimated by the maximum likelihood estimate (MLE) method, which involves iterative re-weighted least squares (IRLS) (McCullagh and Nelder 1989). Thus, GLM helps attain the basic objective of computing the probability (i.e., $0 < p_t < 1$) of attack for our CRAM model.

> RQ1: What is the probability of a cyber-attack on a business organization, for year t ($Y_t = 1$), even though it has invested adequate security technology in year t-1 (Sec_{t-1})?

$$P(Y_t = 1) = {}^{Nt}C_{y_t} p_t^{y_t}(1-p_t)^{(n_t-y_t)} \qquad (1)$$

$$\text{M1 } E(Y_t = 1|X = t, Sec_{t-1}) = p_t = \frac{1}{1+e^{-Z_1}} \qquad \text{M3} : E\left(Y_t = 1|X = t, Sec_{t-1}\right) = p_t = G\left(Z_1\right) = \Phi^{-1}(Z_1) = Z_1$$

$$\text{M2} = E\left(Y_t = 1|X = t, t^2, Sec_{t-1}\right) = p_t = \frac{1}{1+e^{-Z_2}} \qquad \text{M4} : E\left(Y_t = 1|X = t, t^2, Sec_{t-1}\right) = p_t = G\left(Z_2\right) = \Phi^{-1}(Z_2) = Z_2$$

where $Z_1 = -\beta_0 + \beta_1 t + \beta_2 \, Sec_{t-1}$; $Z_2 = -\beta_0 + \beta_1 t + \beta_2 t^2 + \beta_3 Sec_{t-1}$; Φ is the normal cumulative density function; t = 1….13; Sec_{t-1} = security technology deployed in year t-1.

4.1.2 Estimating the Security Technology Investment Vis-à-vis Future Probability of Cyber-Attack Trends

In most cases, IT assets are securely placed behind the firewall in the militarized zone (MZ) to minimize chances of system penetration. An International Data Corporation (IDC) study has found that worldwide spending on security appliances grew by 17% to $613 million in 2005 (Mukhopadhyay et al. 2007b). In this context, we would like to predict the use of security technologies needed by organizations to minimize the probability of attacks.

> RQ2: What is predicted security technology (Sec_t) required to reduce the probability of attack (p_t) to a given level in the next year?

The relationship between security technology (Sec_t) and the proposed probability of attack (p_t) is given by Eq. (2) based on model M1.

$$\text{M1} = E\left(Y_t = 1|X = t, Sec_{t-1}\right) = p_t = \frac{1}{1+e^{-(\beta_0+\beta_1 t+Sec_{t-1})}}$$

$$Sec_{t-1} = \frac{Ln\left(\frac{1}{p}-1\right) + \beta_0 + \beta_1 t}{-\beta_2} \qquad (2)$$

where $\boldsymbol{\beta_i}$ = parameters of model M1.

4.1.3 Estimation of Loss Distribution Vis-à-vis Cyber Attacks

We intend to model loss (Li) distribution of each of the attacks (*i* = 1,2…6) as a gamma and exponential distribution, as they tend to be positively skewed and long tailed (Dutta and Perry 2011; Hossack et al. 1983). Exponential distribution is a special case of gamma distribution. This will give CTOs an idea of the expected loss that a cyber-attack could cause to their organizations.

> RQ3: Does gamma and exponential distribution best approximate the average loss data (u) for each malicious attack?

The gamma probability density function (pdf) is given by Eq. (3).

$$f(u|a,b) = \frac{u^{(a-1)}e^{-u/b}}{b^a \ \Gamma(a)} \qquad (3)$$

where u is loss data, $\acute{\Gamma}(.)$ is the gamma function, a and b are constants, gamma(a = 1, u) ≡ Exponential(u).

4.1.4 Quantification of Expected Severity of a Cyber-Attack Using the Collective Risk Model

We used the collective risk model (Hossack et al. 1983) to compute the expected severity, E (S_i), and the variance of the severity, Var (S_i), for each for each attack type, i, using Eqs. (4) and (5), respectively. The collective risk model assumes both the number of attacks, E (Y_i), and the associated average loss, E (L_i), as mutually independent random variables. In this case, the attack, Yi, follows a binomial distribution and the associated loss, L_i, follows a gamma and exponential distribution.

> RQ4: What is the expected severity of a cyber-attack on an organization?

$$E\left(S_i\right) = E\left(Y_i\right) \times E\left(L_i\right) \qquad (4)$$

$$\mathrm{Var}\ (\mathrm{S_i}) = \mathrm{E}\ (\mathrm{Y_i}) \times \mathrm{Var}\ (\mathrm{L_i}) + \mathrm{E}\ (\mathrm{L_i})^2 \times \mathrm{Var}\ (\mathrm{Y_i}) \qquad (5)$$

where i = 1….6.

4.2 CR Mitigation Through Insurance

According to Kunreuther (1997), "Insurance is the only policy tool in the analyst's repertoire that can reward individuals for taking loss reduction measures in advance of a disaster by giving them lower premiums while at the same time providing these same policyholders with compensation should they suffer losses from the insured event" (Kunreuther 1997). By extension, it can be argued that organizations develop procedures for identifying and screening cyber threats (CR) and for mitigating risk (CR insurance) using concepts of probabilistic risk assessment. Prospect theory (Kahneman and Tversky 1979) describes how people make choices in situations where they have to decide between alternatives that involve monetary implications. Starting from empirical evidence, the theory describes how individuals and firms act on loss aversion and evaluate potential losses and gains based on real-life choices. In this section, we first compute the premium for each cyber-attack and then formulate a strategy that ta CTO should implement for mitigating each of the cyber-attacks.

4.2.1 Premium Computation for Cyber Insurance Products

The premium ($\mathrm{Pr_i}$) for insuring against each type of cyber-attack is computed as the expected severity E ($\mathrm{S_i}$) multiplied by the quantity of the overhead loading (OV) plus the variance (Var (Si)) multiplied by the contingency loading (k) (Hossack et al. 1983), as shown in Eq. (6). An insurer uses contingency loading (i) to protect against insolvency and (ii) to ensure an adequate return. We ensure that homogenous CR are only pooled together for premium computation. For example, all firms suffering for virus attacks will be pooled together. We also note that, using utility models, the premium can be fine-tuned based on the wealth and the risk profile of the insured (Mukhopadhyay et al. 2013b).

> RQ5: How much premium ($\mathrm{Pr_i}$) will a cyber-insurer charge for insuring a cyber-attack?

$$\mathrm{Pr_i} = (1 + \mathrm{OV}) \times \mathrm{E}\ (\mathrm{S_i}) + \mathrm{k} \times \sqrt{}\mathrm{Var}\ (\mathrm{S_i}) \qquad (6)$$

The overhead loading (OV) factor accounts for the profit and other related administrative charges, while contingency loading (k) accounts for any variation of CR from its mean.

4.2.2 CR Mitigation Strategy for Each of the Attacks

The basic inputs for this are the frequency of attack, the impact or severity of the attack, and the proposed premium to insure it. The proposed strategies for CR reallocation (Böhme and Kataria 2006) are self-protection (SeP), transferring the risk to a CR insurance company (CI), and resorting to SI (Kesan et al. 2004; Kesan and Majuca 2005; Rejda 2010; Yurcik 2002), as shown in Eq. (7).

> RQ6: What mitigation strategy (MS) can a CTOs choose for each type of malicious attack?

$$\mathrm{MS} = \mathrm{f}\ (\mathrm{p}\ (\mathrm{Y_t}), \mathrm{E}\ (\mathrm{S_i}), \mathrm{Pr_i})$$

$$\mathrm{MS} = \begin{cases} \mathrm{Sep}\ ,\ \ \mathrm{if}(\mathrm{p}(\mathrm{Yt}), \mathrm{E}(\mathrm{Si})) = (\mathrm{Hi}, \mathrm{Hi}) \\ \mathrm{CI}\ ,\ \ \mathrm{if}(\mathrm{p}(\mathrm{Yt}), \mathrm{E}(\mathrm{Si})) = (\mathrm{Lo}, \mathrm{Lo}) \\ \mathrm{SI}, \mathrm{if}(\mathrm{p}(\mathrm{Yt}), \mathrm{E}(\mathrm{Si})) = (\mathrm{Hi}, \mathrm{Lo})\mathrm{or}(\mathrm{Lo}, \mathrm{Hi}) \end{cases} \qquad (7)$$

5 Data & Methodology

We chose the CSI–FBI (1997–2010) survey, as it is the most widely cited dataset. The sample space was spread across both the government and private sectors and multiple industries. The representation of the major sectors is financial (20%), consulting (11%), education (11%), information technology (10%), and manufacturing (8%). Over 40% of respondents were "people responsible for enterprise security" (Bagchi and Udo 2003). Table 8 provides the mean and standard deviation of each attack type.

5.1 Methodology for Validation of Our CRAM Model

To validate our CRAM model, we split our CSI–FBI (1997–2010) data into training and testing sets. They contain 80% and 20% of records, respectively. For evaluating our model for RQ1, we have ensured a lag of one year between security technology deployments, $\mathrm{Sec_{t-1}}$, and the number of users impacted, $\mathrm{Y_t}$. The training set consists of data from 1998 to 2007, and the testing data set has data

Table 8 Mean and standard deviation of the attack types

Measures	TR	Virus	DoS	FF	SP	TPI	UA	AC
Mean	459	351	137	53	105	73	188	347
St dev	145	133	58	15	56	37	91	119
Number	13	13	13	13	13	13	13	13

TR, total respondent; AC, access control from 2008 to 2009. We have also tested the validation of our CRAM model to estimate the probability of cyberattack and for premium computation.

6 Results from Our CRAM Model

In this section, we discuss the results of the CRAM framework as follows: (i) the estimation of the probability of attack by GLM, (ii) investment in security technology to reduce cyber-attacks, (iii) estimation of loss distribution using gamma and exponential distribution, (iv) the expected loss, (v) the premium to be charged by cyber insurers and, (vi) the mitigation strategy for each cyber-attack.

6.1 CR Assessment

We now judge the effectiveness of our logit and probit models.

6.1.1 Estimation of Probability of Attack Over Time

From Figs. 3, 4, 5, 6, 7 and 8 and Tables 9 and 10, it is evident that the logit quadratic (M2) model performs better in the training phase (1998 to 2007) but performs worse than the logit linear (M1) model in the testing phase (2008 to 2009) for all attacks, except on UA and DoS. This is primarily attributed to over-fitting in the training phase, as there are few observed variables for this study. Tables 9 and 10 summarize the coefficients, stand errors, t-statistics, *P* values, and the deviance of the linear models (M1, M3) and quadratic models (M2, M4) for each of the six attacks. As illustrated by Table 9, the logit linear (M1) model and probit linear (M3) models behave identically for the training set data, and for all six attacks the explanatory variable, t, is significant at a 1% and 5% level, respectively, and it is negatively related to the dependent variable. This indicates that, as CTOs become aware over time, t, about attacks and they implement stronger access control (i.e., Sec $_{t-1}$) methods, the probability of attacks (p_t) reduces. From Table 10, we observe that the probit quadratic (M4) models also behave like the logit quadratic (M2) models. We dropped models M2 and M4 as they are not significant for this study.

We narrowed down the logit linear (M1) model for computation of CR for our CRAM framework, as it performs well for both the data training and testing sets.

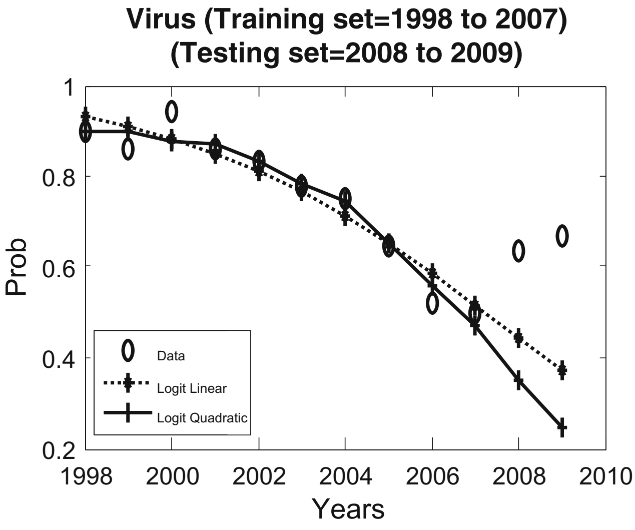


Fig. 3 Logit linear & quadratic model for virus

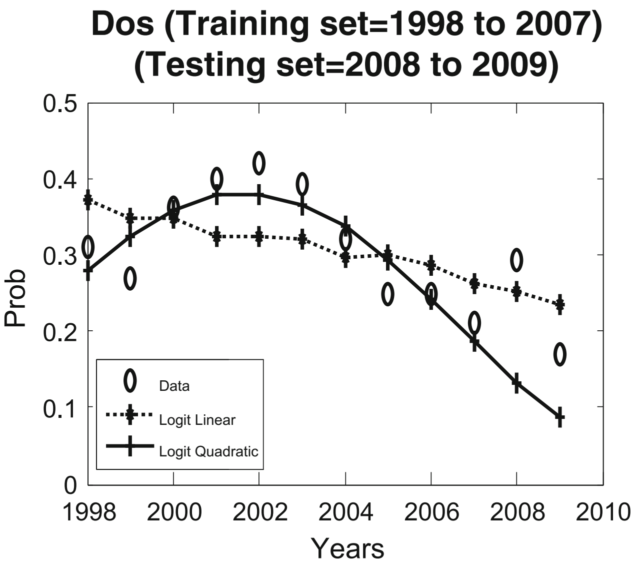


Fig. 4 Logit linear & quadratic model for DoS

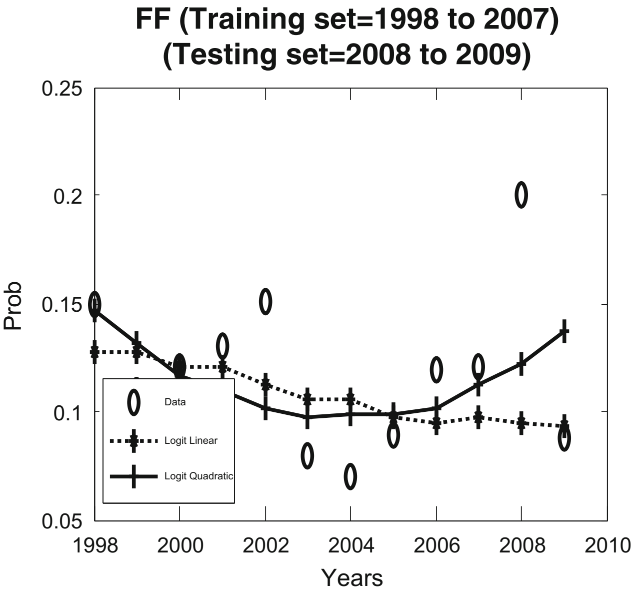


Fig. 5 Logit linear & quadratic model for FF

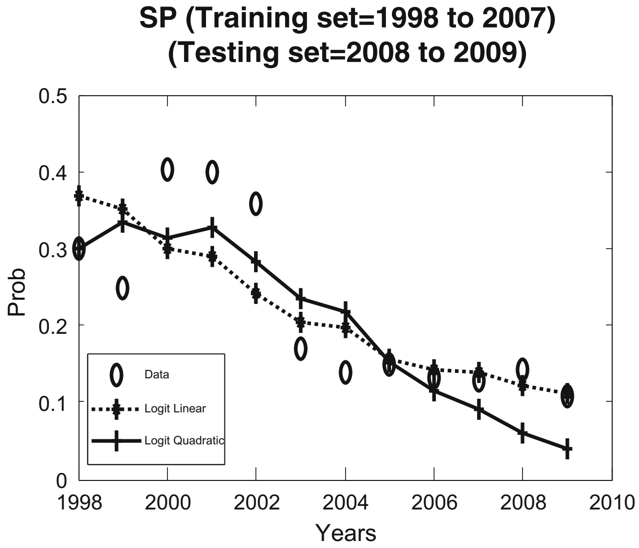


Fig. 6 Logit linear & quadratic model for SP

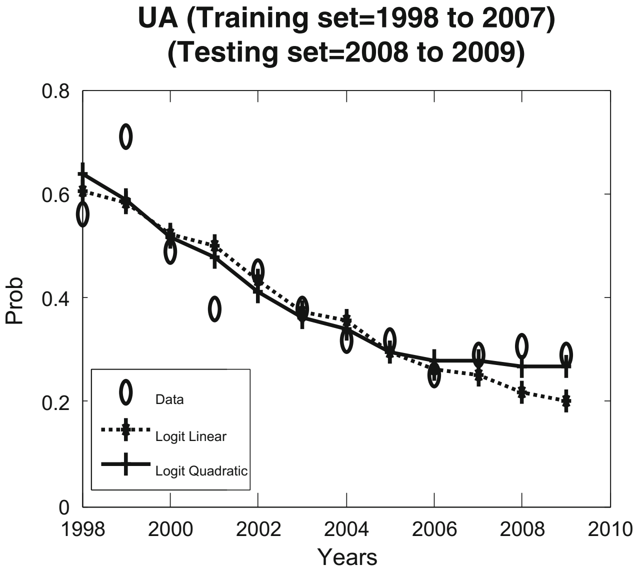


Fig. 8 Logit linear & quadratic model for UA

It is noted that the popularity of a software application leads to the growth of attacks by malicious intruders, following an S curve. Initially, there are few attacks, then they peak at the intermediate stage, and finally, they dwindle away as the popularity of the software reduces. Similarly, security technology diffusion follows an S curve. Here, too, initially only a few security technology deterrents are available, so attacks increase; then at the intermediate stage, the number of deterrents increases rapidly, and finally, few systems remain vulnerable (Alhazmi et al. 2007; Miccolis 2000; Ruohone et al. 2015). Our findings from the CRAM model are in line with the same. Thus, we note from our logit linear model (M1) that the probability of attacks (p_t) decreases over time, t, as stronger access control (i.e., Sec $_{t-1}$) methods are implemented.

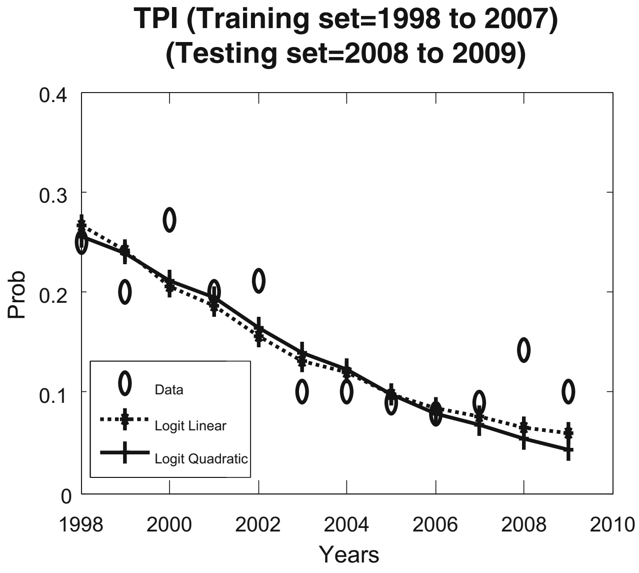


Fig. 7 Logit linear & quadratic model for TPI

6.1.2 Estimating the Security Technology Investment Vis-à-vis Future Probability of Cyber-Attack Trends

CTO of an organization is exploring the proportion of security required to reduce the probability of attack (from a virus, DoS, SP, and UA) a particular level (i.e., from 0.40 to 0.05) to minimize security breaches. Table 11 illustrates that an increase in security technology will help reduce the probability of virus attack.

Software publishers such as Microsoft and Oracle have a planned schedule for the release of patches, and users are generally proactive in patching their operating systems and applications (Austin and Darby 2003; Cavusoglu et al. 2008). Frequent use of Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) will help distinguish human beings from botnets and reduce botnet involvement in DoS attacks. To reduce the probability of SP and UA, greater focus on managerial and compliance issues is required. Compliance with BS7799 has helped organizations to ensure proper security policies, organizational security, IT asset classification, personnel security, physical and environmental security, communication and operations, access control, system development, and BCP/DR. This, in turn, has helped organizations to minimize possible security breaches. Similarly, the probability of unauthorized access will be reduced over the years if security policies focus on using strong passwords, having all users change passwords at frequent intervals, hashing passwords before storing, using digital signatures, recording all transactions in a log file, and maintaining an effective audit trail (Austin and Darby 2003). Regular security awareness programs should be conducted for

Table 9 Coefficients of the logit linear (M1) & probit linear (M3) models for training set

	Logit linear					Probit linear				
	coeff	SE	t	p	dev	coeff	SE	t	p	dev
V	2.827$^{\#}$	0.222	12.745	0.000	53	1.596$^{\#}$	0.127	12.523	0.000	61
	−0.280	0.014	−20.286	0.000		−0.158$^{\#}$	0.008	−20.667	0.000	
	0.000	0.000	0.166	0.868		0.000	0.000	0.489	0.625	
D	−0.703$^{\#}$	0.194	−3.625	0.000	85	−0.434$^{\#}$	0.118	−3.694	0.000	85
	−0.047$^{\#}$	0.011	−4.323	0.000		−0.029$^{\#}$	0.007	−4.393	0.000	
	0.000	0.000	1.079	0.281		0.000	0.000	1.085	0.278	
FF	−1.683	0.287	−5.864	0.000	31	−1.011$^{\#}$	0.149	−6.766	0.000	31
	−0.043$^{\#\#}$	0.016	−2.691	0.007		−0.022$^{\#}$	0.008	−2.670	0.008	
	0.000	0.001	−0.637	0.524		0.000	0.000	−0.667	0.505	
SP	−0.017	0.219	−0.080	0.936	139	−0.030	0.127	−0.238	0.812	136
	−0.159$^{\#}$	0.012	−13.031	0.000		−0.094	0.007	−13.330	0.000	
	−0.001	0.001	−1.597	0.110		0.000	0.000	−1.631	0.103	
TP	−0.660$^{\#\#}$	0.259	−2.546	0.011	37	−0.417$^{\#}$	0.141	−2.957	0.003	36
	−0.172$^{\#}$	0.014	−11.920	0.000		−0.095$^{\#}$	0.008	−12.101	0.000	
	0.000	0.001	−0.644	0.519		0.000	0.000	−0.807	0.420	
UA	0.961$^{\#}$	0.189	5.085	0.000	83	0.601$^{\#}$	0.116	5.188	0.000	84
	−0.185$^{\#}$	0.011	−17.251	0.000		−0.114$^{\#}$	0.007	−17.458	0.000	
	−0.001	0.000	−1.741	0.082		0.000	0.000	−1.829	0.067	

$^{\#}$, $^{\#\#}$, Denote significance at 1%, and 5% level respectively for two tail test

employees, and bulletins highlighting the 'dos and don'ts' of network usage should be circulated to employees (Austin and Darby 2003). Employees should also be sensitized to the possibility that skillful internal or external attackers could resort to social re-engineering to obtain information (Austin and Darby 2003).

6.1.3 Estimation of Loss Distribution Vis-a-vis Cyber Attacks

We model the loss distribution (L_i) for each of type of cyber-attack using gamma and exponential distribution. We assume that loss distribution (L_i) is a random variable. Figure 9 illustrates that gamma distribution best fits losses due to virus

Table 10 Coefficients of the logit quadratic (M2) & probit quadratic (M4) models for training set

	Logit quadratic					Probit quadratic				
	coeff	SE	t	p	dev	coeff	SE	t	p	dev
Virus	2.484$^{\#}$	0.234	10.639	0.000	33	1.384$^{\#}$	0.134	10.327	0.000	33
	−0.001	0.062	−0.018	0.985		0.020	0.034	0.595	0.552	
	−0.024$^{\#}$	0.005	−4.530	0.000		−0.016$^{\#}$	0.003	−5.312	0.000	
	−0.001	0.001	−1.290	0.197		0.000	0.000	−0.984	0.325	
DoS	−1.229$^{\#}$	0.209	−5.895	0.000	25	−0.738$^{\#}$	0.125	−5.898	0.000	26
	0.324$^{\#}$	0.050	6.505	0.000		0.192	0.030	6.445	0.000	
	−0.035$^{\#}$	0.005	−7.626	0.000		−0.021$^{\#}$	0.003	−7.596	0.000	
	0.000	0.000	−0.049	0.961		0.000	0.000	−0.152	0.879	
FF	−1.502$^{\#}$	0.299	−5.014	0.000	27	−0.914$^{\#}$	0.156	−5.861	0.000	27
	−0.183$^{\#\#}$	0.069	−2.650	0.008		−0.097$^{\#\#}$	0.036	−2.660	0.008	
	0.013$^{\#\#}$	0.006	2.082	0.037		0.007$^{\#\#}$	0.003	2.099	0.036	
	0.000	0.001	−0.312	0.755		0.000	0.000	−0.310	0.756	
SP	−0.515$^{\#\#}$	0.239	−2.154	0.031	105	−0.270$^{\#\#}$	0.136	−1.984	0.047	108
	0.142$^{\#\#}$	0.054	2.618	0.009		0.065$^{\#\#}$	0.031	2.070	0.038	
	−0.029$^{\#}$	0.005	−5.667	0.000		−0.015$^{\#}$	0.003	−5.180	0.000	
	−0.001	0.001	−1.871	0.061		−0.001$^{\#\#}$	0.000	−2.158	0.031	
TPI	−0.792$^{\#\#}$	0.279	−2.835	0.005	36	−0.457$^{\#\#}$	0.150	−3.046	0.002	36
	−0.095	0.062	−1.540	0.124		−0.069$^{\#\#}$	0.034	−2.026	0.043	
	−0.008	0.006	−1.292	0.196		−0.003	0.003	−0.796	0.426	
	0.000	0.001	−0.667	0.505		0.000	0.000	−0.872	0.383	
UA	1.125$^{\#}$	0.199	5.666	0.000	77	0.701$^{\#}$	0.122	5.771	0.000	77
	−0.303$^{\#}$	0.047	−6.443	0.000		−0.190$^{\#}$	0.029	−6.554	0.000	
	0.011$^{\#\#}$	0.004	2.596	0.009		0.007$^{\#\#}$	0.003	2.687	0.007	
	−0.001	0.000	−1.336	0.182		0.000	0.000	−1.357	0.175	

$^{\#}$, $^{\#\#}$, Denote significance at 1%, and 5% level respectively for two tail test

Table 11 Prediction of percentage of security techno vis-à-vis probablity of attacks

prob	V	DoS	SP	UA
0.40	0.17	0.23	−0.37	−0.13
0.35	0.23	0.18	−0.32	−0.08
0.30	0.28	0.12	−0.26	−0.02
0.25	0.35	0.06	−0.20	0.04
0.20	0.42	−0.01	−0.13	0.11
0.15	0.50	−0.10	−0.04	0.20
0.10	0.62	−0.22	0.08	0.31
0.05	0.81	−0.40	0.26	0.50

attacks. Figures 10, 11, 12, 13, and 14 show that the loss distribution for each attack type can be estimated by exponential and gamma distribution. We use loss distribution (L_i) to compute the severity of an attack as per Eq. (4). Table 12 lists the mean and standard deviation for these losses, as modeled by exponential and gamma distribution.

6.1.4 Quantification of the Expected Severity of a Cyber-Attack Using Collective Risk Model

We compute the expected severity (i.e., mean and variance) of these attacks using collective risk modeling (Hossack et al. 1983) as defined in Eq. (4). The same is used for a CR mitigation strategy formulation as shown in Fig. 21.

6.2 CR Mitigation Through Insurance

In this section, we solve the decision problem for the CTO: opting for CI, SI, or SP. The inputs are the probability of attack, the impact of an attack, and the premium to mitigate these through CI.

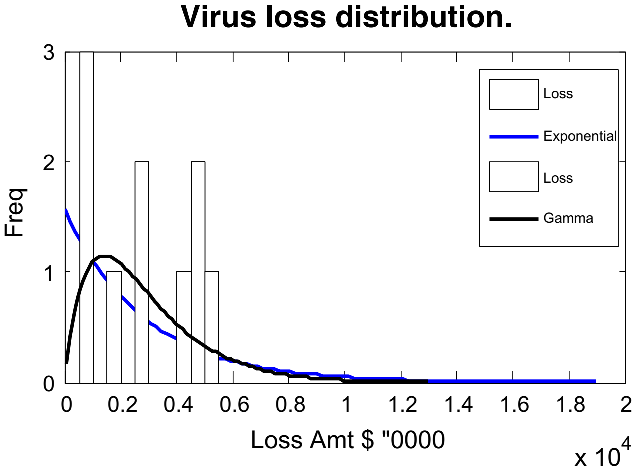


Fig. 9 Loss estimation of virus

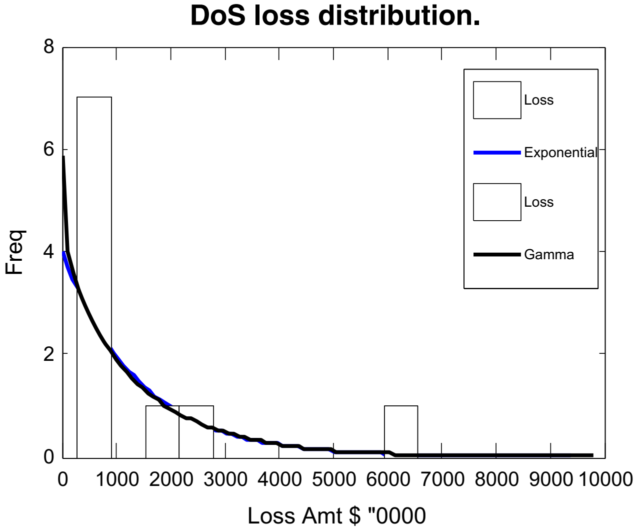


Fig. 10 Loss estimation of DoS

6.2.1 Premium Computation for Cyber Insurance Products

We have assumed that the insured are risk averse and willing to pay a premium to hedge against the financial implications of a cyber-risk or security breach (Harmantzis 2003; McCullagh and Nelder 1989). Our CRAM model computes the predicted premium using Eq. (4). Figures 15, 16, 17, 18, 19 and 20 plot the predicted premium *vis-à-vis* the actual premium and for each of the attacks. We note that our CRAM model predicts the premium adequately based on the probability of attack computed using the GLM model, as well as the impact of the severity estimated by a gamma distribution. Thus, the CRAM model can be effectively used for predicting future premiums.

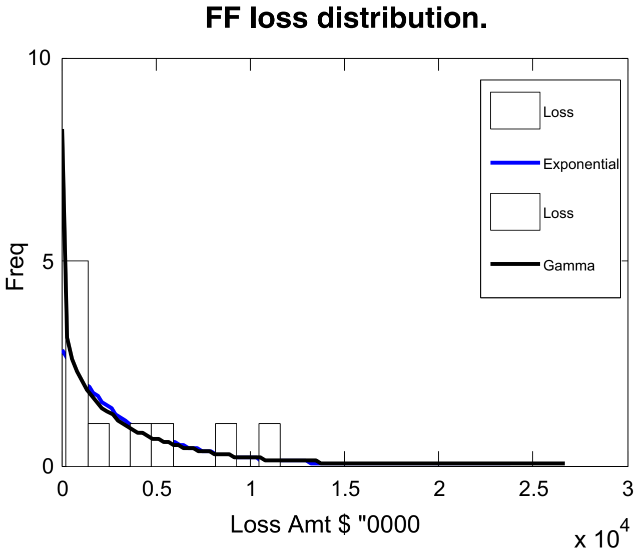


Fig. 11 Loss estimation of FF

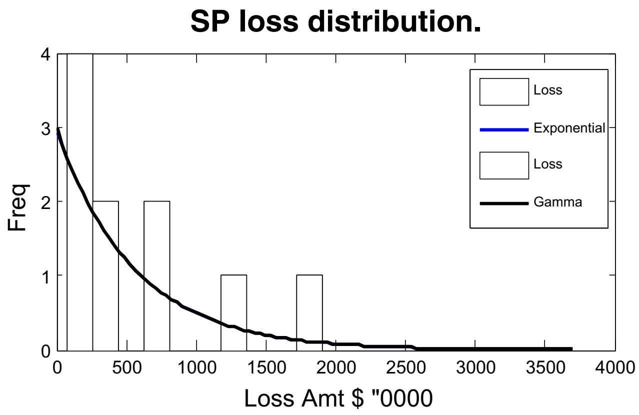


Fig. 12 Loss estimation of SP

6.2.2 CR Mitigation Strategy for Each Attack

Figure 21 illustrates a 2 × 2 matrix where the x-axis represents the probability of a cyber-attack and the y-axis represents the impact of the loss. For this study, we plotted all the data points of CSI–FBI from 1997 to 2010. A majority of attacks (such as FF, TPI, SP, DoS, and UA) lies in the low/low quadrant. All virus attacks and a single UA attack lie in the high/high quadrant. It can be assumed that cyber–risk insurers will readily provide coverage to organizations in the low/low quadrant provided that the insured have adequately invested in IT security and are legally and ethically upright. In this study, we assume that insured organizations are risk averse and that the premium for cyber insurance is higher than the expected loss for each type of attack (Hossack et al. 1983; Mukhopadhyay et al. 2013b).

In case of a virus attack (high, high), CTOs will have to try to reposition their quadrant location to low/high by either adequately implementing IT security measures for self-protection or resorting to self-insurance. Failure to reduce the probability of a virus attack would imply that the premium charged by the insurer is inordinately high (Ogut and Menon 2005; Yurcik 2002).

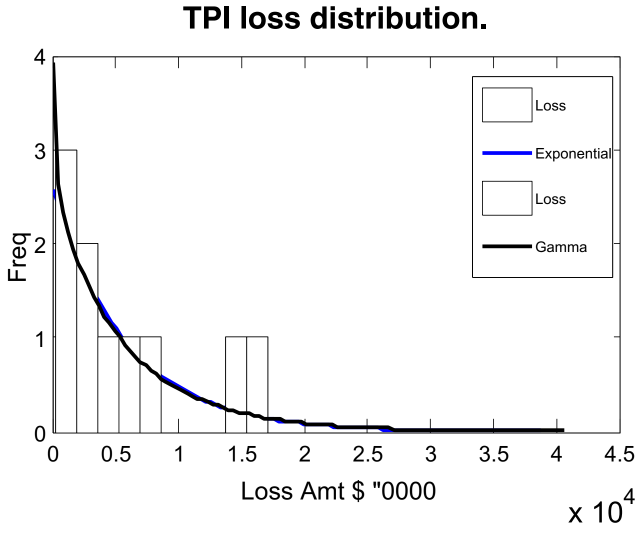


Fig. 13 Loss estimation of TPI

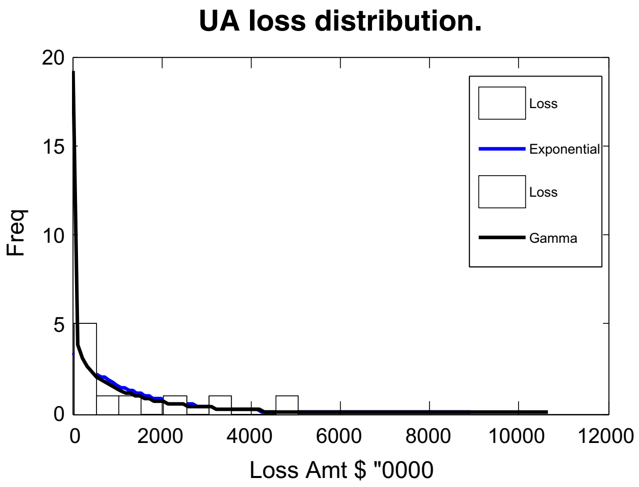


Fig. 14 Loss estimation of UA

In case of a UA attack (high, low), the CTO would prefer to opt for SI if the organization has high cash reserves or revenue streams. This would ensure that the insured saves on premium payments. But, a better strategy would be to slice a portion of the CR for SI and pass on the remainder to an insurer. This would require investing in IT security to move to a lower risk (low, low) quadrant. Opting for SI would mean that the organization invested in exchange-traded and over-the-counter (OTC) financial options to hedge the CR (Mukhopadhyay et al. 2007a).

SI and CI are substitute goods. An organization can choose either, depending on its capital standing and the nature of the CR. Similarly, self-protection and SI are substitutes (Yurcik 2002). Investment in more IT security reduces the requirement of setting aside capital for self-insurance. SP and CI are complementary goods. It might be prudent to invest in self-protection to reduce the initial CR and pass the residual CR on to an insurance company.

7 Discussion

Internet-based attacks are becoming more complex. In the past few years, we have seen a number of large and established organizations with supposedly extensive investments in IT

Table 12 Central tendencies of the loss amount for each attack

	Measure	Virus	DoS	FF	SP	TPI	UA
Gamma	E(L)	2869	729	3870	675	5869	1460
	Stdev(L)	2058	757	4251	675	6107	1687
Exponential	E(L)	2869	729	3870	675	5869	1460
	Stdev(L)	2869	729	3870	675	5869	1460

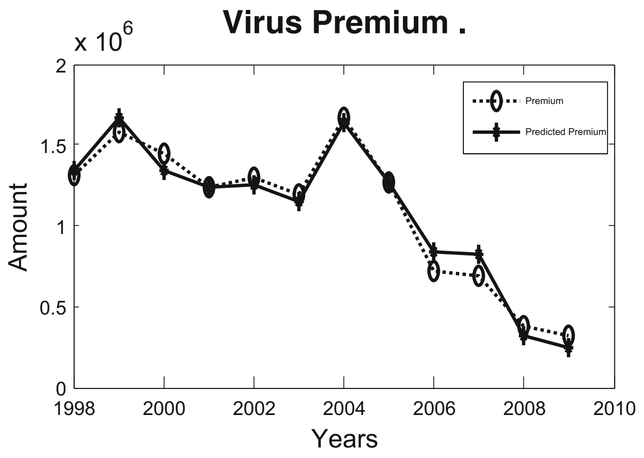


Fig. 15 Premium estimation for virus

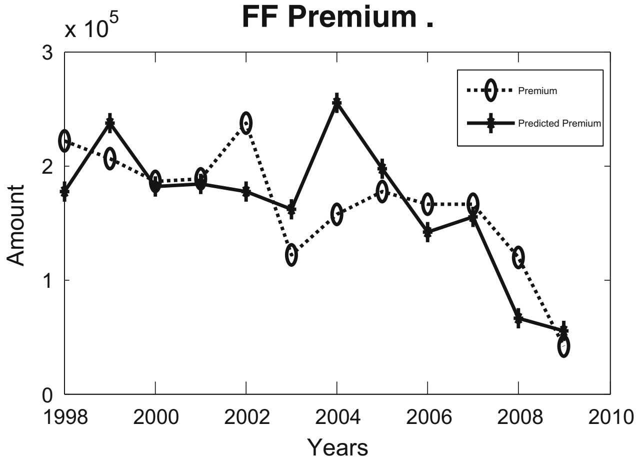


Fig. 17 FF premium estimation

security publicly report huge monetary losses because of data theft (Dash 2011). Stage 1 of the CRAM model makes an important contribution in terms of proposing a GLM-based model (McCullagh and Nelder 1989) for estimating the probability (pt) of a cyber-attack on a firm. Cyber-attacks that do not have a fixed trend, as some new application becomes popular and along with it comes newer vulnerabilities (Ruohone et al. 2015). We argue that linear stochastic models such as logit and probit might be preferred choices, as cyberattacks can be associated with probabilities, and the number of attacks in a given year is independent of previous attacks. We model each attack type separately, as the trends of each differ over time.

Stage 2 of the CRAM model has important managerial implication and will help the CTO plan their information security (Sec_{t-1}) budgets and policies to be implemented to reduce the probability of attack (p_t) over time, as firms are never completely free of vulnerabilities (Mukhopadhyay et al. 2013b). The findings of the CRAM model agree (Alhazmi et al. 2007; Biswas et al. 2017; Miccolis 2000; Roumani et al. 2015; Ruohone et al. 2015) with the fact that, with an increase in security technology and the passage of time, the probability of an attack decreases. Yet many firms still view attacks as "the cost of doing business." This attitude prevents them from taking a more proactive stance toward preventing attacks.

Stage 3 of the CRAM models the loss distribution due to a cyber-attack on a firm, using gamma and exponential distribution as they tend to be positively skewed and long tailed (Dutta and Perry 2011; Hossack et al. 1983).

Stage 4 of the CRAM model estimates the expected severity to an organization, due to a cyber-attack, using the collective risk model (Hossack et al. 1983). This will help CTOs proactively assess expected losses arising from malicious attacks and prioritize their investments based on expected loss, risk-taking capacity, and BCP/DR. Organizations need to view the impact of security breaches as an important component of enterprise risk management strategies. Many banks tend to be more concerned with fraud and, as a result, the cost of fraud is well controlled and has decreased from 15 cents per $100 in 1992 to 5 cents per $100 in 2010 (Dash 2011). However, data loss and fraud are not unrelated, and newer forms of attacks are continually appearing. Researchers at Google have found that 10% of all Web pages could

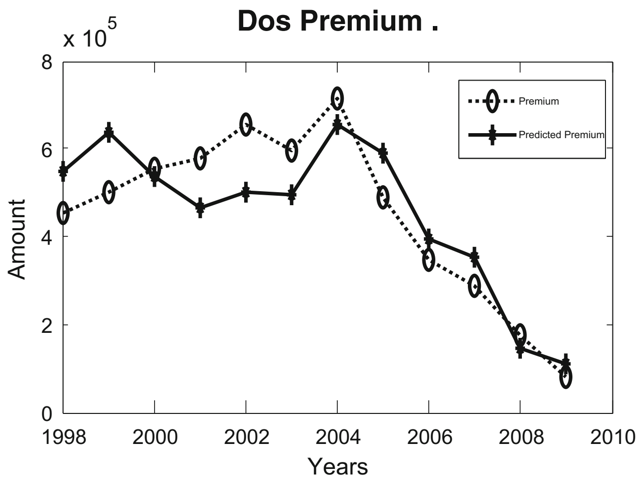


Fig. 16 DoS premium estimation

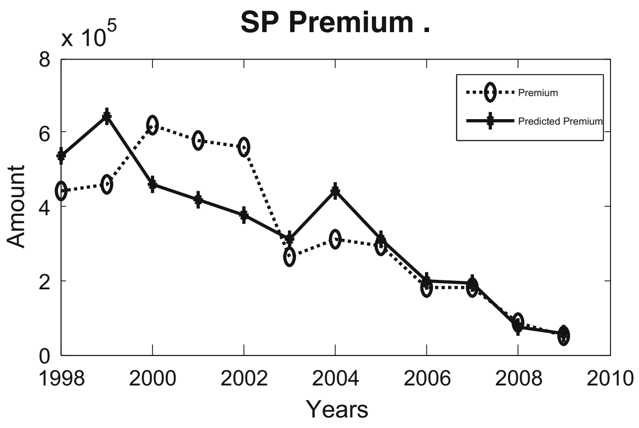


Fig. 18 SPI premium estimation

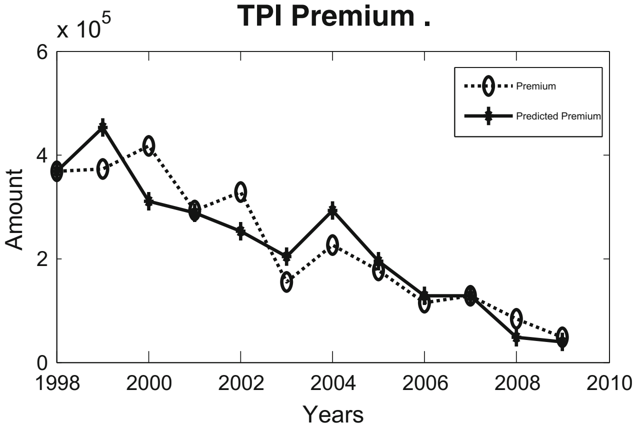


Fig. 19 TPI premium estimation

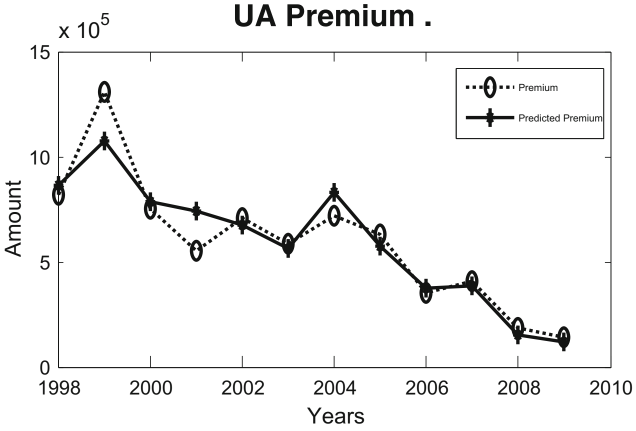


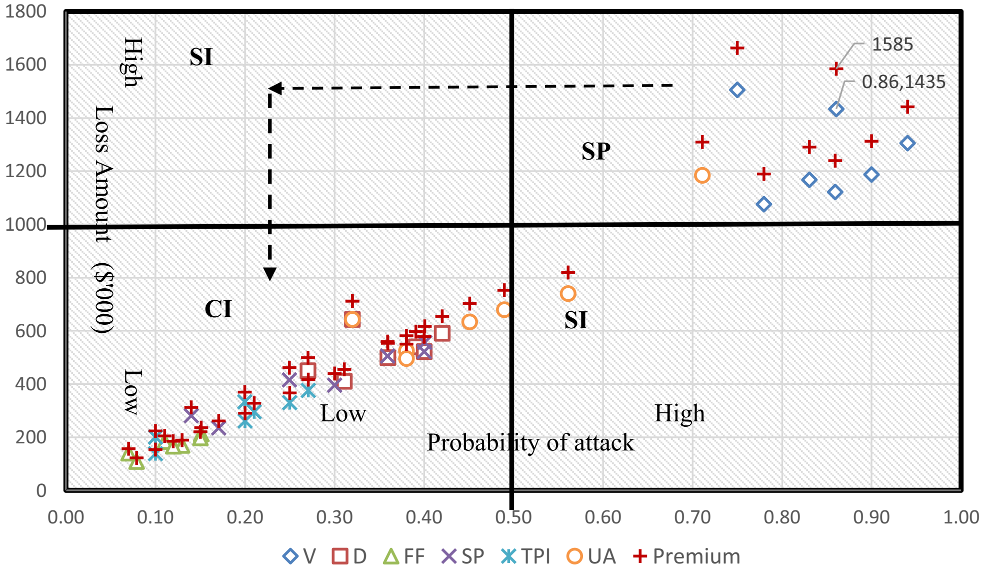
Fig. 20 UA premium estimation

successfully "drive-by download" (i.e., downloads that are made without understanding the consequences they may have) a Trojan virus onto a visitor's computer. Based on a sample of 4.5 million websites, it found that once malicious software is downloaded onto a user's devices, hackers can easily compromise it.

Stage 5 of the CRAM model determines the premium (Pr_i) that the cyber insurers would charge organizations each to indemnify the loss arising from these attacks. Cyber liability legislation mandates the creation of a proper cyber insurance market. This requires firms to adequately invest in IT security and "best practices" for effective risk management. This should lead to social welfare optimization and benefit all stakeholders (Kesan et al. 2004; Kesan and Majuca 2005; Ogut and Menon 2005). The cyber insurer will invest in developing expertise in tracking hackers and promote the development of technologies to curb such activities. Some large companies have obtained cyber insurance for the destruction of data and software, business interruption, data theft, denial of services, and extortion (Austin and Darby 2003). Major cyber-insurers cover network security, liability, content, and electronic media injury, as well as breaches in privacy and confidentiality liability (Mukhopadhyay et al. 2013). Recent offerings address cyber terrorism based on such government laws as the U.S. Terrorism Risk Insurance Act of 2002 (Shedden et al. 2010).

Stage 6 of the CRAM model classifies the losses due to each type of attack into four classes using a 2 × 2 matrix based on the probability and severity of attacks, and it recommends mitigation strategies (i.e., self-protection or SI or CI) for each of the attack types. CI and SI promote an organizational culture that emphasizes the value of IT security. Consequently, it can promote organizational awareness, efficiency, and effectiveness with respect to IT security. Such a shift in attitude means that software designers would strive to develop software that incorporates safeguards thwarting cyber-attacks (Austin and Darby 2003) and reducing insurance premiums. The use of CR insurance by organizations is expected to

Fig. 21 Cyber-risk mitigation strategy for each cyber-risk



promote e-commerce transactions. The reasons for slow adoption of CI are inadequate data to quantify risk and loss amount, an insufficient market base to pool the risk, and a reluctance by technology companies to adopt cyber-insurance products (Bandyopadhyay et al. 2009; Bolot and LeLarge 2008; Ogut and Menon 2005).

The limitations of this study are as follows: (i) we have used the CSI–FBI (1997–2010) survey dataset. The small size of the dataset makes it a bit difficult to train and test our model, (ii) all the cyber-attacks are assumed to be independent, and (iii) correlated CR has not been considered.

8 Conclusion

In this paper, we introduce our CRAM framework to quantify the probability of a malicious attack compromising an organization's IT systems and adversely affecting its top and bottom lines using GLM models (i.e., logit and probit). We also use the concept of collective risk modeling to compute the loss arising from malicious attacks. Our paper further proposes some strategies to mitigate CR by using financial instruments such as SI and CI. These financial instruments are effective complementary tools for organizations that have invested adequately in IT security, security policies and best practices and procedures related to ISMS and compliance with CoBIT or BS7799. It is preferable to seek CI if the risk frequency and severity are low, while SI may be preferred to ensure loss protection by reducing the size of a loss. Organizations generally set aside amounts in their budget to be used for contingent liabilities when a loss occurs. To reduce the size of such losses, organizations need robust BCP/DR processes containing actionable plans for data, backup, archiving, and restoration.

Future research could focus on relaxing the basic assumption that the cyber-attacks and their corresponding losses are independent. It could also use a dataset with more data points than the CSI–FBI data set for modeling cyber risk.

References

Alhazmi, O. H., Malaiya, Y. K., & Ray, I. (2007). Measuring, analyzing and predicting security vulnerabilities in software systems. *Computers and Security, 26*(3), 219–228.

Austin, R.D., Darby, C.R.A. (2003). The myth of secure computing. Harvard Business Review on Point Enhanced Edition.

Baer, W. S., & Parkinson, A. (2007). Cyber insurance in IT security management. *IEEE Security and Privacy, 5*(3), 50–56.

Bagchi, K., & Udo, G. (2003). An Analysis of the growth of the computer and internet security breaches. *Communications of the AIS, 12*, 684–700.

Bandyopadhyay, T., Mookerjee, V. (2017). A model to analyze the challenge of using cyber insurance. *Information Systems Frontiers*, 1–25. https://doi.org/10.1007/s10796-017-9737-3.

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why it managers don't go for cyber-insurance products. *Communications of the ACM, 52*(11), 68–73.

Baskerville, R. L. (1993). Information systems security design methods: implication for information systems development. *ACM Computing Surveys, 25*(4), 375–414.

Baskerville, R. L. (2008). Strategic information security risk management. In W. D. Straub, S. Goodman, & R. L. Baskerville (Eds.), *Information security, policy, processes and practices* (pp. 112–122). Routledge: M E Sharpe.

McCann, E. (2014). Breach alert: Hackers swipe data of 4.5M. http://www.healthcareitnews.com/news/breach-alert-hackers-swipe-data-45m. Accessed 7 Nov 2007

Bell, E. D. (1974). *Secure computer systems: A refinement of the mathematical model*. Bedford: NTIS U.S. Department of Commerce, Mitre Corporation.

Biba, J. K. (1977). Integrity considerations for secure computer systems. MTR-3153, The Mitre Corporation, April 1977.

Biswas B., Mukhopadhyay A. (2017). Phishing detection and loss computation hybrid model: A machine-learning approach. *ISACA Journal, 1*, 22–29

Biswas B., Pal S., Mukhopadhyay A. (2016). AVICS-Eco framework: An approach to attack prediction and vulnerability assessment in a cyber Ecosystem. *Proceedings of the 22nd Americas Conference on Information Systems*. San Diego: Association for Information Systems.

Biswas, B., Mukhopadhyay, A., Dhillon, G. (2017). GARCH-based risk assessment and mean-variance-based risk mitigation framework for software vulnerabilities. *In Proceedings of 23rd Americas Conference on Information Systems*. Association for Information Systems.

Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management. Proceedings of the workshop on New security paradigms (NSPW '01)* (pp. 97–104). New York: ACM.

Böhme, R. (2005). *Cyber-insurance revisited*. Harvard: Workshop on the Economics of Information Security (WEIS).

Böhme, R., Kataria, G. (2006). Models and measures for correlation in cyber-insurance. UK: Workshop on the Economics of Information Security (WEIS) University of Cambridge, 2006, June.

Böhme, R., Schwartz, G. (2010). Modeling cyber-insurance: Towards a unifying framework. Harvard: Workshop on the Economics of Information Security (WEIS), 2010, June.

Bolot, J., & LeLarge, M. (2008). *Cyber insurance as an incentive for internet security*. Hanover: Workshop on the Economics of Information Security (WEIS).

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Bureau of Justice Assistance. (2009). *2009 internet crime report*. Washington, D.C: U.S. Department of Justice.

Calandro, J., Matrejek, E., Pollard, N. (2014). Managing cyber risks with insurance: key factors to consider when evaluating how cyber insurance can enhance your security program. Price Water House Publication number BS-14-0534-A.0614. Available at http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-managing-cyber-risks-with-insurance.pdf.

Campbell, K., Gordon, L. A., & Loeb, M. P. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*, 431–448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). 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), 69–105.

Cavusoglu, H., Cavusoglu, H., & Zhang, J. (2008). Security patch management: share the burden or share the damage? *Management Science, 54*(4), 657–670.

CCTA. (1991). *SSADM-CRAMM subject guide for SSADM version 3 and CRAMM version 2*. London: Central Computer and Telecommunications Agency, IT Security and Privacy Group, Her Majesty's Government.

Clark, D., Wilson, D. (1988). Evolution of a model for computer integrity. *11th National Computer Security Conference, Postscript to Proceedings*, *NIST/NCSC* (pp. 14–27). October 1998.

Cleman, T. R., & Reilly, T. (1999). Correlations and copulas for decision and risk analysis. *Management Science, 45*(2), 28–224.

Courtney, R. (1977). *Security risk assessment in electronic data processing* (pp. 97–104). Arlington: AFIPS.

Cutler, D. M., & Zeckhauser, R. (2003). Extending the theory to meet the practice of insurance. *Brookings-Wharton Papers on Financial Services* (pp. 1–53). Washington, DC: Brookings Institution Press.

Das, S., Mukhopadhyay, A., & Anand, M. (2012). The stock Market response to public announcement of information security breach on a firm: an Exploratory study using firm and attack characteristics. *Journal of Information Privacy and Security JIPS, 7*(4), 27–55.

Das, S., Mukhopadhyay, A., Shukla, G. K. (2013). i-HOPE framework for predicting cyber breaches: a logit approach. *Proceedings of the 46th Hawaii International Conference on System Sciences (HICSS)* (pp. 3008–3017). Hawaii: IEEE. https://doi.org/10.1109/HICSS.2013.256.

Dash, E. (2011). City data theft points up a nagging problem. New York Times, June 9, 2011.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125–127.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security, 20*(8), 715–723.

Dhillon, G., & Torkzadeh, G. (2006). Value focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293–314.

Di, R., Hillairet, M., Picard, M., Rifaut, A., Bernard, C., Hagen, D., Maar, P., & Reinard, D. (2007). Operational risk management in financial institutions: process assessment in concordance with Basel II. *Software Process: Improvement and Practice, 12*(4), 321–330.

Dutta, K., & Perry, J. (2011). 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.

Fang, F., Parameswaran, M., Zhao, X., & Whinston, A. B. (2014). An economic mechanism to manage operational security risks for interorganizational information systems. *Information Systems Frontiers, 16*(3), 399–416.

FBI. (2009). High-tech heist: 2,100 ATMs worldwide hit at once. Available at: http://www.fbi.gov/news/stories/2009/november/atm_111609.

Finkle, J. Freifeld, K. (2014). http://www.reuters.com/article/2014/04/03/us-experian-databreach-idUSBREA321SL20140403. April 2014.

Geer Jr., D., Hoo, K. S., & Jaquith, A. (2003). Information security: why the future belongs to the quants. *IEEE Security and Privacy, 99*(4), 24–32. https://doi.org/10.1109/MSECP.2003.1219053

Gordon, L. A., & Loeb, M. P. (2002). Return on information security investments, myths vs realities. *Strategic Finance, 84*(5), 26–31.

Gordon, L. A., Loeb, M. P., & Sohai, T. L. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81–85.

Gordon, L.A., Loeb, M.P., Lucyshyn, W., Richardson, R. (2009). CSI/FBI computer crime and security survey. GoCSI.com.

Gorman, S. (2012). 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.

Grzebiela, T. (2002). Insurability of electronic commerce risks. *Proceedings of the Hawaii International Conference on System Sciences*, 35, USA.

Guarrao, S. (1987). Principles and procedures of the LRAM approach to information systems risk analysis and management. *Computers & Security, 6*(6), 493–504.

Harmantzis, C.F. (2003). Operational risk management. *ORMS Today*, *30*(1).

Hartwig, R. P., & Wilkinson, C. (2014). *Cyber risks: the growing threat* (pp. 1–27). USA: Insurance Information Institute.

Herath, H., Herath, T. (2011). Copula based actuarial model for pricing cyber, insurance policies insurance markets and companies: analyses and actuarial computations, 2.

Hoffman, J. et al. (1978). *SECURATE—security evaluation and analysis using fuzzy metrics* (pp. 531–540). Proceedings of the AFIPS National Conference Proceedings, Arlingtion

Hossack, B. I., Pollard, J., & Zehnwirth, B. (1983). *Introduction to statistics with applications to general insurance*. Cambridge: Cambridge University Press.

Identity Theft Center. (2007). http://www.idtheftcenter.org/. Last consulted 5–6-2007.

Jensen, F. V. (1996). *Introduction to Bayesian networks*. Secaucus: Springer-Verlag New York, Inc.

Jueneman, R.R. (1989). Integrity controls for military and commercial applications CSC professional. Report CSC/PR-89/3001.

Kahane, Y., Neumann, S., & Taperio, S. C. (1988). Computer backup pools, disaster recovery, and default risk. *Communications of the ACM, 31*(1), 78–83.

Kahneman, D., & Tversky, A. (1979). Prospect theory: an analysis of decision under risk. *Economterica, 47*(2), 263–292.

Keily, G. (2014). eBay suffers massive security breach, all users must change their passwords. http://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/.

Kesan, J. P., & Majuca, R. (2005). *Cyberinsurance as a market-based solution to the problem of cybersecurity: A case study*. Harvard: Fourth Workshop on the Economics of Information Security (WEIS).

Kesan, J.P., Ruperto, P.M., Willam, J.Y. (2004). The economic case for cyber insurance. Working Paper Series No. Paper No. LE04–004, Illinois Law and Economics.

Kunreuther, H. (1997). Managing catastrophic risks through insurance and mitigation. *Proceedings of the 5th Alexander Howden Conference on Financial Risk Management for Natural Catastrophes*, August 24–26, 1997.

Majuca, P., Yurcik, W., Kesan, J.P. (2005). The evolution of cyber insurance. Available at: http://arxiv.org/ftp/cs/papers/0601/0601020.pdf.

Mann, S. (1998). Netcrime: more change in the organization of thieving. *British Journal of Criminology, 38*, 201–229.

McLeod, D. (2015). Increased cyber losses means more litigation over claim. Business Insurance. Available at http://www.businessinsurance.com/article/20150222/NEWS06/303019999/1248.

Meland, P. H., Inger, A. T., & Solhaug, B. (2015). Mitigating risk with cyber insurance. *IEEE Security and Privacy, 6*, 38–43.

Miccolis, J., Shaw, S.(2000). Enterprise Risk Management: An Analytic Approach. New York:Tillinghast – Towers Perrin

Mitra, S., & Ransbotham, S. (2015). Information disclosure and the diffusion of information security attacks. *Information Systems Research, 26*(3), 565–584.

Moore, R. (2005). *Cybercrime: Investigating high-technology computer crime*. Cleveland: Anderson Publishing.

Mukhopadhyay, A. Chakrabarti, B. B., Saha, D., Mahanti, A. (2007a). e-Risk management through self-insurance: an option model.

Proceedings of the Hawaii International Conference on System Sciences, 40. Washington, DC: IEEE Computer Society.

Mukhopadhyay, A., Chatterjee, S., Roy, R., Saha, D., Mahanti, A., Sadhukhan S. K. (2007b). Insuring big losses due to security breaches through insurance: A business model 2014. *Proceedings of the 47th Hawaii International Conference on System Sciences*. Hawaii: IEEE. https://doi.org/10.1109/HICSS.2007.280

Mukhopadhyay, A., Das, S., Sadhukhan, S. K. (2013a). Vulnerable path determination in mobile ad-hoc networks using Markov Model. *Proceedings of the 19th Conference Amercias Conference on Information Systems (AMCIS)*.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukan, S. K. (2013b). Cyber-Risk Decision Models: To Insure IT or Not?. *Decision Support Systems, 56*(1), 11–26.

McCullagh, P., & Nelder, J. A. (1989). *Generalized linear models, 2nd edition*. London: Chapman & HaI/~CRC.

New York Times. (2007). Digital fears emerge after data siege in Estonia. May 29, 2007.

New York Times. (2008). Before the gunfire, cyber -attacks twitter. August 12, 2008.

Newman, J. (2013). Adobe security breach worse than originally thought. http://www.pcworld.com/article/2059002/adobe-security-breach-worse-than-originallythought.html.

Ogut, H., & Menon, N. (2005). *Cyber insurance and IT security investment: Impact of interdependent risk*. Harvard: Fourth Workshop on the Economics of Information Security (WEIS).

Öğüt, H., Raghunathan, S., & Menon, N. (2011). Cyber security risk management: public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis, 31*(3), 497–512.

Ozier, W. (1989). Risk quantification problems and Bayesian decision support system solutions. *Information Age, 11*(4), 229–234.

Reid, R. C., & Stephen, A. F. (2001). Extending the risk analysis model to include market-insurance. *Computers & Security, 20*(4), 331–339.

Rejda, G. E. (2010). *Principles of risk management and insurance* (10th ed.). London: Pearson Publication.

Richardson, R. (2007). *CSI computer crime and security survey* (pp. 1–28). San Francisco: Computer Security Institute Inc..

Robertson, J. (2014). China's hack of 4.5 million U.S medical records? This chart will make you sick. http://www.bloomberg.com/news/2014-08-21/china-s-hack-of-4-5-million-u-s-medical-records-this-chart-will-make-you-sick.html. August 2014.

Roumani, Y., Nwankpa, J. K., & Rouman, Y. F. (2015). Time series modeling of vulnerabilities. *Computers & Security, 51*, 32–40.

Ruohone, J., Hyrynsalmi, S., & Leppänen, V. (2015). The sigmoidal growth of operating system security vulnerabilities: an empirical revisit. *Computers & Security, 55*, 1–20.

Salmela, H. (2008). Analyzing business losses caused by information systems risk: a business process analysis approach. *Journal of Information Technology, 23*(3), 185–202.

Schneier, B. (2000). The insurance takeover. Information Security.

Schroeder, D. (2014). Cyber insurance: just one component of risk management. The Wall-Street Journal, May 27 2014. Available at http:/blogs.wsj.com/cio/2014/03/27/cyber-insurance-just-onecomponent-of-risk-management/.

Shedden, P., Smith, W. R., Ahmad, A. (2010). Information security risk assessments: towards a business practice perspective. Edith Cowan University Research Online, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1097&context=ism.

Shetty, N., Schwartz, G., Felegyhazi, M., & Walrand, J. (2009). *Competitive cyber-insurance and internet security*. London: Workshop on the Economics of Information Security (WEIS).

Smith, E., & Eloff, J. H. P. (2002). A prototype for assessing information technology risks in health care. *Computers & Security, 21*(2), 266–284.

Smith, S.T., & Lim, J.J. (1984). An automated method for assessing the effectiveness of computer security safeguards. In *Computer Security A Global Challenge* (pp. 321–328). Amsterdam: North-Holland Publishing Co..

Smithson, S., Song, P. (2004). Quantifying operational risk. *Risk,* 57–59.

Solms, V. (2005). Information security governance - compliance management vs operational management. *Computers & Security, 24*(6), 443–447.

Tavani, H. (2007). *Ethics and technology: Ethical issues in an age of information and communication technology*. Hoboken: John Wiley.

TechFlash. (2009). Walmart, Amazon.com hit with denial of service attack. December 24, 2009. Available at: http://www.techflash.com/seattle/2009/12/walmart_amazoncom_hit_with_denial_of_service_atack.html.

Times of India. (2013). http://timesofindia.indiatimes.com/tech/tech-news/Cybercrimes-cost-India-4-billion-in-2013-Symantec/articleshow/24551193.cms. Accessed 7 Nov 2017

Straub, W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision-making. *MIS Quarterly, 22*(4), 441–469.

Yurcik, W. (2002). *Cyber insurance: A market solution to the internet security market failure*. Berkeley: Workshop on the Economics of Information Security (WEIS).

Dr. Arunabha Mukhopadhyay , is an Associate Professor of Information Technology & Systems Area at Indian Institute of Management Lucknow (IIM Lucknow). 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. He has published in various referred journals and conferences including DSS, JGITM, 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).

Dr. Samir Chatterjee is Professor and Fletcher Jones Chair of Design, Technology & Management at Claremont Graduate University. He is also considered a leading technology designer and strategist for twenty-first century healthcare. He is the founding director of IDEA Labs (Innovations Design Empowerment Applications Laboratory), initially made possible by a grant from NSF. His main research areas are healthcare informatics, persuasive behavior change, cyber security and human computer interaction. He has published over 130 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), Journal of Medical Internet Research (JMIR), Telemedicine & e-Health Journal, European Journal of Information Systems, Information Systems Frontiers, Computer Communication, IEEE IT Professional, ACM CCR, Communications of AIS, Journal of Internet Technology etc. He has served as an Associate Editor of the MIS Quarterly, a flagship journal in IS. He serves on the editorial board of International Journal of Business Data Communications and Networking, Journal of AIS and Health Systems Journal (from Palgrave Macmillan). His research has been funded by National Science Foundation (NSF), National Institutes of

Health (NIH), Internet2, Michigan Diabetes Center, The California Endowment, Northrop-Grumman, BellSouth, Institute for HeartMath, Loma Linda Foundation and several other corporations. In May 2015, he was awarded the distinguished lifetime achievement award for contributions to Design Science Research, presented by the IS design community. In 2017 he was selected as Schoeller Senior Fellow 2017 by Dr. Theo and Friedl Schoeller Research Center for Business and Society in Nuremberg Germany. He is also Founder & CEO of DCL Health, a wireless healthcare startup.

Dr. Kallol Bagchi received a Ph.D. in Computer Science from Jadavpur University, India, in 1988 and another Ph.D. in Business from Florida Atlantic University in 2001. He is the Nita and Jim Phillips Endowed Professor at the University of Texas at El Paso. He has published in many journals such as International Journal of Electronic Commerce and Communications of the ACM. His present research interests are in global information technology, adoption and diffusion of information technology, security, networking, ecommerce and simulation.

Dr. Peeter Kirs is a Professor of Information Systems in the Department of Accounting and Information Systems at the University of Texas at El Paso. He has published over 25 papers in peer reviewed journals.

Dr. Girja Kant Shukla after completing M.Sc from Lucknow (India) University and PhD (Edinburgh University, U.K.) he taught in Edinburgh University, Poona University(India) and in the Indian Institute of Technology, Kanpur (India) as a Professor in the Department of Mathematics and Statistics. He also worked as a Visiting Faculty in the Indian Institute of Management, Lucknow (India). He has supervised seven PhD students and published about fifty research papers in national and international peer reviewed journals. He was the Editor of Biometric Bulletin (1990–1992) of International Biometric Society. His specialization is in linear models, time-series and data analysis.