Journal of Network Communications and Emerging Technologies (JNCET)
Volume 12, Issue 1, January (2022)

Importance of Insurance Safeguards and Risk Assessment of Cybercrimes and Network Intrusions

Rohitha Goonatilake
Department of Mathematics and Physics, Texas A&M International University, Laredo, TX 78041-1900, USA
harag@tamiu.edu

Susantha Herath
Department of Information Systems, St. Cloud State University, St. Cloud, MN 56301-4498, USA
sherath@stcloudstate.edu

Published online: 11 January 2022

ABSTRACT

Cybercrimes and network intrusions are on the rise in volume and severity. Federal and state laws dealing with these crimes are prosecuting to the fullest extent of the law. As the law deals with violators and other criminal enterprises, software facilitators need to prevent the networks from being victimized by taking measures to safeguard themselves from losses associated with these malicious acts rising from unscrupulous behavior. Unfortunately, software defects that cause unrecoverable damages are frequent. This article emphasizes the severity of these situations and the types of insurance coverages available to minimize the financial losses sustained by these acts and unintended consequences, as a result, using analyses found in the literature. Additional investigations are steered using the FAIR risk taxonomy model and the fundamentals of Bayesian belief networks (BBN) to further the risk assessment related to cyberattacks.

Index Terms – Insurance, Premium, Cybercrime, Computer, Network, Losses.

1. INTRODUCTION

The agencies of federal, state, and local authorities demand all network facilitators to obtain at least a third-party insurance coverage to defend any future losses due to the increasing reports of security breaches, data thefts, and other electronic privacy violations. Current cyber (security) insurance is constructed to mitigate losses resulting from various cyber incidents that include data breaches, business interruption, and network outages. The Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice has been given the tasks of three primary responsibilities: (a) deterring and disrupting computer and intellectual property crimes by bringing them for prosecutions, (b) guiding the appropriate assembly of electronic evidence by investigators to subsequent prosecutions, and (c) providing technical and legal assistance to the field and prosecutors in the U.S. and around the world [1]. CCIPS has established categories of prosecutable computer crimes as first published in February 2007. Computers can be pertinent to a criminal activity in two different ways—the use of the computer as a device in committing a crime and the use of the computers themselves as a focus of the criminal act [2]. However, with regards to the origin of network risk designation, it is the obligation of the network providers to eliminate all risks and outside exposure associated with unscrupulous acts, damages, sabotages, and defects. From analytical thinking, it is not possible to predict future malicious code activity. In some cases, the law is not clear because such cases have not been established yet. It is well known among members of the antivirus in the cyber community that entirely new forms of threats often can emerge without any advanced warning signs. Theft of organizational secrets, commercial losses, taking away academic accomplishments, and business secrets (and losses), technical expertise loss results from network vulnerabilities. The loss of valuable information such as trade secrets and intellectual properties of U.S. organizations contributed to roughly 70% of the market share of a typical U.S. company. Organizations have reported $45 billion and above annual losses of commercial secrets and proprietary information according to a survey of the Fortune 1000 [3]. In 2006, it was reported that there was a total loss of $52,494,290 due to these crimes. This report is based on a survey conducted for 616 computer security practitioners of government, private, and academic institutions in U.S. [4]. Table 1 depicts the cyber losses in dollar amounts recorded by each type of crime in the survey. Generally, the network security liabilities arise from authentic or alleged incidents related to any of the following possible scenarios:

- Transmission of malicious code and computer virus,
- Unauthorized access or use,
- Damages to physical equipment and software,

- Loss of service (DoS), and
- Interruption of service.

The sustainability of the cyber insurance marketplace is that it ensures that the community of all network users to obtain the coverage that is maximized for the market equilibrium prevails. Individual coverages are tailored to their needs in the various marketplaces, and volatile and threat assessment. This refers to the total amount of the net utilities of network users after investing in self-defense, cyber insurance, or both to protect their clientele. An approach to model the impact of selected cyber threats in structuring the cyber risk insurance model has been undertaken. The results provided the basis to quantify possible financial implications to propose by developing an optimal coverage of cyber insurance [5]. An assessment of cyber threats helps everyone better understand security risk, productivity, and utilization and performance given the market conditions.

First, we assume that a transmission network comprises a continuum of risk-averse users. Secondly, a standardized monopolistic and both perfect and oligopolistic competitive cyber insurance market is volatile. A governmental agency ensures that insurers profit under specific restrictions, and network security is typically improved by a regulatory mechanism [6]. Network security liability results from any loss sustained due to either first party only, or first party, and third-party damages. The cyber insurance coverages depend on containment of these liabilities. However, it is costly to safeguard against all possible network attacks and often the insurers will not provide coverage for corporations with inadequate security procedures and safeguards. Sterlicchi [50] asserted that "it's not rocket science for businesses to realize there has to be a trade-off between lessening the risk of any security breaches and the price of insurance." The quantity of risk is established as a product of threat, vulnerability, and asset values, all combined [7]. These are two primary of risk analysis, namely, quantitative, and qualitative, are in discussion. Quantitative risk analysis attempts to allocate significant quantities of them to all aspects of the risk scenarios [8]. This is typically calculated using Risk = Asset x Threat x Vulnerability connected to the performance of the network system. As any other insurance, there should be a proper balance between safety investments and tolerable loss, every software institution must take a mixed approach to manage risk. Self-protection will have the major share in dealing with prevention. In addition, preventive measures, remedial actions, and self-insurance are recommended prior to acquiring cyber insurance. This will be a cost-saving measure, but developing a strategy is paramount to avert risk [9].

Internet Crime Complaint Center (IC3, https://www.ic3.gov/) of the Federal Bureau of Investigation (FBI) in its 2019 Internet Crime Report, highlighted its efforts to monitor trending financial exploitations such as Business E-mail Compromise (BEC), Ransomware, Elderly Fraud, and Tech Support Fraud. Just in 2019 alone, IC3 received a total of 467,361 complaints, with stated losses surpassing $3.5 billion. The most widespread crime categories were Phishing/ Vishing/ Smishing/ Pharming, Non-Payment/ Non-Delivery, Extortion, and Personal Data Breach [10]. The top three highest reported losses were Business E-mail Compromise/E-mail Account Compromise (BEC/EAC), Confidence/Romance Fraud, and Spoofing as seen in Table 1. As for the descriptors therein under the specific crime type, they are related to the medium or tool used to enable the crime and are used for the purpose of IC3 tracking only. They are only available under a secondary criminality type that has been explicitly designated to match the category.

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/ Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/ Rental	$221,365,911	IPR/ Copyright and Counterfeit	$10,293,307
Non-Payment/ Non-Delivery	$196,563,497	Ransomware	$8,965,847
Identity Theft	$160,305,789	Denial of Service/ TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/ Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118

Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/ Vishing/ Smishing/ Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053	Descriptors (medium tracking purposes only)	
Corporate Data Breach	$53,398,278	Social Media	$78,775,408
Lottery/ Sweepstakes/ Inheritance	$48,642,332	Virtual Currency	$159,329,101

Table 1 Dollar Amount Losses by Each Crime Type

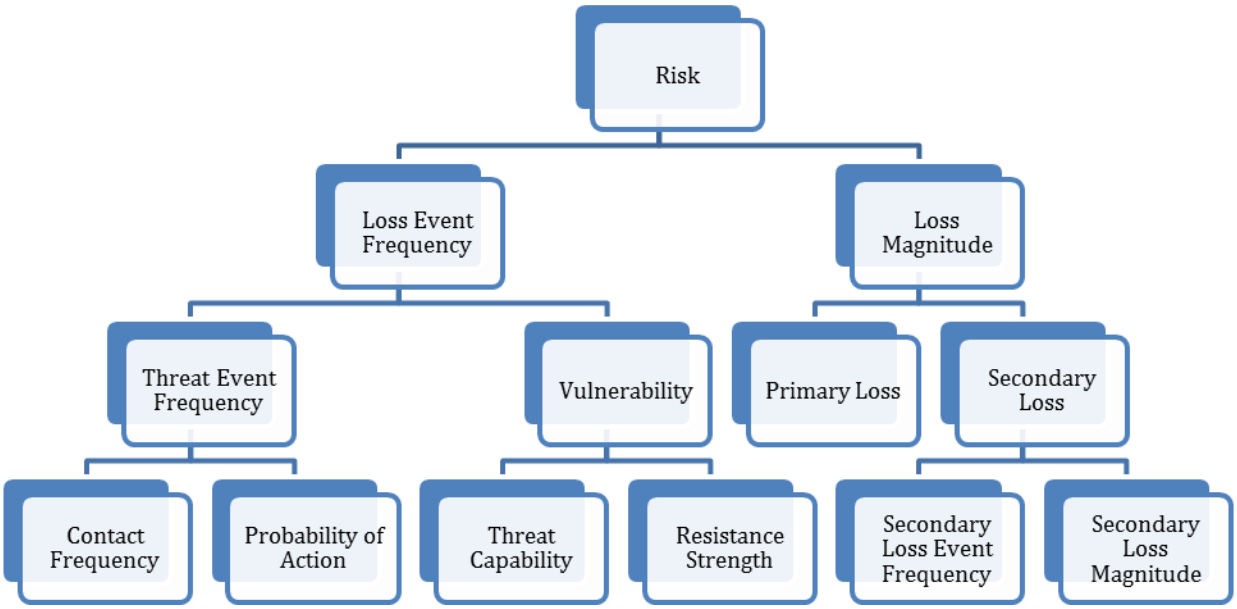
Source: Internet Crime Report, 2019 [4]

Hackers are becoming more aggressive and sophisticated in their attack strategies on networks as hardening software and preventive measures are being researched, developed, and utilized. For example, in the case of ransomware, it is a type of malicious software designed to prevent access to a large computer system by authorized users. Hackers demand a ransom payment (typically cryptocurrency) to restore access. It has been seen in the past that some institutions, including institutions of higher education, were held hostage for ransom jeopardizing the sensitive data of students and their academic records. Recently, there has been a ransomware attack on the computer system of the privately held Colonial Pipeline, one of the major pipeline operators in the U. S. that provides roughly 45% of the East Coast's fuel, including gasoline, diesel, and home heating oil, jet fuel, and resources for military fuel [11]. The Colonial Pipeline, headquartered in Alpharetta, Georgia, was founded in 1962. This underscores the extent of harm that could trigger private and public institutions of this magnitude to a halt. Fuel shortages brought the supplies to a standstill, while the price of gasoline kept skyrocketing. It appears that a ransom to the tune of $5 million has been made to resume the operation back to normal. There were other reported ransomware attacks soon afterward. Hence, it is crucial for consumers to make the right moves and become more proactive and to have better protection as they turn on their computers venturing into cyberspace. All experts agree that it is vital to have antivirus, anti-spyware, and firewall defense that is up to date and active to protect against the daily emergence of new viruses, worms, hackers, adware, and malware that destroy costly artifacts such as digital photos, music files, financial data records, and cause identity thefts. They keep computers secured and adequately protected to operate without a lapse.

Companies across the North American continent are grappling with the question of how best to safeguard client information and moderate network hazard emanating from the uses and abuses of technology [12]. Insurance risk analysis is an assessment or underwriting, which is the procedure widely used by insurers to evaluate and assess the risks associated with a particular insurance policy. This will help in calculating the correct premium for an insured. Coverages at various levels can be designed depending on the extent of the losses likely and monetary losses that could occur due to the theft of sensitive business data. First-party insurance of network hazard policies covers all costs and losses sustained by others because of the failure of the insured's network and its uses of software. The variants of extended coverages are tailored to fit customers' wants by keeping in mind all other anticipated losses and individuals, groups, and types of network systems, nature of commerce, and software capacities and hazards. Consumers and software developers are constantly considering a trusted source of unique, data-driven insights on insurance to empower themselves to avoid losses due to cybercrime and network intrusion [13]. Consumers and professionals seeking insurance information need to be aware of the extent and magnitude of coverage available to address the vulnerabilities that arise from attacks.

The Factor Analysis of Information Risk (FAIR) is a model frequently available to the analysists working on Cybersecurity Risk Assessment (CRA) framework as an excellent approach for quantitative risk analysis in software industries. It is in fact a Bayesian network approach for CRA [14]. This works within the Open FAIR™ Taxonomy concerning the loss event frequency and loss magnitude as seen branched out in terms of risk categories in Figure 1. The applications of Bayesian network approach provide numerous benefits towards developing devices for real-time risk consideration because of their ability to apprise probabilities, given either the availability of evidence or observations [15]. Loss event frequency component in the FAIR model would demonstrate loss event frequencies using statistical dependencies based on threat event frequencies and vulnerabilities. The FAIR model essentially stems from the FAIR taxonomy and statistical practices to carry out quantitative risk assessment [16]. This Bayesian network approach expands the FAIR model to implement cybersecurity risk assessment [17]. The right side of the FAIR model is essentially the components of probable loss magnitude, whereas the left is reserved for the probable loss event frequencies. However, the primary loss is a standalone contribution to the loss magnitude of the risk. The FAIR model provides a basis for analyzing, understanding, and calculating the risk. The main limitation of the FAIR model is the lack of information about

methodology and how the methodologies are put to work suitably [18]. FAIR analysis equipped with the attack graphs allows complex environments to be broken down into more understandable and quantifiable pieces, thus providing interesting new insights into this emerging technique. The impact to FAIR vulnerability and risk provides a mitigation plan that fixes critical vulnerabilities posing less likely risk with greater precision together with detailed analyses [19]. The functions associated with the primary loss and the secondary loss event frequencies in the study are associated with Poisson and binomial distributions, respectively [17].



Source: The Open Group, 2018 [16]

Figure 1 High-Level Open FAIR Risk Taxonomy

A few of the fundamental tools available in Bayesian belief networks (BBN) can also be used to analyze the FAIR risk taxonomy model [20]. For example, we consider that there are four types of cyberattacks considered at the top of the most common types of attacks. The present BBN is described and represented in the presence of these four uncertainties. We investigate how it would be possible to gain the knowledge to make any significant differences between them.

- Brute-force attack (B) - is a trial-and-error strategy utilized by applications to decode encrypted data that include Data Encryption Standard (DES) or user credentials.
- Credential Stuffing (C) - is a method in which the attackers use a steam of compromised user credentials to break into the system for fraudulent use.
- Phishing and Spear Phishing (S) - are forms of e-mail attacks destined to coerce users into compromising actions, like clicking an embedded link or attachment that contains malware aimed at attacking the computer and business applications.
- Malware attacks (M) - is a kind of cyberattack using malware or malicious software that executes activities on users' computer systems or networks, generally without their knowledge.

Additionally, the Bayesian belief network (BBN) provides a basis for modeling the uncertainty with probabilities associated with the most common cyberattack risk factors. BBN is a powerful and fundamental tool in Bayesian machine learning. For the BBN, the entire joint distribution is formulated employing conditional distributions of $B, C, P,$ and M given the risk (R) and that of R given C, B as provided in Figure 2 (together with some possible values for them). In another development, a context for dynamic risk assessment has been established using an evaluation technique termed as Process Unit Life Safety Evaluation (PULSE). This permits the creation of a BBN that manage discrete, continuous, or both variables together (hybrid) [15]. This process of safety and dynamic risk assessment devices have been launched using BBN by the ExxonMobil Research Qatar (EMRQ) and Mary Kay O'Connor Process Safety Center of Qatar (MKOPSC-Q) [21].

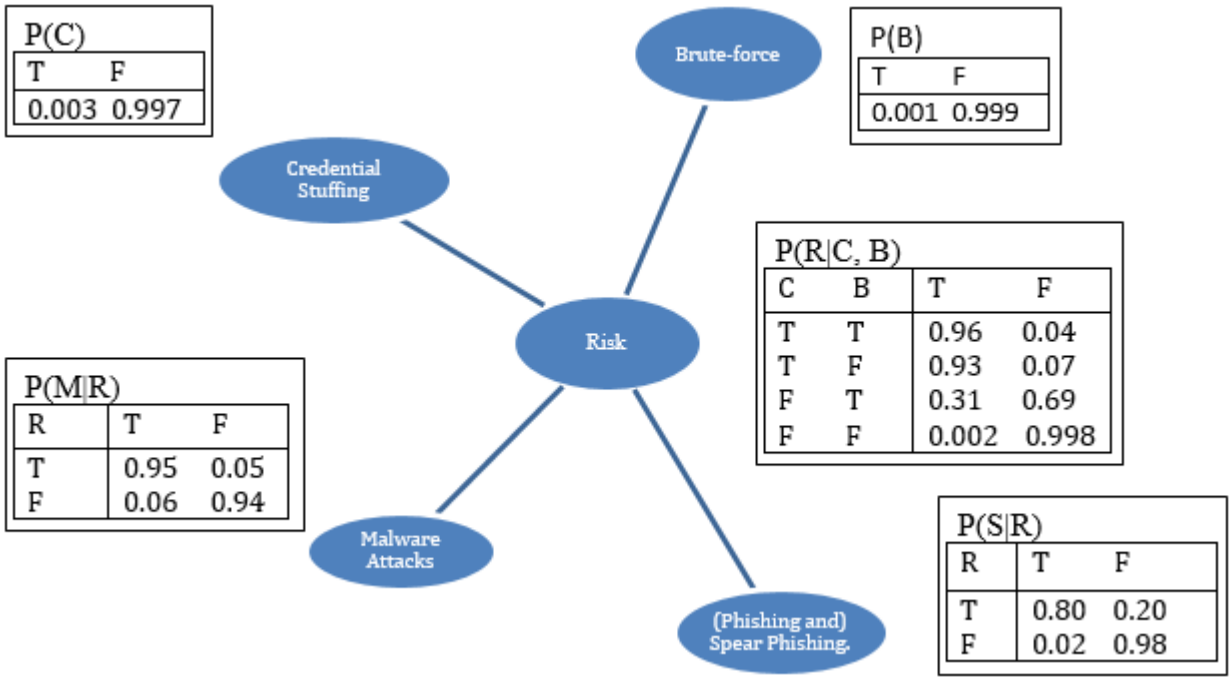


Figure 2 Conditional Probability Distribution (for Each Variable Given its Parents)

The problem of parameter complexity found in the BBN is the full joint distribution formulated using a product of local conditional complexities applying the familiar chain rule as $P(X_1, X_2, \cdots, X_n) = \prod_{i=1,\cdots n}(X_i \,|pa(X_i))$. In fact, there are $2^5 = 32$ – full joint and $2^3 + 2(2^2) + 2(2) = 20$ – BBN parameters [22]. However, an additional, $2^5 - 1 = 31$ – full joint and $2^2 + 2(2) + 2(1) = 10$ – BBN parameters are yet to be defined. The inferences allow BBN to model compactly the full joint distribution in terms of independences existed between the variables in order to streamline the process of acquisition of the underlying probabilistic model. Let the random variables assume values as $C = T, B = T, R = T, M = T,$ and $S = F$, then $P(C = T, B = T, R = T, M = T, S = F) = P(C = T) \times P(B = T) \times P(R = T|C = T,\ B = T) \times P(M = T|R = T) \times P(S = F|R = T) = 4.61 \times 10^{-7}$ [23]. Further inferences comprise of diagnostic and prediction tasks including various probabilistic probes [24]. There are other potential inferences that can be made in Bayesian networks such as computing $P(M = T)$ using blind and interleaved sums and products approaches. The former is computationally costlier than the other. Hackers execute different attack techniques to compromise the computer system. Towards this end, one other possible statistical inference embraces verifying whether the risk posed by brute-force attacks and malware attacks are independent of each other in the presence of a given amount of risk. That is, if the brute-force attacks (B) are independent of malware attacks (M) given the risk (R)? For this, we verify if $P(B|R,\ M) = P(B|R)$ and $P(B,\ M|R) = P(B|R) \cdot P(M|R)$. These are the glimpse of Bayesian belief network approaches at work to predict losses caused by commonly known cyberattacks.

Further, solely depending on the notations from [25], let X denote the prior information made available from a random sample. A decision procedure tells us the decision maker that the amount of experimentation and the possible values of X that would assume. This is a function of the random data, $d[X]$, as the circumstances may be. For example, if the random variable X take on value x, then $a = d[x]$ is considered the appropriate action to be taken. Since a is a function of the outcome of the random variable X, then $d[X]$ is a random valued quantity to the action taken. Accordingly, we define the risk function $R(d, \theta)$, when the actual state of nature is θ, as $R(d, \theta) = E[l(d[X], \theta)]$, where the expectation is calculated according to the probability distribution of the random variable, X, and the loss function is inclusive of the cost of obtaining the experimentation data.

If the decision-maker has particularly advanced data about the present states, it can be described in terms of a prior distribution, and then the Bayes' principle provides the description of the risk function. The Bayes' risk associated with the decision function d and a prior probability distribution $\theta, P_\theta(k)$, is given by $B(d) = \sum_{\forall\, k} R(d, k)P_\theta(k)$. If the data is from the continuous variables, the Bayes' risk corresponding to a prior probability density function of $\theta, P_\theta(y)$, and is given by $B(d) = \int_{-\infty}^{\infty} R(d, y)P_\theta(y)dy$. Upon the computation of the posterior distribution of θ, given $X = x$, we choose the action that minimizes the expected loss $l_h(a)$ calculated using the posterior distribution of θ, given $X = x$, where

$$l_h(a) = E[l(a,\theta)] = \begin{cases} \sum_{\forall k} l(a,k) h_{a|X=x}(k), & \text{if } \theta \text{ is discrete} \\ \int_{-\infty}^{\infty} l(a,y) h_{a|X=x}(y)dy, & \text{if } \theta \text{ is continuous.} \end{cases}$$

We identify the probability of loss when the vulnerability is high, medium, and low, respectively, as provided in Table 2 to calculate the expected losses [26]. The posterior distribution is needed for computations with respect to the posterior distribution of θ, given $X = 1, 2, \text{and } 3$ for each selection. The coverages for θ_1, θ_2, and θ_3 are respectively, assumed to be \$500 million, \$300 million, and \$200 million for the purpose of computations.

$x \backslash k$	θ_1	θ_2	θ_3
1	0.02	0.04	0.07
2	0.09	0.11	0.13
3	0.16	0.18	0.20

Table 2 Coverages & Posterior Distribution of θ

The expected losses (in millions) calculated with respect to the posterior distribution of θ, given $X = 1.2, \text{and } 3$ are the following:

$l_h(a_1) = E[l(a_1,\theta)] = -500 \times 0.02 - 300 \times 0.04 - 200 \times 0.07 = -36,$

$l_h(a_2) = E[l(a_2,\theta)] = -500 \times 0.09 - 300 \times 0.11 - 200 \times 0.13 = -104,$ and

$l_h(a_3) = E[l(a_3,\theta)] = -500 \times 0.16 - 300 \times 0.18 - 200 \times 0.20 = -174.$

Table 3 reports the percentage of claims by some known attack techniques in 2020. It is seen that the losses rise from \$52 billion in 2006 to \$392 billion in 2020, thus showing the severity of the situation that is to be greatly concerned of. This method of computing losses using Bayes' procedures has the great advantage for the calculation of $d[x]$ relevant to the outcome of the experimentation. Additionally, finding $B(d)$ for the determination of the entire function $d[x]$ is naturally more difficult.

Attack Technique	Percentage	Cyber Losses
E-mail/phishing	54%	\$216 billion
Remote access	29%	\$116 billion
Other social engineering	6%	\$24 billion
3rd part compromise	3%	\$12 billion
Brute force (authentication)	3%	\$12 billion
Other	3%	\$12 billion

Source: Help Net Security, September 14, 2020 [27]

Table 3 Percentages of Losses by Different Attack Techniques in 2020

In section 2, network risks will be the focus of discussion followed by network vulnerability in section 3. This theme is complemented by section 4 using software defects and deficiencies. Sections 5 and 6 will be devoted to types of coverage and premium calculations, respectively. Finally, the conclusions will be provided in section 7.

2. NETWORK RISKS

The possibility of experiencing harm, damage or loss from an undertaking is the risk. The extent of network risks depends on the value of asset, the severity of the vulnerability, and the likelihood of a network assault, expressed as Risk = Value × Severity × Likelihood [28]. Based upon the severity and the probabilities alone regardless of the underlying asset factor the color-coding in Figure 3 provides the key to the extent of general risk. The colors selected from darkest red to heavy green depict the descending order of threat levels. However, an asset factor can change the dynamic of this risk assessment and determination of severity altogether.

		Severity			
		Catastrophic (4)	Critical (3)	Marginal (2)	Negligible (2)
Probabilities	Frequent (5)				
	Probable (4)				
	Occasional (3)				
	Remote (2)				
	Improbable (1)				

Source: https://www.vectorsolutions.com/resources/blogs/risk-matrix-calculations-severity-probability-risk-assessment/

Figure 3: Risk Matrix – Severity vs. Probabilities

It is concluded that there will be lasting vulnerabilities in computer security that could expose computer networks and critical infrastructure of U.S. government by either computer attacks or cyber terrorism, or both [29]. Cyber terrorism can be steered from any location in the world with minimum effort, at a low cost, and the least amount of technology sophistication. After all, an internet connection is needed to wreak havoc and bring down the system for widespread damage to its network. Possible network risks can be in many forms. Electrical power failures, surge, outage, and fluctuations are the most frequent physical threats to network activities. Nonetheless, fire or water damage can be the most serious loss of software capabilities contributed from electrical power breakdowns or disturbances. Any interruption or disruption in network continuity of power is sufficient to cause operational stoppages, ranging from just a few sparks to high-voltage surges. The consequences are ranging from minor losses of input data to temporary shutdown of the network. Failure of network hardware components is a potential risk as well. Possible consequences are vast and varied due to these failures that include loss of data or integrity of data, loss of processing time, and interruption of services such as degradation of equipment or loss of software capabilities (http://www.windowsecurity.com). Either catastrophic or partial destruction of a facility can be caused by a network equipment fire. These include loss of the entire system for extended periods. Environmental failures can stem from air-conditioning, humidity, heating, leakage, breakages, and contamination [30]. LANs (Local Area Network) and WANs (Wide Area Network) are the two chief and well-known categories of area networks, while the others have emerged with technology advancements [31]. The possible tools of the cybercrime trade have been identified as password forgeries, software flows, hardware, spyware, wireless LANs, e-mails, and broadband connections [32]. Careful consideration must be granted to the repair and disposition of networking equipment. Commercial repair crew must be supervised by government technical staff as they work on sensitive PC and network equipment. They must be given regular training assignments in necessary skills and ethics involved with emerging technologies while stressing the fact that privacy must be protected at all costs.

The denial of service (DoS), damage to hardware and infrastructure, and discontinuity of service for any reason are considered asserts risks. Security requirements in mobile business applications are vital for obvious reasons. Operating business applications over public networks require additional consideration to prevent attackers from acquiring access to confidential data or otherwise attempt to manipulating data, causing substantial harm for fair dealing, transactions, and practices. The standard issues to be addressed involve identity verification and authentication, authorization consent, confidentiality, and preservation of integrity. State-of-the-art technology in securing business applications typically works for the benefit of enhancing businesses. It has two complementary technological necessities that protect corporate networks and transmitted data against attacks. Firewalls and virtual private networks are two technological products that have been entrusted in dealing with both issues. Firewalls can be characterized as a technology that provides a set of mechanisms to enforce a security policy on data to and from a corporate network center. Since firewalls do not necessarily support privacy and confidentiality, these networks must complement firewalls to protect data in transit [33]. Mobility suffers roaming between networks and operators, possibly changing the source address due to the static configuration of firewalls, potentially leading to discontinuity of service connectivity when networking in progress within the mobile platform. Firewalls are reasonable to secure a network for a defined set of clients, devices, and systems. However, if the set is about to reboot because some reorganization or re-configuration of the firewall, it must be done promptly. Heterogeneity of wireless networks does not allow for comprehensive and coherent support of security features without looking into the applications and necessities that support within the applications themselves [34]. E-commerce is, in reality, a powerful, complex blend ranging from vast commodity exchanges to auction sites considered for a cost-cutting measure to increase sales [35]. This remains particularly true if security is required from wall to wall. As a result, any commercial applications require back to secure trade exchanges such as nonrepudiation. However, fast verification of clients and servers is actualized as it were to a restricted degree and is basically based on freely accessible key frameworks. Additionally, authentication is only done against known identities,

which are easy to forge on untrustworthy computer hardware components available in the open market. DoS attacks can also cause security threats. A DoS attack provides a network, host, or infrastructure that is made obsolete for legitimate users. The DoS attacks fall into one of the three categories below.

1. Vulnerability attack: This is caused by sending a few well-crafted messages to the network applications, or operating system on the host network.
2. Bandwidth flooding: The network system is clogged by sending multiple packets to the host network.
3. Connection flooding: The attacker creates many half-opened or fully opened Transmission Control Protocol (TCP) connectors out of the targeted host.

The DoS attacks affect enterprises from all sectors (e-collaboration, financing, management, etc.), regardless of their magnitude and all localities. Additionally, the e-collaboration related to network security can be addressed using the theories of intrusion detection and distinctive groups of the framework assurance strategies in this regard [36].

3. NETWORK VULNERABILITY

Detecting and responding to network vulnerabilities that puts organizations at risk promptly is crucial to any organizational network structure. It employs preventive measures for real-world exploits and evaluates the suspicious activities of the systems. Vulnerability analyzes the results of vulnerability areas, assesses vulnerability alerts to make recommendations, and establishes a strategy for managing all possible vulnerability scenarios. Prior knowledge of vulnerability assessment and hacking techniques will allow detecting vulnerabilities before the networks are targeted. On the other hand, companies spend additional costs on false positives and false negatives. Let false positive cost and false negative cost of a defense system at time t, be $C_p(\kappa_t, \theta_t)$ and $C_n(\kappa_t, \theta_t)$, respectively, where κ_t be the attack severity at time t and θ_t be the set of structured parameters used to analyze the detection algorithm. The adaptive defense system will be a valuable tool to select the optimal configurations, θ_t by minimizing the combined cost, f given by $f = \min_{\theta_t}\{C_p(\kappa_t, \theta_t) + C_n(\kappa_t, \theta_t)\}$. It is found that an adaptive defense principle based on minimizing the cost will help reduce the combined cost in this arena [37]. In this effort, we learn to configure and use vulnerability techniques to detect weaknesses and prevent network exploitation and sabotage [38]. Gaining adequate knowledge to assess the risk to an enterprise from an array of vulnerabilities and to minimize its exposure to pricey threats will be paramount and necessary, at least. It is the nature of commodity and security trading that provides the prospect for profit, as there is also the risk of loss in trading activities. Commodity trading involves a certain degree of risk that may not be proper for all shareholders to assume. All forms of derivative transactions, including future ones, are complex and risk substantial loss. The past performance is not necessarily indicative of prospects for business dealings and does not necessarily guarantee profit. It is essential to recognize all the risks associated with trading, and consequently, trade needs to be undertaken with cautionary adequate risk capital. Between 1992 and 1995, the volume of thefts related to trade secrets experienced a threefold increase [39]. The plunge of software stock prices is seen, and thereby, fear for investment can cause financial damage to business enterprises. In the late 90's, a boom in corporate spending and information technology (IT) investment, especially for computers and software sectors, led to the present-day's unprecedented strong economy [40]. But with the reports of weak earnings, under-investment in software development, and high inventories enabled the stocks to fall off sharply in the later years.

It is, however, important to minimize downtime associated with the software capabilities of the network servers. Any downtime of the website will result in monetary loss and irreparable damages. The focus of similar efforts in software applications was robot guidance, which demands a high level of recognition capability, and is also a critical consideration to many other applications such as measurement, quality control and inspection. Commercial applications of the new vision software technology have been put to work in the lumber industry to reduce waste and to inspect steel processing furnaces to achieve high safety goals without increasing additional downtime. These basic organizational resources have come beneath expanding assault amid the final decade from previous workers, displeased specialists, competitors, fear-based oppressors, and other government entities [41]. It is recommended to use antivirus software to protect against unwanted filtration, continually probing IT systems for their flaws, and having a strategy to deal with the situations that could go wrong while consolidating responsibility for the company's computer technologies. However, there are other forms of malfunctions that put firms in jeopardy in these days of technological advancement.

4. SOFTWARE DEFECTS AND DEFICIENCIES

There has been a software crisis that began in 1965 until 1985 in terms of lack of skilled software personnel and much-needed investments in software development, thus causing an unexpected inherited major crisis in the field of software engineering (SE). As a result, countless software ventures far exceeded their budgets and schedules in the execution. Some entrepreneurs took advantage of the "software crisis" to justify their incapability to employ satisfactory skilled computer experts. The software emergencies were initially characterized in output but later progressed the emphasis on dominance in this manufacturing sector.

The IBM System/360 Operating System (OS/360) was a typical example of project where the budgeted cost overran the actual cost [42]. This project lasted from the 1960s to the 1970s and created one of the most complex software systems ever designed. The OS/360 was one of the first large software projects undertaken by a group of 1000 programmers. Very expensive mistakes can occur by not developing software simultaneously with planned project growth. Software defects, glitches, and deficiencies can result in property damage, and in some instances, it can even become deadly. Moreover, reduced software security protection allows hackers to steal identities that cost time, money, and can ruin their reputations. Organizations must arrange their compensation efforts based on the asset cataloguing and extent of weaknesses [43]. Severity of network vulnerabilities is recognized based on high, medium, and low levels. As an example, Table 4 identifies the top 10 most at risk host devices by their levels of severity in terms of high, medium, and low on a scale of 1 to 10 as per GFI LANguard Network Security Scanner default reports [44].

IP Address	Host Name	High	Medium	Low
80.164.37.238	TestComp5	10	6	8
80.164.37.214	TestComp1	7	2	8
80.164.37.236	Cluster_s2	7	1	10
80.164.37.66	FSERVER	7	0	7
80.164.37.114	TestHost	5	2	7
80.164.37.220	TESTSTATION	3	0	5
80.164.37.206	FinExec	2	2	8
80.164.37.64	MARKXP	2	1	9
80.164.37.6	Workstation_1	2	1	8
80.165.29.75	Workstation_2	2	1	6

Source: GFI Software Ltd., 2006 [44]

Table 4 Top Ten Vulnerable Hosts by Severity

Some embedded systems used in radiotherapy treatment failed catastrophically, administering lethal doses of radiation to patients and others in vicinity of the facility (Therac 25 incident failure) [45]. The software crisis has been gradually phasing out because it is unrealistic to remain in crisis mode forever. SEs accept obstacles in the field, confront difficulties, challenges, innovations, and competition. Eventually, as it is often said, hard work pays off to solve them gradually.

Network analysis provides much-needed theoretical and computational techniques for designing and operating the systems associated with networks. This active area of research is the beginning of many simple to sophisticated systems of e-collaboration efforts. The most widely used network techniques lead to project planning, implementation, and control. This also provides valuable tools for shaping the planning effort, testing different plants, revealing the overall dimensions and characteristics of the project, establishing efficient managerial responsibilities, setting goals, and identifying realistic prospects. It has significantly assisted project management on nearly all thriving economic ventures. These activities include the overall software development architecture for ensuring effective uses and development [46]. E-collaboration has had an increasingly great impact on the management of organizations in the recent years. The number and variety of its applications continue to grow rapidly and show a wide range of benefits, and no slowdown has been seen on the horizon yet [47]. In fact, except for the advent of the sophisticated high-speed supercomputers, the extent of this impact seems to have no boundaries compared to any other recent development. An analysis of information trade flows, measures the efficiency of transports, logistics, and IT-based products and practices emphasizing the importance of e-collaboration, electronic commerce, and electronic data exchange. IT penetrates all territorial boundaries today, bringing a single global community to a higher level of competitiveness. It also makes most global business processes smoother to realize cost-effective, and fair universal market. A fully integrated, highly equipped, multi-staged complex system equipped with properly facetted insurance coverage has the advantages for export or import of goods between destinations and a process that can be electronically managed totally. Attacker profiling is the concept of separating the nature of the infrastructure from the characteristics of malicious agents who have undertaken strategic decisions in the well-thought-out environment [48]. This process integrates a new analysis tool like ApproxTree+ that incorporates attacker profiling capabilities into the novice design [49].

It is important to address the issues pertaining to e-collaboration from the insurance perspective. Finding the issues in this regard in a timely fashion serve the private and the public clients a huge favor. Creating innovative products is the art of technological advancement of today's society for every benefactor. For every need, there is an attempt to find a technological solution. Putting this solution to work would be as important as it was invented. Finally, relevant studies to find the exact and perfect solutions must be done and maybe carried out to better serve the organization. In every facet of this development, e-collaboration pertains considerably to safeguard the provider's concerns, the facilitators, and the users in the same breath. Furthermore, openness to new ideas, new technologies, new methods for trading, and innovative ways of conducting business have been the solutions to the challenges faced by today's global trading community. Technology for specific tasks gives a unified procedure, devices, or machines, involving computers and their programing codes to produce the preferred outcomes. Maintaining and troubleshooting software prevents, identifies, or solves problems in technological apparatus. These are the basic conditions essential for trade technology to take place. The assumptions of these structures to work perfectly for the benefit of e-collaboration is somewhat a fantasy. E-collaboration effort equipped with proper insurance and risk management design is the prudent exercise in this arena to safeguard the point of view of public and private interests from threats, attacks, and losses.

5. TYPES OF COVERAGE

The types of cyber insurance coverage can vary. Liabilities, full coverage, long-term loss recovery, loss of properties and infrastructure failures including catastrophic coverage are some of the provisions made available on insurance. Network security liabilities provide protection against actual or alleged incidents of transmission of malicious code, unauthorized access, use or loss of service. This can be either first-party damage coverage or third-party liability coverage. There is no doubt that the need for cyber insurance is growing at present. With latest computer viruses spreading every day, the business society is waking up every day to protect themselves beyond just acquiring virus protections. Traditional policies do not protect electronic losses, and property-casualty policies are limited to physical properties. A widely available IT insurance fills in the wider disparities of traditional industrial liability insurance. This is receiving much-needed reputation all over the globe due to the unprecedented advancement of technology.

The threat likelihood is the probability that a potential threat event might occur. The threat likelihood should be assessed based on the prevailing data. Table 5 categorizes the information from "high" to "low" in terms of the extent of coverage when a vulnerability exists. Furthermore, to effectively control the threat assessment based on information and security resources, the types of information falling into each cell should generally receive the largest portion of their security budget. The figures in the cell are the probability of vulnerabilities for nine possible scenarios. For example, the probability of loss when the vulnerability is high, and the coverage is high amounts to be 0.02.

	Vulnerability			
Coverage		High	Medium	Low
	High	0.02	0.04	0.07
	Medium	0.09	0.11	0.13
	Low	0.16	0.18	0.20

Table 5 Coverage vs. Vulnerability Matrix

Everyone recognizes that there is the risk of conducting commerce utilizing the Internet, so merely recognition of this fact by clients is getting to be more extensive. Insurance premiums for cyber insurance are likely to surpass $2 billion in the next four to five years (http://www.iii.org). In the U.S. along, there is at least a larger disparity in the cost of premiums. It costs somewhere between $12,000 to $20,000 for every million dollars for first-party and third-party converges. As for liabilities, they are estimated to be in-between $7,000 to $10,000 [50]. This type of insurance is appropriate for everyone who embarks on business either using a computer or managing commerce on the Internet. It is the key for anyone with a receptacle of private information, such as credit card transactions that could be hacked into and lead to widespread thefts. Research has shown many companies, both large and small scaled, undervalue the risks of electronic commerce. A 2002 survey [51] of 501 IT and risk managers found that only 55% had reviewed their prevailing insurance for electronic risk coverage. Most likely, a company's common risk protections will not be satisfactory to avert misfortunes coming about from IT exposure. There have been doubts as to which cyber risks can be covered under traditional trade and commercial liability policies. However, it is now clear to ensure the precise inclusion and exclusion of various products [52]. They do not cover risks associated with data and other associated forms of network security risks. Sensibly designed cyber risk coverage is to protect a variety of IT scenarios, some of which include insuring computer equipment, identity theft insurances (protect against hacking or unintentional circulation of exclusive data), and commercial disruption insurance

covers the loss of income because of an attack or blackout [53]. Internet liability protections covers a wide assortment of circumstances, counting the spread of a computer infection or similar liabilities from an assault. This causes misfortunes to a third party, failure of security is causing organizations to be inaccessible to third parties and allegations of either copyright (or trademark) violation, libel, and denigration in a business website [51]. Finally, there can be scenarios that lead to unintentional consequences solely on security failure.

A network facilitator can purchase an insurance policy that pays $I(x)$ of the loss x. In order to safeguard against possibly providing an incentive a loss to incur, all feasible insurance policies maintain $0 \leq I(x) \leq x$. One group of feasible insurance policies is designed in such a way that claims will not be paid unless the loss exceeds a deductible amount d as defined by

$I_d(x) = \begin{bmatrix} 0, & x < d \\ x - d, & x \geq d \end{bmatrix}$. This type of insurance policy is called stop-loss or excess-of-loss insurance, which solely depends on products or applications [54]. Cyber insurance coverages generally require higher premiums and deductibles due to challenges such as lack of quantifiable data available on the risk associated with cybercrimes. Depending on the size of the business and the extent of coverage required, premiums can run into hundreds of thousands of dollars. If the assessment of an insurer does not find sufficient levels of protection, computer network security, and the continuous hardening of software, the coverage can be denied unless they meet the recommended security specifications by the insurers [55]. If an organization seeks additional protection against losses due to excess claims by an individual or an organization, it is called reinsurance. Reinsurance products are purchased to cover the difference between the amounts in the policies and the anticipated extended risk.

6. PREMIUM CALCULATIONS

For the corresponding analysis involving insurance coverage and adequate protection, there are four premium determination techniques which can be identified in terms of models that integrate the shared costs to be allocated. The four methods, namely, inherent premiums, fund purposes, rate of return objectives, and risk-based objectives are widely analyzed to address the present losses and predict future losses. E-risk is, on the other hand, defined as the option of risk from an electronic event. They consist of all potential compromises such as mishandling of network security apparatuses, the compromise of the business webserver, and inaccurate or indecent material posted on the website, service provider's or Internet service provider's malfunctions [56]. A premium calculation model for an insurance underwriter using the Collective Risk Model [54] assesses the expected loss in terms of stochastic variables unique to the model [57]. The premium can be estimated by analyzing the insurance products that suit the demands of today's computer entrepreneurs under modest assumptions [58]. A framework of premium calculation for cyber insurance industries by modeling potential electronic intrusion with the findings and impacts of steady-state simulation is considered in a similar study. An actuarial framework in the models is the operational financial losses with the theorized power outages that is based on the assessment of cyber-reliability. An expected mean time to restore power (MTTRP) is a measure that is frequently used to evaluate the severity of cyber risks [59]. The system that is subjected to attacks over time provides an analysis of a particular type of stochastic process with a sequence of states $\{X_i\}$ [60]. A network system suffers monetarily after software defects and deficiencies can be determined based on high, medium, and low levels. The cost incurred in making this system operable contains several objects, such as a loss due to the inability to facilitate clients, maintenance, and repair costs. If the system is to be replaced, it incurs replacement costs together with the cost of lost service. Let us assume that the expected costs, as appeared in Table 6 provide the expected cost for various states, given the conditions they are currently in due to prevalent system failures.

State	Condition	Expected Cost due to System Failures
0	Same as before	0
1	Low severity	$1,000
2	Medium severity	$10,000
3	High severity	$100,000

Table 6 Expected Cost vs. States

Let X_i denote the severity of failure at the end of i^{th} attack. It is assumed that the stochastic process is a finite-state Markov chain with a transition matrix as in Table 7.

State	-	1.00	2.00	3.00
0	-	0.13	0.15	0.72
1	-	0.18	0.20	0.62
2	-	-	0.88	0.12
3	1.00	-	-	-

Table 7 Probability Transition Matrix

The $n-$step transition probabilities $p_{i\,j}^{(n)}$ are the probabilities that a process in state i will be in state j after n extra moves. This is, basically, $p_{i\,j}^{(n)} = P\{X_{n+m} = j | X_m = i\}, n \geq 0, i, j \geq 0$. By noting that the 4-step transition probabilities are symbolically denoted by, $p_{i\,j}^{(4)} \geq 0$ for all i, j, it is evident that every level is positive recurrent and belongs to one level only. For an irreducible ergodic Markov chain [60] is the process with $\lim_{n\to\infty} p_{i\,j}^{(n)}$ exists, that is independent of i, and $\lim_{n\to\infty} p_{i\,j}^{(n)} = \pi_j$ with $\sum_{\forall j} \pi_j = 1$, and $j \geq 0$. The steady-state equations can be written as

$$\begin{aligned}
\pi_0 &= \pi_3 \\
\pi_1 &= 0.13\pi_0 + 0.18\pi_1 \\
\pi_2 &= 0.15\pi_0 + 0.20\pi_1 + 0.88\pi_2 \\
\pi_3 &= 0.72\pi_0 + 0.62\pi_1 + 0.12\pi_2 \\
1 &= \pi_0 + \pi_1 + \pi_2 + \pi_3
\end{aligned}$$

The solution of this system of equations is $\pi_0 = 0.27, \pi_1 = 0.04, \pi_2 = 0.42,$ and $\pi_3 = 0.27$. Thus, the expected average cost that represents this maintenance task is $0 \times \pi_0 + 1{,}000 \times \pi_1 + 10{,}000 \times \pi_2 + 100{,}000 \times \pi_3 = \$31{,}240{,}000$. This expected average cost can be incorporated into any method of premium calculation in the choice of cyber insurance product under consideration.

An insurance scheme is an instrument that diminishes the unfavorable monetary effect of arbitrary circumstances that avoid the fulfillment of sensible commitments. Additionally, this definition can be purposefully broad. An insurance scheme can be in place following the identification of various situations where random losses to occur. This model does not incorporate several aspects of insurance practices and economic realities. In large part, building a comprehensive model for insurance systems is constructed using the equivalence principle. To formalize this principle, we define the insurer's loss, L, as the random amount of the present value of claims to be reimbursed by the difference between the insurer and the premiums to be paid by the insured. The equivalence principle requires that $E[L] = 0$, where E is the expected value taken with respect to the posterior distribution. Equivalently, the premium will be calculated based on the assumption that $E[\text{Present value of claims}] = E[\text{Present value of the claim premiums}]$. The equivalence principle is used as a mean for determining insurance premiums. The calculation of premium and establishing the growth of coverage entails evaluating the likely losses and how much risk an organization is wanting to assume. The limitations and features of individual coverage can vary from one product to coverage on these grounds. It is proper to consult with an insurance agent and seek to determine the extent of exposures from a specific risk together with, the worst-case scenario and the likely scenario [61]. The major roles of an insurance business include developing new types of insurance coverage, selling policies, underwriting about risk evaluation, policy insurance, maintaining accurate records, and paying insurance claims in a timely manner [62]. The approaches to reduce electronic commerce insurance premium is to include agreeing to higher deductibles or only procuring catastrophic coverage. The major corporations in the cyber insurance arena offer numerous internet liability products. These insurance enterprises often package various forms of cyber insurance products together to offer more wide-ranging coverages, realizing what customers naturally demand. Although their products are interrelated, the corporations all have their specialty zones. In addition to acquiring cyber insurance products, there are some measures firms can take on their own to avert losses in the first place [63]. Since fires and arsons cause overwhelming harm, satisfactory likelihood must be doled out to the higher claims in premium calculation. In actuarial science literature, some standard distributions have been considered in dealing with this issue depending on obvious scenarios to unpredictable ones (for examples, lognormal, Pareto, a mixture of exponential distributions) for a wider array of research on the topics to be continued [54].

7. CONCLUSIONS

Commercial entities invest a huge sum of money, time, and effort in developing partners, investors, and most importantly, consumers who trust the actual marketplace. Securing this data brings that the same level of confidence online to ensure global economies to flourish. Any organization wishing to secure electronic data faces a stark, and an obvious choice. Without a secure network protection, they face increasing risk and intranet technologies and expenses, and incomplete security implementations. With secure network capabilities, organizations forcefully move online with assurance, boosting current market partnerships by driving aggressively into future markets, enterprises, and making use of other trading opportunities. It is vital that these risks be taken seriously to handle the circumstances at all levels of the decision-making process. Security preparedness should be in place to safeguard the interests of the organization, customers, and both. Assessing computer exposures has become more than a study of theories; it is rather a way to think about the extent of unintended consequences and prepare the public for the ultimate benefits of a secured network. In the meantime, safeguarding the world marketplace ensures that future global economies will last for many

years to come. Loss sustained due to revealing business secrets may have disadvantages over-investing in future innovation markets usually done through aggressive R&D expenditures [64].

The loss of data cannot be compromised on the face of the premium and the cost to protect them. Ransomware brings organizations and enterprises to a rapid halt. Businesses need to realize that there must be a trade-off between reducing the risk arising from cybercrimes, network intrusions, security breaches, and the cost of insurance premiums. It is expensive, and sometimes businesses will not obtain coverage for network providers with poor records of IT security measures. As a result, these organizations are reluctant to sign up for new cyber insurance knowing the dire consequences they would confront. The extent of transnational computer crime is not easy to gauge as we determine which portion of the activity constitutes a crime. Some innocent uses are possibly harbingering both criminal use of telerobotics and the criminal justice system's uses that are subject to change with the evolving technology [65]. The former is the area of robotics that is concerned with the control of robots from a distance. Accordingly, the discussion provides a groundwork for techniques, computations, and particularly, for future expansion of the topics as far as cybersecurity is concerned. It is intended to safeguard the sensitive data, losses, and to take appropriate measures to prevent computer network security vulnerabilities.

REFERENCES

[1] CCIPS (2021). The Computer Crime and Intellectual Property Section (CCIPS) http://www.cybercrime.gov, Computer Crime & Intellectual Property, United States Department of Justice (2021). Retrieved from: https://www.justice.gov/criminal-ccips/ccips-documents-and-reports (September 29, 2017)
[2] Reichel, Philip L. (2008). Comparative Criminal Justice Systems: A Topical Approach, Fifth Edition, Pearson Education, Inc. Upper Saddle River, NJ 07458
[3] ASIS (1999). Trends in Proprietary Information Loss, Survey, American Society for Industrial Security (ASIS), PriceWaterhouseCoopers
[4] Internet Crime Report (2019). FBI's Internet Crime Complaint Center (IC3), FBI National Press Office, Washington, D.C. February 11, 2020, https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf
[5] Pavlik, Lukas (2018). Possibilities of modelling the impact of cyber threats in cyber risk insurance MATEC Web Conf. 210 04032 (2018), DOI: 10.1051/matecconf/201821004032
[6] Pal, R., Golubchik, L., Psounis, K., and Hui, P., (2014). Will cyber-insurance improve network security? A market analysis, IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, 2014, pp. 235-243, doi: 10.1109/INFOCOM.2014.6847944.
[7] CSI/FBI Publication (2006). Eleven Annual CSI/FBI Computer Crime and Security Survey, Computer Security Institute
[8] Caballero, Albert (2013). Information Security Essentials for IT Managers, Computer and Information Security Handbook, 2013.
[9] Meland, P. H., Tondel, I. A. and Solhaug, B. (2015). Mitigating Risk with Cyberinsurance, in IEEE Security & Privacy, vol. 13, no. 6, pp. 38-43, Nov.-Dec. 2015, doi: 10.1109/MSP.2015.137.
[10] H., Matthew (2020). Inaugural quarterly Infoblox Cyberthreat Intelligence Report: essential reading for enterprise security professionals, December 13, 2020
[11] Reeder, Joe R. and Hall, Cadet Tommy (2021). Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack, The Cyber Defense Review, 15, Summer 2021
[12] Kalinich, Kevin (2005). Network Risk Insurance: A Layman's Overview, WHITE PAPER FOR: Montreal 2005 CRIMS, Perspective – Network Risk & Intellectual Property, Aon FSG Technology and Professional Risks, pp. 1-6
[13] III (2021). Insurance Information Institute, Inc., https://www.iii.org/article/commercial-general-liability-insurance
[14] Le, A., Chen, Y., Chai, K. K., Vasenev, A., & Montoya, L. (2019). Incorporating FAIR into Bayesian Network for Numerical Assessment of Loss Event Frequencies of Smart Grid Cyber Threats. Mobile networks & applications, 24(5), pp. 1713–1721. https://doi.org/10.1007/s11036-018-1047-6
[15] Kanes, R., Marengo, M. C. R., Abdel-Moati, H., Cranefield, J., and Véchot, L. (2017). Developing a framework for dynamic risk assessment using Bayesian networks and reliability data, Journal of Loss Prevention in the Process Industries, Volume 50, Part A, 2017, pp. 142-153, ISSN 0950-4230, https://doi.org/10.1016/j.jlp.2017.09.011. (https://www.sciencedirect.com/science/article/pii/S0950423017303571)
[16] The Open Group (2018). The Open FAIR™ tool with Sipmath™ Distributions guide to the theory of operation, https://publications.opengroup.org/g181. 2019.
[17] Wang, Jiali, Neil, Martin, and Fenton, Norman (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model, Computers & Security, Volume 89, 2020, 101659, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.101659.
[18] Joshi, Chanchala and Singh, Umesh Kumar (2017). Information security risks management framework – A step towards mitigating security risks in university network, Journal of Information Security and Applications, Volume 35, 2017, pp. 128-137, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2017.06.006
[19] Anderson, Beth (2018). FAIR vulnerability determined using attack graphs. Athens: The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). Retrieved from https://tamiu.idm.oclc.org/login?url=https://www.proquest.com/conference-papers-proceedings/fair-vulnerability-determined-using-attack-graphs/docview/2153616296/se-2?accountid=7081
[20] Chiappa, S., Isaac, W.S. (2019). A Causal Bayesian Networks Viewpoint on Fairness. In: Kosta E., Pierson J., Slamanig D., Fischer-Hübner S., Krenn S. (eds.) Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data. Privacy and Identity 2018. IFIP Advances in Information and Communication Technology, Vol 547. Springer, Cham. https://doi.org/10.1007/978-3-030-16744-8_1
[21] Amin, M. Tanjin, Khan, Faisal, Ahmed, Salim, and Imtiaz, Syed (2019). A novel data-driven methodology for fault detection and dynamic risk assessment. Can J. Chem Eng. 2020; 98: pp. 2397–2416. https://doi.org/10.1002/cjce.23760
[22] Tesfamariam, Solomon; Woldesellasse, Haile; Xu, Min; and Asselin, Edouard (2021). General corrosion vulnerability assessment using a Bayesian belief network model incorporating experimental corrosion data for X60 pipe steel, Journal of Pipeline Science and Engineering, In Press, Corrected Proof, Available online 4 September 2021
[23] Sudarwanto, S., L. Ambarwati, and I. Hadi (2019). Development of rental property insurance models with Generalized Linear Models (GLM), Journal of Physics: Conference Series 1402 (December 2019): 077104. http://dx.doi.org/10.1088/1742-6596/1402/7/077104.
[24] Bishop, Christopher M. (2006). Pattern Recognition and Machine Learning, Springer Science + Business Media, LLC
[25] Hillier, Frederick S. and Lieberman, Gerald J. (1996). Operations Research, Second Edition, Holden-Day, Inc., San Francisco, CA, 1967
[26] Kenett, Ron S.; Zacks, Shelemyahu; and Amberti, Daniele (2013). Modern Industrial Statistics, John Wiley & Sons, Ltd.
[27] Help Net Security (2020). Cyber losses are increasing in frequency and severity, (IN)SECURE Magazine, September 14, 2020

[28] Shameli-Sendi, Alireza (2020). An efficient security data-driven approach for implementing risk assessment, Journal of Information Security and Applications, 54: 102593, 2020.
[29] Wilson, Clay (2003). Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress (CRS Report for Congress RL32114), October 17, 2003
[30] Henry, Paul, Samuel Chun, Robby Fussell, William Yarberry, Bonnie Goins, Christopher Pilewski, Chris Hare, Franjo Majster, and James Tiller (2006). ISPs and Denial-of-Service Attacks, Information Security Management Handbook on CD-ROM 2006 Edition, 2006.
[31] TechGenix Ltd (2021). Guide for Protecting Local Area Networks and Wide Area Networks (LANs/WANs): A little old but with some theoretical things, October 16, 2002, http://www.windowsecurity.com
[32] Juhnke, Deborah H. (2002-2004). Cyber Terrorism or Cyber Crime? 2002-2004 Computer Forensics Inc. Retrieved from: http://www.forensics.com
[33] Walter, Thomas; Schoo, Peter; Haller, Jochen; and Robinson, Philip (2001). WiTness – Wireless Trust for Mobile Business Position Statement, IST-Programme/KA2/AL: IST-2001-2.1.3. The project WITNESS is supported by the European Community
[34] European Commission (2004). Towards a middleware for collaborative working environments, Information Society Directorate-General Emerging Technologies and Infrastructures, EU 7th Framework Programme, May 4, 2004, Brussels
[35] ISS (2021). Internet Security Systems (ISS): Secure E-business - New Markets at the Speed of Information; Online Opportunities at the Speed of Thought http://www.tarrani.net/Security/securityebus.pdf
[36] Czirkos, Z., Hosszú, G., and Kovács, F. (2008). E-Collaboration Enhanced Host Security. In N. Kock (Ed.), Encyclopedia of E-Collaboration, pp. 172-177. IGI Global. http://doi:10.4018/978-1-59904-000-4.ch027
[37] Zou, Cliff C.; Duffield, Nick; Towsley, Don; and Gong, Weibo (2006). Adaptive Defense Against Various Network Attacks, IEEE Journal on Selected Areas in Communications: High-Speed Network Security (J-SAC), 24(10), pp. 1877-1888, October 2006
[38] Kotenko I. and Ulanov A. (2007). Multi-agent Framework for Simulation of Adaptive Cooperative Defense Against Internet Attacks. In: Gorodetsky V., Zhang C., Skormin V.A., Cao L. (eds) Autonomous Intelligent Systems: Multi-Agents and Data Mining. AIS-ADM 2007. Lecture Notes in Computer Science, vol 4476. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-72839-9_18
[39] Heffernan, Richard J. and Smartwood, Dan T. (1996). ASIS: Report Trends in Intellectual Property Loss Survey Report, 4, March 1996
[40] Doms, M. (2004). The boom and bust in information technology investment, Federal Reserve Bank of San Francisco Economic Review, pp. 19–34.
[41] Fitzpatrick, W.M. and Burke, D.R. (2001). Virtual Venturing and Entry Barriers: Redefining the Strategic Landscape, S.A.M. Advanced Management Journal, Autumn 2001
[42] Yuan, Chao, Du, Jinze, Yue, Min, and Ma, Tao (2020). The Design of Large-Scale IP Address and Port Scanning Tool, Sensors, 10.3390/s20164423, 20, 16, (4423), (2020).
[43] Eschelbeck, Gerhard (2005). The Laws of Vulnerabilities: Which security vulnerabilities really matter? Information Security Technical Report, Vol. 10, Issue 4, 2005, pp. 213-219, ISSN 1363-4127, https://doi.org/10.1016/j.istr.2005.09.005.
[44] Security & Managing Software (2006). Network Vulnerability Summery-Executive Report, GFI Software Ltd.
[45] Leveson, Nancy G. and Turner, Clark S. (1993). An investigation of the Therac-25 accidents, IEEE Computer, Vol. 26, No. 7, pp. 18-41
[46] Auerbach, M., Imtiaz, A., and Mittwoch, J.B.H. (2006). Collaboration within Tool and Die Making Industry Through Open-Source ERP-Solution with Integrated CRM-Functionalities, ICE 2006 12th International Conference on Concurrent Enterprising (Innovative Products and Services through Collaborative Networks), Palazzo delle Stelline, Milan, Italy, June 26-28, 2006
[47] Goksoy, Aslı; Vayvay, Ozalp; Yılmaz, Beliz Ozsoy; and Yılmaz, Ahmet (2014). Chapter 34 - Electronic Collaboration in Strategic Decision-Making Processes, IGI Global, 2014
[48] Lenin, A., Willemson J., and Sari, D.P. (2014). Attacker Profiling in Quantitative Security Assessment Based on Attack Trees. In: Bernsmed K., Fischer-Hübner S. (eds.) Secure IT Systems. NordSec 2014. Lecture Notes in Computer Science, Vol. 8788. Springer, Cham. https://doi.org/10.1007/978-3-319-11599-3_12
[49] Dantu, Ram, Kolan, Prakash, and Cangussu, Joaõ (2009). Network risk management using attacker profiling, Security and Communication Networks, Security Comm. Networks. 2009; 2:83–96. Published online 24 September 2008 in Wiley InterScience (www.interscience.wiley.com) DOI: 10.1002/sec.58
[50] Sterlicchi, John (2005). Why CIOs Won't Sign Up for New Cyber-Crime Insurance, Sterlicchi in America, pp. 14, Winter 2005
[51] Brown, Rachel (2005). IT Insurance Becoming a Popular Option, Kansas City Daily Record, March 03, 2005. Retrieved from: http://www.wfl-stl.com/news/03_30_05.htm
[52] Hunt, T.D. (2019). The internet of buildings: Insurance of cyber risks for commercial real estate. Oklahoma Law Review 71 (2): pp. 397–452.
[53] DiGrazia, K. (2018). Cyber insurance, data security, and blockchain in the wake of the Equifax breach, Journal of Business & Technology Law 13 (2): pp. 255–277.
[54] Bowers Jr., Newton L. et al. (1997). Actuarial Mathematics, Second Edition, The Society of Actuaries, Schaumburg, IL
[55] Kolodzinski, Oscar (2002). Cyber-insurance issues: Managing risk by tying network security to business goals: Certified public accountant. The CPA Journal, 72(11), pp. 10-11. Retrieved from https://tamiu.idm.oclc.org/login?url=https://www.proquest.com/scholarly-journals/cyber-insurance-issues-managing-risk-tying/docview/212276106/se-2?accountid=7081
[56] Mukhopadhyay, A.; Chatterjee, S.; Saha, D.; Mahanti, A.; and Sadhukhan, S.K. (2006). e-Risk Management with Insurance: A Framework Using Copula Aided Bayesian Belief Networks, Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), 2006
[57] Dubendorfer, Thomas et al. (2004). An Economic Damage Model for Large-Scale Internet Attack, 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE '04), pp. 223-228
[58] Goonatilake, Rohitha (2004). Development, Evaluation and Analysis of a 20-Year Deferred Annuity Product, Econ Papers: Economics at your fingertips, https://econwpa.ub.uni-muenchen.de/econ-wp/ri/papers/0409/0409003.pdf
[59] Yang, Z. et al. (2020). Premium Calculation for Insurance Businesses Based on Cyber Risks in IP-Based Power Substations, in IEEE Access, vol. 8, pp. 78890-78900, 2020, doi: 10.1109/ACCESS.2020.2988548.
[60] Ross, Sheldon M. (1981). Introduction to Probability Models, Second Edition, Academic Press, Inc., New York, NY
[61] Thomas, R. (2007). Some Novel Perspectives on Risk Classification. Geneva Pap Risk Insur Issues Pract 32, 105–132 (2007). https://doi.org/10.1057/palgrave.gpp.2510118
[62] Condon, Robert J. (1975). Data Processing Systems Analysis & Design, Reston Publishing Company, Inc., Reston, VA 22090
[63] Das, Kumer Pial; and Mahavier, William Ted (2012). Further Results for the Joint Distribution of the Surplus Immediately Before and After Ruin Under Force of Interest, Journal of Statistical Theory and Practice, 6 (2), pp. 344-353, published by Taylor and Francis
[64] Schweitzer, V.G. (1993). Cisplatin-Induced Ototoxicity: The effect of Pigmentation and inhibitory Agents, Laryngoscope 103 (Supplement), 59
[65] Reichel, Philip L. and Albanese, Jay S. (2014). Handbook of Transnational Crime and Justice, Saga Publications, Inc., Los Angeles, CA; London: SAGE, 2013, ©2014

Authors

Dr. Rohitha Goonatilake, professor of mathematics, received his Ph.D. in Applied Mathematics from Kent State University, Kent, OH in Fall 1997 and received his master's in the areas of applied mathematics, mathematics, and actuarial sciences, and a bachelor's in mathematics/science. He joined TAMIU in the Summer of 1999 and has completed 23+ years of service for TAMIU. He and his team were awarded multiple funded grants by both the National Science Foundation (NSF) and the U.S. Department of Education to promote mathematics education in areas of need in Laredo by providing scholarships to juniors and seniors at TAMIU to prepare them to become talented, skillful, and highly qualified teachers to teach immediately after graduation. Dr. Goonatilake was a recipient of the Scholar of the Year Award in 2006 and the University Honors Faculty of the Year in 2013. He was a PI for more than six program-funded grants and Co-PI for more than 12 different program grants since joining TAMIU. He has a very active research agenda that involves network anomaly detection, probability, disease prevalence, and microeconomics. He was extensively involved with many STEM activities throughout the years for local high school and middle school students, outreach efforts with local high schools, and other community involvements for many years through enrichment workshops and summer opportunities for the local community.

Dr. Susantha Herath is a professor at St. Cloud State University, St. Cloud, MN. He holds a Ph.D. in computer engineering. His current research interests are in risk management, cyber security, and information assurance. He has 25+ years of college-level teaching experience at graduate and undergraduate levels and 30+ years of research experience. He has published over 100 peer-reviewed articles. He has submitted over 45 competitive grant proposals and received over $ 4 million in funding. Susantha is a senior member of the IEEE.