Information Systems Frontiers (2023) 25:1757–1778
https://doi.org/10.1007/s10796-021-10232-7

# Cyber-risk Management Framework for Online Gaming Firms: an Artificial Neural Network Approach

**Kalpit Sharma**[1] · **Arunabha Mukhopadhyay**[1]

Accepted: 6 December 2021 / Published online: 9 January 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

**Abstract**
Hackers have used Distributed-Denial-of-Service attacks to overwhelm a firm's cyber-resources resulting in disrupted access to legitimate end-users. Globally, DDoS attacks cost firms between US$ 120 K to US$ 2 M for each incident. Apart from the monetary loss, they also disrupt service quality and damage the brand reputation of firms. In 2018-2019, Massively Multiplayer Online Gaming (MMOG) firms witnessed 74% of the total DDoS attacks. MMOG firms form a lucrative segment for hackers because of their large customer base and the massive incentive to cause disruptions and losses. Our Feedforward Neural Network-based Cyber-risk Assessment and Mitigation (FNN-CRAM) model consists of three modules: assessment, quantification, and mitigation. The cyber-risk assessment module uses FNN, which takes seven inputs comprising DDoS attack intensity and duration for five DDoS attack types, vulnerability data (i.e., their counts and score), and the vulnerability trends over time. This layer is connected to a ten-neuron hidden layer and one neuron output layer that estimates the probability of these attacks. We also observe that the probability of these DDoS attacks follows a Weibull distribution. Next, our cyber-risk quantification module computes the expected loss. We note that expected losses due to these DDoS attacks follow a gamma distribution. Our cyber-risk mitigation module uses a heat matrix to help the CTO (i) prioritize the cyber-risk associated with a DDoS attack and (ii) decide whether to reduce, accept, or pass the cyber-risk using technological and cyber-insurance interventions.

**Keywords** DDoS · MMOG · Cyber-risk · Neural network · Cyber-insurance

## 1 Introduction

Online games have emerged as popular entertainment options, bringing massive revenues for the makers and numerous challenges for developers and end-users alike. A large number of players in online games is one of its essential USPs (Gough, 2019). Immensely successful games must continually provide scalability and responsiveness to the end-users (Yahyavi & Kemme, 2013). Online games with many simultaneous users are known as Massively Multiplayer Online Games (MMOGs), such as World of Warcraft, Final Fantasy, Elder Scrolls, Star Wars Online, and Guild Wars. MMOGs produce massive network traffic and overhead processing loads (Liu et al., 2013). The main challenges in the online game industry are that of (a) scalability, that is, providing gameplay to millions of users simultaneously, (b) consistency, (c) security and, (d) fast response time or all of these collectively. In the absence of any of these, customer satisfaction suffers (Yahyavi & Kemme, 2013). The features that make MMOGs popular are the same, which attackers exploit. Many end-users engaging in networked ecosystems to play, conduct financial transactions, and virtual currency exchange transforms it into an opportunity to cause disruptions. In many of these DDoS attacks, when the gaming firm is engrossed in mitigating these disruptions, these attackers can siphon off credentials or harm firms' cyber-resources elsewhere.

In 2014, Lizard Squad, a hacker group, took down Sony's PlayStation Network and Microsoft's Xbox Live during Christmas week (Smith, 2014). The group; claimed to be launching the attack "for laughs" but continued causing damage to educate the two giants about strengthening

✉ Kalpit Sharma
fpm18012@iiml.ac.in

Arunabha Mukhopadhyay
arunabha@iiml.ac.in

[1] Department of Information Technology & Systems, Indian Insititute of Management Lucknow, Prabandh Nagar, IIM Road, Lucknow 226013, UP, India

their cyber-security. They chose Christmas as they wanted to harm many users owing to peak transaction volume. In 2019, 51% of the network DDoS attacks lasted less than 15 min, but many attacks persistently attacked the same target (Avital et al., 2020).

Distributed Denial of Service (DDoS) attacks in which the hacker aims to make a firm or network resource unavailable to legitimate users either temporarily or indefinitely, thereby disrupting online services (Tanenbaum & Wetherall, 2010). One of its simpler variants, the Denial of Sevice (DoS) attack, inundates the firms' systems by attacking their operating systems or network-based services. Cyber-attackers execute these attacks in two forms. The first form exploits a software vulnerability and uses it to inundate the system with illegitimate data packets to crash, freeze, or restart an operating system due to buffer overflow (Peng et al., 2007). The second form is more potent than the former because it harms the network services and disrupts larger regions of the Internet. It utilizes useless illegitimate traffic to occupy network resources; thus, any user connected to the compromised network can become an easy target for attackers. While it is easy to mitigate the first form of attack by regular patching software vulnerabilities, the second form is challenging to prevent (Peng et al., 2007).

The distributed nature of these attacks increases the attack surface and makes them difficult to trace (Avital et al., 2020). Hackers install malicious botnets on unsuspecting end-user's systems and convert them into a "zombie" machine (Peng et al., 2007). In the background, the "zombies" launch illegitimate traffic to a target machine, mixed with its usual data traffic. Mirai botnet is one such popular method amongst hackers in recent times (Peng et al., 2007). This method of launching DDoS attacks makes it easy to execute. Thus, the recent emergence of DDoS-for-hire markets establishes their lucrativeness as a minimal cost-high impact option for attackers (Yue et al., 2019).

Vulnerabilities in software running on local and remote machines is the chief cause of the increasing probability of such attacks (Tanenbaum & Wetherall, 2010). Vulnerabilities are mistakes in computer code that expose the software and the system to attackers, thereby changing, tampering, and destroying sensitive information (Dowd et al., 2006). Almost half of the security vulnerabilities present themselves at the programming level (Peng et al., 2007). Many remote servers still rely on obsolete protocols (such as CharGEN, etc.) to function. Attackers utilize this fact to attack the system through these outdated yet widespread protocols to inundate the server with illegitimate traffic, resulting in a cascading effect on the connected network (McKeay, 2017).

,The impact of DDoS attacks might range from temporary website outages to substantial financial losses to firms dependent on real-time high-level service quality (e.g., E-Commerce, Entertainment, BFSI) (McKeay, 2017). DDoS attack mitigation is not spontaneous, and delays result in further losses. On average, the DDoS attack lifecycle ranges from attack to recovery from a few hours to several months. In 2018, the losses due to DDoS attacks ranged from US$ 120 K to US$ 2 M (Bezsonoff, 2017). The online gaming industry witnesses 74% of the total attacks recorded by their security provider service (Bezsonoff, 2017; McKeay, 2017). The BFSI, entertainment, and e-commerce firms are the next big targets for hackers as the losses are enormous for these industries. In 2019, a two-week-long DDoS attack targeted an unnamed streaming application enterprise that peaked at 292,000 requests per second, originating from 402,000 different Internet Protocol (IP) addresses. The enterprise lost about US$200 million, with a peak loss of US$500,000 per hour (Shani, 2019). In 2016, many large digital organizations, including Netflix, Spotify, Twitter, BBC, CNN, the New York Times, and other entertainment services such as HBO Now and Elder Scrolls, were offline because of the infamous Dyn server attack (Brown, 2016). Enterprises lose approximately US$50,000 per hour when under a DDoS attack (Bezsonoff, 2017). Figure 1 depicts yearly losses due to DDoS attacks as recorded by the Internet Crime Complaint Centre.

In this study, the five kinds of DDoS attacks that we analyze for cyber-risk exploit different IT assets and deny access to various components of the IT ecosystem. DDoS attacks chiefly disrupt the "availability" aspect of the CIA triad, but hackers may also tamper information, steal credentials amidst the confusion of the DDoS attacks. Hackers use the Character Generation protocol (CharGEN attack) to flood the local machine through peripheral devices (e.g., printers). Similarly, they compromise Universal Plug and Play (UPnP) ports to launch a Simple Service Delivery Protocol Flood (SSDP Flood) DDoS attack. Hackers use Domain Name Server (DNS) Flood and User Datagram Protocol (UDP) Flood, thus, tampering with remote DNS cache servers to deny access to users by disrupting the domain name translation process. Network Time Protocol (NTP)Flood pumps vast traffic through network time servers and, thus, congest and renders it inaccessible to legitimate users for time synchronization. Table 1 summarizes DDoS attacks in this study across various features.

This study explores three main research questions through Artificial Neural Network-based (Han et al., 2017) cyber-risk management framework for DDoS attacks on MMOG firms. First, we quantify the cyber-risk resulting from DDoS attacks by estimating their probability of occurrence. We estimate an MMOG firm's expected losses due to DDoS attacks. Subsequently, we use the probability of DDoS attacks and their expected loss to suggest mitigation strategies to an MMOG firm's CTO. An MMOG firm may accept, reduce, or transfer cyber-risk to a cyber-insurer (Kesan et al.,

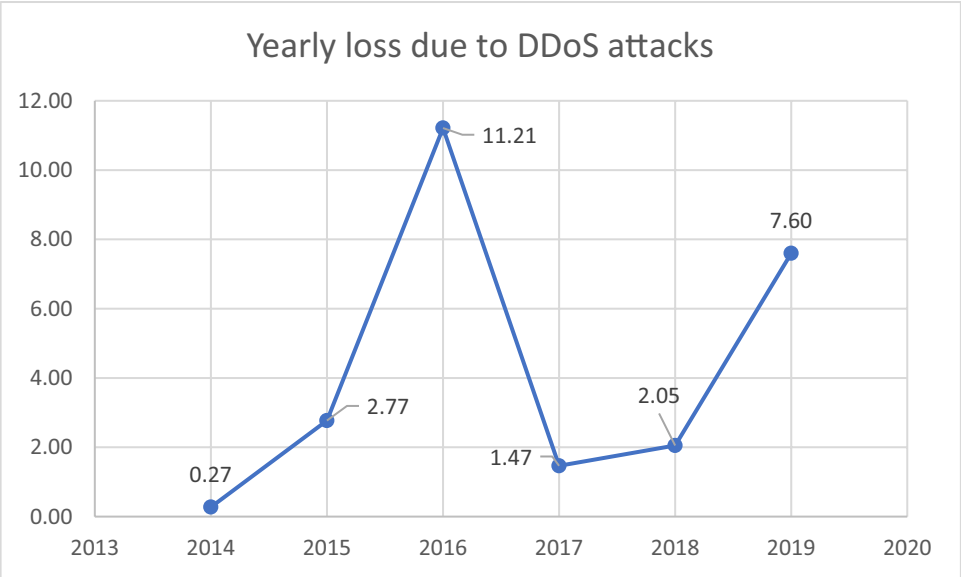



**Fig. 1** Yearly DDoS losses (2014-2019, IC3 reports, in billions)

**Table 1** DDoS variants and their characteristics

| Attack | Route | CVE | CVSS | IT asset compromised | | | Incidents | CIANR |
|---|---|---|---|---|---|---|---|---|
| | | | | RS | LC | NW | | |
| DNS Flood | DNS server | 2009-0234 | 6.4 | Y | – | – | Mirai DYN attack (2016) | A |
| CharGEN attack | Peripheral devices | 1999-0103 | 5.0 | – | Y | – | – | A |
| SSDP Flood | Plug and play devices | 2019-14323 | 5.0 | – | Y | – | – | A |
| NTP Flood | Network Time Protocol | 2019-11331 | 6.8 | – | – | Y | – | A |
| UDP Flood | UDP packets | 2016-10229 | 10.0 | Y | Y | – | – | A |

RS = Remote Server, LC = Local Client, NW = Network, VD = Vulnerability Detail, CVE = Common Vulnerabilities and Exposures, CVSS = Common Vulnerability Scoring System, CIANR = Confidentiality, Availability, Integrity, Non-repudiation

2013; Kleindorfer & Kunreuther, 1999; Rejda, 2007). We contribute to the academic literature by devising a framework to quantify and mitigate cyber-risk for MMOG firms using a feedforward neural network (FNN). On average, it takes 180 days for a vulnerability to be publicly disclosed by agencies such as CERT (Ransbotham et al., 2012). Thus, hackers can exploit the vulnerabilities from the previous quarter and launch zero-day attacks based on the currently exposed vulnerabilities. Therefore, our model incorporates the variables from the previous quarter, improving its accuracy. Moreover, we provide chief technology officers (CTOs) and managers with a tool to gauge alternative paths to cyber-risk mitigation in terms of potential investment in technology, cyber-insurance, or both. The aforementioned exercise in the context of the MMOG industry is crucial given the worsening of gamers' experience linked with the emergence of DDoS attacks.

The remainder of this paper is organized as follows. The following section provides an overview of existing cyber-risk management literature. Section 3 explains the proposed model, and Section 4 describes the data used for the analysis. Section 5 analysis covers the methodology, and Section 6 reports the empirical findings. Section 7 discusses the results, insights, future scope, and limitations of the study. Finally, Section 8 concludes the paper.

## 2 Literature Review

Cyber-risk management has been at the helm of cybersecurity research since the advent of Newer Information Technology for businesses (Gordon et al., 2003). The process for cyber-risk management comprises three main activities. We estimate the likelihood and impact of a cybersecurity breach to quantify the cyber-risk entailed by the breach mentioned earlier. The likelihood and the impact of a breach inform our subsequent strategies to mitigate the risk. We decide upon technological or financial & economic interventions

**Table 2** Cyber-risk assessment methods

| Authors | Description |
|---|---|
| IT Risk (Westerman, 2007) | Risk-Severity heat matrix |
| OCTAVE method (Dorofee & Alberts, 2002; CCC, 2003) | Identify operationally critical assets |
| CORAS approach (Stolen, 2002) | Abstraction of evaluated target and communication between stakeholders |
| ISRAM method (Kabacak & Sogukpinar, 2005) | Risk Analysis in complex information systems |

to reduce the probability of cybersecurity and its impact on the firms (Courtney, 1977).

## 2.1 Cyber-risk Assessment

Assessment of risk helps identify and subsequently quantify the probability of a cybersecurity incident occurring, provided the security protocols were in place. The cyber risk assessment also helps evaluate the efficacy of the IT risk management compliance structure already in place in organizations. Cyber risk assessment methods intend to identify information assets (such as hardware, systems, laptops, customer data, and intellectual property) under cyber-attack and their associated risks. Information assets are divided into multiple classes according to the perceived risk in order of their severity and broken into sub-parts to correctly identify the risky component of the asset and its type (tangible, intangible, etc.) (O'Reilly et al., 2018). Table 2 records studies from the literature aimed at assessing cyber-risk.

## 2.2 Cyber-risk Quantification

Cyber risk quantification methods rely on the probability of a risky incident occurring and rigorous estimation of loss amount for such incidents. Thus, the accuracy of such methods depends on the accuracy of risk identification and loss calculation. Loss estimation methods also evolve according to the unit of analysis and definition of loss for which we are undertaking the exercise mentioned above. Thus, the expected loss for an entity resulting from cyberattacks depends not only on the incident but also on our ability to estimate its loss accurately. These estimations also vary in their methodological rigor depending upon the type and granularity of data available to calculate them. Cyber risk quantification methods range from mathematical risk modeling to data mining methods using empirical data from security providers (Campbell & Stamp, 2004). Table 3 details different studies undertaken to quantify cyber-risk.

Broadly, the literature classifies the cyber-risk quantification methods into three heads: qualitative methods, quantitative methods, and hybrid methods. Qualitative methods deal with social, human, and behavioral motivations behind asset classification based on threats. A risk assessment matrix aids in arranging the different motivating factors for various asset classes (Baskerville, 1993). The OCTAVE approach aims at identifying operationally critical assets in an organization and their interconnections with other assets. It considers threats to these assets and vulnerabilities (organizational and technological) that make it a target for threats (Alberts & Dorofee, 2002). The CORAS approach uses a model-based security assessment to describe the evaluated target's appropriate abstraction, communicate between different stakeholders involved in this process, and document generated results (Stolen et al., 2002). Information Security Risk Analysis Method (ISRAM) allows managers and staff to analyze risk in complex information systems (Karabacak & Sogukpinar, 2005). CCTA Risk and Management Method (CRAMM) uses survey questionnaires to identify assets, grouping them according to vulnerabilities. It also evaluates security controls in an organization (CCTA, 1991).

Many of the first quantitative approaches tried to model the cyber risk scenario as an uncertainty model where the probability of cyber risk occurrence is studied. Most of these classification models use traffic attributes such as the TCP/IP layer used for the attack, quanta of bits used, and packet structure to typify cyber-attacks presence. Quantitative methods can be studies on the two broad heads depending upon vagueness in results and overlap with other risk profiles. Soft computing head uses cognitive fuzzy, fuzzy AHP methods and rough sets to estimate the likelihood of attacks. The other branch deals with econometric and data mining methods (Biswas et al., 2018, 2021; Samtani et al., 2017; Tripathi & Mukhopadhyay, 2020; Wang et al., 2020).

We use statistical methods that use prior knowledge of a cyber breach and update current evidence to model the classification's uncertainty. Logit and probit models have been used to calculate the probability of a cyber risk occurring using CSI-FBI survey data from 1997 to 2010 (Mukhopadhyay et al., 2019). Machine learning methods such as Bagger classifier and CART-based hybrid classifiers efficiently assess phishing attacks (Biswas & Mukhopadhyay, 2017).

On the other hand, augmented decision tree classifiers, along with Chi-square and Symmetric uncertainty, helped analyze DDoS feature vectors from the CAIDA dataset (Balkanli et al., 2015). Copula-based methods, which are quite popular with actuarial researchers, quantified cyber risk and, thus, were used to propose insurance approaches in complex risk modeling situations such as cyber-attacks (Herath &

**Table 3** Cyber-risk quantification methods

| Qualitative | Quantitative | | | Hybrid |
|---|---|---|---|---|
| | Fuzzy based | Econometric & statistical | Data Mining | |
| Parker approach (Parker, 1981) | Cognitive fuzzy logic approach (Smith & Eloff, 2006) | Time series based (Biswas et al., 2017) | Expert System based (Baskerville, 1993) | RISKPAC approach (CSC, 1988; Baskerville, 1993) |
| OCTAVE method (Dorofee & Alberts, 2002; CCC, 2003) | Fuzzy AHP method (Wu et al., 2009) | Density estimation approach (Alhazmi et al., 2007) | Text Mining based (Samtani et al., 2018; Biswas et al., 2018) | Attack Tree and BBN approach (Zhang et al., 2010) |
| CORAS approach (Stolen, 2002) | Rough set and fuzzy c-means clustering (Chimplee et al., 2006) | Copula based approach (Herath et al., 2007) | GLM based approach (Mukhopadhyay et al., 2017) | RITE (Dhillon & Blackhouse, 2000) |
| ISRAM method (Kabacak & Sogukpinar, 2005) | - | Game-theoretic model (Cavusoglu et al., 2004;2008; Zhang et al., 2020) | Decision tree classifier (Balkanli et al., 2015) | VFA (Dhillon & Blackhouse, 2006) |
| CRAMM approach (SANS institute, 2002) | - | VaR approach (Jaisingh, 2001; Qi et al., 2010) | Neural Network-based approach (Wang et al., 2020) | - |
| - | - | Investment in IT security (Gordon & Loeb, 2002) | Hidden Markov model (Arnes et al., 2006; Srivastava et al., 2008; Pak et al., 2009; Das et al., 2019) | - |
| - | - | ALE method (Bojanc & Blazic, 2008) | - | - |

Herath, 2011). Cyber risk attack vectors can be efficiently modeled using density estimation methods, thus augmenting the accuracy of a method that relies upon distribution statistics to classify (Alhazmi et al., 2007). The fuzzy logic-based RiMaHCoF method was able to quantify cyber-risks in overlapping and conflicting risk classes (Smith & Eloff 2002).

Decision trees and their other variants like ensemble methods and hybrid classifiers are quite efficient with provision for decision rules to inform future decisions for classifying similar incident vectors. Using only a few independent features constructs a very highly complex tree, and its pruning is problematic, given the trade-off with its accuracy (Biswas et al., 2016). Thus, significant stress is finding an interpretable quantitative method to ascertain the probability of a cyber-attack occurring.

Hybrid methods use data from qualitative questionnaires to estimate likelihood by utilizing mathematical modeling. RiskPac method uses managers' questionnaire responses about IT security, IT audits, and IT risks to estimate risk and expected loss (Baskerville, 1993; Courtney, 1977). RITE method uses Responsibility (R), Integrity (I), trust (T), and ethicality (E) to provide a wholesome idea about vulnerabilities and risk perceptions in firms (Dhillon & Backhouse, 2000). Social, human, and interpersonal issues also play an essential role in risk quantification under a value-focused approach (Dhillon & Torkzadeh, 2006).

Impact evaluation forms the next important part of the risk assessment step. We try ascertaining the impact of security breaches either in terms of attacks and vulnerabilities or financial and economic indicators of a firm. Event study methodology uses virus attacks, DoS attacks, phishing attacks, and security vulnerabilities to find the cost of a security breach (Campbell & Stamp, 2004; Cavusoglu et al., 2008). Financial methods aim at quantifying the effect of breaches on the financial indicators of the firm, such as stock prices and insurance choices (Bandyopadhyay et al., 2009; Campbell et al., 2003).

On average, it takes 180 days for a vulnerability to be publicly disclosed by an agency such as CERT (Ransbotham et al., 2012). Thus, hackers can exploit the previous quarter's vulnerabilities and launch zero-day attacks based on the currently exposed vulnerabilities. Therefore, our model incorporates the variables from the previous quarter, improving its accuracy. Secondly, our FNN-CRAM tries to compute the proportions of cyberattacks in a particular quarter, unlike past studies. Thus, we have chosen a Feedforward Neural network over classification techniques in the extant literature such as Decision trees, SVM, K-nearest neighbor method, and logistic regression (Han et al., 2017). Lastly, previous studies have focused on cyber-risk management for individuals and traditional industries like e-commerce and healthcare. This study executes cyber-risk management for

**Table 4** Cyber-risk mitigation methods

| Authors | Type of intervention | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|---|
| Hoffman et al., 1978 | Tech | Y | - | - | - | - | - | - | - |
| Ozier, 1989 | Tech | Y | Y | Y | - | - | - | - | - |
| Mukhopadhyay et al., 2007 | Tech | Y | - | - | - | - | - | - | - |
| Guarrao, 1987 | Tech | - | Y | | Y | - | - | - | - |
| Baskerville, 1993 | Tech | - | Y | Y | - | - | - | - | - |
| Mukhopadhyay et al., 2019 | Tech | - | - | Y | - | - | - | - | - |
| Cashell, 2004 | Fin | - | - | - | - | Y | - | - | - |
| Ko et al., 2006 | Fin | - | - | - | - | - | Y | | - |
| Kesan & Majuca, 2005 | Fin | - | - | - | - | - | - | Y | - |
| Bohme & Kataria, 2006 | Fin | - | - | - | - | - | - | Y | - |
| Bohme & Schwartz, 2010 | Fin | - | - | - | - | - | - | Y | - |
| Zhang et al., 2020 | Fin | - | - | - | - | - | - | - | Y |

A = Vulnerability assessment, B = Threat identification, C = Security measures, D = Controls, E = Economic impact of cyberattack, F = Financial impact on firm performance, G = Utility based approach, H = Game theoretic approach, Fin = Financial, Tech = Technological

the online gaming industry, and results are generalizable to industries requiring high real-time service quality.

### 2.3 Cyber-risk Mitigation

The last step of the cyber-risk management process involves suggesting ways to mitigate the risk, given the probability and impact of cybersecurity breaches. Researchers have suggested technological as well as financial interventions to mitigate cyber-risks. Technological interventions have focused on vulnerability assessment (Hoffman et al., 1978; Mukhopadhyay et al., 2007; Ozier, 1989), threat identification (Baskerville, 1993; Guarro, 1987; Ozier, 1989), design of security protocols (Mukhopadhyay et al., 2019), and controls (Guarro, 1987). On the other hand, financial interventions have dealt with cyber-insurance as a tool to deter as well as strengthen a firm's security attitude and mitigate cyber-risks (Böhme & Kataria, 2006; Böhme & Schwartz, 2006; Kesan et al., 2013, 2005; Majuca et al., 2006). Table 4 categorizes different studies belonging to financial or technological interventions.

## 3 Feedforward Neural Network-based Cyber-risk Assessment and Mitigation model (FNN-CRAM)

According to the opportunity theory of crime, apart from the initial stimulus, the hacker looks out for vulnerabilities in the systems in an environment with minimal or no checks (or security controls) (Cohen & Felson, 1979). Hackers also weigh their benefits compared to costs in terms of effort, time, and punishments, if any. On the other hand, firms under attack follow a layered approach towards fear appeals originating from cyber-attacks. They gauge the probability of the event's occurrence and the magnitude of its impact on them. Eventually, they enlist their protective responses and evaluate their efficacy (Boss et al., 2015; Bulgurcu et al., 2010; Rogers, 1975). According to rational choice theory, decision-makers choose the alternative best suited to their subjective preference structure (Becker, 1990; McCarthy, 2002). The process of cyber-risk management closely follows from risk theory (Kunreuther, 1997). It states that uncertain scenarios need to be dealt with risk assessment, quantification followed by mitigation by weighing costs and benefits. Based on the discussion above, our proposed FNN-CRAM model consists of three modules – Cyber-risk Assessment, Cyber-risk Quantification, and Cyber-mitigation for an MMOG firm, as shown in Fig. 2.

### 3.1 Cyber-risk Assessment

We model each one of the five DDoS attacks separately to assess cyber-risk for an MMOG firm. We assume that DDoS attacks follow the binomial distribution, and their proportions in a particular quarter give the probability of their occurrence (Mukhopadhyay et al., 2019; Nelder, 1989). Figure 3 depicts the cyber-risk assessment module.

Table 5 provides literature support for the variables used in the proposed model.

As shown in Fig. 4, The probability ($p_t$) of DDoS attacks adversely slowing down the operations of an MMOG firm if the intensity of rogue traffic (bps) and its duration (duration) is high (Cavusoglu et al., 2008; Sharma & Mukhopadhyay, 2020a; Yue et al., 2019).

The probability ($p_t$) of a DDoS attack increases over time (t) as hackers repeatedly launch attacks by exploiting zero-day vulnerabilities in software used by MMOG firms

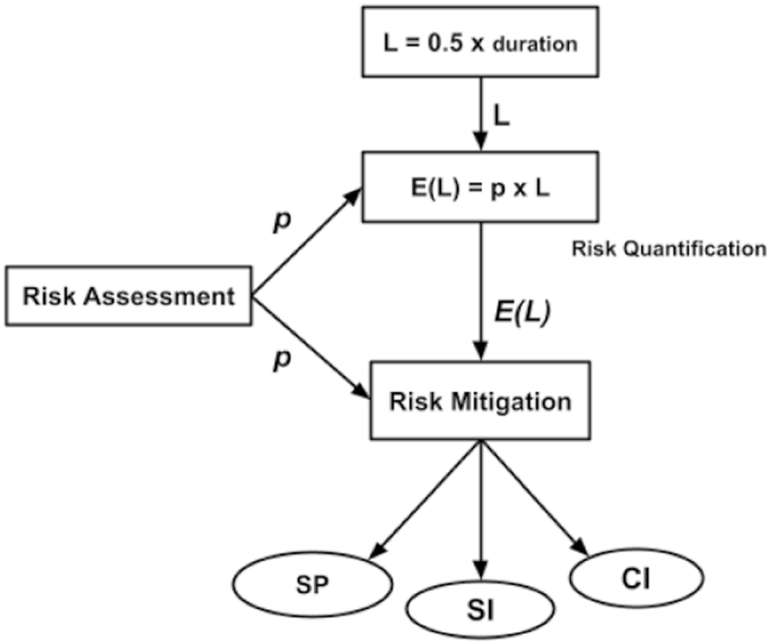



**Fig. 2** FNN-CRAM model for MMOG firms

(Mukhopadhyay et al., 2019; Wang et al., 2020). Computer emergency response team (CERT) takes six months (or two quarters) to disclose a vulnerability (Ransbotham et al., 2012) publicly. For example, on 30th June 2021 (where $t_{quarter} = 2$), the vulnerabilities from January to March 2021 ($t_{quarter} = 1$) and April to June 2021 ($t_{quarter} = 2$) are not yet disclosed by CERT. So, hackers can launch zero-day DDoS attacks by exploiting vulnerabilities (vC) from January to March 2021 and April to June 2021. Suppose CERT announces the vulnerabilities at the end of quarter 2 (i.e., 30th June 2021). Thus, on the 30th June 2021 ($t_{quarter} = 2$) and beyond, the overall vulnerabilities (vC/t) will come down as the technology vendors issue the respective patches. Moreover, the MMOG firms will increase security defenses (e.g., firewalls, cyber-insurance), train staff in best practices, design mitigation plans, and develop frameworks for bug-free software products (Angst et al., 2017; Cavusoglu et al., 2008). Thus, we suggest that vulnerabilities (vC/t and $vC/t^2$) tend to decrease over time which helps in reducing the probability ($p_t$) of DDoS attacks as security patches are available. By the end of June 2021 ($t_{quarter} = 2$), the hacker can exploit the vulnerabilities of quarters 1 and 2, respectively. Thus we intend to model the probability of DDoS attack ($p_t$) using lagged variables such as $(vC/t)_t$, $(vC/t^2)_{t-1}$), as this phenomenon can be equated to autoregressive model (Geurts et al., 1977; Gujarati, 2009). Similarly, the hacker tends to launch a high-intensity and longer duration zero-day DDoS attack because of the unavailability of security patches in quarters 1 and 2 (i.e., Jan to March and April to June 2021). Thus, we intend to model the DDoS attack ($p_t$) probability using lagged variables such as $bps_{t-1}$ and $duration_{t-1}$ (Geurts et al., 1977; Gujarati, 2009).

Similarly, in August 2021, NIST and MITRE publicly announce the vulnerabilities' details along with the severity score (i.e., CVSS). As a result, the technology vendors focus on creating security patches for vulnerabilities with the highest severity scores (i.e., vscr) (Arora et al., 2008; Kannan & Telang, 2005). It will reduce the probability ($p_t$) of DDoS attacks. They have higher chances of culminating in attacks because they take longer to get patched before being exploited (Biswas et al., 2016; Cavusoglu et al., 2008; Das et al., 2019; Peng et al., 2007; Tripathi & Mukhopadhyay, 2020).

Thus, we investigate.

RQ1a: What is the proportion (probability)of each kind of DDoS attack compromising the MMOG systems?

Our model estimates the probability ($0<p<1$) that a DDoS attack occurs to assess the cyber-risk for each kind of DDoS attack. The first stage of this model helps us estimate the probability for each type of DDoS attack by training, validating, and testing the Feedforward Neural Network (FNN) (Hagan & Demuth, 2014). The extant literature has used Weibull distribution to model the probability of

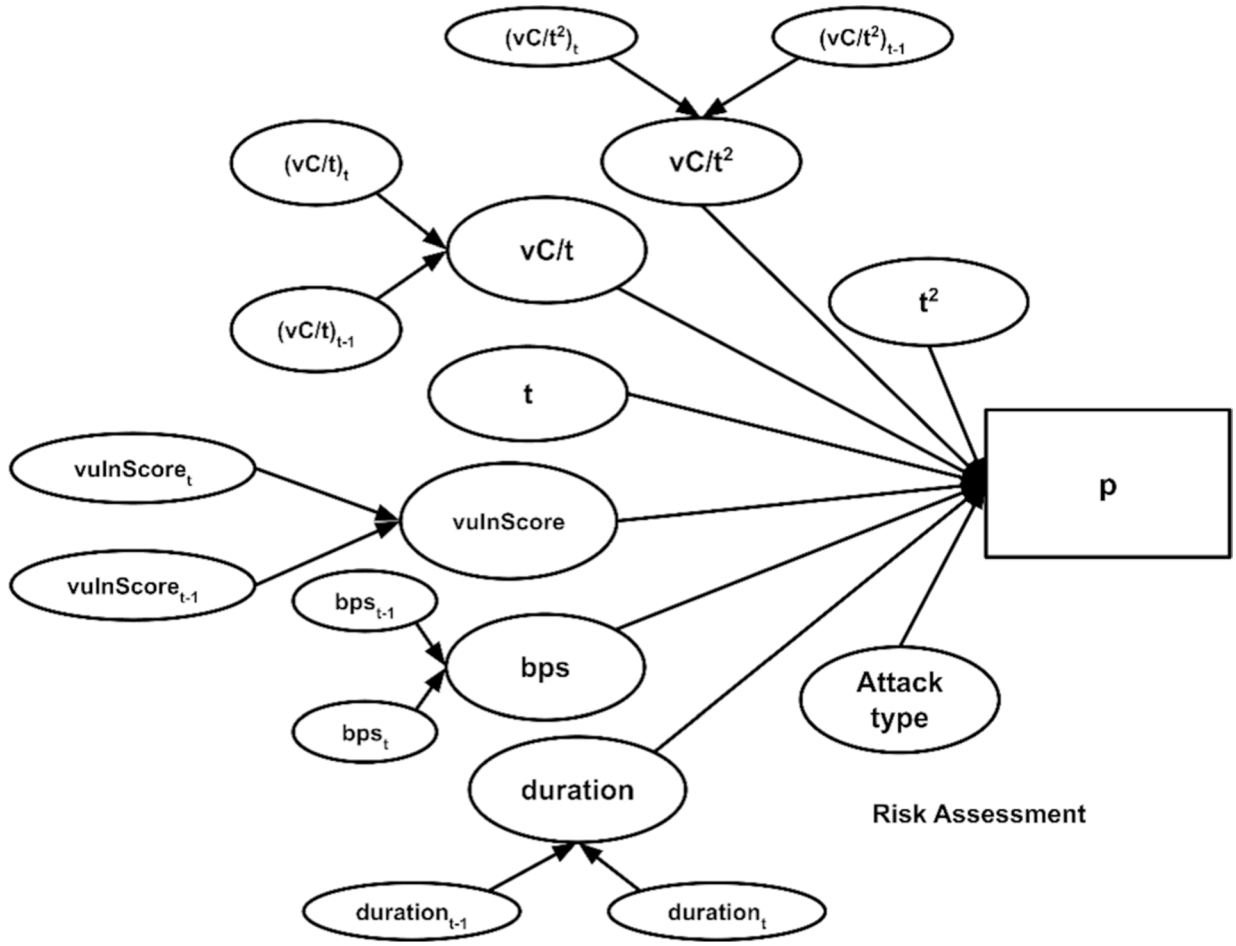



**Fig. 3** Cyber-risk assessment module for FNN-CRAM model.

**Table 5** Model variables and relevant literature support

| Variable name | Variable symbol | Literature |
|---|---|---|
| Attack type | Attack type | (McKeay, 2017; Peng et al., 2007; Wang et al., 2020) |
| Attack intensity | $bps_t$, $bps_{t-1}$ | (Peng et al., 2007; Tanenbaum & Wetherall, 2010; Wang et al., 2020; Zhang et al., 2020) |
| Attack duration | $duration_t$, $duration_{t-1}$ | (Peng et al., 2007; Tanenbaum & Wetherall, 2010; Wang et al., 2020; Zhang et al., 2020) |
| Vulnerability Score | $vulnScore_t$, $vulnScore_{t-1}$ | (Arora et al., 2008; Kannan & Telang, 2005; Peng et al., 2007; Ransbotham et al., 2012; Shahriar & Zulkernine, 2012; Zhang et al., 2020) |
| Vulnerability count | vC | (Arora et al., 2008; Kannan & Telang, 2005; Peng et al., 2007; Ransbotham et al., 2012; Shahriar & Zulkernine, 2012; Zhang et al., 2020) |
| Time | t, $t^2$ | (Biswas & Mukhopadhyay, 2018; Mukhopadhyay et al., 2019) |
| Vulnerability trend over t | $(vC/t)_t$, $(vC/t)_{t-1}$ | (Cavusoglu et al., 2008, 2009; Ransbotham et al., 2012) |
| Vulnerability trend over $t^2$ | $(vC/t^2)_t$, $(vC/t^2)_{t-1}$ | Created for this study |
| Probability of attack for MMOG | p | (Biswas et al., 2017; Biswas & Mukhopadhyay, 2018; Das et al., 2019; Mukhopadhyay et al., 2019) |

| Days | 0 to 180 days | | | | | | 225 days | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M | J | F | Mr | A | May | June ($1^{st}$ to $29^{th}$) | $30^{th}$ June | Jul | Ag | S | O | N | D |
| Q | Q1 | Q1 | Q1 | Q2 | Q2 | Q2 | Q2 | Q3 | Q3 | Q3 | Q4 | Q4 | Q4 |
| TP | t-1 | | | t | | | | t+1 | | | t+2 | | |
| SH | CERT: Vulnerability Q1 and Q2: Not disclosed | | | | | | Jan | Feb | Mar | Apr | May | Jun | Jul |
| CERT | | | | | | | Vulnerability Q1 and Q2: Disclosed in a *lagged* manner | | | | | | |
| MITRE | MITRE: CVSS for Q1 and Q2: Not disclosed | | | | | | CVSS for vulnerabilities of Q1 and Q2 disclosed in a *lagged* manner | | | | | | |
| H | Zero-Day attack by hackers | | | | | | | | | | | | |
| OEM | | | | | | | *Patch creation* | *Patch release* | | | | | |
| Firm | | | | | | | | Patch deployment | | | | | |
| | bps, duration = (High, High) for Q1 and Q2 | | | | | | | bps, duration = (Low, Low) | | | | | |
| | $p_t$ is high | | | | | | $p_t$ is high | $p_{t+1}$ tends to reduce | | | | | |

M= Months, Q = Quarters, TP =Time period, SH = Stakeholder, H = Hackers, OEM = Original Equipment Manufacturer,

**Fig. 4** Stakeholder view of DDoS attack lifecycle

failures. Thus, we also test whether the probability of a DDoS attack follows the same.

RQ 1b: Which probability distribution best approximates the occurrence of DDoS attacks in the MMOG industry?

### 3.2 Cyber-risk Quantification

The next stage of the proposed model deals with quantifying the cyber-risk viz-a-viz expected loss calculation. DDoS attack results in disruption of service to legitimate users. Thus, the loss due to DDoS attack is proportional to the duration of the attack (Bezsonoff, 2017; Yue et al., 2019). The expected loss indicates the severity of the DDoS attack in terms of monetary loss to the firm. According to a Neustar report, a firm loses US$ 0.5 million per hour of a DDoS attack (Bezsonoff 2017; Sharma & Mukhopadhyay, 2020b, 2020a; Tripathi & Mukhopadhyay, 2020). We use this information to calculate loss and subsequently expected loss (Courtney, 1977), the product of the probability of attack with the loss incurred due to attack (Campbell et al., 2003). In the extant literature, expected loss values follow the long-tail distribution, and thus, we check if gamma distribution best approximates the same (Dutta & Perry, 2011).

RQ2a: What is the expected loss for each type of DDoS attack in the MMOG industry?

RQ 2b: What probability distribution best estimates the expected loss caused due to each type of DDoS attack in the MMOG industry?

### 3.3 Cyber-risk Mitigation

The final stage of the proposed model pertains to cyber-risk mitigation by suggesting ways to reduce the risk and the severity of the DDoS attacks in the MMOG industry. The primary inputs for this stage are the risk (Probability of attack) values and severity (Expected loss) values. These help us decide whether the firm CTO should choose between reducing (self-protection), accepting (self-insurance), or transferring (cyber-insurance) risk (Böhme, 2005; Böhme & Schwartz, 2006; Kesan et al., 2013, 2005; Majuca et al., 2006).

RQ3: What cyber-risk mitigation strategies should CTOs use for each kind of DDoS attack in MMOG firms?

## 4 Data

This study has used a dataset of DDoS attacks in the MMOG industry captured by a reputed CDN through its cybersecurity service. The dataset contains 10,329 records with six attack attributes each. The attributes, namely bits per second (*bps*), packets per second (*pps*), start timestamp, end

**Table 6** Summary statistics for the attack dataset (from 2012 Q2 (t1) to 2018 Q2 (t25))

| Attack type | Count | | $N_{final}$ | $D_{training}$ | $D_{testing}$ | | Min | Max | Mean | Std. Dev. |
|---|---|---|---|---|---|---|---|---|---|---|
| UDP Fragment, DNS Flood (UD) | 3,155 | Q | 23 | 2013 Q4 to 2017 Q3 | 2017 Q4 to 2018 Q2 | bps | $1.5^{\#}$ | $28^{\wedge}$ | $3^{\wedge}$ | 3 |
| | | M | 54 | 2013 M10 to 2017 | 2018 M1 to 2018 M2 | duration$^{@}$ | 0.2 | 69 | 19 | 14 |
| NTP Flood (NF) | 2,671 | Q | 19 | 2014 Q1 to 2017 Q3$^{\dagger}$ | 2017 Q4 to 2018 Q2 | bps | $112^{\#}$ | $19^{\wedge}$ | $1^{\wedge}$ | 2 |
| | | M | 45 | 2014 to 2017 | 2018 M1 to 2018 M4 | duration$^{@}$ | 0.3 | 69 | 20 | 14 |
| UDP Fragment, CharGEN Attack | 2,030 | Q | 20 | 2013 Q3 to 2017 Q2 | 2017 Q3 to 2018 Q2 | bps | $0.5^{\#}$ | $19^{\wedge}$ | $1^{\wedge}$ | 1 |
| | | M | 54 | 2013 M9 to 2017 | 2018 M1 to 2018 M4 | duration$^{@}$ | 0.1 | 69 | 20 | 14 |
| SSDP Flood | 1,465 | Q | 16 | 2014 Q3 to 2017 Q3 | 2017 Q4 to 2018 Q2 | bps | $363^{\#}$ | $22^{\wedge}$ | $1^{\wedge}$ | 1 |
| | | M | 43 | 2014 M8 to 2017 | 2018 M1 to 2018 M4 | duration$^{@}$ | 0.4 | 69 | 21 | 15 |
| UDP Flood | 1,008 | Q | 17 | 2012 Q2 to 2017 Q3$^{*}$ | 2017 Q3 to 2018 Q2 | bps | $0^{\#}$ | $28^{\wedge}$ | $2^{\wedge}$ | 4 |
| | | M | 55 | 2012 to 2017 | 2018 M1 to 2018 M4 | duration$^{@}$ | 0.2 | 68 | 19 | 14 |
| $N_{total}$ | 10,329 | | | | | | | | | |
| vulnScore | 23,712 | | 25 | — | — | — | 0 | 10 | 6 | 2 |
| t | 25 | | 25 | — | — | — | — | — | — | — |
| $t^2$ | 25 | | 25 | — | — | — | — | — | — | — |
| vC | 23,712 | | 25 | — | — | — | — | — | — | — |

Training set = 2012 Q2 ($t_1$) to 2017 Q1 ($t_{20}$), Testing dataset = 2017 Q2 ($t_{21}$) to 2018 Q2 ($t_{25}$)

$^{\#}$ in kbps, $^{\wedge}$ in Gbps, $^{*}$except for 2013 Q4 and 2014 Q1, $^{\dagger}$except for 2014 Q3, $^{@}$ in hours, Q = Quarterly, M = Monthly

timestamp, type of attack, indicate the intensity and duration of the attack and the internet protocol to launch it. The attributes – *bps* and *pps* are highly correlated. Thus, we only use *bps* to gauge the intensity of the attacks. We derive the *duration* of the attack using the start and end timestamp of attacks. Next, we convert attack intensity, the *bps* attribute, into Gbps (Gigabits per second) and *duration* in hours to adjust for scale variations. The dataset comprises five different DDoS attacks: UC, UD, NTP Flood, SSDP Flood, and UDP Flood. The attack data range from 2012 to 2018. Table 6 details the number of records of each kind of DDoS attack.

We aggregate attack records into quarters and years. Thus, for each quarter from 2012 to 2018, we have a total number of attacks and breakdown into five DDoS attacks. We derive the mean attack intensity (in Gbps) and the mean duration of each kind of DDoS attack for each quarter over the same time. Some DDoS attack types do not occur in the initial years, and we have missing values for those attacks, respectively. The pre-processed data informs about the count and kind of DDoS attacks in each quarter and the month of the year. It reduces the volatility in daily data and makes the trend easily discernible (Geurts et al., 1977). CERT and MITRE announce that the vulnerability data only after two quarters (i.e., 180 days) have elapsed since the initial discovery. Thus, the probability of DDoS attacks depends upon this timeline. Therefore, we use the quarterly and monthly aggregates for all the variables to match attack data with vulnerability data (Cavusoglu et al., 2008; Ransbotham et al., 2012).

We gather vulnerability time-series data from the National Vulnerability Database (NVD) XML feeds provided by the National Institute of Standards and Technology (NIST). The vulnerability dataset has a publish date, update date, Common Vulnerability Scoring System (CVSS) Score, and vulnerability type. We chose all vulnerabilities of the DoS type for the period matching the DDoS attack timeline (i.e., 2012 Q2 to 2018 Q2). The data is aggregated quarterly and monthly for the years, as mentioned earlier. We choose the number of vulnerabilities and the average vulnerability scores for the same period as additional variables of attack probability. An unpatched vulnerability can also result in multiple DDoS attacks if vendors do not mend before hackers know about them.

## 5 Methodology

The research methodology consists of three prominent stages: cyber-risk assessment, cyber-risk quantification, and cyber-risk Mitigation. In the cyber-risk assessment stage, we identify the assets that increase the vulnerability of information systems to DDoS attacks. The second stage quantifies the cyber-risk of DDoS attacks with the help of variables mentioned earlier. We use the probability and severity of attacks in the last step to suggest mitigation strategies to absorb the cyber-risk.

$$p_t = \mathrm{FNN}(bps_t,\ bps_{t-1},\ dur_t,\ dur_{t-1},\ t,\ t^2,\ (vc/t)_t,\ (vc/t^2)_t,\ (vc/t)_{t-1},\ (vc/t^2)_{t-1},\ vscr_t,\ vscr_{t-1})$$

We propose a feedforward neural network (FNN) to compute the probability ($p_t$) of five kinds of DDoS attacks on an MMOG firm. The probability ($p_t$) of attack depends on time-dependent variables such as bps, duration, vulnerability score, and counts. We use these variables from both the current quarter (t) as well as the previous quarter (t-1) as discussed in the proposed model (Geurts et al., 1977; Gujarati, 2009). FNN has been used extensively to model time-series data and performs better for independent variables with non-linearity (Allende et al., 2002; Desai & Bharati, 1998; Krohn et al., 2019). Thus, we have chosen an FNN over classification techniques such as Decision trees, SVM, K-nearest neighbor method, and logistic regression (Han et al., 2017). Our proposed FNN model consists of three layers, namely, the input (I) layer, the hidden (H) layer, and the output (O) layer. FNN topology consists of seven input neurons, ten hidden neurons, and one output neuron (Hagan & Demuth, 2014). Our FNN model takes the input in the form of the independent variables (i.e., bps, duration, vC/t, $vC/t^2$, vscr), which are non-linear with respect to the dependent variable ($p_t$). Each neuron in the FNN behaves like a multi-input regression model (Hagan & Demuth, 2014; Kelleher & Tierney, 2018). Inputs are multiplied by weights generated through the Nguyen-Widrow algorithm (Nguyen & Widrow, 1990). Next, the product passes through a transfer function such as log-sigmoid, which adjusts for the non-linearity in the inputs. Finally, the probability ($p_t$) of attacks, which lies between zero to one, is computed through the satlins transfer function.

We use an 80:10:10 ratio for training, validation, and testing datasets (Hagan & Demuth, 2014; Han et al., 2017). The Levenberg-Marquardt algorithm trains the FNN until meeting the stopping criterion (i.e., either minimum gradient or validation stop) (Levenberg, 1944). We use Mean Squared Error (MSE) as the metric to evaluate the training, validation, and testing performance (Hagan & Demuth, 2014). The trained FNN computes the probability (or proportion) of each kind of DDoS attack. Next, we fit a Weibull distribution to the computed probabilities (or proportions) and estimate its parameter (Hossack et al., 1999). Using the estimated parameters, we calculate the mean and standard deviation for each kind of DDoS attack.

On the other hand, the loss in each DDoS attack is calculated using a US$ 0.5 million loss per hour (Bezsonoff, 2017). Expected Loss for each data record is computed and a gamma distribution fitted to the same (Dutta & Perry, 2011). Mean and standard deviation values for expected loss for each DDoS attack follow.

The next stage of the study suggests mitigation strategies by appropriately visualizing the risk (probability of the attack) and severity (expected loss of the attack). We use a $2 \times 2$ heat matrix to help the firm choose between self-protection, self-insurance, or cyber-insurance depending upon the boundary values for high-low risk and severity values (Mukhopadhyay et al., 2019). The firms should

**Table 7** Algorithm for cyber-risk management

| | |
|---|---|
| | ***Cyber-risk Assessment*** |
| Step 1 | **Input:** $D = (Y_D, X_D)$<br>$Y_D = p$<br>$X_D = [bps_t, duration_t, t, t^2, vulnScore_t, (vC/t)_t, (vC/t^2)_t,$ # t quarter<br>$bps_{t-1}, duration_{t-1}, vulnScore_{t-1}, (vC/t)_{t-1}, (vC/t^2)_{t-1}]$ # (t-1) quarter |
| Step 2 | **Output:** $p_t = FNN(D_{training})$ # Topology 7-10-1<br># Initialize the weights using the Nguyen-Widrow algorithm.<br># $D_{training} : D_{validation} : D_{testing} = 80:10:10$<br><br>If MSE(p) = min_threshold<br>Then stop the training |
| Step 3 | Fit Weibull distribution on *p* values |
| | ***Cyber-risk Quantification*** |
| Step 4 | Expected loss, E(L) = p * 0.5 * (duration) |
| Step 5 | Fit a Gamma distribution on *E(L)* values |
| | ***Cyber-risk mitigation*** |
| Step 6 | Propose mitigation strategies<br>*If p =Hi* AND *E(L) = Hi, then* Self-Protection (SP)<br>*Else if p = Hi* AND *E(L) = Lo* OR *p = Lo* AND *E(L) = Hi, then* Self-insurance (SI)<br>*Else if p = Lo* AND *E(L) = Lo, then* Cyber-insurance (CI) |

FNN = Feedforward Neural Network

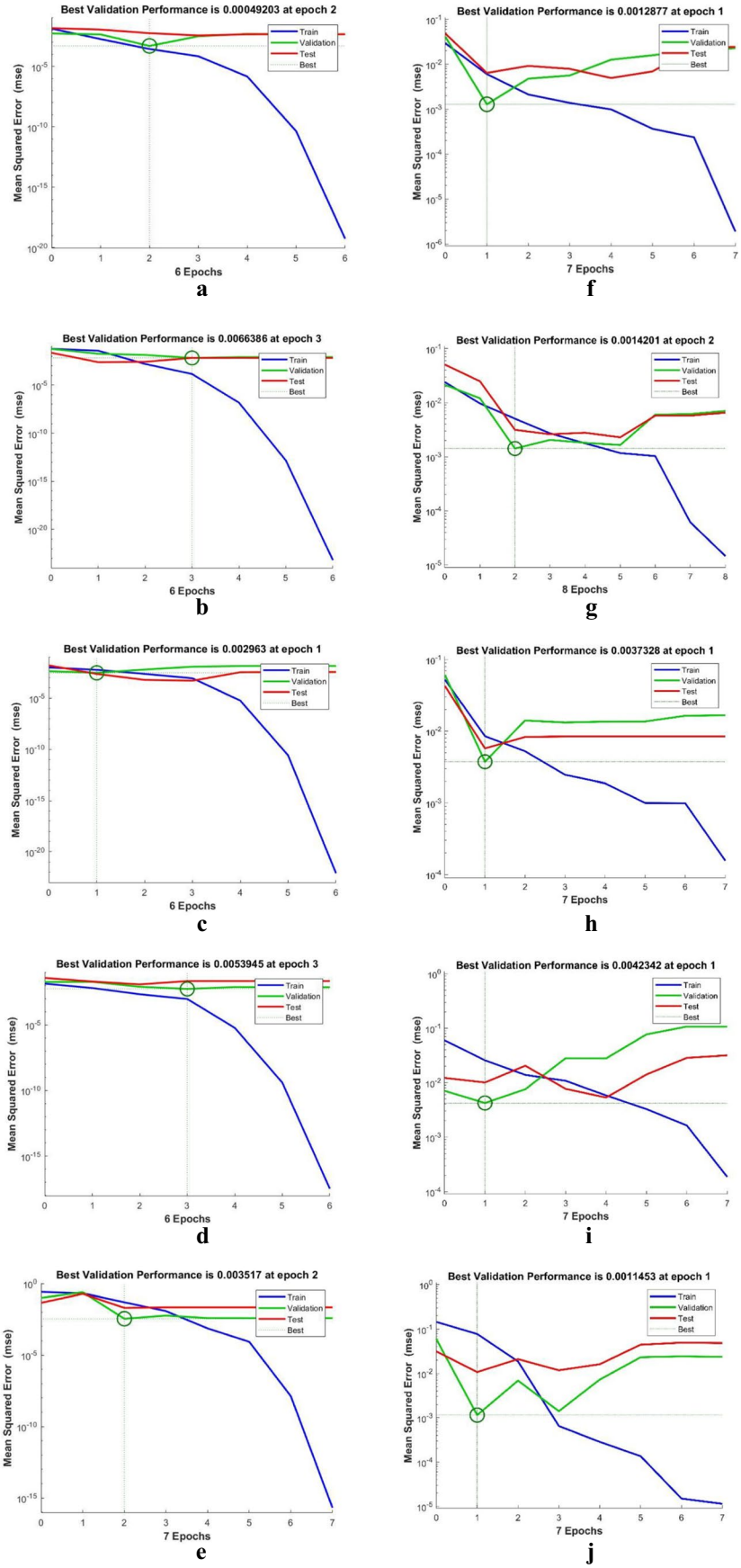



**Fig. 5** **a** Performance plot of FNN for quarterly NTPFlood data. **b** Performance plot of FNN for quarterly SSDP-Flood data. **c** Performance plot of FNN for quarterly UC data. **d** Performance plot of FNN for quarterly UD data. **e** Performance plot of FNN for quarterly UDPFlood data. **f** Performance plot of FNN for monthly NTPFlood data. **g** Performance plot of FNN for monthly SSDP-Flood data. **h** Performance plot of FNN for monthly UC data. **i** Performance plot of FNN for monthly UD data. **j** Performance plot of FNN for monthly UDPFlood data

choose self-protection if they have high risk-high severity attacks (Rejda, 2007). Firms with low risk-high severity (or vice-versa) attacks should go for cyber-insurance (Majuca et al., 2006). Low risk-Low severity attacks on firms should be self-insured to absorb the losses (Kesan et al., 2005). Table 7 details the algorithm used for analyzing the DDoS attacks.

## 6 Results

This section details the results from the three stages of this study. The first stage takes variables as input and generates probability values and distribution for each DDoS attack type. The second stage estimates the expected loss and its distribution. The last stage suggests ways to mitigate the cyber-risk in each DDoS attack type.

### 6.1 Cyber-risk Assessment

As shown in Fig. 5, the training is stopped when validation performance reaches its minimum value in any epoch.

Table 8 details the mean-squared error performance for each attack across quarterly as well as monthly data. We observe that the mean-squared error for monthly aggregated data is worse off than quarterly aggregation. Moreover, most firms take quarterly budgetary decisions, and thus, the granularity mentioned above matches it (Blau et al., 2019).

Figure 6 compares the actual probabilities of each DDoS attack and computed probabilities from the FNN model after training. Table 9 tabulates the performance metric of neural networks for each attack. UD (i.e., combination of UDP Fragment and DNSFlood) attack has the highest test dataset accuracy at 99.76%, as shown in Fig. 6. While UC (i.e., the combination of UDP Fragment and CharGEN attack) has the lowest accuracy at 98.76%, as shown in Fig. 6. While on monthly data, we have SSDPFlood attacks with the highest test dataset accuracy of 99.78% and the lowest test accuracy of 98.93% for UDPFlood attacks, as shown in Fig. 6, respectively.

**Table 8** Mean-squared error (MSE) for each attack during training

| Attack type | $MSE_{quarterly}$ | $MSE_{monthly}$ |
|---|---|---|
| NTPFlood | 0.001 | 0.005 |
| SSDPFlood | 0.003 | 0.004 |
| UC | 0.005 | 0.007 |
| UD | 0.005 | 0.019 |
| UDPFlood | 0.035 | 0.050 |

**Table 9** Probability of DDoS attacks for the testing window

| Year and quarter | NTP Flood | SSDP Flood | UC | UD | UDP Flood |
|---|---|---|---|---|---|
| 2017 Q3 | –* | –* | 0.17 | –* | 0.12 |
| 2017 Q4 | 0.34 | 0.15 | 0.06 | 0.22 | 0.22 |
| 2018 Q1 | 0.17 | 0.07 | 0.15 | 0.48 | 0.12 |
| 2018 Q2 | 0.16 | 0.10 | 0.11 | 0.44 | 0.18 |
| Test Accuracy (%) | 99.74 | 99.24 | 98.76 | 99.76 | 99.66 |

* included in the training dataset

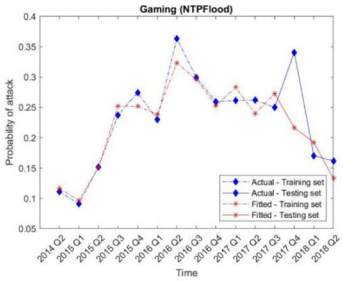
Table 9 records the computed probability of different DDoS attacks for the testing dataset. UD attacks have the highest probability of occurrence for 2018 Q2, while UC attacks have the lowest probability in 2017 Q4.

We validate and test our FNN model on the last 20% of the records for each attack. Thus, we use the last three quarters of NTPFlood, SSDPFlood, and UD attacks for those mentioned above. Similarly, the last four quarters for UC and UDPFlood attacks serve the same purpose. In all five DDoS attacks, the FNN model correctly estimates the trend in the actual data. Table 10 tabulates the parameter estimates of Weibull distribution for risk values along with mean and standard deviations. UD attacks have the highest average risk value at 0.28, while UDPFlood attacks have the lowest average risk values at 0.2 (refer to Table 10). The distribution of risk values is positively skewed for SSDPFLood, UC, and UDPFLood attacks, as depicted in Fig. 7, and 4. UD and NTPFlood attacks are essentially unskewed, as shown in Fig. 7.

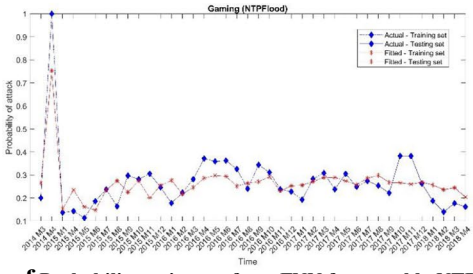
### 6.2 Cyber-risk Quantification

Table 11 informs about the expected loss in the testing dataset for five types of DDoS attacks. SSDP attacks have the lowest expected loss at US$ 0.44 million in 2018 Q2, while UD attacks culminate into the highest expected losses at US$ 2.8 million in 2017 Q4.

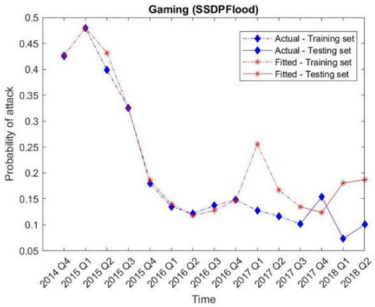
After calculating expected loss values, we fit a gamma distribution on expected loss values. UD attacks have the highest average expected loss at US$ 2.23 million (refer to Table 12). In comparison, UC has the lowest average expected loss at US$ 1.83 million (refer to Table 12). Figure 8 depicts distribution curves for expected loss values. Except for UC attacks, all other attacks' expected losses are positively skewed distributions, as shown in Fig. 8.



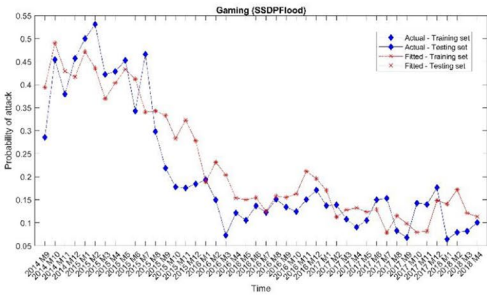

**a Probability estimates from FNN for quarterly NTPFlood data**



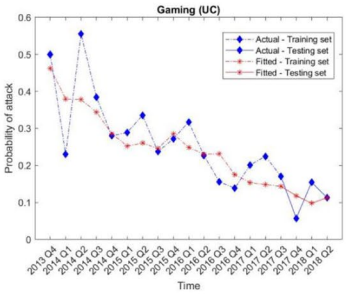

**f Probability estimates from FNN for monthly NTPFlood data**



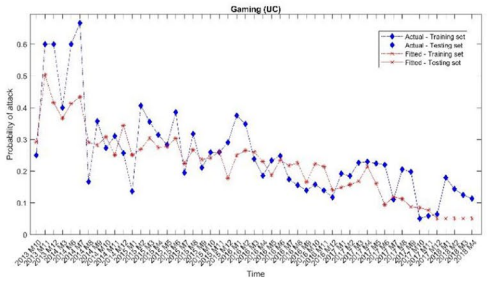

**b Probability estimates from FNN for quarterly SSDPFlood data**



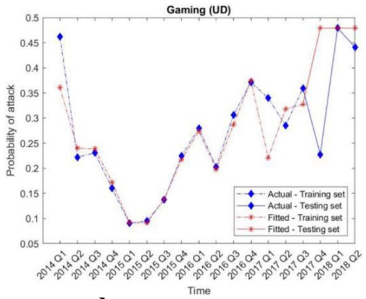

**g Probability estimates from FNN for monthly SSDPFlood data**



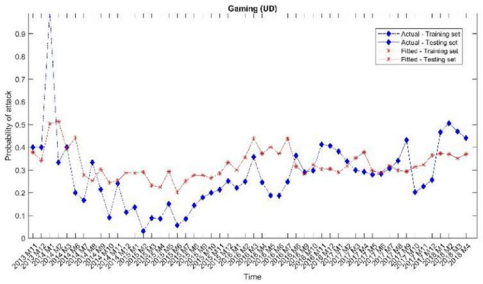

**c Probability estimates from FNN for quarterly UC data**



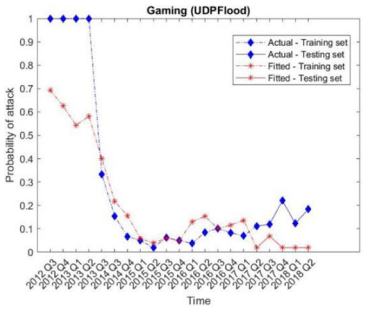

**h Probability estimates from FNN for monthly UC data**



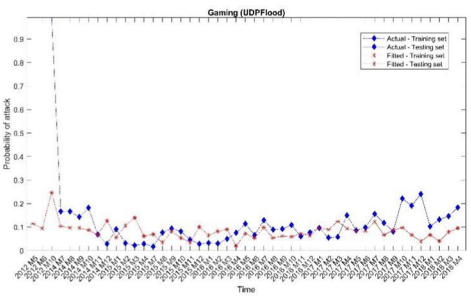

**d Probability estimates from FNN for quarterly UD data**




**i Probability estimates from FNN for monthly UD data**




**e Probability estimates from FNN for quarterly UDPFlood data**




**j Probability estimates from FNN for monthly UDPFlood data**

◂**Fig. 6** **a** Probability estimates from FNN for quarterly NTPFlood data. **b** Probability estimates from FNN for quarterly SSDPFlood data. **c** Probability estimates from FNN for quarterly UC data. **d** Probability estimates from FNN for quarterly UD data. **e** Probability estimates from FNN for quarterly UDPFlood data. **f** Probability estimates from FNN for monthly NTPFlood data. **g** Probability estimates from FNN for monthly SSDPFlood data. **h** Probability estimates from FNN for monthly UC data. **i** Probability estimates from FNN for monthly UD data. **j** Probability estimates from FNN for monthly UDPFlood data

**Table 10** Weibull parameter estimates for risk distribution

| Attack type | a | b | Mean | Std. Dev. |
|---|---|---|---|---|
| NTPFlood | 0.24 | 3.99 | 0.22 | 0.004 |
| SSDPFlood | 0.26 | 2.05 | 0.23 | 0.014 |
| UC | 0.27 | 2.63 | 0.24 | 0.010 |
| UD | 0.31 | 2.51 | 0.28 | 0.014 |
| UDPFlood | 0.19 | 0.92 | 0.20 | 0.047 |

a = Shape parameter, b = Scale parameter

Positively skewed distribution hints at the long-tail nature of expected losses. Such distributions have a large number of smaller amounts of expected losses and a very small number of larger expected loss amounts. Thus, DDoS attacks with smaller impacts occur relatively frequently, while severe DDoS attacks are a rarity. The impact of a less frequent attack can accumulate over time and result in massive losses (Peng et al., 2007).

### 6.3 Cyber-risk Mitigation

Figure 9 depicts the risk-severity heat matrix for each kind of DDoS attack. Each ordered pair on the heat matrix represents the computed probability (p) as computed by the cyber-risk assessment module and expected loss (E(L)), as calculated by the cyber-risk quantification module. Our model will help the CTO accept, reduce, or transfer cyber-risk to a cyber-insurer (Kesan et al., 2013; Kunreuther, 1997; Rejda, 2007). UDPFLood attacks are in the high risk-high severity quadrant, with high expected losses, while most other attacks are in the low-low quadrant, with low expected losses. Enterprises at risk for UDPFlood attacks should consider implementing self-protection. Technological interventions such as stringent firewalls or intrusion detection systems or divert excess or illegitimate traffic to backup servers or content delivery networks (CDNs) will decrease the probability of UDPFlood DDoS attacks and thus lower expected losses. Besides, enterprises can subscribe to cyber-insurance policies to move into the low-low quadrant. Attack records in the High-Low and Low-High quadrants should decide between cyber-insurance or self-insurance depending upon the budgets for absorbing losses and preference over insurance premiums.

## 7 Discussion

This study focuses on the cyber-risk management of DDoS attacks in the MMOG industry. The MMOG industry has faced 74% of the total attacks in 2018-2019 (McKeay, 2017). Gaming firms not only suffer monetary losses due to disrupted gameplay, but cyber-attacks damage their reputation amongst end-users, who have scalability, low latency, and immersive experience as the top demands (Wu & Hsu, 2018). The model proposed in the paper consists of three stages (or modules). The first stage of the framework deals with the cyber-risk assessment. We have used Feedforward neural network (Han et al., 2017) to compute the probability of each kind of DDoS attack. Newer vulnerabilities in the software and hardware make it difficult to compute the proportion of attacks. Our model incorporates attack features along with vulnerability counts and severity. On average, it takes 180 days for a vulnerability to be publicly disclosed by an agency such as CERT (Ransbotham et al., 2012). Thus, hackers can exploit the vulnerabilities from the previous quarter and launch zero-day attacks based on the currently exposed vulnerabilities. Therefore, our model incorporates the independent variables from the previous quarter, improving its accuracy. We also include the interaction effect of the dependence of vulnerabilities trends over time. Neural networks can fit non-linear functions over data efficiently, making them indispensable for computing the probability of attacks for ever-changing attack features (Han et al., 2017). This module can be extended to other industries where high real-time performance and service quality are desired (Wu & Hsu, 2018).

The second stage of the framework quantifies losses for each kind of DDoS attack. We calculate quarterly losses for each DDoS type in the MMOG industry. The severity of the attacks also depends on their probability of occurrence. Thus, expected losses for each DDoS type provide a better estimation of the financial impact of these attacks (Mukhopadhyay et al., 2019). The expected loss distribution follows gamma distribution as they are positively skewed and long-tailed (Dutta & Perry, 2011).

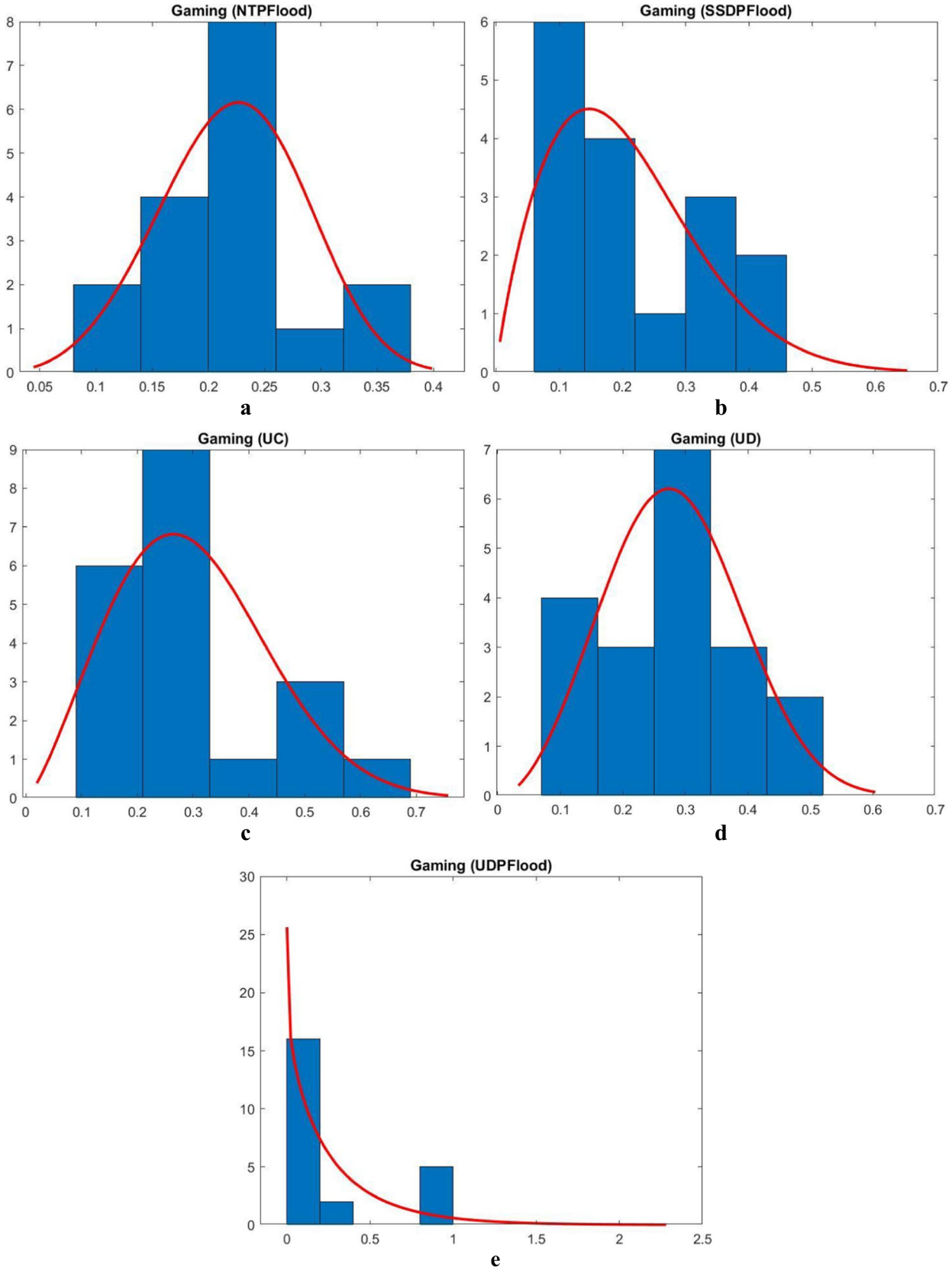



**Fig. 7** **a** Weibull distribution for NTP. **b** Weibull distribution for SSDP. **c** Weibull distribution for UC. **d** Weibull distribution for UD. **e** Weibull distribution for UDP Flood

**Table 11** Expected Loss for the testing dataset

| Year and quarter | NTP Flood | SSDP Flood | UC | UD | UDP Flood |
|---|---|---|---|---|---|
| 2017 Q3 | –* | –* | 2.00 | –* | 2.12 |
| 2017 Q4 | 2.17 | 0.61 | 1.60 | 2.80 | 1.29 |
| 2018 Q1 | 1.26 | 0.53 | 1.27 | 2.74 | 1.07 |
| 2018 Q2 | 1.18 | 0.44 | 0.98 | 2.00 | 1.16 |

* included in the training dataset

**Table 12** Gamma parameter estimates for expected loss distribution

| Attack type | a | b | Mean | Std. Dev. |
|---|---|---|---|---|
| NTPFlood | 2.06 | 1.02 | 2.10 | 2.14 |
| SSDPFlood | 4.66 | 0.47 | 2.18 | 1.02 |
| UC | 5.61 | 0.33 | 1.83 | 0.60 |
| UD | 3.56 | 0.63 | 2.23 | 1.39 |
| UDPFlood | 0.72 | 2.98 | 2.15 | 6.39 |

The third stage of the framework suggests ways to mitigate cyber-risk. CTOs of the MMOG firms have a crucial task in choosing mitigation strategies that do not bleed into profits and assures appropriate risk hedging when under cyber-attacks. In this study, we suggest four risk classes under which we have mapped different DDoS attack records. Attacks under high risk and high severity scenarios have to reduce their cyber-risk by subscribing to self-protection (Böhme & Kataria, 2006; Johansmeyer, 2021; Mukhopadhyay et al., 2019). Self-protection entails developing systems such as firewalls, backup CDNs, and intrusion detection systems. Attacks falling in high risk-low severity or low risk-high severity have a choice between self-insurance and cyber-insurance. They have to choose between the two substitutes depending upon the availability of budget, and in comparison, they will have to pay otherwise to the risk premium. Low risk-low severity attacks can straightaway subscribe to cyber-insurance because risk premiums are within acceptable limits for the range of risk values they bore. The extreme risk class (Hi-Hi) has to treat self-protection and cyber-insurance as compliments (Kesan et al., 2013; Majuca et al., 2006; Rejda, 2007). The practice of subscribing to SI or CI disciplines the internal working of product development teams. It coerces them to be mindful of cybersecurity flaws and vulnerabilities that might otherwise make it susceptible to attacks (Austin & Darby, 2003).

We contribute to the academic discussion by suggesting a novel variable and framework for cyber-risk management in the MMOG industry. Our study is one of the first studies to quantify and mitigate cyber-risk in MMO games using feedforward neural networks. The proposed model uses both attack-specific and MMOG platform-specific traits in quantifying cyber-risk. We also introduce novel variables incorporating a decreasing trend in vulnerabilities due to cybersecurity spending for quantifying cyber-risk. Lastly, we suggest cyber-insurance coupled with self-protection as a viable method to mitigate cyber-risk in the MMOG industry due to DDoS attacks.

MMOG firms value latency, scalability, and brand reputation as drivers of revenue. Our study has the following managerial implications. First, it provides CTOs with a tool with easy-to-understand steps and actionable insights in the form of cyber-risk management to mitigate DDoS attacks in the MMOG industry. The $2 \times 2$ cyber-risk mitigation heat-matrix provides exact mitigation steps along with probable investment strategies. Thus, managers could gauge whether the firm needs to invest in technology, cyber-insurance, or both. These mitigation strategies will discourage the hackers from causing financial loss to the firm and increase customer confidence in the authenticity of MMOG firms' offerings.

The current study is limited by the use of a proxy for cybersecurity spending. The MMOG firms strategically guard the actual data about the cybersecurity budget, and thus, its availability would improve the model's accuracy. We have used anonymized cyber attack data; therefore, firm-level variables do not form part of the model. Better datasets with firm-level details will improve the accuracy and validity of the model further. Using alternate data sources such as hacker forums and online gaming community discussions can help predict imminent DDoS attacks by incorporating a sliver of hacker behavior.

## 8 Conclusions

In this study, we estimate the probability of different DDoS attacks happening in the MMOG industry. We use a Feed-forward Neural Network to compute the proportion of each kind of DDoS attack. We also investigate which probability distribution best approximates the risk values in each DDoS attack type. Next, we use principles of risk analysis

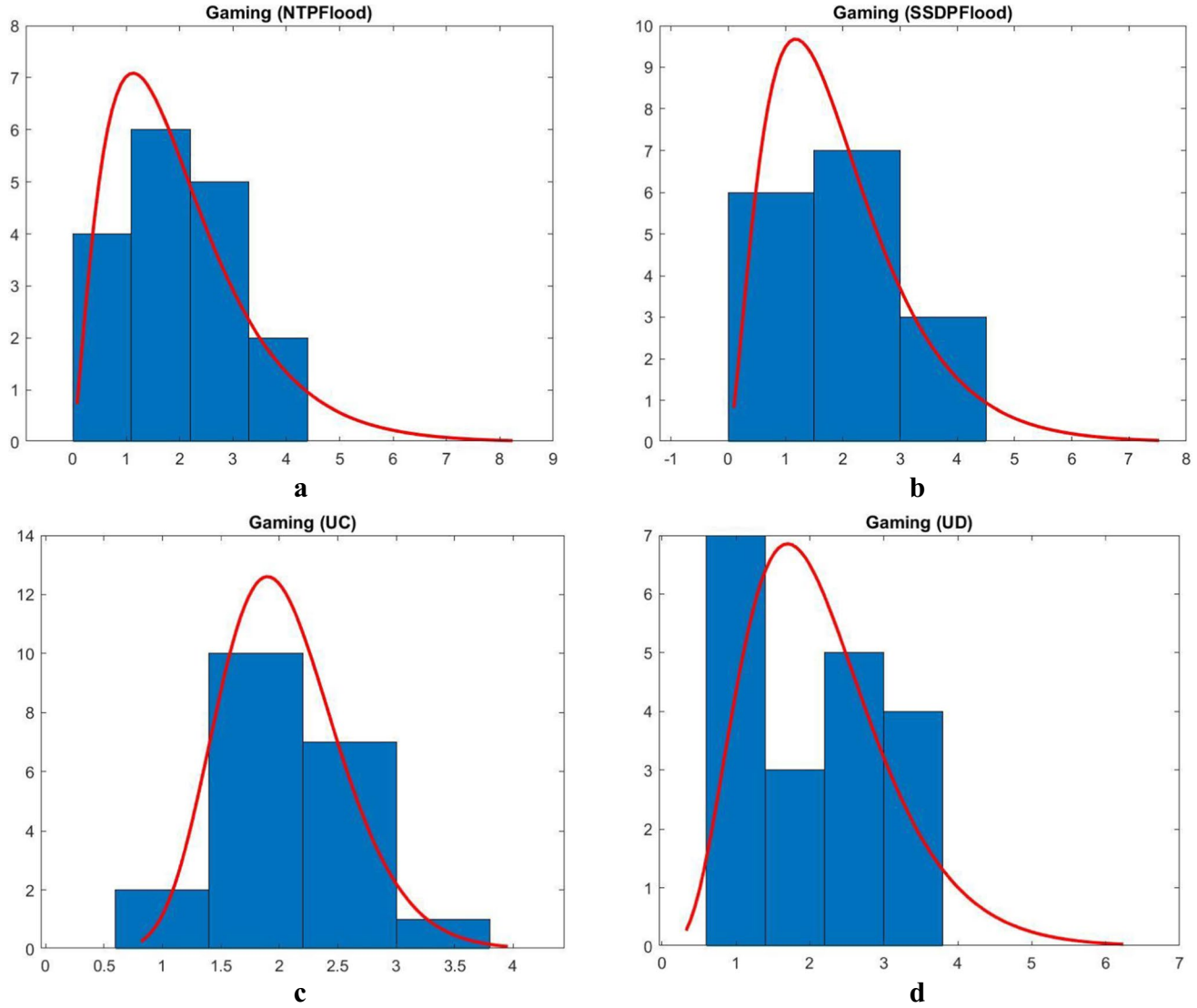



**Fig. 8** **a** E(L): Gamma distribution for NTP Flood. **b** E(L): Gamma distribution for SSDP Flood. **c** E(L): Gamma distribution for UC. **d** E(L): Gamma distribution for UD

and calculate the expected loss values for these attacks and the probability distribution that fits. The last stage of the study uses risk (i.e., probability of an attack) and severity (i.e., expected loss of attacks) to suggest ways to mitigate cyber-risk. Cyber-insurance is advisable to firms who have DDoS attacks with low risk as well as low severity. We advise that MMOG firms with high risk and high severity attacks should subscribe to cyber-insurance after implementing self-protection. This study contributes by incorporating novel variables related to cybersecurity spending and vulnerabilities, enabling DDoS attacks.

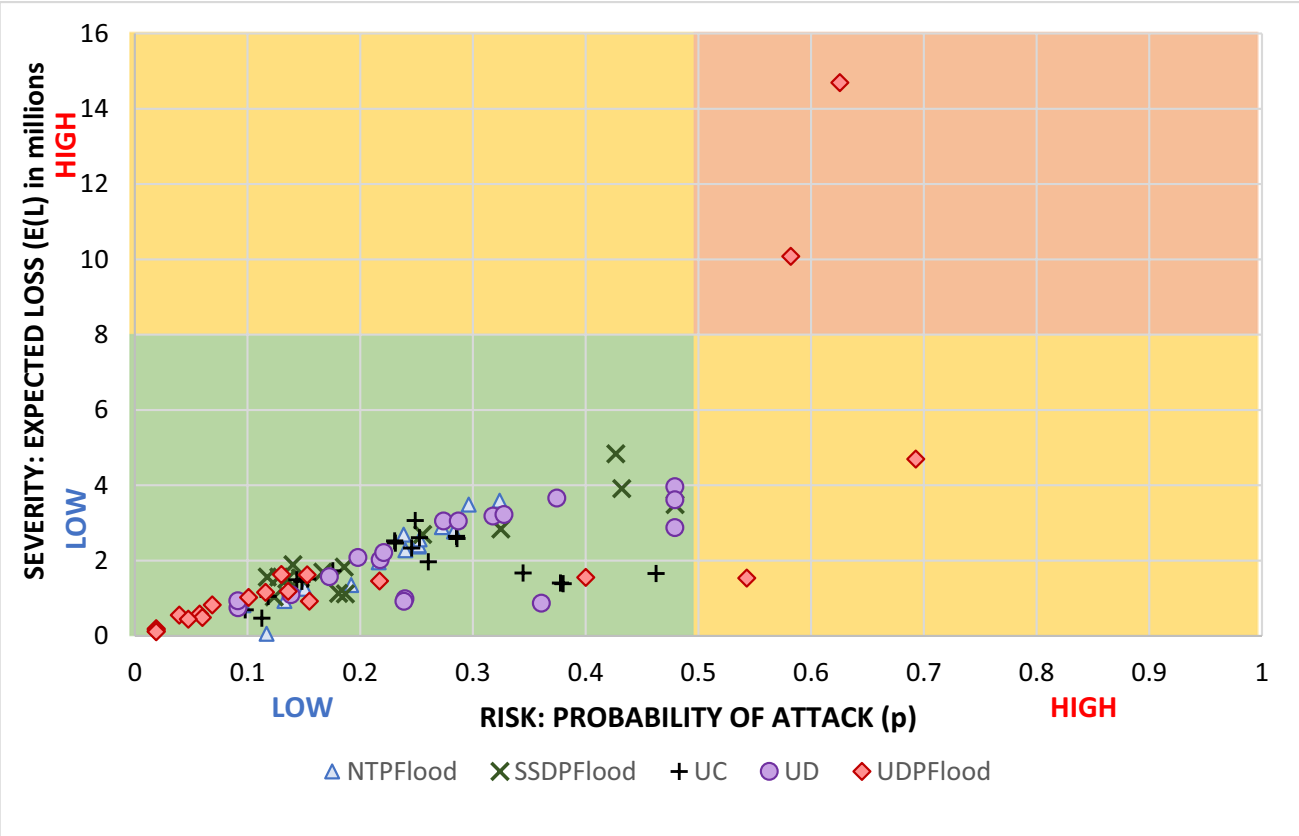



**Fig. 9** Risk-severity heat matrix

## Declarations

**Conflict of Interest** The authors declare that there is no conflict of interest.

## References


Alberts, C., & Dorofee, A. (2002). *Managing Information Security Risks*, Pearson Education (US). https://www.ebook.de/de/product/3252338/christopher_alberts_audrey_dorofee_managing_information_security_risks.html. Accessed 12 Oct 2021

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. https://doi.org/10.1016/j.cose.2006.10.002

Allende, H., Moraga, C., & Salas, R. (2002). Artificial neural networks in time series forecasting: a comparative analysis. *Kybernetika* (88), 685–707

Arora, A., Telang, R., & Xu, H. (2008). Optimal policy for software vulnerability disclosure. *Management Science, (54*(4), 642–656. https://doi.org/10.1287/mnsc.1070.0771

Austin, R. D., & Darby, C. A. R. (2003). The myth of secure computing. *Harvard Business Review* (81:6), Harvard Business School Publication Corp., pp. 120–126

Avital, N., Zawoznik, A., Azaria, J., & Lambert, K. (2020). 2019 Global DDoS Threat Landscape Report: Imperva. *Imperva Blog*, Imperva, February. https://www.imperva.com/blog/2019-global-ddos-threat-landscape-report/. Accessed 12 Oct 2021

Balkanli, E., Zincir-Heywood, N., A., & Heywood, M. I. (2015). Feature selection for robust backscatter DDoS detection. In *Proceedings - Conference on Local Computer Networks, LCN* (Vol. 2015-Decem), IEEE, October, pp. 611–618. https://doi.org/10.1109/LCNW.2015.7365905

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. https://doi.org/10.1145/1592761.1592780

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR), 25*(4), 375–414. https://doi.org/10.1145/162124.162127

Becker, G. (1990). *The Economic Approach to Human Behavior*. University of Chicago Press

Bezsonoff, N. (2017). The state of DDoS attacks in 2017: neustar blog. *The State of DDoS Attacks in 2017 | Neustar Blog*, Neustar, October. https://www.home.neustar/blog/neustar-global-attacks-and-cyber-security-insight-report. Accessed 12 Oct 2021

Biswas, B., & Mukhopadhyay, A. (2017). Phishing detection and loss computation hybrid model: a machine-learning approach. *ISACA Journal* (1), 22–29. https://www.isaca.org/Journal/archives/2017/Volume-1/Pages/phishing-detection-and-loss-computation-hybrid-model.aspx. Accessed 12 Oct 2021

Biswas, B., & Mukhopadhyay, A. (2018). G-RAM framework for software risk assessment and mitigation strategies in organisations. *Journal of Enterprise Information Management, 31*(2), 276–299. https://doi.org/10.1108/JEIM-05-2017-0069

Biswas, B., Mukhopadhyay, A., Bhattacharjee, S., Kumar, A., & Delen, D. (2021). A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums. *Decision Support Systems*, 113651. https://doi.org/10.1016/j.dss.2021.113651

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

Biswas, B., Mukhopadhyay, A., & Gupta, G. (2018). 'Leadership in Action: How Top Hackers Behave' A big-data approach with text-mining and sentiment analysis. In *Proceedings of the 51st Hawaii International Conference on System Sciences*. https://doi.org/10.24251/hicss.2018.221

Biswas, B., Pal, S., & Mukhopadhyay, A. (2016). AVICS-eco framework: an approach to attack prediction and vulnerability assessment in a cyber ecosystem. In *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*

Blau, A., Burt, A., Groysberg, B., & Yampolskiy, R. V. (2019). *Cybersecurity*, Harvard Business Review Press. https://www.ebook.de/de/product/35460600/harvard_business_review_alex_blau_andrew_burt_boris_groysberg_roman_v_yampolskiy_cybersecurity.html. Accessed 12 Oct 2021

Böhme, R. (2005). Cyber-Insurance Revisited. In *Workshop on the Economics of Information Security (WEIS)*, Harvard

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

Böhme, R., & Schwartz, G. (2006). Models and measures for correlation in cyber-insurance. *2006 Workshop on the Economics of Information Security (WEIS)*, pp. 1–26

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly: Management Information Systems, (39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Brown, J. (2016). How amazon responded to the Dyn DDoS attack. *CIO Dive*, October. https://www.ciodive.com/news/how-amazon-responded-to-the-dyn-ddos-attack/429050. Accessed 12 Oct 2021

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems* (34:SPEC. ISSUE 3), pp. 523–548. https://doi.org/10.2307/25750690

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Campbell, P. L., & Stamp, J. E. (2004). A Classification scheme for risk assessment methods. Sandia National Laboratories, Sandia Report

Cavusoglu, H., Cavusoglu, H., & Jun, Z. (2008). Security patch management: share the burden or share the damage? *Management Science* (54:4), INFORMS, pp. 657–670. https://doi.org/10.1287/mnsc.1070.0794

Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. (2009). Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems. *Information Systems Research, (20*(2), 198–217. https://doi.org/10.1287/isre.1080.0180

CCTA (1991). SSADM-CRAMM subject guide for SSADM Version 3 and CRAMM Version 2, London

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review, (44,* 4. https://doi.org/10.2307/2094589

Courtney, R. H. (1977). Security risk assessment in electronic data processing systems. In *AFIPS Conference Proceedings - 1977 National Computer Conference, AFIPS 1977*, pp. 97–104. https://doi.org/10.1145/1499402.1499424

Das, S., Mukhopadhyay, A., Saha, D., & Sadhukhan, S. (2019). A Markov-Based Model for information security risk assessment in healthcare MANETs. *Information Systems Frontiers, (21*(5), 959–977. https://doi.org/10.1007/s10796-017-9809-4

Desai, V. S., & Bharati, R. (1998). A comparison of linear regression and neural network methods for predicting excess returns on large stocks. *Annals of Operations Research, (78,* 0. https://doi.org/10.1023/A:1018993831870

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125–128. https://doi.org/10.1145/341852.341877

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal, 16*(3), 293–314. https://doi.org/10.1111/j.1365-2575.2006.00219.x)

Dowd, M., McDonald, J., & Schuh, J. (2006). *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*. Addison-Wesley Professional

Dutta, K., & Perry, J. (2011). A tale of tails: an empirical analysis of loss distribution models for estimating operational risk capital. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.918880

Geurts, M., Box, G. E. P., & Jenkins, G. M. (1977). Time series analysis: forecasting and control. *Journal of Marketing Research, 14*. Wiley. https://doi.org/10.2307/3150485

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. *Communications of the ACM, 46*(3), 81–85, ACM. https://doi.org/10.1145/636772.636774

Gough, C. (2019). MMO Gaming - Statistics & Facts. https://www.statista.com/topics/2290/mmo-gaming/. Accessed 12 Oct 2021

Guarro, S. B. (1987). Principles and procedures of the LRAM approach to information systems risk analysis and management. *Computers and Security, 6*(6), 493–504, Elsevier. https://doi.org/10.1016/0167-4048(87)90030-7

Gujarati, D. (2009). *Basic Econometrics*. McGraw-Hill Irwin

Hagan, M. T., H. B. Demuth, M. H. Beale and O. De Jesús (2014). Neural Network Design, Martin Hagan

Han, J., Kamber, M., & Pei, J. (2017). *Data Mining: Concepts and Techniques*. Elsevier LTD

Herath, H. S. B., & Herath, T. C. (2011). Copula-based actuarial model for pricing cyber-insurance policies. *Workshop on the Economics of Information Security, 2,* 1

Hoffman, L. J., Michelman, E. H., & Clements, D. (1978). Securate - Security evaluation and analysis using fuzzy metrics.. In *AFIPS Natl Comput Conf Expo Conf Proc*, Vol. 47, 531–540

Hossack, I. B., Pollard, J. H., & Zehnwirth, B. (1999). Introductory statistics with applications in general insurance. *Introductory Statistics with Applications in General Insurance*. https://doi.org/10.1017/cbo9781139173322

Johansmeyer, T. (2021). Cybersecurity insurance has a big problem. *Harvard Business Review*, Harvard Business Review. https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem. Accessed 12 Oct 2021

Kannan, K., & Telang, R. (2005). Market for software vulnerabilities? Think again. *Management Science, 51*(5), 726–740. https://doi.org/10.1287/mnsc.1040.0357

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information Security Risk Analysis Method. *Computers & Security, 24*(2), 147–159. https://doi.org/10.1016/j.cose.2004.07.004

Kelleher, J. D., & Tierney, B. (2018). *Data Science*. MIT Press Ltd. https://www.ebook.de/de/product/30073177/john_d_academic_leader_of_the_information_communication_and_entertainm

ent_research_institute_technological_university_dublin_kelleher_brendan_lecturer_at_the_school_of_computing_dublin_institute_of_technology_tierney_data_science.html. Accessed 12 Oct 2021

Kesan, J. P., Majuca, R., & Yurcik, W. (2005). Cyberinsurance as a market-based solution to the problem of cybersecurity - a case study. In *Fourth Workshop on the Economics of Information Security* (Vol. 2), pp. 97–120

Kesan, J., Yurcik, W., & Majuca, R. P. (2013). The economic case for cyberinsurance. *Dissent* (Vol. Aut / Win)

Kleindorfer, P. R., & Kunreuther, H. (1999). The complementary roles of mitigation and insurance in managing catastrophic risks. *Risk Analysis*. https://doi.org/10.1023/A:1007097906602

Krohn, J., Beyleveld, G., & Aglae, B. (2019). Deep learning illustrated: a visual, interactive guide to artificial intelligence. *Addison-Wesley Professional* (Vol. 53), Addison Wesley Pub Co Inc. https://www.ebook.de/de/product/33154294/jon_krohn_grant_beyleveld_aglae_bassens_deep_learning_illustrated_a_visual_interactive_guide_to_artificial_intelligence.html. Accessed 12 Oct 2021

Kunreuther, H. (1997). Managing catastrophic risks through insurance and mitigation. In *5th Alexander Howden Conference on "Financial Risk Management for Natural Catastrophes"*, Gold Coast, Australia, pp. 1–31. https://core.ac.uk/download/pdf/6649681.pdf

Levenberg, K. (1944). A method for the solution of certain non-linear problems in least squares. *Quarterly of Applied Mathematics, 2*(2), 164–168. https://doi.org/10.1090/qam/10666

Liu, D., Li, X., & Santhanam, R. (2013). Digital games and beyond: what happens when players compete? *MIS Quarterly: Management Information Systems, 37*(1), 111–124. https://doi.org/10.25300/MISQ/2013/37.1.05

Majuca, R. P., Yurcik, W., & Kesan, J. P. (2006). *The Evolution of Cyberinsurance*. http://arxiv.org/abs/cs/0601020. Accessed 12 Oct 2021

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology* (28:1), Annual Reviews 4139 El Camino Way, PO Box 10139, Palo Alto, CA 94303-0139, USA, pp. 417–442

McKeay, M. (2017). Q4 2017 State of the Internet Security Report. *Akamai Technologies*. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf. Accessed 12 Oct 2021

Mukhopadhyay, A., Chakrabarti, B. B., Saha, D., & Mahanti, A. (2007). E-risk management through self insurance: an option model. In *Proceedings of the Annual Hawaii International Conference on System Sciences*, IEEE. https://doi.org/10.1109/HICSS.2007.192

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber Risk Assessment and Mitigation (CRAM) framework using logit and probit models for cyber insurance. *Information Systems Frontiers, 21*(5), 997–1018. https://doi.org/10.1007/s10796-017-9808-5

Nguyen, D., & Widrow, B. (1990). Improving the learning speed of 2-layer neural networks by choosing initial values of the adaptive weights. In *IJCNN. International Joint Conference on Neural Networks* (pp. 21–26). IEEE. https://doi.org/10.1109/ijcnn.1990.137819

O'Reilly, P. D., Rigopoulos, K., Witte, G., & Feldman, L. (2018). 2017 Annual Report: NIST/ITL Cybersecurity, & Program. Gaithersburg, MD, September. https://doi.org/10.6028/NIST.SP.800-203

Ozier, W. (1989). Risk quantification problems and bayesian decision support system solutions. *Information Age* (11:4). Westbury Subscription Services, pp. 229–234. http://dl.acm.org/citation.cfm?id=69134.69141. Accessed Oct 2021

Nelder, J. A. (1989). *Generalized Linear Models*. Taylor & Francis Ltd. https://www.ebook.de/de/product/3601523/p_university_of_chicago_chicago_illinois_usa_mccullagh_john_a_imperial_college_london_uk_nelder_generalized_linear_models.html. Accessed 12 Oct 2021

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys, 39*(1), 3. https://doi.org/10.1145/1216370.1216373

Ransbotham, S., Mitra, S., & Ramsey, J. (2012). Are markets for vulnerabilities effective? *MIS Quarterly, 36*(1), 43. https://doi.org/10.2307/41410405

Rejda, G. E. (2007). *Principles of Risk Management and Insurance, 10th Edition*, Pearson

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems, 34*(4), 1023–1053. https://doi.org/10.1080/07421222.2017.1394049

Shahriar, H., & Zulkernine, M. (2012). Mitigating program security vulnerabilities. *ACM Computing Surveys, 44*(3), 1–46. https://doi.org/10.1145/2187671.2187673

Shani, T., & Imperva (2019). *Imperva*, June. https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/. Accessed 12 Oct 2021

Sharma, K., & Mukhopadhyay, A. (2020a). Cyber risk assessment and mitigation using logit and probit models for DDoS attacks. In *26th Americas Conference on Information Systems (AMCIS), 2020*, Salt Lake City

Sharma, K., & Mukhopadhyay, A. (2020b). Assessing the risk of cyber-attacks in the online gaming industry: a data mining approach. *ISACA Journal* (2)

Smith, D. (2014). Why hacker gang 'Lizard Squad' took down Xbox live and playstation network. *Business Insider*, December. http://www.businessinsider.com/why-hacker-gang-lizard-squad-took-down-xbox-live-and-playstation-network-2014-12. Accessed 12 Oct 2021

Smith, E., & Eloff, J. H. P. (2002). A prototype for assessing information technology risks in health care. *Computers & Security, 21*(3), 266–284. https://doi.org/10.1016/s0167-4048(02)00313-9

Stolen, K., Braber, F., den, Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S. H. … Aagedal, J. O. (2002). *Model-Based Risk Assessment-the CORAS Approach*

Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks*, (5th ed.), Pearson. https://www.amazon.com/Computer-Networks-5th-Andrew-Tanenbaum/dp/0132126958?SubscriptionId=AKIAIOBINVZYXZQZ2U3A&tag=chimbori05-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=0132126958. Accessed 12 Oct 2021

Tripathi, M., & Mukhopadhyay, A. (2020). Financial Loss Due to a Data Privacy Breach: an empirical analysis. *Journal of Organizational Computing and Electronic Commerce*, *30*(4), 381–400. https://doi.org/10.1080/10919392.2020.1818521

Wang, M., Lu, Y., & Qin, J. (2020). A dynamic MLP-based DDoS attack detection method using feature selection and feedback. *Computers & Security*, *88*, 101645. https://doi.org/10.1016/j.cose.2019.101645

Wu, S. L., & Hsu, C. P. (2018). Role of authenticity in Massively Multiplayer Online Role Playing Games (MMORPGs): determinants of virtual item purchase intention. *Journal of Business Research, 92,* 242–249. https://doi.org/10.1016/j.jbusres.2018.07.035

Yahyavi, A., & Kemme, B. (2013). Peer-to-peer architectures for massively multiplayer online games. *ACM Computing Surveys, 46*(1), 1–51. https://doi.org/10.1145/2522968.2522977

Yue, W. T., Wang, Q. H., & Hui, K. L. (2019). See no evil, hear no evil? Dissecting the impact of online hacker forums. *MIS Quarterly:*

*Management Information Systems, 43*(1), 73–95. https://doi.org/10.25300/MISQ/2019/13042

Zhang, Z., Nan, G., & Tan, Y. (2020). On-premises software: competition under security risk and product customization. Information systems research articles in advance. *Information Systems Research*, 1–17. https://doi.org/10.1287/isre.2019.0919

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

**Kalpit Sharma** is a Doctoral student at theIndian Institute of Management (IIM) Lucknow. He has published articles injournals and conferences of international repute, including Americas Conferenceon Information Systems (AMCIS), Pre-International Conference On InformationSystems (ICIS) workshops, Journal of Organizational Computing and ElectronicCommerce, and ISACA Journal. His research interests include cyber-risk issuesin information systems, the economics of cybersecurity, healthcare IT, ITgovernance, and crowd-based digital business models.

**ArunabhaMukhopadhyay** is a Professor of Information Technology & Systems Area at the Indian Institute of Management Lucknow (IIM Lucknow). He has obtained his Ph.D.and Post Graduate Diploma in Business Management (PGDBM) from the IndianInstitute of Management Calcutta (IIM Calcutta) in Management InformationSystems. He has published in various refereed journals and conferences,including Decision Support Systems (DSS), Information Systems Frontier (ISF),Journal of Organizational Computing and E-commerce (JOCEC), Journal of GlobalInformation Technology Management (JGITM), JIPS, International Journal ofInformation Systems and Change Management (IJISCM), Decision, IIMB Review,Hawaii International Conference on System Sciences (HICSS), Americas Conferenceon Information Systems (AMCIS), Pre-International Conference On InformationSystems (ICIS) workshops, Global Information Technology Management Association(GITMA), Conference of Information Systems and Technology Management (CISTM),International Conference on E-Governance (ICEG). He is the recipient of theBest Teacher in Information Technology Management award in 2013 and 2011, bythe Star-DNA group B-School Award and the 19th Dewang Mehta Business SchoolAward, 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), TelemedicineSociety of India (TSI), Indian Insurance Institute (III), Actuarial Society ofIndia (ASI), All India Management Association (AIMA), System Dynamics Societyof India (SDSI) and, Operations Research Society of India (ORSI).