ANN model for cyber-risk management for DDoS attacks in Massively Multiplayer Online Gaming

Kalpit Sharma
Doctoral Student
Indian Institute of Management Lucknow
fpm18012@iiml.ac.in

Arunabha Mukhopadhyay
Professor
Indian Institute of Management Lucknow
arunabha@iiml.ac.in

Extended 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$ 120K to US$ 2M for each incident. Apart from the monetary loss, they also disrupt service quality and damage brand reputation for 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. In this study, we aim to estimate the probability of each kind of DDoS attack and the expected loss associated with them. We use an artificial neural network to predict the probability of DDoS attacks. Besides DDoS attack features, we also use vulnerability data and its trend to improve the model's predictability. We ascertain the distribution of risk and expected loss values, thus, computed. Subsequently, we suggest ways to mitigate the cyber-risk by aiding the CTO of MMOG firms to accept, reduce, or pass cyber-risk.

Keywords

DDoS, MMOG, Cyber-risk, Neural Network, Cyber-insurance

ANN model for cyber-risk management for DDoS attacks in Massively Multiplayer Online Gaming

Introduction

Distributed Denial of Service (DDoS) attacks aim at disrupting legitimate users' access to shared cyber-resources for a firm or group of firms. One of its simpler variants, Denial of Service (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. The second type is more potent due to its harming the network services and disrupting larger Internet regions. 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 of software vulnerabilities, the second form is challenging to prevent (Peng et al. 2007).

This study focuses on recent variant DoS attacks, distributed in their execution, and thus named DDoS attacks. The distributed nature of these attacks increases the attack surface and makes it difficult to trace. Hackers install malicious botnets on unsuspecting end-users' systems and convert it into a "zombie" machine. The "zombies" launch illegitimate traffic to a target machine, mixed with its usual data traffic, in the background. Mirai botnet is one such popular method amongst hackers in recent times. This method of launching DDoS attacks make 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 (Peng et al. 2007).

The impact of DDoS attacks might range from temporary website outage to substantial financial losses to firms dependent on real-time high-level service quality (e.g., E-Commerce, Entertainment, BFSI, etc.). DDoS attack mitigation is not spontaneous, and delays result in further losses. On average, the DDoS attack lifecycle, from attack to recovery, ranges from a few hours to several months. In 2018, firms lost between US$ 120K to US$ 2M due to DDoS attacks. An unnamed streaming service lost US$ 0.5 million per hour of a 2-week long DDoS attack by the next year. According to Akamai, the online gaming industry witnesses 74% of the total attacks recorded by their security provider service. The BFSI, entertainment, and e-commerce firms are the next big targets for hackers as the number of losses is enormous for these industries. In 2019, an unnamed streaming application enterprise was the target of a two-week-long DDoS attack 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. 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.

Online games have emerged as popular entertainment options, which bring in massive revenues for the makers, along with numerous challenges for developers and end-users alike. A large number of players in online games is one of its essential USPs. Immensely successful games have to continually provide not only scalability but also responsiveness to the end-users. The particular online games type with many users is known as Massively Multiplayer Online Games (MMOGs). Some of the popular MMOGs are Final Fantasy, World of Warcraft, , Elder Scrolls, Star Wars Online, Guild Wars, etc. MMOGs produce massive network traffic and overhead processing loads (Liu et al. 2013). The main challenges in the MMOG industry are that of (a) scalability, that is, providing gameplay to millions of users concurrently, (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 and Kemme 2013). The features that make MMOGs popular are the same, which attackers exploit. The large number of 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 this study, the six kinds of DDoS attacks that we analyze for cyber-risk exploit different IT assets and deny access to various IT ecosystem components. DDoS attacks chiefly disrupt the "availability" aspect of the CIA triad, but hackers may also tamper with information, steal credentials, etc., amidst the confusion of the DDoS attacks. Hackers use Character Generation protocol to flood the local machine through peripheral devices. Similarly, they compromise Universal Plug and Play (UPnP) ports by exploiting UPnP vulnerabilities to inundate the local client with illegitimate traffic. In some DDoS attacks such as DNS Flood and UDP Flood, attackers tamper with remote servers (e.g., DNS cache server) to deny users access to further browsing by disrupting the domain name translation process. The more dangerous variant of DDoS is NTP Flood. It uses Network Time Protocol to pump vast traffic through network edges and, thus, to congest and render it inaccessible to legitimate users.

Proposed Model

Table 1 tabulates different variables used as predictors in the proposed model, along with relevant literature support. While Figure 1 depicts the proposed model for this study.

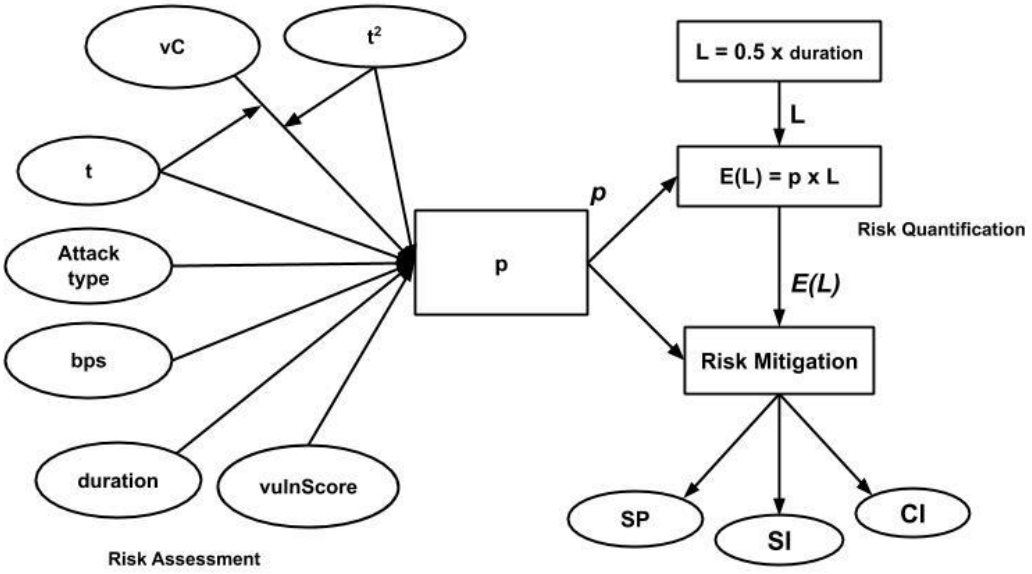


Figure 1: Proposed Model for cyber-risk management in the MMOG industry

vC = Vulnerability count, t = Time, SP = Self-protection, SI = Self-insurance, CI = Cyber-insurance

Table 1: Model variables and relevant literature support

Variables	Literature
Attack type	(McKeay 2017; Peng et al. 2007; Wang et al. 2020)
bps	(Peng et al. 2007; Tanenbaum and Wetherall 2010; Wang et al. 2020; Zhang et al. 2020)
duration	(Peng et al. 2007; Tanenbaum and Wetherall 2010; Wang et al. 2020; Zhang et al. 2020)
Vulnerability Score (vulnScore)	(Arora et al. 2008; Kannan and Telang 2005; Peng et al. 2007; Ransbotham et al. 2012; Shahriar and Zulkernine 2012; Zhang et al. 2020)
Vulnerability count (vC)	(Arora et al. 2008; Kannan and Telang 2005; Peng et al. 2007; Ransbotham et al. 2012; Shahriar and Zulkernine 2012; Zhang et al. 2020)
Time (t, t^2)	(Biswas and Mukhopadhyay 2018; Mukhopadhyay et al. 2019)
vC/t	(Cavusoglu et al. 2008, 2009; Ransbotham et al. 2012)
vC/t^2	Created for this study
Probability of attack (p)	(Biswas and Mukhopadhyay 2017, 2018; Das et al. 2019; Mukhopadhyay et al. 2019)

Research Questions

RQ1: (a) What is the probability of each kind of DDoS attack compromising the MMOG systems?
(b) Which probability distribution best approximates the occurrence of DDoS attacks in the MMOG industry?

RQ2: (a) What is the expected loss for each type of DDoS attack in the MMOG industry?
(b) What probability distribution best estimates expected loss caused due to each type of DDoS attack in the MMOG industry?

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

Data

We use 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 timestamp, type of attack, indicate the intensity and duration of the attack and the internet protocol used executing 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. We convert attack intensity, that is, the bps attribute, into Gbps (Gigabits per second) and duration in hours to adjust for scale variations. The dataset comprises six different DDoS attacks: CharGEN, DNS Flood, NTP Flood, SSDP Flood, UDP Fragment, and UDP Flood. CharGEN and DNS Flood attacks occur with UDP Fragment attacks in the dataset. Therefore, we label all such records as a new form of attack, namely, UC and UD, respectively. The attack data range from 2012 to 2018.

Methodology

Table 6: Algorithm for Cyber-risk Management

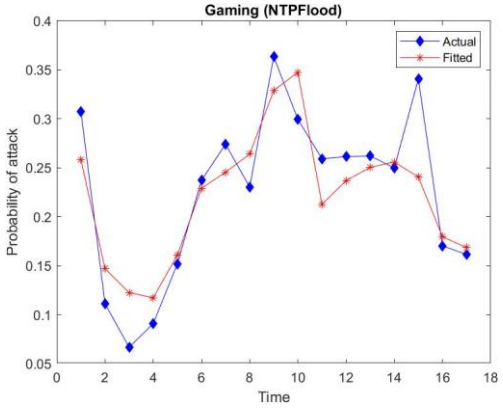
	Cyber-risk Assessment
Step 1	Construct the feature vector X_D = [bps, duration, t, t^2, vulnScore, vC/t, vC/t^2]
Step 2	Split the Dataset (D) into training, validation, and testing datasets in an 80:10:10 ratio.
Step 3	Initialize the weights using the Nguyen-Widrow algorithm.
Step 4	Train the FNN model with the training dataset.
Step 5	Stop training when the validation gradient (MSE) reaches the minimum.
Step 6	p: $\hat{y}$ = predict(FNN, D)
Step 7	Fit Weibull distribution on *p* values
	Cyber-risk Quantification
Step 8	p: $\hat{y}$ = predict(FNN, D)
Step 9	E(L) = p * 0.5 * (duration)
Step 10	Fit a Gamma distribution on *E(L)* values
	Cyber-risk mitigation
Step 11	Propose mitigation strategies *If p =Hi* AND *E(L) = Hi, then* Self-Protection (SP) *Else if p = Hi* AND *E(L) = Lo* OR *p = Lo* AND *E(L) = Hi, then* Self-insurance (SI) *Else if p = Lo* AND *E(L) = Lo, then* Cyber-insurance (CI)

Results

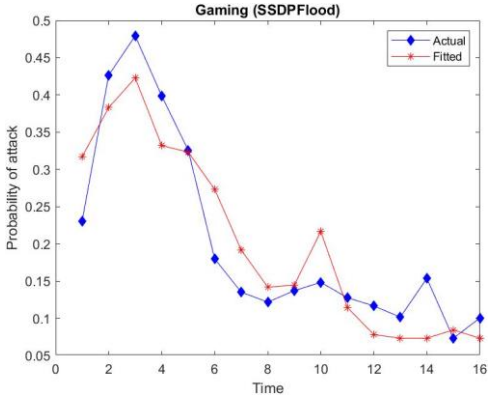
Cyber-risk Assessment

Figure 2 compares the actual probabilities of each DDoS attack and predicted probabilities from the FNN model after training. Table 7 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% (refer Figure 2 (d)). While UC (i.e., the combination of UDP Fragment and CharGEN attack) has the lowest accuracy at 98.76% (refer Figure 2 (c)).

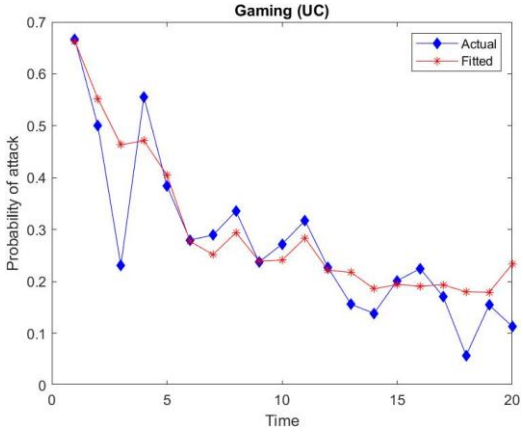
We test our FNN model on the last 10% of the records; thus, the last three quarters for NTPFlood, SSDPFlood, and UD attacks. Similarly, the test dataset comprises the last four quarters for UC and UDPFlood attacks. In all five DDoS attacks, the FNN model correctly predicts the trend in the actual data. Table 8 tabulates the parameter estimates of Weibull distribution for risk values along with mean and standard deviations. UDPFlood attacks have the highest average risk value at 0.30 (refer to Table 8), while SSDPFlood attacks have the lowest average risk values at 0.2 (refer to Table 8).



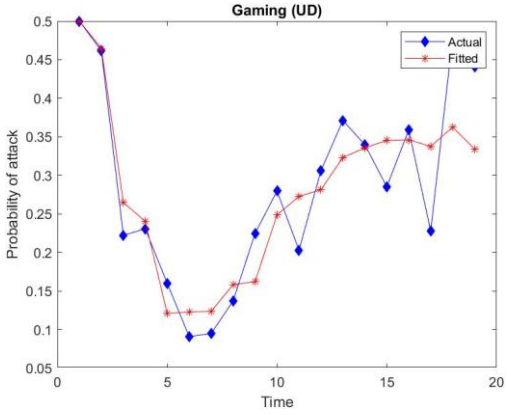
(a) NTP Flood (2017 Q4 to 2018 Q2, t= 16 to 18)



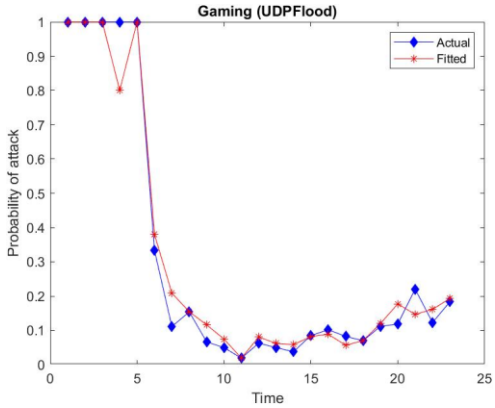
(b) SSDP Flood (2017 Q4 to 2018 Q2, t= 14 to 16)



(c) UC (2017 Q3 to 2018 Q2, t = 17 to 20)



(d) UD (2017 Q4 to 2018 Q2, t = 18 to 20)



(e) UDP Flood (2017 Q3 to 2018 Q2, t = 23 to 25)

Figure 2: Probability estimation using FFN for the MMOG industry

Table 7: Performance Metrics for each attack type on the test dataset

Attack type	ANN Topology	Test accuracy (MSE) (in %)	Test time window
NTPFlood	7-10-1	99.74	2017 Q4 to 2018 Q2
SSDPFLood	7-10-1	99.24	2017 Q4 to 2018 Q2
UC	7-10-1	98.76	2017 Q3 to 2018 Q2
UD	7-10-1	99.76	2017 Q4 to 2018 Q2
UDFlood	7-10-1	99.66	2017 Q3 to 2018 Q2

Table 8: Weibull parameter estimates for risk distribution

Attack type	a	b	Mean	Std. Dev.
NTPFlood	0.24	3.88	0.22	0.004
SSDPFlood	0.23	1.81	0.20	0.014
UC	0.33	2.33	0.29	0.018
UD	0.31	2.92	0.28	0.011
UDPFlood	0.29	0.92	0.30	0.110

a = Shape parameter, b = Scale parameter

Cyber-risk Quantification

Next, we fit gamma distribution on expected loss values. UDPFlood attacks have the highest average expected loss at US$ 3.04 million (refer to Table 9). While SSDPFlood has the lowest average expected loss at US$ 1.93 million (refer to Table 9). Except for UC attacks, all other attacks' expected losses are positively skewed distributions. (Peng et al. 2007).

Table 9: Gamma parameter estimates for expected loss distribution

Attack type	a	b	Mean	Std. Dev.
NTPFlood	2.30	0.86	2.00	1.72
SSDPFlood	2.57	0.75	1.93	1.44
UC	15.23	0.13	2.03	0.27
UD	4.85	0.44	2.14	0.94
UDPFlood	0.73	4.13	3.04	12.54

Cyber-risk Mitigation

Figure 3 depicts the risk-severity heat matrix for each kind of DDoS attacks. UDPFLood attacks are in the high risk-high severity quadrant, with high expected losses, while most other types of attack are in the low-low quadrant, with low expected losses. MMOG enterprises at risk for UDPFlood attacks should consider implementing self-protection. Technological interventions such as scrubbing centers, firewalls, intrusion detection systems, backup servers, or content delivery networks (CDNs) will decrease the probability of UDPFlood DDoS attacks and thus lower expected losses too. Besides, MMOG enterprises can subscribe to cyber-insurance policies to move into the low-low quadrant. Attack records in 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 (Akamai 2015; Das et al. 2019; Kesan et al. 2013, 2005; Rejda 2007).

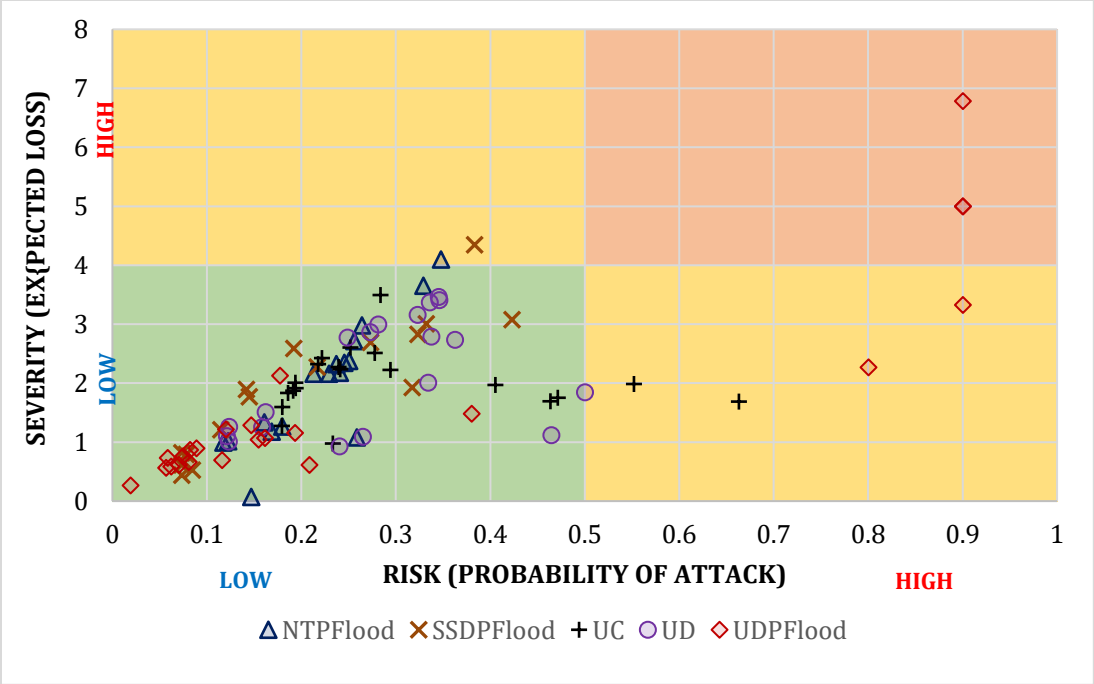


Figure 3: Risk-Severity heat matrix

Conclusion

We contribute to academics by proposing a GLM based model that incorporates cybersecurity spending over time by using vulnerability trends as a proxy. Predictors such as vC/t and vC/t² inform us about whether the cybersecurity spending gets absorbed in the internal functioning (e.g., code development, code review, code testing, etc.) or not. The extent to which aids in removing existing vulnerabilities and preventing new ones is a strong predictor of DDoS attacks' future probability. The use of novel variables also indicates whether unethical enterprises (such as hackers) are discouraged from compromising systems in the future. Lesser vulnerabilities also mean an increase in resources used by hackers to break through the systems. The theoretical framework mentioned earlier states that increased resources or complexity generally discourages hackers from launching such conspicuous attacks.

Managers of MMOG firms at risk of DDoS attacks can incorporate the following best practices from our work. MMOG firms value latency, scalability, and brand reputation as drivers of revenue in their industry. Thus, cyber-risk management of DDoS attacks in the MMOG industry gives managers a tool to uphold KPIs mentioned earlier. The present study gives them an operationalizing route for hedging the risks by either accepting, passing, or reducing risk by subscribing to hybrid strategies of technological and cyber-insurance tools

In this study, we estimate the probability of different DDoS attacks happening in the MMOG industry. We use a Feedforward Neural Network to predict the proportion of each kind of DDoS attacks. We also investigate which probability distribution best approximates the risk values in each DDoS attack type. Next, we use risk analysis principles and calculate the expected loss values for these attacks and probability distribution that fits. The last stage of the study uses risk (i.e., probability of the attack) and severity (i.e., expected loss of attacks) to suggest ways to mitigate cyber-risk. We advise that MMOG firms with high risk-high severity attacks should subscribe to cyber-insurance after implementing self-protection. This study contributes by incorporating novel predictors related to cybersecurity spending and vulnerabilities, enabling DDoS attacks.

References

Akamai. 2015. *The Cost of Denial-of-Service Attacks*, Ponemon Institute. (https://www.akamai.com/us/en/multimedia/documents/content/the-cost-of-denial-of-services-attacks.pdf).

Arora, A., Telang, R., and Xu, H. 2008. "Optimal Policy for Software Vulnerability Disclosure," *Management Science* (54:4), pp. 642–656. (https://doi.org/10.1287/mnsc.1070.0771).

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

Biswas, B., and Mukhopadhyay, A. 2017. "Phishing Detection and Loss Computation Hybrid Model: A Machine-Learning Approach," *ISACA Journal* (1), pp. 22–29. (https://www.isaca.org/Journal/archives/2017/Volume-1/Pages/phishing-detection-and-loss-computation-hybrid-model.aspx).

Biswas, B., and Mukhopadhyay, A. 2018. "G-RAM Framework for Software Risk Assessment and Mitigation Strategies in Organisations," *Journal of Enterprise Information Management* (31:2), pp. 276–299. (https://doi.org/10.1108/JEIM-05-2017-0069).

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and 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), pp. 837–864. (https://doi.org/10.25300/MISQ/2015/39.4.5).

Bulgurcu, B., Cavusoglu, H., and 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).

Cavusoglu, Hasan, Cavusoglu, Huseyin, and 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, Huseyin, Raghunathan, S., and Cavusoglu, Hasan. 2009. "Configuration of and Interaction between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems," *Information Systems Research* (20:2), pp. 198–217. (https://doi.org/10.1287/isre.1080.0180).

Cohen, L. E., and Felson, M. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review* (44:4), p. 588. (https://doi.org/10.2307/2094589).

Das, S., Mukhopadhyay, A., Saha, D., and Sadhukhan, S. 2019. "A Markov-Based Model for Information Security Risk Assessment in Healthcare MANETs," *Information Systems Frontiers* (21:5), pp. 959–977. (https://doi.org/10.1007/s10796-017-9809-4).

Kannan, K., and Telang, R. 2005. "Market for Software Vulnerabilities? Think Again," *Management Science* (51:5), pp. 726–740. (https://doi.org/10.1287/mnsc.1040.0357).

Kesan, J. P., Majuca, R., and 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., and Majuca, R. P. 2013. "The Economic Case for Cyberinsurance," *Dissent* (Vol. Aut / Win). (http://search.informit.com.au.wwwproxy0.library.unsw.edu.au/documentSummary;dn=291645822148222;res=IELAPA).

Liu, D., Li, X., and Santhanam, R. 2013. "Digital Games and beyond: What Happens When Players Compete?," *MIS Quarterly: Management Information Systems* (37:1), pp. 111–124. (https://doi.org/10.25300/MISQ/2013/37.1.05).

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).

Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., and Shukla, G. K. 2019. "Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance," *Information Systems Frontiers* (21:5), pp. 997–1018. (https://doi.org/10.1007/s10796-017-9808-5).

Peng, T., Leckie, C., and Ramamohanarao, K. 2007. "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems," *ACM Computing Surveys* (39:1), p. 3.

(https://doi.org/10.1145/1216370.1216373).
Ransbotham, S., Mitra, S., and Ramsey, J. 2012. "Are Markets for Vulnerabilities Effective?," *MIS Quarterly* (36:1), p. 43. (https://doi.org/10.2307/41410405).
Rejda, G. E. 2007. *Principles of Risk Management and Insurance, 10th Edition*, Pearson. (https://www.amazon.com/Principles-Management-Insurance-Pearson-Finance/dp/0132992914?SubscriptionId=AKIAIOBINVZYXZQZ2U3A&tag=chimbori05-20&linkCode=xm2&camp=2025&creative=165953&creativeASIN=0132992914).
Rogers, R. W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology* (91:1), pp. 93–114. (https://doi.org/10.1080/00223980.1975.9915803).
Shahriar, H., and Zulkernine, M. 2012. "Mitigating Program Security Vulnerabilities," *ACM Computing Surveys* (44:3), pp. 1–46. (https://doi.org/10.1145/2187671.2187673).
Tanenbaum, A. S., and 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).
Wang, M., Lu, Y., and Qin, J. 2020. "A Dynamic MLP-Based DDoS Attack Detection Method Using Feature Selection and Feedback," *Computers & Security* (88), p. 101645. (https://doi.org/10.1016/j.cose.2019.101645).
Yahyavi, A., and Kemme, B. 2013. "Peer-to-Peer Architectures for Massively Multiplayer Online Games," *ACM Computing Surveys* (46:1), pp. 1–51. (https://doi.org/10.1145/2522968.2522977).
Zhang, Z., Nan, G., and Tan, Y. 2020. "On-Premises Software: Competition Under Security Risk and Product Customization. Information Systems Research Articles in Advance," *Information Systems Research*, pp. 1–17. (https://doi.org/10.1287/isre.2019.0919).