Proceedings of the 2023 Pre-ICIS SIGDSA Symposium

Special Interest Group on Decision Support and Analytics (SIGDSA)

12-10-2023

Managing Cyber-Risk Perpetuated by Vulnerabilities: A Co-occurrence Network Analysis

Swati Jain
Indian Institute of Management Lucknow, phd21020@iiml.ac.in

Arunabha Mukhopadhyay
Indian Institute of Mangement Lucknow, arunabha@iiml.ac.in

Managing Cyber-Risk Perpetuated by Vulnerabilities: A Co-occurrence Network Analysis

Research-in-Progress (Extended Abstract)

Swati Jain
Indian Institute of Management Lucknow
phd21020@iiml.ac.in

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

Abstract

The organizations incur excessive losses due to cyber-attacks, especially after the Covid-19 pandemic. Such attacks lead to customer churn, reduced productivity, loss of trust and reputation, and diminished profits. The more the number and severity of vulnerabilities are, the higher the threat exposure of an organization is. The increased online operations expose organizations more to cyber-attacks. Hence there is a need to study cyber-risk management to combat cyber-attacks perpetuated by exploiting vulnerabilities. Our study is based on the Protection-Motivation Theory to assess, quantify, and mitigate the cyber risk perpetuated by the weaknesses in the digital system of an organization. We perform co-occurrence network analytics to assess the cyber-risk associated with the presence of vulnerable information technology (IT) systems. We quantify the losses incurred by the cyber-attacks on a firm. Lastly, we suggest cyber-risk mitigation strategies via-a-vis vulnerability progression inside the organization to safeguard it against cyber-attacks.

Keywords

Vulnerabilities, Co-occurrence Network graph, Cyber-risk management, Distributed Denial-of-Service attack, Cross-Site Scripting attack, SQL injection.

Introduction

Multiple cyber-attacks incidents collectively underscore the peril posed by vulnerabilities in Information Technology (IT) systems, including internet-facing applications, operating systems, databases, and network components. When exploited, these vulnerabilities enable attackers to infiltrate networks and execute malicious actions, potentially leading to data breaches, including the theft of personal information such as names, email addresses, phone numbers, and credit card details(Jain et al., 2023; Jain & Mukhopadhyay, 2022). To counteract these cyber threats, our research makes a valuable contribution by introducing the management model, based on the Protection Motivation Theory (PMT), for the cyber-risk stemming from the vulnerabilities. The model evaluates the cyber-attack risk, quantifies it in terms of expected losses, and offers mitigation strategies aligned with industry-recognized NIST cybersecurity standards. Our objective is to assess (i) the likelihood of cyber-attacks stemming from the cyber-risk associated with vulnerabilities, (ii) the expected financial losses resulting from cyber-attacks exploiting vulnerabilities, and (iii) effective mitigation strategies to thwart cyber-attacks.

Proposed Management Model for Cyber-Risk generated due to Vulnerabilities

Our Management Model for Cyber-Risk generated due the presence of vulnerabilities consists of three modules: Cyber-Risk Assessment (CRA), Cyber-Risk Quantification (CRQ), and Cyber-Risk Mitigation (CRM), to assess, quantify, and mitigate the cyber-risk generated due to vulnerabilities inside the IT assets of an organization. CRA module computes the likelihood of the cyber-attack (p) by exploiting vulnerabilities. This module is guided by the threat appraisal component of the Protection Motivation Theory (PMT) (Boss et al., 2015; Rogers, 1975), Cyber Kill Chain (CKC) (Lockheed Martin, 2011), and NIST-guided Vulnerability Management Process. CRQ module calculates the resultant expected losses (EL) due to the exploitation of the vulnerabilities. Finally, based on the coping appraisal component of PMT (Boss et al., 2015; Rogers, 1975), and NIST-guided Vulnerability Management Process, we propose the CRM module.

Data and Methodology

Initially, we scrap the text data that describes the existing vulnerabilities (CVEs): the attack surface where they are present such as operating systems (Windows, macOS) or Applications (Google Chrome and Microsoft Office), web interfaces; the vendors whose IT assets have the vulnerabilities; ways in which attackers exploit the vulnerabilities; consequences on their exploitation; and resultant consequences. Next, we preprocess it. Then we find the co-occurrence of the words in the corpus. Based on the pair co-occurrence frequency, we pick the top 50 co-occurred words and plot them in a co-occurrence graph. In the next phase, using co-occurrence network analytics, we compute the probability of occurrence of cyber-attacks (p) that could be conducted by exploiting the vulnerabilities. Then after, we calculate the severity of a cyber-attack risk by computing the estimated losses. Lastly, we plot each data point (organization) on 2*2 risk-severity matrix based on probability and expected losses obtained from CRA and CRQ modules, respectively. Finally, based on the quadrant the organization lies in, we propose mitigation strategies to accept, reduce, or transfer cyber-attack risk.

Results

The co-occurrence graph indicates that the vulnerabilities in the cybersecurity landscape serve as the entry gate and allow the attackers to get into the digital system. Vulnerabilities allow unauthorized access to attackers who manipulate the systems using arbitrary code, reset admin passwords, gain elevated privileges, and execute malicious code remotely, thereby obtaining sensitive information, such as personal or financial data. Vulnerabilities are commonly reported in widely used email services, Cisco routers, through cache poisoning and DNS manipulation. The findings are in line with the attackers move guided by the CKC. Broadly, we notice that the vulnerabilities lead to Distributed Denial-of-Service, cross-site scripting, SQL injection. Based on the probable cyber-attacks, we suggest the mitigation strategies.

Conclusion

In an ever-evolving digital landscape, defenders must remain vigilant, monitoring for suspicious activities and consistently improving their security posture to safeguard critical systems and sensitive information from potential breaches. We found that the cyberattacks conducted due to the exploitation of vulnerabilities have high probability of occurrence and high impact. Hence, the organizations should take the suggested mitigation strategies to reduce the cyber-risk and finally pass on the residual risk to the cyber-insurers.

References

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*, *39*(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Jain, S., Jain, S., & Mukhopadhyay, A. (2023). Is US healthcare prepared to resist a DoS attack? *INDAM 2023 @ SBM - NMIMS MUMBAI*.

Jain, S., & Mukhopadhyay, A. (2022). Impact of Cyber-attack on Organizations: Threat Exposure Assessment, Quantification, and Mitigation. *Bright Internet Global Summit (BIGS) 2022,Pre-International Conference on Information Systems (ICIS) 2022, Copenhagen*.

Lockheed Martin. (2011). *The Cyber Kill Chain*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

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