NPRC Journal of Multidisciplinary Research
Vol. 1, No. 2, July 2024. Pages: 122-127
ISSN: 3059-9148 (Online)
DOI: https://doi.org/10.3126/nprcjmr.v1i2.69333

Issues of Cyber security and its solutions in Nepalese Context

Lokesh Gupta
Computer Science Department, D.R K.N Modi University, Newai, Rajasthan, India
lgupta.np@gmail.com
https://orcid.org/0009-0006-1014-5790

Received: March 09, 2024; Revised & Accepted: June 25, 2024

Abstract
In today's digital age, the internet's expansion has brought great convenience but also raised cyber threats. So, identify the issue of cyber-security and its solution in Nepalese context is significant. Descriptive design and qualitative methods were employed, with data sourced from Google Scholar and analyzed through thematic analysis. The study shows a myriad of issues stemming from inadequate cyber security awareness in Nepal, including increased vulnerability to cyber-attacks, data breaches, and societal, economic, and regulatory consequences. Bridging the gap in cyber security awareness is imperative to mitigate risks effectively and foster a secure digital environment in Nepal. Strategies emphasizing education, training, and regulatory frameworks are vital for addressing these challenges and promoting technological advancement and societal trust. This study proposes AI-driven solutions to address the lack of cyber security awareness in the Nepalese context, offering a unique approach to mitigate cyber threats and foster a secure digital environment.

Keywords: Cyber security, awareness, AI, education, data

Introduction
In today's digital age, the proliferation of technology has brought about unparalleled convenience and connectivity (Banerjee, 2023). However, this advancement has also ushered in a new era of threats and vulnerabilities, with cyber-attacks becoming increasingly pervasive and sophisticated. Amidst this landscape, one of the most pressing issues facing individuals and organizations alike is the pervasive lack of awareness surrounding cyber security (Abrahams, Ewuga, Dawodu, Adegbite, & Hassan, 2024).
While cyber security breaches continue to make headlines, the root cause often traces back to a fundamental lack of understanding and awareness among users. From unsuspecting individuals falling victim to phishing scams to businesses neglecting basic security protocols,

NPRC Journal of Multidisciplinary Research
Vol. 1, No. 2, July 2024. Pages: 122-127
ISSN: 3059-9148 (Online)
DOI: https://doi.org/10.3126/nprcjmr.v1i2.69333

the consequences of this deficiency are far-reaching and profound. This research paper seeks to delve into the multifaceted issues arising from the dearth of cyber security awareness, examining its implications across various domains and proposing strategies to address this critical challenge.

In the Nepalese context, studying cyber security issues and proposing solutions holds significant importance due to the nation's emerging digital landscape (Poudel, 2023). As Nepal undergoes rapid technological advancements, including increased internet connectivity and digital service adoption, the threat of cyber-attacks escalates. Given the vulnerabilities inherent in the country's technological infrastructure, understanding and addressing cyber security concerns become imperative. Critical systems such as government networks, financial institutions, and healthcare services are increasingly reliant on digital platforms, making them potential targets for cyber threats (George, Baskar, & Srikaanth, 2024). Moreover, with growing concerns about data privacy and protection, especially amidst the digitization of services, it is essential to develop robust cyber security measures to safeguard sensitive information and ensure the security of individuals and organizations operating within Nepal. By identifying weaknesses and proposing effective solutions, this study contributes to strengthening Nepal's cyber defense mechanisms and promoting a secure digital environment for all stakeholders.

Objective

The main objective of this study is to identify the issue of cyber-security and its solution in Nepalese context.

Methods

The research used a descriptive design and qualitative methods to explore the subject. Data were gathered from Google Scholar. Thematic analysis was used to identify patterns and themes in the data. Through coding and categorization, the study aimed to expose detailed insights. The iterative process of thematic analysis allowed for a thorough exploration of the data, ensuring strong findings. The focus was on understanding the context and conducting in-depth analysis, in line with qualitative research principles.

Results

Level of awareness on cyber security

Lack of awareness of cyber security can lead to numerous issues, both for individuals and organizations. Here are some of the key problems that can arise:

Data Breaches: Ignorance about cyber security best practices often leads to weak passwords, sharing sensitive information, or falling for phishing scams. This can result in data breaches where personal or confidential information gets compromised.

Financial Loss: Cyber-attacks such as ransomware, where attackers encrypt data and demand payment for its release, can result in significant financial losses for individuals and businesses who are unaware of how to prevent or mitigate such attacks.

NPRC Journal of Multidisciplinary Research
Vol. 1, No. 2, July 2024. Pages: 122-127
ISSN: 3059-9148 (Online)
DOI: https://doi.org/10.3126/nprcjmr.v1i2.69333

Identity Theft: Poor cyber security awareness can make individuals susceptible to identity theft, where attackers steal personal information to impersonate them or commit fraudulent activities.

Reputation Damage: For businesses, a cybersecurity breach can damage their reputation and erode customer trust. This can lead to loss of clients, partners, and ultimately revenue.

Legal and Regulatory Consequences: Many industries are subject to regulations regarding the protection of sensitive information. Failing to comply with these regulations due to lack of awareness can result in legal penalties and fines.

Disruption of Services: Cyber-attacks can disrupt services and operations, causing downtime and affecting productivity. This can be particularly damaging for critical infrastructure, such as healthcare or utilities, where lives may be at stake.

Intellectual Property Theft: Companies that don't adequately protect their intellectual property can fall victim to theft or espionage, resulting in loss of competitive advantage and innovation.

Compromised Devices: Ignorance about cybersecurity risks can lead to the compromise of personal devices, such as computers and smartphones, through malware or other malicious software.

Supply Chain Risks: Businesses interconnected through supply chains are vulnerable to cyber-attacks targeting weaker links. Lack of awareness about supply chain cybersecurity can lead to cascading breaches across multiple organizations.

Psychological Impact: Being a victim of cybercrime can have psychological effects, including Stress, anxiety, and a sense of vulnerability. This can impact both individuals and employees within organizations.

Addressing these issues requires comprehensive cyber security education and training programs for individuals and organizations alike. It's essential to stay informed about current threats and best practices to mitigate risks effectively.

Issues of Cyber security

Lack of awareness of cyber security can lead to a multitude of issues across various sectors and levels of society. Some of the prominent issues stemming from this lack of awareness include:

Increased Vulnerability to Cyber Attacks: Individuals who are unaware of common cyber threats such as phishing emails, malware, and social engineering tactics are more likely to fall victim to cyber-attacks. This can result in financial losses, identity theft, and unauthorized access to personal or sensitive information.

Data Breaches: Businesses and organizations with inadequate cyber security awareness may neglect essential security measures, leading to data breaches. These breaches can compromise customer data, intellectual property, and proprietary information, resulting in reputational damage, legal liabilities, and financial penalties.

Loss of Intellectual Property: Industries reliant on innovation and intellectual property, such as technology and pharmaceuticals, are particularly vulnerable to cyber-attacks. Without proper cyber security measures in place, companies risk losing valuable intellectual property

NPRC Journal of Multidisciplinary Research
Vol. 1, No. 2, July 2024. Pages: 122-127
ISSN: 3059-9148 (Online)
DOI: https://doi.org/10.3126/nprcjmr.v1i2.69333

through theft or espionage, hindering their competitive advantage and stifling innovation.

Disruption of Critical Infrastructure: Critical infrastructure sectors such as energy, transportation, and healthcare are prime targets for cyber-attacks. A lack of awareness of cybersecurity best practices among infrastructure operators can result in disruptions to essential services, potentially endangering public safety and causing widespread economic damage.

Social Engineering Exploitation: Cybercriminals often exploit human psychology through social engineering techniques to manipulate individuals into disclosing sensitive information or performing actions that compromise security. Lack of awareness makes individuals more susceptible to these tactics, increasing the likelihood of successful social engineering attacks.

Compliance Violations and Regulatory Penalties: Many industries are subject to regulatory requirements regarding data protection and cybersecurity. Organizations that fail to comply with these regulations due to a lack of awareness may face significant fines, legal penalties, and damage to their reputation.

Impact on National Security: Inadequate cybersecurity awareness poses a threat to national security by making critical infrastructure, government systems, and defense networks vulnerable to cyber-attacks. A breach of national security infrastructure could have far-reaching consequences, including disruption of essential services, compromise of sensitive information, and undermining of national sovereignty.

Cybersecurity Skills Gap: The lack of cybersecurity awareness contributes to a broader skills gap in the cybersecurity workforce. Without a sufficient pool of knowledgeable professionals, organizations struggle to implement effective cybersecurity strategies and respond to evolving cyber threats adequately.

Handling Issues with the help of AI

As artificial intelligence (AI) continues to permeate various facets of our lives, from business operations to personal devices, the importance of cybersecurity has become increasingly paramount. However, the rapid integration of AI technologies often outpaces the general awareness of cybersecurity risks associated with them. This paper explores the intricate relationship between AI implementation and cybersecurity awareness, shedding light on the multifaceted issues that arise from a lack of understanding in this domain.

The Growing Influence of AI

AI technologies offer unprecedented opportunities for innovation and efficiency across diverse sectors, including healthcare, finance, manufacturing, and transportation. From machine learning algorithms streamlining decision-making processes to autonomous systems enhancing operational capabilities, the potential benefits of AI are vast. However, as organizations rush to harness the power of AI, they often overlook the inherent cybersecurity vulnerabilities that accompany these advancements.

Unique Cybersecurity Challenges in AI

Unlike traditional software systems, AI algorithms exhibit complex and often unpredictable behavior, posing unique challenges for cybersecurity professionals. Adversarial attacks, wherein malicious actors manipulate AI models by injecting subtle perturbations into input

NPRC Journal of Multidisciplinary Research
Vol. 1, No. 2, July 2024. Pages: 122-127
ISSN: 3059-9148 (Online)
DOI: https://doi.org/10.3126/nprcjmr.v1i2.69333

data, highlight the vulnerabilities inherent in AI systems. Moreover, the opaque nature of AI algorithms complicates efforts to detect and mitigate potential security breaches, exacerbating the risks associated with AI implementation.

Impact of Cybersecurity Ignorance in AI Adoption

A lack of awareness surrounding cybersecurity issues in AI implementation can have profound consequences across multiple dimensions. Organizations may inadvertently deploy AI systems with exploitable vulnerabilities, exposing sensitive data to unauthorized access or manipulation. Moreover, the reliance on AI-driven decision-making processes amplifies the potential impact of security breaches, leading to financial losses, reputational damage, and regulatory scrutiny.

Ethical Implications

Beyond the immediate cybersecurity concerns, the intersection of AI and cybersecurity raises profound ethical questions. Biased algorithms, unchecked surveillance mechanisms, and the proliferation of deepfakes underscore the ethical dilemmas inherent in AI deployment. Without adequate awareness and oversight, AI systems risk perpetuating existing biases, infringing on privacy rights, and undermining societal trust in technological advancements.

Strategies for Enhancing Cybersecurity Awareness in AI Implementation addressing the challenges posed by the lack of cybersecurity awareness in AI implementation requires a concerted effort from stakeholders across academia, industry, and government. Education and training programs should be developed to equip cyber security professionals with the necessary skills to assess and mitigate AI-related risks effectively. Additionally, regulatory frameworks must evolve to keep pace with technological advancements, ensuring that AI deployments adhere to stringent cyber security standards.

Conclusion

The aim of this study is to identify the issue of cyber-security and its solution in Nepalese context. The findings highlight the multifaceted challenges stemming from inadequate awareness, ranging from increased vulnerability to cyber-attacks to ethical implications of AI deployment. Strategies aimed at enhancing cyber security awareness must be prioritized across sectors, emphasizing education, training, and regulatory frameworks. By bridging the gap in cyber security knowledge, stakeholders can mitigate risks and foster a secure digital environment conducive to technological advancement and societal trust.

References

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A Review of Cybersecurity Strategies in Modern Organizations: Examining the Evolution and effectiveness of Cybersecurity Measures fordata protection. *Computer Science & IT Research Journal, 5*(1), 1-25.

Banerjee, S. K. (2023). The Influence of Technology on Social Interaction Among Students in the Digital Age. *International Journal of Research Publication and Reviews, 4*(9),

NPRC Journal of Multidisciplinary Research
Vol. 1, No. 2, July 2024. Pages: 122-127
ISSN: 3059-9148 (Online)
DOI: https://doi.org/10.3126/nprcjmr.v1i2.69333

1094-1101.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal, 2*(1).

Poudel, A. (2023). Unlocking Nepal's Digital Potential: Overcoming Security Hurdles inthe Age of Digitalization.

Dhungana, Raj Kumar; Gurung, Lina Dr; and Poudyal, Hem (2023) "Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal," Journal of Cybersecurity Education, Research and Practice: Vol. 2023: No. 2, Article 5. DOI: 10.32727/8.2023.17

Neupane, S. (2019). Interaction on IT BILL 2075. ICT frame. Kathmandu: Internet Society Nepal.