Abstract

This project provides an in-depth analysis of cybersecurity, focusing on the 2021 Facebook data breach, international cybersecurity regulations, and the development of effective cybersecurity policies. The Facebook breach highlighted critical vulnerabilities in data protection and the need for enhanced security measures across digital platforms. It emphasizes the importance of adopting security frameworks such as ISO/IEC 27001, NIST, and GDPR to mitigate risks and ensure compliance with legal standards. The project further explores the ethical considerations of cybersecurity practices, the significance of continuous monitoring and security evaluation methods, and the role of organizational policies in fostering a secure digital environment. Through comprehensive cyber security measures that include security audits, penetration testing for vulnerability and assessments of risks where organizations can identify vulnerabilities on the system and strengthen or improve their defenses. The conclusion outlines recommendations for organizations to adopt proactive security practices, prioritize employee training, and stay ahead of evolving threats to ensure the protection of sensitive data and maintain stakeholder trust.

Table of contents

1.Introduction

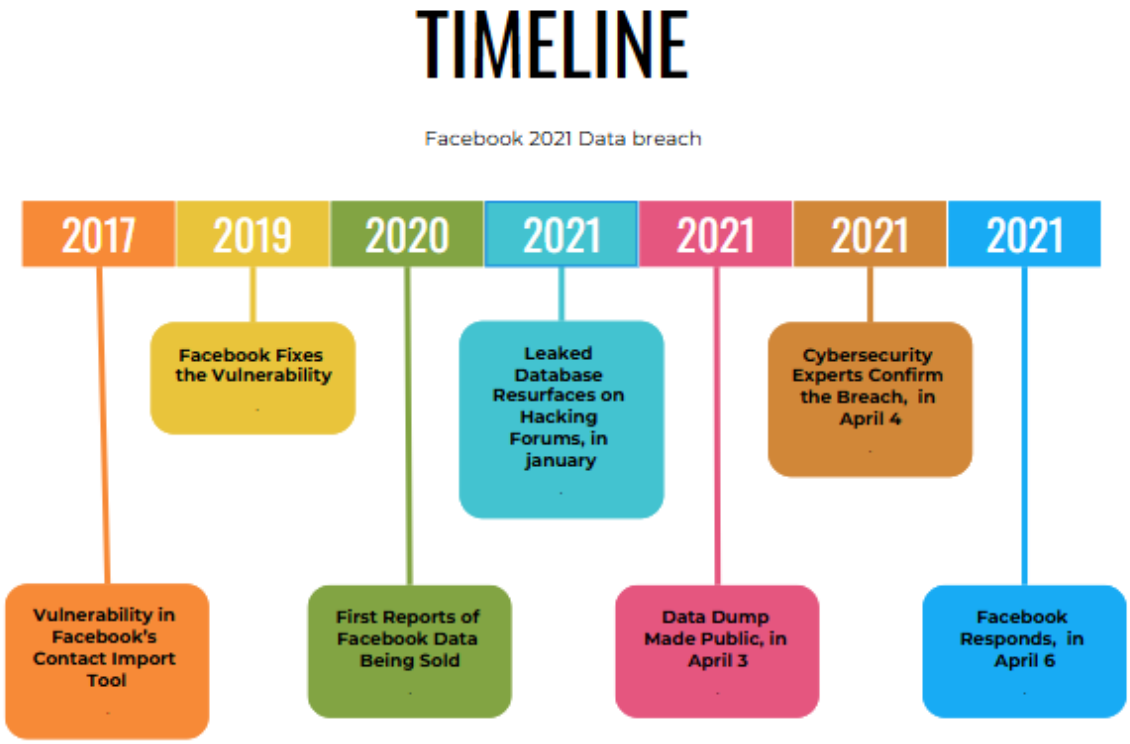
In today's digital world, cybersecurity threats are becoming more frequent, with both individuals and businesses moving more of their activities online and storing sensitive information digitally. A significant and recent example of a cybersecurity breach is the Facebook data breach. Breach of 2021, where the personal information of over **533 million users** was exposed online. This breach revealed a variety of sensitive data, including full names, phone numbers, email addresses, and location details, raising significant concerns about user privacy and data protection. The incident occurred due to a vulnerability in Facebook's contact import feature, which allowed attackers to scrape a large volume of user data without proper authorization.

This research will examine both Nepalese and international cybersecurity laws considering their applicability in protecting data and combating cyber threats. By examining these legal frameworks, the research aims to understand how they address the challenges posed by data breaches and cybersecurity incidents. In addition, ethical and legal considerations will be discussed, particularly how systems designed to handle sensitive data must comply with privacy laws. The role of ethical hacking in identifying vulnerabilities and improving cybersecurity measures will also be considered as a crucial part of the response to such threats.

The purpose of this project is to analyze the Facebook data breach of 2021, investigating the underlying causes, the broader impact of the breach, and the lessons that can be learned. Additionally, the research will assess standard security practices and evaluation methods, such as the **ISO/IEC** 27001, NIST Cybersecurity Framework, and **OWASP** Top 10, to evaluate how organizations can strengthen their digital security systems and protect against similar breaches in the future.

2. Understanding the 2021 Facebook Data Breach

2.1 Timeline of the breach



1. **2017 – 2018: Attackers Take Advantage of Facebook's Contact Import Feature**

Cybercriminals find a **scraping vulnerability** in Facebook's Contact Import Tool, allowing them to collect user data, including phone numbers, full names, and email addresses, without consent.

2. **April 2019: Facebook Patches the Security Flaw**

Facebook detects and patches the vulnerability, preventing further data scraping. However, the already stolen data remains in circulation on hacking forums and the dark web.

3. **June 2020: Stolen Data Appears for Sale**

Cybercriminals start selling Facebook user data on underground forums, exposing millions of users to potential scams, identity theft, and phishing attacks.

4. **January 2021: Massive Database Resurfaces**

The **533 million-user database** is spotted being shared among hackers, increasing the risk of misuse. At this point, the data is no longer just being sold—it is freely exchanged among cybercriminals.

5. **April 3, 2021: Data Breach Exposed to the Public**

A hacker **posts the entire database for free** on a well-known hacking forum, making it accessible to anyone, including scammers and cybercriminals.

6. **April 4, 2021: Cybersecurity Expert Confirms the Breach**

Alon Gal, CTO of Hudson Rock, confirms the leak and shares details on Twitter, drawing global media attention to the breach.

7. **April 6, 2021: Facebook Responds**

Facebook acknowledges the breach but claims the data was scraped from public profiles rather than obtained through hacking. The company does not notify affected users individually, leading to further criticism.

2.2. What Happened?

The **2021 Facebook Data Breach** exposed the personal details of over **533 million** users from nearly 100 countries around the globe. This information comprised names, telephone numbers, email addresses, locations, and much more. The **Contact Import Tool** within Facebook appears to have been the root cause of the recent massive data leak. This tool enabled the attackers to effectively collect details of the users without their agreement.

It wasn't a classic hack. The breach was executed via an automated data scraping process. Over 2017-2018, cybercriminals found a loophole in the phone number system for relating them back to Facebook user accounts. This made scraping huge volumes of user data much easier without Facebook's security mechanisms raising an alarm. Though Facebook had already closed up this gap in 2019, forum data was already long trading over dark web forums.

That leaked information came up for sale in underground markets back in 2020. In a report at the beginning of January 2021, it was stated that the entire database was up for distribution out to cybercriminals who wanted it. The situation became even worse after a hacker publicly disclosed, on the 3rd of April 2021, that he was making the whole database available for free on a popular hacking forum. That in effect made it possible for absolutely anybody, including scammers, hackers, or even serious cybercriminals, to obtain personal information about millions of Facebook users.

This raised concerns among global citizens over privacy and data security. Facebook acknowledged the incident, but claimed the data was not stolen; rather it was **"scraped."** According to the social media giant, the information was obtained from public profiles and not directly hacked from secured databases. However, Facebook made no effort to inform the affected users of this, inviting severe criticism regarding its attitude toward user privacy.

2.3 Causes of the Data Breach

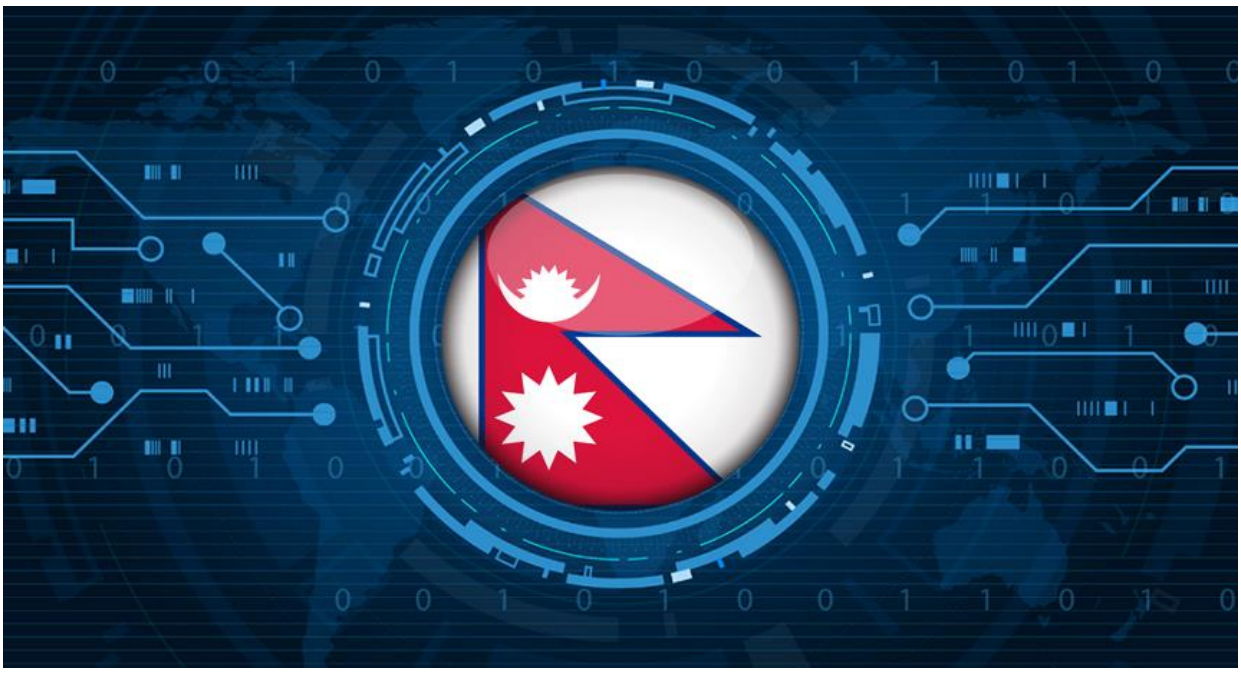
The 2021 Facebook data breach was caused by a scraping vulnerability in its contact import tool. Attackers took advantage of this flaw by feeding phone numbers in bulk into Facebook's "Find Friends" feature via an automated script. This tool would return user profile information associated with that number, making it possible for attackers to gather user-related information without the user's consent. This vulnerability existed for some extent before it was patched in 2019., but by then, attackers were already harvesting significant amounts of personal data details. Facebook's statement was directed at clarifying that the breach was not a direct hack of the site but abuse of one of its publicly available tools.

2.4 Impact of the Breach

The fallout of the 2021 Facebook data breach was immense for the affected individuals and the organization itself. The breach laid open personal matters such as telephone numbers and email addresses, which inevitably increased the threat levels of identity theft, phishing, and social engineering attacks. The leaked information enabled attackers to design targeted scams to hoodwink users into providing further personal information or financial dealings. For Facebook, the breach sullied its name and left public anger in its wake, with a grave stare over its data protection practices. Legally, Facebook is undergoing investigations and lawsuits, with penalties likely, for not having protected user data and not doing more to avert the exploitation of such vulnerability.

3. Cybersecurity Laws: Nepal vs. International Standards

3.1 Cybersecurity Laws in Nepal



The Electronic Transactions Act of 2008 serves as the primary legislation regulating cyber-crimes in Nepal. It outlines the framework for electronic transactions, digital signatures, and the protection of data. The Act promotes the growth of e-commerce by securing digital transactions and concerning issues in various cyber-crime forms including hacking, data break-ins, and identity theft.

Under certain conditions within the Act, these arise in connection with government discretion in providing penalties against unauthorized access to computers, stealing of data, and cyber frauds. The further description of the law goes for the protection of electronic evidence, encouraging safe online behavior, and ensuring adherence to digital security standards. However, enforcement in Nepal has been handicapped by a lack of resources, specialized expertise, and basic legal infrastructure.

3.2 International Cybersecurity Regulations

International cybersecurity regulations aim to protect data and ensure security across borders. Key regulations include:

General Data Protection Regulation (GDPR):

The GDPR, enacted by the EU, establishes stringent regulations on data collection, storage, and it further provides deterrent penalties for transgressions such as above. In this way, everyone invests in sharing, prioritizing transparency, user consent, and security.

California Consumer Privacy Act (CCPA):

It is the "California Consumer Privacy Act" (CCPA) that gives Californian residents the rights to access and have control of their private data, personal information, and privacy., delete, and opt out. It focuses on improving privacy protections and imposing penalties on violators.

Cybersecurity Act of Singapore:

This Act establishes a legal framework for protecting critical information infrastructure, reporting cybersecurity events, and addressing cyber threats, supported by a national cybersecurity agency.

The Data Protection Act 2018 (UK):

This Act implements GDPR in the UK, enhancing privacy rights and strengthening protections for personal data.

3.3Comparative Analysis: Nepal vs. International Cyber Laws

Limited Scope in Nepal: Nepal's Electronic Transactions conspects-ups for electronic transactions and cybercrimes but lacks comprehensive data protection, unlike GDPR and CCPA, which offer broader privacy protections.

Weak Enforcement: Nepal faces challenges with enforcement due to limited resources and legal infrastructure. In contrast, international laws like GDPR have strong enforcement mechanisms, ensuring better compliance.

Weaker Penalties: Penalties for cybersecurity violations in Nepal are less severe than international laws. For example, GDPR imposes fines up to 4% of annual turnover, whereas Nepal's penalties are lower.

Lack of Clear Data Protection: Nepal’s laws don’t provide clear guidelines on data protection or user consent, while GDPR and CCPA offer detailed rules for managing personal data.

Challenges with Emerging Threats: Nepal's laws lack the flexibility needed to keep up with the constantly changing and evolving cyber threats, wherein foreign regulations, such as Singapore's Cybersecurity Act, are regularly updated to address emerging risks and challenges in the cybersecurity field.

Requirement of Alignment: Nepal’s cybersecurity laws need to be revised to match international standards such as the GDPR, in order to enhance data protection, enforcement measures, and overall cybersecurity practices.

4. Legal and Ethical Considerations in System and Product Development

4.1. Legal Considerations

Ensuring legal adherence while developing systems or products is of utmost importance in compliance and liability avoidance. The important legal parameters that come into play are:

Compliance with Data Protection Laws: Organizations now have strict laws like GDPR and CCPA that make it mandatory for them to acquire the consent from users before collecting any data or place restrictions on data usage. Non-compliance with these laws leads to penalties and a bad reputation.

Intellectual Property Rights and Software Licensing: IP laws should be respected by ensuring that the particular software or system under development does not infringe upon anyone else's copyrights, patents, or trademarks. Licensing of third-party libraries and open-source components should adequately protect the rights of both the developer and the user.

Regulatory Requirements for Software Security: Specific industries have specific security regulations, such as HIPAA for healthcare and PCI DSS for payment processing. These frameworks set rules for encryption, secure coding, and audit trails to protect sensitive data.

Considering such legal issues is meant to make systems and products more secure, compliant, and less susceptible to facing future injunctions arising from legal issues from the time of product inception till implementation.

4.2. Ethical Considerations

When considering the development of a system or product, equal importance should be given to ethical standards to ensure responsible technology usage while duly respecting the rights of its users. Some key ethical standards are:

User's right to privacy and data protection: Ethical developers prioritize the user's right to privacy by taking seriously how their systems deal with personal data, including minimal data collection, protection of data from unauthorized access, and transparency concerning the use of any data collected about the user.

Transparency in Handling Security Vulnerabilities: Security vulnerabilities should be handled in an ethical manner. This means diligently identifying and reporting the vulnerabilities in a timely manner to the users and, in some cases, publicly if warranted. Unethical action is delaying or ignoring the existence of a flaw that may put users at risk.

Societal Impact and Users' Considerations: Developers ought to consider societal implications of their technology. This includes avoiding the creation of systems easily adaptable for criminal purposes such as surveillance or discrimination. Ethical decisions also entail ensuring equal opportunity for all users regardless of their background.

Inculcated ethical considerations along design and development will add more ethics.

4.3. Policy Development in Cybersecurity

Effective cybersecurity policies are vital for protecting sensitive information, maintaining trust, with legal and regulatory requirements. Key elements include:

Importance of Strong Cybersecurity Policies: A clear cybersecurity policy outlines the Organization's approach to protecting data and mitigating cyber threats, as well as ensuring compliance. It helps mitigate risks, improve decision-making, and foster a security-focused culture.

Components of a Cybersecurity Policy: A comprehensive policy includes:

Access Control of data: Rules to restrict access to sensitive data to authorized personnel only.

Incident Response and Reporting: Procedures for identifying and managing security incidents.

Data Protection and Privacy: Regulations for storing and sharing personal data in accordance with laws such as GDPR or CCPA.

Employee Training and Awareness: Ongoing education to reduce human error, a common cause of breaches.

Ethical Dilemmas in Digital Forensics and Data Monitoring: Cybersecurity policies may raise ethical concerns, such as monitoring employee activities or collecting digital evidence, which could infringe on privacy. Policies should define the scope and limits of monitoring to balance security and privacy.

Case Studies on Ethical Lapses: Reviewing past ethical lapses, like failures to protect customer data or disclose breaches, can provide lessons for improving future policies and avoiding legal and reputational damage.

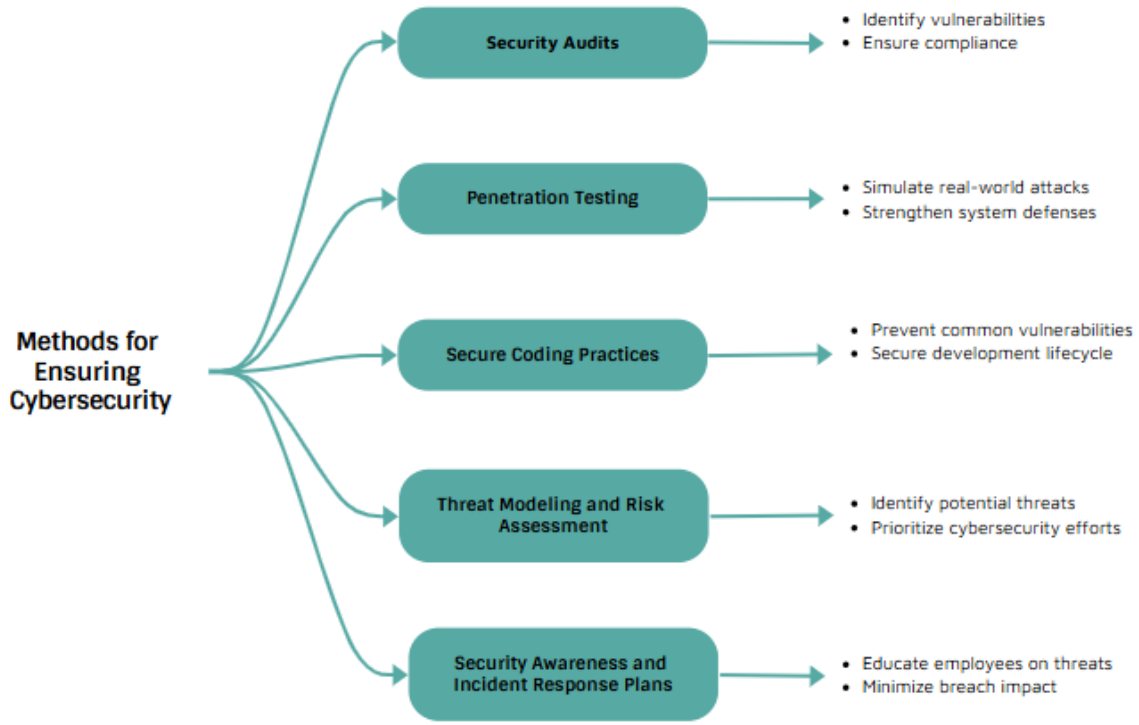
Continuous Review and Improvement: Cybersecurity policies must evolve to address emerging threats and regulatory changes. Regular reviews help organizations stay ahead of new risks, reduce vulnerabilities, and maintain trust.

In summary, strong and ethically responsible cybersecurity policies are key to protecting assets, complying with regulations, and fostering a culture of security.

5.Evaluating Security of Digital Systems

Evaluating digital system security involves methods like security audits, penetration testing for any vulnerability, and risk assessments to identify vulnerabilities and protect against threats. It also includes following security frameworks such as ISO/IEC 27001 and NIST, which guide organizations in applying best practices to secure data and systems.

5.1. Methods for Ensuring Cybersecurity



Security Audits:

Audits evaluate systems, policies, and controls to identify vulnerabilities and ensure compliance, improving security.

Penetration Testing:

Penetration helps to identify system vulnerabilities before any unauthorized malicious hackers can take advantage of them.

Secure Coding Practices:

Secure coding minimizes risks by addressing vulnerabilities, ensuring applications are resistant to common attacks.

Threat Modeling and Risk Assessment:

Threat modeling detects risks early, while risk assessment ranks cybersecurity efforts by impact and likelihood.

Security Awareness and Incident Response Plans:

Training educates employees on threats, and response plans outline steps to detect, manage, and recover from breaches.

5.2. Security Standards and Frameworks.

Security standards and frameworks provide structured guidelines to help organizations improve cybersecurity, manage risks, and ensure compliance. Key frameworks include:

ISO/IEC 27001: This standard outlines an ISMS to manage sensitive data, ensuring confidentiality, availability, and integrity while promoting continuous improvement.

NIST Cybersecurity Framework: The primary focus is on continuous monitoring while helping organizations implement and enhance their cybersecurity practices.

OWASP Top 10: The OWASP Top 10 finds major web applications security risks, including SQL injection and (XSS) cross-site scripting. It serves as a critical resource for addressing the vulnerabilities during the software development lifecycle.

PCI DSS: PCI DSS ensures the protection of payment card data of customers by instituting sets of security requirements upon organizations which process credit card transactions. Compliance with PCI DSS assists in preventing fraud and in the protection of business and consumers.

CIS Controls: CIS Controls are 18 top priority security best practices that focus on asset management, access control, incident response, and other areas. They afford practical steps to bolster cybersecurity defenses.

5.3 Effectiveness of Security Evaluation Methods

Security evaluation methods, such as penetration testing, security audits, and risk assessments, are effective in identifying vulnerabilities and strengthening an organization's defenses. These methods provide a comprehensive view of potential threats by detecting weaknesses across systems and applications. By proactively assessing risks and their potential impact, organizations can allocate resources effectively to address critical vulnerabilities before they are exploited.

Additionally, frameworks like NIST and ISO/IEC 27001 help align security practices with industry standards with Continuous monitoring and regular evaluations contribute to ongoing improvements, allowing organizations to adapt to new threats and reduce both technical and organizational vulnerabilities, ultimately strengthening overall cybersecurity posture.

6. Conclusion and Recommendations

The 2021 Facebook data breach mentioned the important need for robust cybersecurity measures and the importance of data protection. As digital landscapes evolve, so too must the strategies to secure private data and prevent unauthorized access. This breach underlined the significance of proactive vulnerability management, timely response, and the need for companies to continuously improve their security practices.

To prevent future breaches, organizations should prioritize implementing strong security policies, conducting regular security audits, and adopting industry-recognized frameworks such as ISO/IEC 27001 and NIST. Furthermore, organizations must stay ahead of emerging threats by regularly updating their security measures and adopting new technologies that enhance data protection. Through these proactive steps, businesses can mitigate risks, protect user data, and maintain trust with stakeholders.

References

a) *Facebook data breach: What & how it happened?* (no date) *Twingate*. Available at: https://www.twingate.com/blog/tips/Facebook-data-breach (Accessed: 09 February 2025).

b) Bowman, E. (2021) *After data breach exposes 530 million, Facebook says it will not notify users*, *NPR*. Available at: https://www.npr.org/2021/04/09/986005820/after-data-breach-exposes-530-million-facebook-says-it-will-not-notify-users (Accessed: 09 February 2025).

c) *A short glance at Cyber Law and data security in Nepal* (2024) *OnlineKhabar English News*. Available at: https://english.onlinekhabar.com/a-short-glance-at-cyber-law-and-data-security-in-nepal.html (Accessed: 09 February 2025).

d) Khatapana (no date) *Nepal's cybersecurity journey: From vulnerability to vigilance (2020-2024)*, *Khatapana*. Available at: https://khatapana.com/blogs/264/nepals-cybersecurity-journey-from-vulnerability-to (Accessed: 09 February 2025).

e) *Effective strategies for enhancing cybersecurity in Nepal - Greentick Consulting Organization in Nepal* (2023) *Green Tick Nepal | Consulting Organization in Nepal*. Available at: https://gtn.com.np/2023/08/effective-strategies-for-cybersecurity-in-nepal/#:~:text=Implementing%20robust%20encryption%2C%20access%20controls,cyber%20threats%20in%20real%20time. (Accessed: 09 February 2025).