



**Islington college**  
(इरिलिङ्टन कलेज)

## **CC5052NI Risk, Crisis & Security Management**

**50% Individual Coursework**  
**on**

**Legal Issues in Security Management in Nepal**

**Semester 3**  
**2024-25 Autumn**

**Student Name: Sulav Parajuli**

**London Met ID: 23047483**

**College ID: NP01NT4A230182**

**Assignment Due Date: 01/10/2025**

**Assignment Submission Date: 01/05/2025**

**Submitted To: Akash Ojha**

**Count: 2199**

*I confirm that I understand my coursework needs to be submitted online via MST Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.*

**A Coursework Submitted  
on  
Legal Issues in Security Management in Nepal**

**Semester 3  
2024-25 Autumn**

**Student Name: Sulav Parajuli**

**London Met ID: 23047483**

**College ID: NP01NT4A230182**

**Assignment Due Date: 01/10/2025**

**Assignment Submission Date: 01/05/2025**





**Submitted To: Akash Ojha**

**Count: 2199**




## 17% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

### Match Groups

- 
**40 Not Cited or Quoted 17%**  
 Matches with neither in-text citation nor quotation marks
- 
**0 Missing Quotations 0%**  
 Matches that are still very similar to source material
- 
**0 Missing Citation 0%**  
 Matches that have quotation marks, but no in-text citation
- 
**0 Cited and Quoted 0%**  
 Matches with in-text citation present, but no quotation marks

### Top Sources

- 12%  Internet sources
- 2%  Publications
- 15%  Submitted works (Student Papers)

### Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

## **Acknowledgment**

I would like to express my sincere gratitude to everyone who assisted me in completing this report, which is titled "Legal Issues in Security Management in Nepal." Without the guidance, inspiration, and assistance I received from a number of people, it would not have been possible. This has been a rewarding and challenging experience.

First and foremost, I want to sincerely thank Mr. Akash Ojha, my tutor, for his helpful advice and guidance throughout the writing and research stages. His advice and support had an important influence on this report and helped me learn more about the subject.

I am extremely grateful to Islington College for giving me the chance to complete this report as my coursework. This chance gave me the opportunity to learn more about cybersecurity and legal challenges in Nepal while also researching a significant topic.

Additionally, I want to thank my friends for their advice, conversations, and support, all of which improved my ideas and arguments. In conclusion, I am extremely thankful of my family and friends for their constant encouragement and support during this journey.

I acknowledge that this report is important in addressing the increasing legal issues in cybersecurity in Nepal. I hope that this report helps to improve the cybersecurity frameworks in Nepal.

## **Abstract**

The report highlights legal issues in cyber security management by comparing Nepal and the US country by country. Despite providing a few basic protections against cybercrimes, digital signatures, and electronic transactions in Nepal, the Electronic Transactions Act 2008 and the National Cyber Security Policy 2023 are still very limited, lack enforcement power, and do not meet international standards. In addition to leaving large gaps in areas like risk management, breach reporting, and data protection, this adds to vulnerable cyberspace. However, the US has put in place complex but decentralized rules like HIPAA, which protects sensitive health care data, and the CCPA, which grants people control over their personal data and establishes strict guidelines for organizations. The report shows how the CCPA's broad and customer-oriented approach has been effective in resolving modern privacy and data security issues that the outdated Electronic Transactions Act of Nepal cannot resolve. In order to show how Nepal could learn from the United States in its pursuit for stronger cybersecurity laws, more efficient enforcement mechanisms, and more cybersecurity awareness, this report looks at these differences. This will help in the process of addressing vulnerabilities and building a stronger cybersecurity framework in order to establish Nepal as a secure and reliable digital participant. A case study of the 2020 Foodmandu Data Breach and lessons learned are also included in this research to demonstrate how weak Nepal's cybersecurity laws are.

## Contents

Acknowledgment .....	i
Abstract .....	ii
1. Introduction and Rationale.....	1
1.1. Aim .....	1
1.2. Objectives .....	1
2. Literature Review.....	2
2.1. Legal Frameworks in Nepal.....	2
2.2. Legal Frameworks in the United States .....	2
3. Methodology and Analysis .....	3
3.1. Issues in Nepal’s Cybersecurity Framework .....	3
3.2. Comparative Analysis .....	4
3.3. Case Study: Foodmandu Data Breach (2020).....	4
3.3.1. Key Legal Issues and Analysis .....	5
3.3.2. Lessons from the Foodmandu Breach.....	6
4. Recommendations.....	7
5. Conclusion .....	8
Bibliography .....	9

# **1. Introduction and Rationale**

Effective legal frameworks are crucial for cybersecurity management, as seen by the rise in cyberthreats including ransomware attacks, identity theft, and data breaches. Because of Nepal's increasing utilization of technology and the obvious weaknesses in its cybersecurity infrastructure, this report focuses on the legal issues in security management in context of Nepal. Nepal faces several challenges in protecting its people and organizations from evolving cyberthreats. (Timalsena & Malla, 2022)

The Electronic Transactions Act of 2008 and the National Cyber Security Policy of 2023 are two of Nepal's main cybersecurity laws, but they are out of date and have insufficient enforcement tools. Due to these flaws, people and companies are now more vulnerable to data theft and cyberattacks. Developed countries like the United States, on the other hand, have created sophisticated legislative frameworks like the Federal Trade Commission (FTC) and the California Consumer Privacy Act (CCPA), which provide guidance on how to handle modern cybersecurity issues.

This particular topic is especially important because it enables a comparison of the strengths and weaknesses of the legal systems in the United States and Nepal, highlighting best practices that Nepal might follow. By addressing these topics, the report hopes to add to the continuing discussion on enhancing cybersecurity regulations in Nepal, ensuring a more secure and robust digital environment for its people and companies.

## **1.1. Aim**

- To identify issues with legal framework of Nepal and learn about different national and international framework

## **1.2. Objectives**

- To gain insight into the current legal frameworks governing cybersecurity in the United States and Nepal.
- To evaluate and contrast the two nations' compliance rules, paying close attention to international alignment, enforcement methods, and data privacy.
- To pinpoint Nepal's legal policy shortcomings and provide solutions based on knowledge gained from the frameworks in the USA.

- To improve knowledge of international cybersecurity standards and how they affect developing nations.

## **2. Literature Review**

### **2.1. Legal Frameworks in Nepal**

- I. **Electronic Transactions Act, 2008 (ETA):** Nepal's fundamental legislation for controlling electronic transactions and preventing cybercrime is the Electronic Transactions Act, 2008 (ETA). In addition to making provisions for digital signatures and verifying the law, it makes hacking, identity theft, and unauthorized access to computer systems illegal. The ETA hasn't been updated to take into account modern threats like ransomware, phishing, and data breaches, despite its initial importance. Important components like required breach notification, severe penalties for data misuse, or guidelines for protecting sensitive data are also absent. This has led to a weak legal framework that is unable to sufficiently protect people and organizations from modern cybersecurity risks. (Government Of Nepal, 2008)
- II. **National Cyber Security Policy, 2023:** Nepal's first broader framework for addressing cyberthreats and improving digital resilience is the National Cyber Security Policy 2023. Approved on August 8, 2023, it emphasizes digital security, vital system protection, and protecting citizens from online harassment and hacking (The Kathmandu Post, 2024). Establishing a National Internet Gateway (NIG), a Cyber Security Center, and encouraging the growth of workforce education and digital literacy are important initiatives. However, the strategy is criticized for possible surveillance expansion, privacy problems, and concerns about NIG censorship. For implementation to be successful, safety precautions and the preservation of digital rights must be addressed. (Republica, 2023)

### **2.2. Legal Frameworks in the United States**

- I. **California Consumer Privacy Act (CCPA):** The CCPA is a significant state-level privacy law that gives customers complete authority over their personal information. These rights include the capacity to view the data that has been gathered on them, remove data, and refuse to have it sold. Companies must put strong security measures in place and give appropriate privacy notifications. Although the law only applies in California, its principles



have impacted privacy practices nationwide. (State of California Department of Justice, 2024)

- II. **Federal Trade Commission (FTC):** An essential regulatory body dealing with data security and privacy issues in the US is the Federal Trade Commission. It has the power to take action against organizations that fail to safeguard customer data and enforces rules against false information security practices. Additionally, the FTC publishes guidelines for protecting sensitive data and aims to guarantee organizations handle personal data in a fair and open manner. (Federal Trade Commission, 2024)

### 3. Methodology and Analysis

#### 3.1. Issues in Nepal's Cybersecurity Framework

There are several major issues with Nepal's present cybersecurity legal framework. They are:

1. **Absence of Comprehensive Legislation:** Ransomware, phishing, and advanced persistent threats (APTs) are examples of developing cyberthreats that are not addressed by the Electronic Transactions Act 2008 (ETA). Because of this, organizations are unprepared to handle sophisticated cyberattacks.
2. **Weak Enforcement Mechanisms:** It is difficult to properly punish cybercriminals in Nepal due to the absence of strong enforcement mechanisms in the country's legislation. Clear policies for incident response, breach reporting, and penalties for failure to comply are lacking.
3. **Limited Resources and Awareness:** Nepal still has a low level of cybersecurity awareness. Many people and organizations lack the assets and knowledge necessary to put effective security practices into action.
4. **International Guidelines Misalignment:** Nepal's cybersecurity laws are inconsistent to international standards like GDPR or ISO 27001. International trust and collaboration are compromised by the asymmetry.

These issues need to be dealt with as soon as possible by the Government of Nepal in order to make Nepal's cyberspace a safe space for the people and organizations to operate on.

### **3.2. Comparative Analysis**

Nepal's legal frameworks are far inferior to international standards, particularly those in the United States. Nepal's framework, which is based on the Electronic Transactions Act of 2008 and the National Cyber Security Policy of 2023, struggles to keep up with the fast evolving digital world. The rules are outdated and ineffective in addressing modern challenges like phishing, ransomware, and data breaches. Furthermore, Nepal's enforcement mechanisms are ineffective, leaving people and companies vulnerable to a number of these cyberattacks.

On the other hand, guidelines such as the California Consumer Privacy Act (CCPA) and Federal Trade Commission (FTC) encourage people by giving them control over their personal data. These frameworks give consumer rights, breach reporting, and data protection more priority. Effective enforcement procedures that maintain these elements guarantee accountability. Even though Nepal still has serious capacity issues, studying these models can help the country's cybersecurity condition.

Nepal's lack of resources and awareness is its biggest problem. Many people and organizations still do not fully comprehend the importance of cybersecurity, which makes it difficult to implement even the most basic safeguards. Nepal's incapacity of adapting its policies to international norms further isolates it from international aid and collaboration.

### **3.3. Case Study: Foodmandu Data Breach (2020)**

One of Nepal's top food delivery services, Foodmandu, experienced a serious data breach in March 2020 that resulted in the exposure of about 50,000 consumers' personal data. Names, phone numbers, email addresses, and delivery addresses were among the compromised data. This information was made public by a hacker, raising the possibility of identity theft, phishing scams, and other cyber exploitation. (Phuyal, 2022)

This case highlights the critical legal issues surrounding data security in Nepal, particularly in the context of the country's underdeveloped cybersecurity legislation. The incident offers insights into the gaps in Nepal's existing legal framework and demonstrates the urgency of creating stronger policies for cybersecurity, data protection, and breach reporting.

### 3.3.1. Key Legal Issues and Analysis

1. **Delayed Breach Notification:** The absence of legal breach reporting requirements in Nepal's legal system was one of the most important issues brought to light by the Foodmandu data breach. Even though the breach revealed private information, Foodmandu failed to alert impacted individuals right away. Thousands of people were left vulnerable for a long time as a result of this delayed response. (Ghimire, 2023)

**Legal Issue:** Companies are not required by law to notify customers of a breach within a certain amount of time, as is required in other jurisdictions such as the General Data Protection Regulation (GDPR) in the European Union, under current laws such as the Electronic Transactions Act of 2008 (ETA).

**Impact:** Users might not have changed their passwords or been alert to phishing attempts if they had received the message sooner.

2. **Insufficient Legal Oversight:** Although it was designed to address concerns such as identity theft, hacking, and cybercrimes, Nepal's fundamental Electronic Transactions Act, 2008 (ETA) lacks specific measures for managing data breaches or enforcing data protection procedures.

**Legal Issue:** The ETA is out of date and does not include specific provisions for reporting breaches, penalties for negligence, or recommendations for protecting sensitive information. Because there isn't enough comprehensive oversight, companies like Foodmandu can't be held responsible for security breaches brought on by negligence or insufficient safeguards.

**Impact:** The hack exposed how the ETA failed to make sure businesses took the necessary precautions to protect consumer data or act quickly in the event of a breach.

3. **Lack of Cybersecurity Preparedness:** The breach revealed Foodmandu's lack of insufficient cybersecurity preparedness. The incident highlighted the platform's absence of important security features, including frequent security audits, penetration testing, and sufficient employee training. (Republica, 2020)

**Legal Issue:** International frameworks like ISO 27001 or even regional recommendations might have assisted Foodmandu in putting strong security measures in place, even though Nepal lacks clear national regulations for cybersecurity activities.

**Impact:** If Foodmandu had followed stricter cybersecurity guidelines, the hack probably could have been avoided. The likelihood of such breaches is increased by Nepal's weak cybersecurity regulations, which also limit a company's capacity to create advance threat mitigation plans.

4. **Gaps in Data Protection and Consumer Rights:** The Foodmandu data breach shows that Nepal's data protection regulations are insufficient to safeguard the private information of its customers. Although many aspects of privacy and security are covered by the Electronic Transactions Act (ETA), there is no defined framework for consumer rights in the case of a data breach. (HimalayanTimes, 2020)

**Legal Issue:** Customers in Nepal are left without options in the event of data misuse or unauthorized access to their information due to the lack of data protection regulations like the General Data Protection Regulation (GDPR) in Europe.

**Impact:** There are only few legal options available to users whose personal information was compromised for restitution or other remedies.

### 3.3.2. Lessons from the Foodmandu Breach

1. **Mandatory Breach Notification Requirements:** The mandatory breach notification required by Nepali legislation is highlighted in the Foodmandu case. Establishing specific guidelines for when organizations should notify the public and effect clients could mitigate the impact of data breaches and protect clients.
2. **Comprehensive Cybersecurity Legislation:** The Foodmandu breach highlights the requirement for reforming Nepal's cybersecurity laws to include comprehensive regulations for data security, breach response, and penalties for negligence. Regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) could serve as models for the development of comprehensive data protection and breach response laws in Nepal.
3. **Cybersecurity Training and Awareness:** A general lack of organizational-level cybersecurity awareness training was one of the primary causes of the breach. To protect customer data, each organization should be required to conduct penetration tests, provide regular security training, and keep up-to-date security procedures.
4. **Enforcement and Accountability:** The breach revealed a lack of accountability and penalties for organizations which do not protect customer data. There is an urgent need for

law enforcement organizations in Nepal that make sure organizations follow data privacy laws and face legal repercussions if the breach occurs.

The Foodmandu data leak serves as a reminder of legal issues in context of security management in Nepal. Nepal must update its legal frameworks, implement strong data protection measures, and ensure improved enforcement of cybersecurity standards in order to prevent similar breaches in the future.

#### **4. Recommendations**

Based on the analysis, the following recommendations are proposed to strengthen Nepal's cybersecurity framework:

1. **Develop Comprehensive Legislation:** Introduce a unified cybersecurity law encompassing data privacy, breach reporting, and penalties for non-compliance. Align the legislation with international standards such as GDPR or ISO 27001.
2. **Establish Robust Enforcement Mechanisms:** Strengthen enforcement through dedicated cybersecurity regulatory bodies, clear guidelines, and penalties.
3. **Enhance Cybersecurity Awareness:** Conduct nationwide awareness campaigns targeting individuals, businesses, and government entities.
4. **Promote Employee Training:** Invest in employee training programs to develop skilled cybersecurity professionals.
5. **Adopt a Consumer-Centric Approach:** Give people more control over their data by including privacy-focused rules in national laws

## **5. Conclusion**

In conclusion, Nepal's current cybersecurity legal framework faces significant challenges in addressing modern cyber threats. The Electronic Transactions Act 2008 and National Cyber Security Policy 2021 provide a basic structure but are outdated and lack important provisions for data protection, breach notifications, and effective enforcement. The Foodmandu data breach (2020) highlights how these gaps leave individuals and organizations vulnerable to cyberattacks. For Nepal to improve its cybersecurity environment, it is crucial to update its laws and regulations to better address new and emerging threats. This includes introducing clear rules for breach reporting, stronger penalties for data misuse, and better mechanisms for enforcing cybersecurity practices. Additionally, raising awareness and improving cybersecurity training across both the public and private sectors will be key to building a more resilient digital ecosystem. By strengthening its legal framework and increasing cybersecurity preparedness, Nepal can better protect its citizens and businesses from cyber risks, ensuring a safer and more secure digital future.

## Bibliography

Federal Trade Commission, 2024. <https://www.ftc.gov/news-events/news/press-releases>. [Online]  
Available at: <https://www.ftc.gov/news-events/news/press-releases>  
[Accessed 2024].

Ghimire, K., 2023. An International Journal of Nepal Library Association. *Cyber-Attack Issues: Laws & Policies and the Role of Librarians*, Volume 2, p. 19.

Government Of Nepal, 2008. *The Electronic Act, 2008*. [Online]  
Available at:  
[https://radiantca.com.np/assets/nav\\_file/Electronic%20Transaction%20Act%202063.pdf](https://radiantca.com.np/assets/nav_file/Electronic%20Transaction%20Act%202063.pdf)

HimalayanTimes, 2020. *HimalayanTimes*. [Online]  
Available at: <https://thehimalayantimes.com/business/foodmandu-portal-hacked>  
[Accessed 2024].

Phuyal, S., 2022. *infosecwriteups*. [Online]  
Available at: <https://infosecwriteups.com/case-study-foodmandu-breach-a3970282cb70>  
[Accessed 2024].

Republica, 2020. *Republica*. [Online]  
Available at: <https://myrepublica.nagariknetwork.com/news/foodmandu-s-website-hacked-50-thousand-users-data-dumped>  
[Accessed 2024].

Republica, 2023. *Republica*. [Online]  
Available at: <https://myrepublica.nagariknetwork.com/news/govt-approves-national-cyber-security-policy-2023/?>  
[Accessed 2024].

State of California Department of Justice, 2024. *CCPA*. [Online]  
Available at: <https://oag.ca.gov/privacy/ccpa>  
[Accessed 2024].

The Kathmandu Post, 2024. *Kathmandu Post*. [Online]  
Available at: <https://kathmandupost.com/science-technology/2023/08/17/government-s-cybersecurity-policy-raises-privacy-and-implementation-concerns?>  
[Accessed 2024].

Timalsena, R. B. & Malla, A., 2022. A Study on Cyber Crime Cases in Nepal: Challenges and Recommendations. *A Study on Cyber Crime Cases in Nepal: Challenges and Recommendations*, pp. 12-25.

U.S. Department of Health and Human Services, 2024. *HHS*. [Online]  
Available at: <https://www.hhs.gov/hipaa/for-professionals/index.html>  
[Accessed 2024].