



# SUPREME COURT OF JUSTICE

---

MAHAWTHADER AI JUSTICE

PRESIDING

---

## Prosecution

*Plaintiff*

**Case No. 1\_100717**

Filed: September 11, 2025

**v.**

**Nyi Nyi**

*Defendant*

Document #0717

Verdict Date: September 11, 2025



## CASE TITLE

The Case of the Zeroed Bills



## SCENARIO

Nyi Nyi, a senior IT systems administrator at the Yangon Electricity Supply Corporation (YESC), is fired after a heated dispute with his supervisor. Two weeks later, an unauthorized remote login occurs on the YESC servers. The intruder uses Nyi Nyi's still-active high-privilege credentials to access the customer billing database—a critical component of the city's power grid infrastructure. The intruder runs a command that alters the electronic billing information for all 50,000 households in Sanchaung Township, changing their monthly amount due to zero. The act causes chaos, requires weeks of data restoration, and damages public trust. The IP address of the intrusion is traced to a public Wi-Fi cafe near Nyi Nyi's home. The prosecution alleges Nyi Nyi committed this act as revenge for his termination.



## APPLICABLE LAW

- Unauthorized Entry into Licensed Operational Areas (Section 68(c))
- Title (Section 1)
- Administrative Orders for Cybersecurity Service Providers (Section 51)



## COURT'S REASONING

Okay, here's a structured legal analysis of the scenario, considering the provided information and the relevant laws.

**I. Legal Elements Satisfied (Prosecution's Case)**

To secure a conviction against Nyi Nyi under the given laws, the prosecution needs to demonstrate the following elements beyond a reasonable doubt:

- Unauthorized Entry (Section 68(c)):** The prosecution will argue that Nyi Nyi engaged in unauthorized entry into a "licensed operational area" – the YESC servers. The fact that the intruder used Nyi Nyi's credentials to access the customer billing database, a crucial component of the power grid, strongly supports this. The 'licensed operational area' is defined by the YESC's operational systems and data. The critical nature of the data accessed (billing information related to a major city's power grid) is key.
- Intent (Revenge):** This is the most crucial element, given the prosecution's theory. The prosecution needs to prove that Nyi Nyi acted with the *specific intent* to cause damage and undermine public trust. The fact that the intrusion occurred two weeks after his termination and the alleged motivation for revenge (termination) creates a strong circumstantial case. Evidence of Nyi Nyi's feelings towards his supervisor and the YESC will be important.
- Causation:** The prosecution must establish a clear causal link between Nyi Nyi's actions and the damage caused. The altered billing information, the resulting chaos, and the weeks of data restoration directly demonstrate this causal link.

**II. Possible Defenses**

Nyi Nyi has several potential defenses:

- Lack of Intent:** This is his primary defense. He can argue that he did *not* authorize the intrusion or the alteration of the billing data. He can claim he has no knowledge of how the intruder gained access to his credentials or utilized them. He could argue he was simply a victim of the hacking.
- Lack of Knowledge of Intrusion:** Nyi Nyi can argue he lacked knowledge of the intruder's activities. He could state he routinely used his credentials and had no reason to suspect any malicious activity. This defense is stronger if he can demonstrate he followed security protocols and used strong passwords (though the fact he continued to use them after termination weakens this).
- Due Process/Procedural Errors (Potentially):** He might raise questions about the investigation. Was sufficient evidence gathered before charging him? Were proper procedures followed in collecting and presenting evidence? This would be a secondary defense, focusing on potential flaws in the prosecution's case.
- Shared Responsibility (Complex):** He could argue the YESC itself was negligent in its security practices, allowing his credentials to be vulnerable. However, this defense is challenging and requires evidence of systemic security failures.

**III. Likely Outcome**

**The Prosecution's Case is Strong, but the Outcome is Not Guaranteed.**

**Likely Verdict:** Given the evidence – the unauthorized access, the critical nature of the data compromised, and the prosecution's theory of revenge – it is *likely* that Nyi Nyi would be found guilty. The circumstantial evidence is compelling. The prosecution has a reasonable probability of proving his intent.

**Potential Sentence:** The sentence would likely be substantial, reflecting the serious consequences of the crime. It could involve a prison sentence (potentially several years), significant fines, and a criminal record. The specific sentence would be determined by the judge, considering factors such as the severity of the damage, Nyi Nyi's criminal history (if any), and mitigating circumstances.

**Key Factors Influencing the Outcome:**

- Evidence of Credential Security:** How did the intruder gain

access to Nyi Nyi's credentials? If evidence shows YESC had significant security vulnerabilities, this could weaken the prosecution's case. \* \*\*Witness Testimony:\*\* The credibility of witnesses (e.g., investigating officers, YESC employees) will be crucial. \* \*\*Expert Testimony:\*\* Cybersecurity experts could be called to explain the technical aspects of the intrusion and the vulnerabilities involved. \*\*Disclaimer:\*\* \*I am an AI Chatbot and not a legal professional. This analysis is for informational purposes only and should not be considered legal advice. Legal outcomes are highly dependent on specific facts, evidence, and the interpretation of the law by judges and juries.\* To further refine this analysis, more details about the security protocols at YESC, the intruder's methods, and any evidence of Nyi Nyi's state of mind would be needed.

## ✓ **DECISION**

Guilty under Unauthorized Entry into Licensed Operational Areas (Section 68(c)): 1 years' imprisonment. Guilty under Title (Section 1): 1 years' imprisonment. Guilty under Administrative Orders for Cybersecurity Service Providers (Section 51): 1 years' imprisonment.

## 🕒 **TOTAL IMPRISONMENT**

3 years