Republic

of

the

Philippines

**SORSOGON**

**STATE**

**UNIVERSITY**

**College**

**of**

**Information**

**and**

**Communication**

**Technology**

**Information**

**Technology**

**Bulan**

**Campus**

*Zone-8,*

*Bulan,*

*Sorsogon*

Tel.

No.;

056

311-0103

;

Email

address:

bsit\_pc@sorsu.edu.ph



**TASK #2: CYBERSECURITY THREAT INCIDENT**

**IT 322 - INFORMATION ASSURANCE AND SECURITY I**

2nd Semester A.Y. 2023-2024

Prepared by: Leony Balbuena Brizuela Date: 11/02/2024

Program Year-Block: BSIT 3-2

Data Breach Issues Affect Philippines as Country Works to Strengthen Cyber Defences

The country's cybersecurity flaws have drawn criticism to the government. According to a recent assessment, the Philippines is highly vulnerable to cyberattacks because of its extensive internet use, low cybersecurity awareness, and inadequate cybersecurity infrastructure.

On October 13, hackers vandalized and momentarily took down the website of the lower house of the Philippine Congress, the House of Representatives. Data leaks were also recently experienced by the Philippine Statistics Authority (PSA) and the Department of Science and Technology.

On October 3, after the insurer allegedly declined to pay a C$410,000 ransom, hackers gained access to a significant amount of personal data stored on the servers of the Philippine Health Insurance Corporation (PhilHealth). The data breach impacted thirteen million people, including Filipino employees abroad.

The PSA acknowledged that there had been a data breach that affected its Community-Based Monitoring System, which is a digital system for collecting and processing data used to carry out programs aimed at reducing poverty. According to the PSA, the data breach did not affect personal information like birth certificates and national ID numbers.

Millions of Filipinos' personal information, including information from vital organizations like the Bureau of Internal Revenue, the National Bureau of Investigation, and the Philippine National Police, was compromised in a significant data breach that occurred in April 2023. Later, compromised Philippine government subdomains' stolen data logs surfaced on the Russian black market.

A wave of recent cyberattacks against private sector companies and government websites have hit the Philippines, jeopardizing national security and exposing millions of people's personal information. The Armed Forces of the Philippines (AFP) have established a "cyber command" and are hiring cyber specialists to strengthen the nation's cyber defenses. Manila has also outlawed the use of AI-powered software by its armed forces as it can produce a virtual character that emulates the speech and motion of an actual person, posing privacy and security risks.