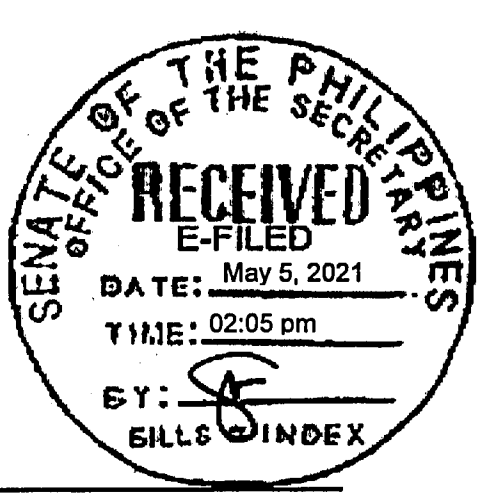
EIGHTEENTH CONGRESS OF THE)
REPUBLIC OF THE PHILIPPINES)
Second Regular Session)



SENATE

P.S. Res. No. 713

Introduced by **SENATOR LEILA M. DE LIMA**

RESOLUTION
URGING THE APPROPRIATE SENATE COMMITTEE TO CONDUCT AN INQUIRY, IN AID OF LEGISLATION, ON THE REPORTS OF SERIOUS DATA BREACH OF SENSITIVE COURT DOCUMENTS FROM THE OFFICE OF THE SOLICITOR GENERAL WHICH HAS THE DANGEROUS POTENTIAL OF CAUSING SEVERE CONSEQUENCES TO ONGOING JUDICIAL PROCEEDINGS INVOLVING KEY GOVERNMENT AGENCIES, WITH THE END IN VIEW OF REVIEWING PERTINENT LAWS TO STRENGTHEN THE PROTECTION OF THE FILIPINO PEOPLE, INSTITUTIONS, AND INFORMATION RESOURCES FROM CYBER-ATTACKS AND OTHER CYBER THREATS

WHEREAS, Article II, Section 5 of the 1987 Philippine Constitution provides that "[t]he maintenance of peace and order, the protection of life, liberty, and property, and promotion of the general welfare are essential for the enjoyment by all the people of the blessings of democracy";

WHEREAS, Republic Act No. 10175, also known as "Cybercrime Prevention Act of 2012," states that "[t]he State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology (ICT) to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts";

WHEREAS, the same law mandates for the State to "adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection,

investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation";

WHEREAS, on 1 May 2021, it was reported that "[f]or at least two months, some 345,000 sensitive court documents from the Office of the Solicitor General of the Philippines related to ongoing legal cases were made publicly available online and could have been accessed by anyone who knew where to look." Said data exposure was disclosed by the security company TurgenSec;[1]

WHEREAS, according to said news report, "information in the documents [which was leaked] could affect ongoing court cases and might be used to identify witnesses or attempt to intimidate victims." The overwhelming implication of such data breach cannot thus be denied, considering that the Office of the Solicitor General (OSG) represents the government in any litigation that goes to the Philippine Supreme Court or Court of Appeals;[2]

WHEREAS, TurgenSec said that the nature of these documents "is of particular concern as it may have the potential to disrupt [or] undermine ongoing judicial proceedings." The attack exposed information to the public "where anyone with a browser and internet connection could access it." Documents exposed were said to have contained sensitive keywords such as "Private", "Confidential", "Password" and "Witness". The breach also included topics on intelligence, terrorism, drugs, execution, the opposition, the military, on COVID-19, and even on President Rodrigo Duterte;[3]

WHEREAS, the security firm said that given the "particularly alarming" nature of the incident, it emailed the OSG and the Philippine government twice in March, but it did not get responses on both occasions. The breach, it stressed, has led to information falling "now in the hands of malicious actors who could do considerable damage with it if mitigation steps are not taken";[4]

---

[1] Elliott, V. (1 May 2021) *345,000 sensitive legal documents from the PH government have been exposed online.* Retrieved last 3 May 2021 from: https://www.rappler.com/nation/sensitive-legal-documents-philippine-government-have-been-exposed-online
[2] Ibid
[3] Deiparine, C. (2 May 2021) *DOJ: Solgen's office looking into reported data breach.* Retrieved last 03 May 2021 from: https://www.philstar.com/headlines/2021/05/02/2095356/doj-solgens-office-looking-reported-data-breach
[4] *Ibid.*

WHEREAS, despite the alarming situation, the Department of Justice (DOJ) for its part said that it has not yet received official information on the matter;[5]

WHEREAS, this is neither the first attack against the OSG, nor an isolated incident. In December 2016, hackers which identified themselves as the Phantom Troupe were able to deface the OSG website. The OSG assured the public then that the "incident is being taken seriously", and that they have already augmented their security measures and even engaged the assistance of the intelligence and investigation agencies of the government. Despite such assurance, however, the latest breach still occurred compromising hundreds of thousands of sensitive documents;

WHEREAS, despite having a "National CyberSecurity Plan 2022" in place which was launched by the Department of Information and Technology (DICT) as far back as 2017 which aimed to institutionalize the adoption of Information Security Governance and Risk Management approaches that are based on global standards and which sought to establish the National Computer Emergency Response Team (NCERT) to enable the government to swiftly respond and recover from cyber-attacks, both the government and private firms in the country were left in the dark in various episodes of cyber-attacks;

WHEARAS, a cyber-security firm made an assessment that the Philippines was the seventh country most attacked by cybercriminals in the last quarter of 2019. The same report said that "the nation continued to be one of the most attractive targets for cybercriminals, as 3.9 million web threats were detected" in computers of the clients of the said company across the country during the October to December period of 2019;[6]

WHEREAS, in 2016, the country suffered its "worst-ever government data breach" on the Commission on Election's (COMELEC) website where an anonymous group was able to access personal information, including fingerprint data and passport information, with around 70 million people said to have been compromised. Consequently, a second hacker group called "LulzSec Philippines" was believed to

---

[5] Cabuenas, J. (3 May 2021) *Data breach exposed 345,000 sensitive SolGen documents in April —British cybersecurity firm.* Retrieved last 03 May 2021 from: https://www.gmanetwork.com/news/scitech/technology/785985/data-breach-exposed-345-000-sensitive-solgen-documents-in-april-british-cybersecurity-firm/story/

[6] Esmael, L. (28 January 2020) *PH vulnerable to cybercriminals.* Retrieved last 2 May 2021 from: https://www.manilatimes.net/2020/01/28/news/national/ph-vulnerable-to-cybercriminals/677814/

have posted COMELEC's entire database online several days later. Amid claims that no sensitive information was released, according to multiple reports, cyber-security firm Trend Micro believes the incident is the biggest government-related data breach in history and that authorities are only downplaying the problem. Despite such attempts by the authorities to underemphasize the incident, the firm warned that "every registered voter in the Philippines is now susceptible to fraud and other risks";[7]

WHEREAS, in past years, several agencies of the Philippine Government continued to suffer several cyber-attacks resulting to data breaches of important information. Some of these incidents include the reported intrusion into the Armed Forces of the Philippines' military personnel database leaking information of thousands of their members[8], and the Tech4Ed project of the Department of Information and Technology (DOST) with more than four million lines of data downloaded by the hacker among many other related incidents;[9]

WHEREAS, on 7 December 2020, the vulnerability of the country to cyber-attacks was confirmed by no less than National Security Adviser Hermogenes Esperon Jr. when he admitted in a Senate Hearing that the country has no "operations center" to defend against cyber-attacks on a national level[10], raising concerns on the preparedness and seriousness of the government in addressing this prevailing problem;

WHEREAS, the OSG should inform the Senate of the extent of damage caused by the cybersecurity breach, as well as the litigants whose information were compromised. The OSG must "publicly outline the extent of the information exposed and breached, and what steps are being taken to ensure this cannot happen again";

WHEREAS, the exposure of information of a particularly highly sensitive nature must not be ignored. Before using their resources in private cases, the OSG must first ensure that their core functions are done including protecting the interest

---

[7] Chi, L. (11 April 2016) *Philippines elections hack 'leaks voter data'*. Retrieved last 2 May 2021 from: https://www.bbc.com/news/technology-36013713

[8] Mangosing, F. (3 April 2021) *Philippine military probes reported breach of its database*. Retrieved last 3 May 2021 from: https://newsinfo.inquirer.net/1102917/philippine-military-probes-reported-breach-of-its-database

[9] Manila Bulletin (26 April 2019) *Tech4Ed website breached*. Retrieved last 3 May 2021 from: https://mb.com.ph/2019/04/26/tech4ed-website-breached/

[10] Gotinga, J. (7 December 2021) *PH has no cybersecurity operations center, says Esperon in Dito Telecom hearing*. Retrieved last 3 May 2021 from: https://www.rappler.com/nation/esperon-says-philippines-no-cybersecurity-operations-center-senate-hearing-dito-telecom

and private information of their clients, which are agencies of the national government;

WHEREAS, the OSG must be as swift as it has been in going after its declared enemies, in tracking down the perpetrators of the continued cyber-attacks against it which jeopardizes not only matters of State concern, but as well as pertinent information relating to government agencies and private individuals which could have also been likely leaked;

WHEREAS, the far-reaching ramifications of this breach could lead to greatly influencing ongoing court cases, and may even lead to the information being used to identify witnesses or attempt to intimidate victims. Therefore, such cyber-attacks demand a thorough investigation and a swift recalibration of government policy on cyber-security;

WHEREAS, there is a need to urgently address the persisting vulnerabilities of our cyber-security infrastructures and expeditiously put in place policies and safeguards to protect our citizens and institutions from assaults and exploitation of hackers and criminals;

WHEREAS, it is imperative to investigate the continuous proliferation and alarming trend of cyber-attacks against the Government and private firms in the country and put an end in the manipulation, abuse and misuse of pertinent information of the public to the advantages of these online lawbreakers;

NOW, THEREFORE, BE IT RESOLVED BY THE SENATE, to urge the appropriate Senate Committee to conduct an inquiry, in aid of legislation, on the reports of serious data breach of sensitive court documents from the Office of the Solicitor General which has the dangerous potential of causing severe consequences to ongoing judicial proceedings involving key government agencies, with the end in view of reviewing pertinent laws to strengthen the protection of the Filipino people, institutions, and information resources from cyber-attacks and other cyber threats.

Adopted,

LEILA M. DE LIMA