

The Challenges and Polemics of Securing Indonesia's National Data Centers

Background

Indonesia decided to establish a National Data Center, or Pusat Data Nasional (PDN), to improve the efficacy and effectiveness of data-integrated public services. The PDN is the government's response to the challenges of providing public services and utilizing digital technology. The policy's primary goal is to improve budgetary efficiency in data management. PDN is designed to cover the entire Indonesian archipelago, with four points in specific areas. Specifically, Batam, Riau Islands; Labuan Bajo, East Nusa Tenggara; and the Future Indonesia New National Capital (IKN) Nusantara in East Kalimantan, with French government assistance.

Various government agencies, including those at the national and regional levels, have created 27,000 apps [1]. To accommodate this, data centers must be established, and this entails a considerable financial investment. Many government agencies built their own data centers (DC) or worked with third-party vendors. As a result, the existence of these data centers becomes redundant, and, in some cases, unsustainable. These procedures also contradict the central government's "one data" policy [2]. Based on these premises, Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems (SPBE) was signed in the midst of debates over the benefits and drawbacks of "data centralization" concepts. The Ministry of Communication and Informatics (MoCI) is the sole agency in charge of developing PDN, and they immediately used their internal resources and procedures.

Following the President's Joko Widodo's directive to accelerate the digitalization and transformation process at the end of his term, the MoCI decided in 2022 to establish a cloud-based temporary national data center (PDNS). This policy is strengthened by Presidential Regulation No. 132/2022, which addresses the National Electronic-Based Government System Architecture. Since then, 282 services from 210 governmental institutions have already provided data to the PDNS. PDNS facilities are currently located in two zones: Cikarang (PDNS-1) and Surabaya (PDNS-2), with a backup facility in Tangerang and a cold-site [3] in Batam.

Indonesia's PDNS database takes advantage of cloud technology while adhering to global standards. National DCs and other critical infrastructure should be built on the highest level of DC infrastructure. Tier-3 for large-scale and Tier-4 DCs that are entirely "fault tolerant," individual equipment failure will have no impact on operations due to independent distribution paths and multiple physically isolated systems [4]. The design includes interoperability at all levels and a disaster recovery center (DRC). Everything appears to be functioning properly. Is this true?

Table 1.
Data Center Tiers Standard Classification (Source: PhoenixMap)

PARAMETERS	TIER 1	TIER 2	TIER 3	TIER 4
Uptime guarantee	99.671%	99.741%	99.982%	99.995%
Downtime per year	<28.8 hours	<22 hours	<1.6 hours	<26.3 minutes
Component redundancy	None	Partial power and cooling redundancy (partial N+1)	Full N+1	Fault tolerant (2N or 2N+1)
Concurrently maintainable	No	No	Partially	Yes
Price	\$	\$\$	\$\$\$	\$\$\$\$
Compartmentalization	No	No	No	Yes
Staffing	None	1 shift	1+ shift	24/7/365
Typical customer	Small companies and start-ups with simple requirements	SMBs	Growing and large businesses	Government entities and large enterprises
The main reason why companies select this tier	The most affordable data center tier	A good cost-to-performance ratio	A fine line between high performance and affordability	A fault-tolerant facility ideal for consistently high levels of traffic or processing demands

Polemics and incidents

The public was shocked by a security incident that occurred in mid-June 2024. PDNS-2 has been subjected to a cyberattack in the form of ransomware since Monday, June 17, 2024, at approximately midnight. PDNS became inaccessible on Thursday, June 20, 2024. As a result, public services that rely on PDNS data, such as immigration, were rendered inaccessible, resulting in the widespread paralysis of Indonesian public services.

For more than a week, most public services have been paralyzed due to a lack of data and applications to support digital services for the public. After days of public pressure, the government revealed that PDNS had been breached by hackers who planted ransomware and demanded rewards. Previously, MoCI always stated that there was an "incident," and that the MoCI team was recovering services from "disturbances" via press release No. 409/HM/KOMINFO/06/2024.

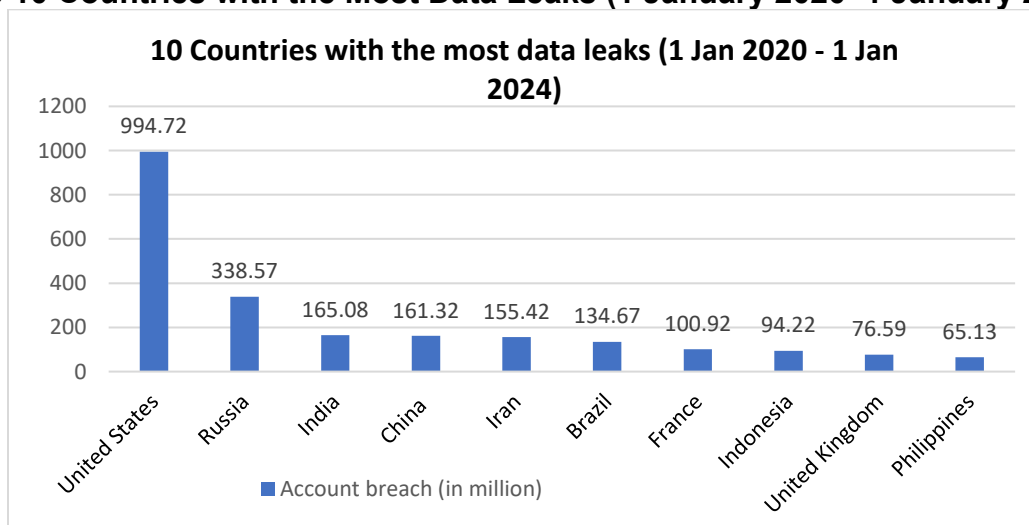
The MoCI and the National Cyber and Crypto Agency (BSSN) are two government agencies that have addressed (and are accountable for) the issue of PDNS. Which, two weeks after the incident, declared that it had "given up" on the fight against ransomware. However, it refused to pay the ransom [5]. As a result, the extracted data cannot be retrieved. Unfortunately, only 2% of the data was backed up, implying that only about five agencies' data could be recovered. [6] [7]

Controversies continued to arise. First, regarding the architectural design and construction of PDN and PDNS, the disadvantages of data centralization became evident during this incident. Several technical opinions resurfaced, such as the debate between centralized data versus distributed and modular monolithic architectures. Additionally, the architectural and security designs created by the Ministry of Communication and Informatics (MoCI) lacked public and stakeholder participation. Consequently, there was no significant input or involvement from the public, especially the technical community.

Second, there have been heated discussions about the government's lack of cyber security. Previously, the data of a number of government institutions, including the General Election Commission (KPU) and the Health and Social Security Administering Agency (BPJS), was compromised and sold. For example, sensitive information from the Indonesian Strategic Intelligence Agency (BAIS) of the Indonesian Military (TNI) and the Indonesia Automatic Finger Identification System (INAFIS) of the National Police (Polri) has been compromised and sold on the dark web [8] [9].

Personal data breaches occurred at least 113 times over the last two years, for a total of 302 digital security incidents. On average, 25 incidents occur per month. According to SAFEnet monitoring, 36 instances will occur in 2022 and 77 in 2023. [10] According to Surfshark, between January 2020 and January 2024, approximately 3.96 billion digital accounts experienced data leaks. During this time, Indonesia had the eighth highest number of data leaks in the world, with an estimated 94.22 million compromised accounts (see Graph 1). [11]

Graph. 1.
Top 10 Countries with the Most Data Leaks (1 January 2020–1 January 2024)

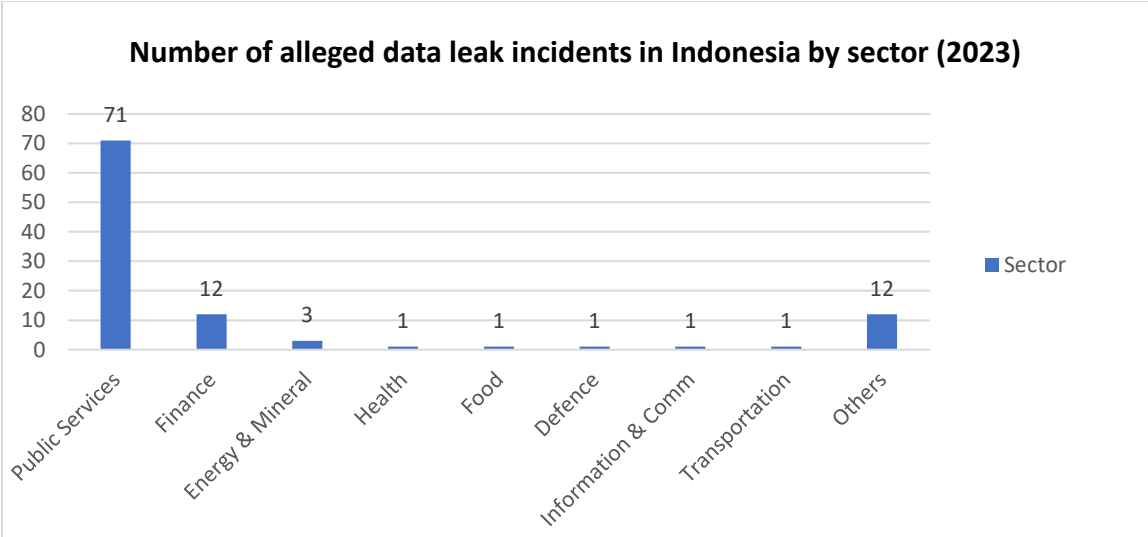


Source: Surfshark (2024)

According to a report by the National Cyber and Crypto Agency (BSSN), throughout 2023 there were 103 suspected data leak incidents detected in Indonesia. Of all suspected

data leaks detected in 2023, 69% or 71 incidents occurred in the government administration sector (see Graph 2) [12]. BSSN stated that 74 million traffic anomalies from January to May 2024, and more than 44 million were malware activities [13].

Graph. 2.
Number of Data Leaks Incident in Indonesia 2023 – By Sector
(source: Katadata, 2024)



Source: Katadata (2024)

Critical Lessons-Learned

The current paralysis of PDNS proves the government's lack of commitment, capacity, competence and consistency in carrying out the vital infrastructure development process, which has been claimed to be safe and reliable and applying high standards. In terms of planning and development of vital critical infrastructure, PDNS has potential risk of Single Point of Failure (SPOF) which is a defect in the design, implementation, or configuration of a circuit or system. SPOF denotes a single defect or malfunction that has the potential to terminate the operation of an entire system. Therefore, agencies that store data in PDNS are unable to take any action in this situation, except to wait and rely on the efforts of MoCI and BSSN.

Despite the fact that BSSN had "predicted" the ransomware attack [14] and MoCI had reassured us that the security of PDN and PDNS was guaranteed, there are no valid guarantees; all are simply false pledges. The present ransomware attack on PDNS must be attributed to MoCI and BSSN. A recent online petition was launched to request that the Minister of Communication and Information, Budi Arie Setiadi, resign in order to

publicly apologize and accept responsibility for this situation [15]. More than 25,000 individuals had signed the petition as of July 6, 2004 [16].

Additionally, the government is required to adhere to the Personal Data Protection Law No. 27/2022 and assume responsibility. For instance, data owners should be informed of any attempted breaches, as well as any breaches that have occurred. When PDNS breached this processes is bypassed.

Future Securing PDN/PDNS

It is necessary to ensure the security of data centers through different means in order to avoid the data leaks in the future. First, thorough audit that encompasses procurement and tender-and-winning processes, as well as the most stringent work standards that have been implemented. Indonesian President Joko Widodo has recently ordered an audit of government data centres on Friday [17]. Indonesia's Development and Finance Controller (BPKP) is required to conduct this audit. In the internal MoCI and BSSN, comprehensive audit of cyber security technology and human resources at PDN/PDNS.

Second, accountability. The issue cannot be resolved by merely patching the leak. Leadership is the fundamental issue. The demand for the Minister of Communications and Information Technology to resign is a logical outcome in this instance. Indonesia has consistently appointed ICT ministers to political positions, rather than placing them with experts who possess a comprehensive understanding of data protection and security, as well as a vision and mission for effective information technology governance.

Third, enhance cybersecurity governance and data security. Back-ups are absolutely necessary. The data of critical users is stored in DCs, while vital and critical data is stored in PDN/PDNS. In order to mitigate data loss, it is imperative that all critical data be routinely backed up and stored in a distinct location. Backups should be encrypted and evaluated on a regular basis to guarantee that they can be restored accurately. A Data Recovery Centre (DRC) can be of critical importance in the event of a primary system disruption and can be promptly implemented to mitigate damages.

Fourth, enhancing the capacity of personnel from the MoCI, BSSN, and PDN/PDNS, as well as the intrusion detection system (IDS) and network monitoring tools. It is also essential to adopt a collaborative, multi-stakeholder approach to the strengthening and security of digital infrastructures. In order to mitigate cyber threats, it is imperative that the government collaborate with technology companies and non-governmental organisations to exchange information and resources [18].

Concluding Remarks

PDN and PDNS are critical national infrastructures that rely on technology. Ransomware attacks highlight the vulnerabilities of this digital infrastructure. However, the solution is not to terminate PDN and PDNS. Despite the fact that many people, including the technical community and the general public who receive government services, are disappointed with the current concepts of PDN and PDNS, finding ways to improve and secure these systems is essential.

Preventive measures must be diligent and comprehensive. Protecting personal data and addressing national cybersecurity vulnerabilities are crucial. To ensure accountability and the highest level of security, reprocessing and auditing are essential. Additionally, demonstrating trustworthy leadership and the ability to overcome breaches is vital. Currently, public trust is declining, so policymakers must exercise caution and take necessary steps to restore it.

Reference

[1] ANTARA Indonesia National News Agency. May 17, 2023. Minister Anas Looks to Tidy Up 27,000 Apps Using SPBE. <https://en.antaranews.com/news/282012/minister-anas-looks-to-tidy-up-27000-apps-using-spbe>

[2] Open Government Partnership. Indonesia. Commitments: Implement One Data Policy Indonesia [ID0113]. <https://www.opengovpartnership.org/members/indonesia/commitments/ID0113/>

[3] A cold site is basically an empty building, backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site. Retrieved from https://csrc.nist.gov/glossary/term/cold_site

[4] Velimirovic, A. 25 November 25, 2021. Data Center Tiers Explained. Phoenix Nap. <https://phoenixnap.com/blog/data-center-tiers-classification>

[5] Poerwoto, Y.P. June 22, 2024. Government Resigns to Data Loss Due to PDN Attack by Ransomware, Roy Suryo Urges Budi Arie to Resign. Tribun News. <https://www.tribunnews.com/nasional/2024/06/27/pemerintah-pasrah-data-hilang-imbac-pdn-diserang-ransomware-roy-suryo-desak-budi-arie-mundur>

[6] Rakhmayanti I & Putri N. June 28, 2024. The Reason National Data Center Backups Are Only 2% Finally Revealed. CNBC Indonesia.

<https://www.cnbcindonesia.com/tech/20240628080944-37-550082/alasan-backup-pusat-data-nasional-hanya-2-akhirnya-terungkap>

[7] Tanamal, Y. & Sekar. A. June 29, 2024. Public Urge Immediate Data Collection After Ransomware Attack. The Jakarta Post.

<https://www.thejakartapost.com/indonesia/2024/06/29/public-urge-immediate-data-recovery-after-ransomware-attack.html>

[8] Indonesia Business Post. June 27, 2024. BAIS, Police's INAFIS data breached and sold on Dark Web. <https://indonesiabusinesspost.com/insider/bais-polices-inafis-data-breached-and-sold-on-dark-web/>

[9] Suhenda, D. June 26, 2024. Police to probe reported fingerprint sales data on dark web. The Jakarta Post. <https://www.thejakartapost.com/indonesia/2024/06/26/police-to-probe-reported-fingerprint-data-sales-on-dark-web.html>

[10] SAFENet. 2023. Report: Digital Rights Situation in Indonesia Had Worsened. Southeast Asia Freedom of Expression Network. <https://safenet.or.id/2023/03/the-digital-rights-situation-in-indonesia-had-worsened/>

[11] Ahdiat, A. July 2, 2024. Indonesia is among the 10 countries with the largest data leaks. Katadata. <https://databoks.katadata.co.id/infografik/2024/07/02/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar>

[12] Ahdiat, A. June 26, 2024. The Most Indonesian Data Leaks are from the Government Sector. Katadata. <https://databoks.katadata.co.id/datapublish/2024/06/26/kebocoran-data-ri-terbanyak-dari-sektor-pemerintahan>

[13] CNN Indonesia, May 16, 2024. BSSN Detects 44 million Malware Activities Until May 2024. <https://www.cnnindonesia.com/teknologi/20240516184354-185-1098626/bssn-deteksi-44-juta-aktivitas-malware-hingga-mei-2024>

[14] ANTARA Indonesia National News Agency. June 27, 2024. BSSN said that in 2023 it predicted that there would be a cyber attack in 2024. <https://www.antaraneews.com/berita/4171341/bssn-sebut-pada-2023-sudah-prediksi-akan-ada-serangan-siber-di-2024>

[15] Balowski, J. (trans.). June 27, 2024. SafeNET lunches petition calling on information minister to resign over cyber attack. Asia Pacific Solidarity Network. <https://www.asia-pacific-solidarity.net/news/2024-06-27/safenet-lunches-petition-calling-information-minister-resign-over-cyber-attack.html>

[16] Change.org. June 26, 2024. PDNS Hit by Ransomware, Minister of Communication and Information Budi Arie Setiadi Must Resign!

https://www.change.org/p/pdns-kena-ransomware-menteri-kominfo-budi-arie-setiadi-harus-mundur?source_location=petitions_browse

[17] Sulaiman S. & Widiyanto, S., June 28, 2024. Indonesia president orders audit of data centers after cyberattack. Reuters.

<https://www.reuters.com/technology/cybersecurity/bulk-indonesia-data-hit-by-cyberattack-not-backed-up-officials-say-2024-06-28/>

[18] Monash University, Indonesia. June 25, 2024. National Security Alert: Analyzing Ransomware Attacks and Preventative Measures.

<https://www.monash.edu/indonesia/news/national-security-alert-analyzing-ransomware-attacks-and-preventative-measures>