# Cybersecurity and Cyber Resilience in Indonesia: Challenges and Opportunities

**By:** Katya Loviana
**Editor:** M. Perdana Karim


As technology constantly develops, the topic of cybersecurity and the act of cybercrime also became more diverse, complex, and advanced. The pandemic that significantly transformed the role of technology in people's working and personal lives has made cybersecurity more important than ever. Lohrmann even called the year 2020 the year of the Cyber Pandemic.[1] Thus, the current discussion of cybersecurity has started to shift from cybersecurity to cyber resilience, that is the capability to anticipate for, respond to, and recover from cyberattacks.[2]

In Indonesia, the landscape of cybersecurity and/or cyber resilience is heading towards development. Indonesia's Global Security Index in 2020 achieved a rank of 24 globally and 6 in the Asia Pacific region with a score of 94.88[3] however, in 2021, Sularso from *Badan Siber dan Sandi Negara* (BSSN) stated that Indonesia is included within the top 10 countries with the most source and target of anomalies in cybersecurity with 190 million attacks coming from and 1 billion attacks targeted to Indonesia.[4] These cyberattacks consequently come with a burdening cost for the society and government, such as the case of BPJS data breach in 2021 that leaked 297 million personal data of Indonesian citizens with an approximate cost of Rp600 trillion.[5] Seeing these ups and downs in the Indonesian cybersecurity and cyber resilience landscape, what are the core challenges faced that trigger them?

[1] Lohrmann, D., 2020. 2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic. [online] Available at: <https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html> [Accessed 7 April 2022].
[2] IT Governance, n.d. What is cyber resilience | IT Governance UK. [online] Available at: <https://www.itgovernance.co.uk/cyber-resilience> [Accessed 7 April 2022].
[3] International Telecommunication Union, 2020. Global Security Index 2020: Measuring commitment to cybersecurity. ITU Publications. [online] Available at: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf> [Accessed 7 April 2022].
[4] Sularso, G.., 2022. Diskusi Keamanan Siber Bagi Para Pemangku Kebijakan Pandemi CfDS.
[5] CSIRT, 2021. Indonesia Rugi Lebih Dari 600 trilyun Rupiah Akibat Kebocoran 279 Juta Data Penduduk. [online] Available at: <https://csirt.id/pers-release-124052021> [Accessed 2 April 2022].

## Challenges

The challenges faced in Indonesia regarding cybersecurity and cyber resilience can be divided into three main pillars: regulation, technology, and human capital. From the regulation point of view, there is still no single law that regulates cybersecurity in Indonesia. The draft bill for cybersecurity and cyber resilience, that is *Rancangan Undang-Undang Keamanan dan Ketahanan Siber*, was canceled due to protests towards its burdening conditions for business entities.[6] Hence, to this day, the issue still moves under few 'umbrella' regulations regarding cyberspace, such as Law No. 19 /2016 on Electronic Information and Transaction, Law No. 36 / 1999 on Telecommunication, and Ministry of ICT Regulation No. 5 / 2017 on Internet Protocol-Based Telecommunication Network Security.[7]

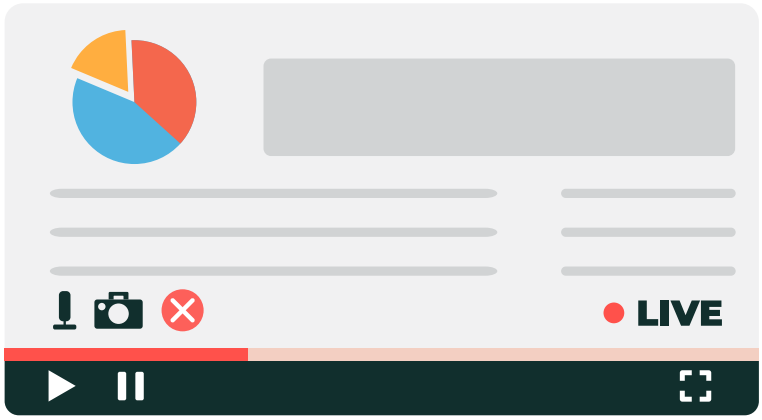
From a technical point of view, Indonesia has yet to have any patent on technological products.[8] This creates a challenge for Indonesia to ensure the safety of the products used widely by the society for both personal and work needs. Even worse, a survey by Secure Code Warrior stated that 86% of developers do not view application security as a priority.[9] This further puts Indonesia's cybersecurity and cyber resilience at risk, especially when training at offices often 'forget' the importance of briefing backup and security measures in using technologies.

Within the government itself, the development of an Electronic-Based Government System (SPBE) is commonly defined as digital transformation to app-based government administration. The apps are also seen as not sustainable, overlapping with each other, and contradict the main purpose of their development, that is to ease the previously complicated bureaucracy system.[10] These flaws in Indonesia's cybersecurity and resilience urgently need to be resolved, which leads to the next and most important pillar: human capital.

---

[6] CIPS, 2021. Ringkasan Kebijakan | Perlindungan Keamanan Siber di Indonesia. [online] Available at: <https://id.cips-indonesia.org/post/ringkasan-kebijakan-perlindungan-keamanan-siber-di-indonesia> [Accessed 7 April 2022].
[7] Shafira, I., 2021. Analyzing Indonesia's National Cybersecurity Strategy. [online] Available at: <https://cfds.fisipol.ugm.ac.id/2021/07/28/analyzing-indonesias-national-cybersecurity-strategy/> [Accessed 7 April 2022].
[8] Sutedja, A., 2022. Diskusi Keamanan Siber Bagi Para Pemangku Kebijakan Pandemi CfDS.
[9] Secure Code Warrior, 2022. Secure Code Warrior Survey Finds 86% of Developers Do Not View Application Security As a Top Priority. [online] Available at: <https://www.securecodewarrior.com/press-releases/secure-code-warrior-survey-finds-86-of-developers-do-not-view-application-security-as-a-top-priority> [Accessed 9 April 2022].
[10] Yayusman, M., 2022. Diskusi Keamanan Siber Bagi Para Pemangku Kebijakan Pandemi CfDS.

As the operator of technology, human capital plays the most important part in improving and strengthening cybersecurity and cyber resilience in Indonesia. Often, individuals report data breaches and unauthorized spread of personal information. However, these cases of "data breaches" are mostly not categorized as "breaches" because individuals, without knowledge, publish their personal data unsafely on the internet. This is one among many examples of the low levels of knowledge on security in using technology. Due to the fear of missing out (FOMO), people, and even authorities, often jump into on-trend technology innovation without learning about it beforehand. Thus, education and socialization for awareness-building cybersecurity is needed for everyone in Indonesia to catch up with the rapid technological development safely. Furthermore, from the CIA (Confidentiality, Integrity, Availability) triad, integrity is often left out. Many cases of data breaches tend to come from internal aspects as data is the new oil that people pay well for.[11] Other times, these cases happen unintentionally, which relates back to the importance for everyone to understand cybersecurity and the need for strengthening working culture and SOPs to prevent internal cyberattacks.




## Opportunities

Despite the challenges, the situation also presents opportunities for cybersecurity and cyber resilience strengthening in Indonesia. For starters, there is a growing awareness regarding the issue. More companies are starting to put security as a priority. From the government point of view, Presidential Regulation no 28/2021 (Peraturan Presiden No. 28 Tahun 2021) about BSSN Reorganization puts hope for improvement in cybersecurity as it gives BSSN space to work more effectively, efficiently, and right on the target.[12] Other than that, training and certification are also facilitated by the government and organizations, such as Digital Talent Scholarship held by KOMINFO,[13] Cybersecurity Training 2021 held by InfraDigital Foundation and Mastercard Center for Inclusive Growth,[14] and courses on Cybersecurity held by Google.[15] As people are getting familiarized with using technology, learning and understanding the topic through many choices of platforms will hopefully be easier.

[11] Sutcliffe and Co., n.d. The 8 Most Common Causes of Data Breach. [online] Available at: https://www.sutcliffeinsurance.co.uk/news/8-most-common-causes-of-data-breach/ [Accessed 9 April 2022].
[12] Peraturan Presiden (PERPRES) No.28 Tahun 2021 tentang Badan Siber dan Sandi Negara.
[13] KOMINFO, n.d. Tentang Kami: Informasi tentang Digitalent Scholarship Kominfo. [online] Available at: <https://digitalent.kominfo.go.id/tentang-kami> [Accessed 9 April 2022].
[14] Media Indonesia, 2021. Cybersecurity Training 2021 Libatkan 6.000 Siswa dan 158 Guru SMK di Jawa Barat. [online] Available at: <https://mediaindonesia.com/teknologi/452839/cybersecurity-training-2021-libatkan6000-siswa-dan-158-guru-smk-di-jawa-barat> [Accessed 9 April 2022].
[15] Google Digital Garage. n.d. Introduction to Cybersecurity. [online] Available at: <https://learndigital.withgoogle.com/digitalgarage/course/introduction-to-cybersecurity> [Accessed 9 April 2022].

On the regulation side itself, even though Indonesia has not ratified the Data Protection Bill (*Rancangan Undang-Undang Perlindungan Data Pribadi)*, there are still other regulations being committed besides the one aforementioned. Such as the Presidential Regulation regarding The Protection of Vital Information Structure (*Peraturan Presiden tentang Perlindungan Infrastruktur Informasi Vital* (IIV)). As the BSSN has been advocating for a quad-helix cooperation, the *Perpres Perlindungan IIV* is vital in ensuring that the government maintains the security of vital infrastructure in times of crisis. As it is known that through Article 99 of Government Regulation number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, it is stated that there are eight sectors that fall into strategic categories, including government administration, energy and mineral resources, transportation, finance, health, food, information technology and telecommunications, and defense.[16] From those strategic sectors even if one of those fail, may lead to a national crisis, as evident by the 2019 Java Blackout as from the failure of the energy sector lead to the downfall of almost all sectors that heavily relied on the usages of electricity.

Technology itself can also play an important role in strengthening cybersecurity and cyber resilience. Google, being one of the largest technology company in the world, serving billions of users across its different products, has many best practices of how technology can be used to strengthen cybersecurity and cyber resilience.[17] Google always pays attention to the security aspects in its product design using three main security pillars. Google builds one of the world's most advanced security infrastructures so products are *secure by default*. It strictly upholds responsible data practices so every product we build is *private by design*. It also builds easy to use privacy and security settings so *you're in control*.[18]

While regulations and technology are key opportunities that Indonesia have in the fight for cybersecurity, another opportunity that we have and are still currently developing for is data governance. Indonesia is currently developing its own e-government based system (*Sistem Pemerintahan Berbasis Elektronik*) though currently it is still far from finished.

Without the development and implementation of a good data governance, none of the aforementioned opportunities that Indonesia has can suffice. Good data governance such as data classification, the ratification of the Data Protection Bill, and most importantly the understanding of a need to build a strong cyber resilience prior to or as part of e-government, are important keys in tackling Indonesia's cybersecurity challenges.[19]

---

[16] cyberthreat, cyberthread.id, N.A.S., 2021. Infrastruktur Informasi Vital Nasional dan Ancaman Siber [online]. cyberthreat.id. Available at: https://cyberthreat.id/read/12955/Infrastruktur-Informasi-Vital-Nasional-dan-Ancaman-Siber [Accessed 25 April 2022].
[17] Aryanti, B., 2022. Diskusi Keamanan Siber Bagi Para Pemangku Kebijakan Pandemi CfDS.
[18] Aryanti, B., 2022. Diskusi Keamanan Siber Bagi Para Pemangku Kebijakan Pandemi CfDS.
[19] Pangerapan, S., 2022. Diskusi Keamanan Siber Bagi Para Pemangku Kebijakan Pandemi CfDS.

## Conclusion

Cybercrime will always exist in line with the increasing use of technology and vast technological development. With that, cybersecurity and cyber resilience in Indonesia needs to constantly be updated. Cybersecurity is everyone's responsibility. Thus, preventive measures and collaborative actions are significantly needed through a quad-helix collaboration involving the four major sectors of society: industry, government, research institutes, and the public. In the end, it all comes down to human capital. There needs to be leadership in understanding cybersecurity innovations, endurance in learning cybersecurity, and an attitude to maintain integrity in preventing internal cyberattacks. The key is to fit technology with human capital needs and capabilities, not to force technology on humans.