 DOI: http://dx.doi.org/10.18860/j.v16i1.32563

RECONSTRUCTING THE LEGAL FRAMEWORK OF TRADE SECRET PROTECTION *VIS-À-VIS* CYBER THEFT: A Cross-Jurisdictional Comparative Study

Hari Sutra Disemadi[1]; Upankar Chutia[2]; Windi Afdal[3]; Vicko Taniady[4]; and David Tan[5]

[1,3,5]Faculty of Law, Universitas Internasional Batam, Indonesia;
[2]Alliance School of Law, Alliance University, India;
[4]Faculty of Law, Monash University, Australia
Email: hari@uib.ac.id

Received: April 11, 2025; Reviewed: May 12, 2025; Accepted: May 26, 2025;
Published: June 30, 2025

Abstract

The growing incidence of cyber theft has exposed critical deficiencies in trade secret protection regimes, particularly in jurisdictions lacking integrated cybersecurity measures. This study analyses the legal frameworks of Indonesia, India, and Australia, using the United States' Defend Trade Secrets Act (DTSA) as a benchmark to evaluate their capacity to address digital trade secret misappropriation. Employing a comparative legal

methodology, it examines statutory provisions, judicial interpretations, and enforcement mechanisms relevant to cybersecurity threats. The findings reveal that while Indonesia has enacted a trade secret statute, it lacks procedural safeguards specifically designed to address cyber theft. India and Australia, by contrast, depend on disjointed protections rooted in contract law, breach of confidence, and general cybercrime statutes. None of the jurisdictions provide a robust legal framework incorporating vital cybersecurity components such as ex-parte seizure, digital evidence management, or encryption standards. These shortcomings highlight a critical vulnerability in safeguarding proprietary information amidst escalating cyber threats. The study underscores the urgent need for legislative reform to align trade secret protection with contemporary cybersecurity challenges. Its insights contribute to the ongoing academic and legal discourse on the adequacy of current laws in mitigating cyber-enabled intellectual property violations.

Meningkatnya insiden pencurian siber telah mengungkap kelemahan mendasar dalam rezim perlindungan rahasia dagang, terutama di yurisdiksi yang belum mengintegrasikan langkah-langkah keamanan siber dalam kerangka hukumnya. Studi ini menganalisis sistem hukum Indonesia, India, dan Australia, dengan membandingkannya terhadap Defend Trade Secrets Act (DTSA) dari Amerika Serikat untuk menilai efektivitasnya dalam menangani penyalahgunaan rahasia dagang secara digital. Dengan pendekatan hukum komparatif, kajian ini mengevaluasi ketentuan undang-undang, doktrin yurisprudensi, dan mekanisme penegakan yang relevan terhadap ancaman siber. Hasilnya menunjukkan bahwa meskipun Indonesia memiliki undang-undang khusus, perlindungan prosedural terhadap pencurian siber belum memadai. India

dan Australia justru mengandalkan perlindungan yang terfragmentasi melalui hukum kontrak, asas kepercayaan, dan regulasi kejahatan siber umum. Tidak satu pun dari ketiga negara menyediakan kerangka hukum menyeluruh yang mencakup unsur penting seperti penyitaan ex-parte, pengelolaan bukti digital, atau standar enkripsi. Kekosongan ini menunjukkan lemahnya perlindungan terhadap informasi bisnis sensitif di tengah meningkatnya ancaman digital. Studi ini menekankan urgensi reformasi legislatif untuk menyelaraskan perlindungan rahasia dagang dengan tantangan keamanan siber modern. Temuan ini memberi kontribusi penting bagi wacana akademik dan hukum terkait perlindungan kekayaan intelektual di era digital.

Keywords: *cyber theft, digital misappropriation, legal enforcement, trade secrets.*

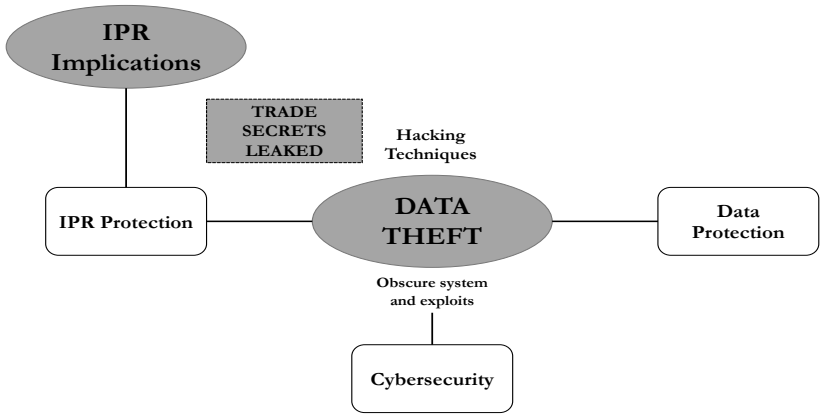
Introduction

As the world continues to adopt new and emerging digital technologies,[1] cybersecurity becomes an increasingly relevant issue.[2] The anonymous nature of the digital space,[3] coupled with the capability to manipulate data, has presented serious threats to the safety of data and privacy,[4] adding to the importance of analysing issues relevant to the realm of data protection and privacy, which has

[1] Silvia Massa et al., "Digital Technologies and Knowledge Processes: New Emerging Strategies in International Business. A Systematic Literature Review," *Journal of Knowledge Management* 27, no. 11 (January 2023): 330–87, https://doi.org/10.1108/JKM-12-2022-0993.
[2] Mohd Noorulfakhri Yaacob, Syed Zulkarnain Syed Idrus, and Mariam Idris, "Managing Cybersecurity Risks in Emerging Technologies," *International Journal of Business and Technopreneurship (IJBT)* 13, no. 3 (October 2023): 253–70, https://doi.org/10.58915/ijbt.v13i3.297.
[3] Lina Eklund et al., "Beyond a Dichotomous Understanding of Online Anonymity: Bridging the Macro and Micro Level," *Sociological Research Online* 27, no. 2 (June 2021): 486–503, https://doi.org/10.1177/13607804211019760.
[4] Abou_el_ela Abdou Hussien, "Cyber Security Crimes, Ethics and a Suggested Algorithm to Overcome Cyber-Physical Systems Problems (CybSec1)," *Journal of Information Security* 12, no. 1 (2021): 56–78, https://doi.org/10.4236/jis.2021.121003.

gathered serious attention in recent years. Countries like Indonesia, India, and Australia have continuously improved the legal frameworks and enforcement of this particular legal issue to ensure that the utilisation of digital technologies does not come at the cost of damages caused by cyber-attacks and other forms of cybersecurity risks. However, cybersecurity issues do not only revolve around traditional data protection and privacy frameworks. The continuous adoption of emerging digital technologies has led to the condition where other aspects of life are highly prone to cybersecurity risks. Such is the case with commerce, which has become almost entirely reliant on digital technologies, prompting many businesses to conduct some of their operations online, including storing important and sensitive data, such as trade secrets.

Figure 1: Mind Map of Trade Secret-Data Theft Interplay



Source: Researcher's Illustration

As highlighted in the figure above, the interplay between trade secrets and data theft involves the realm of IPR protection, cybersecurity, and overall data protection. Trade secrets, as an important aspect of businesses, are among some of the data that are under serious threat due to the rising instances of cyber

theft,[5] which exploits the loopholes within many digital systems[6] and significantly impacts businesses and their competitive advantage.[7] Traditional cybersecurity risks associated with the digital economy largely revolve around data protection and privacy,[8] despite the widespread impact of cybersecurity risks, affecting even the domain of intellectual property rights (IPR).[9] Due to the rising threats posed by the risks of cyber theft to trade secrets, it is imperative to expand the understanding of cybersecurity and its connection to the IPR realm. Assessing ways to improve cybersecurity measures to mitigate the risks of cyber theft through the existing IPR regimes can provide valuable insights into the potential of security-conscious legal mechanisms that can be utilised.

A trade secret is a key asset that, unfortunately, is often not associated with cybersecurity protections, despite its continued rising relevance in the digital discourse.[10] With the fact that cyber theft occurrences continue to rise amidst the existence of cybersecurity measures and cybersecurity provisions,[11] it is

[5] Michael Ettredge, Feng Guo, and Yijun Li, "Trade Secrets and Cyber Security Breaches," *Journal of Accounting and Public Policy* 37, no. 6 (2018): 564–85, https://doi.org/10.1016/j.jaccpubpol.2018.10.006.

[6] Tripti Singh, "Cybercrime And International Law: Jurisdictional Challenges And Enforcement Mechanisms," *African Journal of Biomedical Research* 27, no. 3S (September 2024): 697–708, https://doi.org/10.53555/AJBR.v27i3S.2101.

[7] William F Crittenden, Victoria L Crittenden, and Allison Pierpont, "Trade Secrets: Managerial Guidance for Competitive Advantage," *Business Horizons* 58, no. 6 (2015): 607–13, https://doi.org/10.1016/j.bushor.2015.06.004.

[8] Clément Labadie and Christine Legner, "Building Data Management Capabilities to Address Data Protection Regulations: Learnings from EU-GDPR," *Journal of Information Technology* 38, no. 1 (January 2023): 16–44, https://doi.org/10.1177/02683962221141456.

[9] Chirag Mavani et al., "The Role of Cybersecurity in Protecting Intellectual Property," *International Journal on Recent and Innovation Trends in Computing and Communication* 12, no. 2 (February 2024): 529–38, https://ijritcc.org/index.php/ijritcc/article/view/10935.

[10] Ionela Andreicovici, Sara Bormann, and Katharina Hombach, "Trade Secret Protection and the Integration of Information Within Firms," *Management Science* 71, no. 2 (May 2024): 1213–37, https://doi.org/10.1287/mnsc.2021.03484.

[11] This is a well-known fact supported by countless empirical evidence. A number of relevant data has been compiled in a Forbes article. *See* Mariah St. John, "Cybersecurity Stats: Facts And Figures You Should Know – Forbes Advisor," Forbes, August 2024, https://blog.cedsolutions.com/33254/cybersecurity-stats-facts-and-figures-you-should-know/. Although not all of the empirical data categorically fall into 'data theft', they are all nonetheless relevant due to how weaknesses in cybersecurity often cause overlapping instances of cybercrimes. *See also* Hafiz Shahzad Pervaiz and Shaukat Hussain Bhatti,

justified to continue to look for ways to improve the cybersecurity landscape in the legal realm. IPR law as a legal branch, particularly the trade secret regime, can provide a significant layer of protection for this issue. This can also help increase the level of protection for trade secrets, which are at serious risk of cyber theft in the increasingly digitalised world.[12] This study focused specifically on Indonesia, India, and Australia due to the inherent similarities of these countries' digital economies. Indonesia, as the biggest digital economy in the Southeast Asia region, projected to reach USD 146 billion in gross merchandise value (GMV) by 2025,[13] India with one of the biggest digital economies in the world, estimated to contribute over USD 355 billion to its GDP in 2021,[14] and Australia with an emerging digital economy, which contributed approximately AUD 136.6 billion in 2021-22, making up 6.3% of the nation's total economic output,[15] all creating a promising future for the countries' involvements in global economy.

These countries have also experienced various cyberattacks that have significantly impacted the perceived safety and security of their digital spaces. In 2021, Indonesia's national health insurance agency (BPJS Kesehatan) suffered a

"Analyses of Cybercrime Regulations Falling behind New Technologies," *Journal of Social Sciences Review* 3, no. 1 (March 2023): 460–69, https://doi.org/10.54183/jssr.v3i1.181.

[12] Juriah Abd Jalil and Halyani Hassan, "Protecting Trade Secret from Theft and Corporate Espionage: Some Legal and Administrative Measures," *International Journal of Business and Society* 21, no. S1 (2020): 205–18, https://openurl.ebsco.com/EPDB%3Agcd%3A11%3A11575179/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A141429605&crl=c&link_origin=www.google.com.

[13] Grace Nadia Chandra, "Indonesia to Double the Size of Current SE Asia's Digital Economy 2030," Jakarta Globe, November 2021, https://jakartaglobe.id/business/indonesia-to-double-the-size-of-current-se-asias-digital-economy-2030.

[14] Noshir Kaka et al., "Digital India: Technology to Transform a Connected Nation" (Mumbai, 2019), https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

[15] Australian Bureau of Statistics, "Digital Activity in the Australian Economy, 2021-22," Australian Bureau of Statistics, October 2023, https://www.abs.gov.au/articles/digital-activity-australian-economy-2021-22.

massive data breach impacting over 279 million citizens.[16] India is even recognised as the second most targeted country in Asia for cyberattacks, according to data in a report done by CloudSEK in 2024.[17] In Australia, the Australian Cyber Security Centre (ACSC) reported a 13% increase in cyber incidents in the 2020-21 financial year.[18] These incidents underscore a critical challenge for these thriving digital economies: safeguarding digital assets, including potentially sensitive trade secrets and intellectual property, from increasingly sophisticated cyber threats. Most importantly, all the countries above are relying solely on traditional cybersecurity legal frameworks, whereas the European Union and the United States are increasingly integrating cybersecurity into intellectual property rights (IPR) protection. The United States, in particular, has enacted the Defend Trade Secrets Act, which has facilitated the integration of cybersecurity measures and mechanisms into the protection of trade secrets, thereby altering the global landscape of IPR protection.[19]

Trade secrets are one of the regimes of intellectual property rights (IPR) that are continuously discussed in the literature as the world goes deeper into the digital age. This continued relevancy stems mainly from the digital nature of businesses in today's society, as iterated in a study conducted by Ubaydullaeva.[20] According to Saias, the digital nature of businesses is the main reason behind the

[16] Rahel Narda Chaterine and Dani Prabowo, "Kemenkominfo Duga 279 Juta Data Penduduk Yang Bocor Identik Dengan Data BPJS Kesehatan," Kompas, May 2021, https://nasional.kompas.com/read/2021/05/21/15192491/kemenkominfo-duga-279-juta-data-penduduk-yang-bocor-identik-dengan-data-bpjs.

[17] CloudSEK Information Security, "CloudSEK Annual Threat Landscape Report 2024" (Bengaluru, March 2024), https://www.cloudsek.com/whitepapers-reports/cloudsek-annual-threat-landscape-report-2024.

[18] Australian Cyber Security Centre (ACSC), "ACSC Annual Cyber Threat Report 2021–22" (Canberra, July 2022), https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf.

[19] Sharon Sandeen, "Out of Thin Air: Trade Secrets, Cybersecurity, and the Wrongful Acquisition Tort Authors," *Minnesota Journal of Law, Science & Technology* 19, no. 2 (2018): 373–404, https://scholarship.law.umn.edu/mjlst/vol19/iss2/3/.

[20] Anna Ubaydullaeva, "Know-How and Trade Secrets in Digital Business," *International Journal of Law and Policy* 2, no. 3 (March 2024): 38–52, https://doi.org/10.59022/ijlp.162.

rise of trade secret theft through various kinds of cybercrimes that constitute 'cyber theft'.[21] Both studies provided insight into the cause and the risks associated with it, while simultaneously highlighting the challenge of regulating this phenomenon. Another study, conducted by Wiebe and Schur, expands the assessment of risks associated with the use of digital technologies, particularly in data-driven networks.[22] This risk assessment even argues that the European Union's Trade Secret Directive may not be sufficient in addressing the challenges of protecting trade secrets in the digital space, particularly in an environment where features and operational capacities are heavily impacted and heavily reliant on large volumes of data.

In a specific lens on Indonesia, a study conducted by Dzulfania, Karyati, and Haerani highlights the evolving nature of trade secrets and how it is constantly shifting as Indonesia's digital economy continues to grow.[23] The study crucially links trade secret protection with data protection. Unfortunately, it fails to connect the legal issue with Law No. 27 of 2022, instead focusing only on Law No. 19 of 2016 for aspects of data protection and privacy. This can be considered an oversight in the analysis as Law No. 27 of 2022 concerning Personal Data Protection serves as the main framework for data protection and privacy. Literature has also addressed the challenges of trade secret protection in countries like India and Australia, as seen in studies

[21] Marco Alexandre Saias, "Unlawful Acquisition of Trade Secrets by Cyber Theft: Between the Proposed Directive on Trade Secrets and the Directive on Cyber Attacks," *Journal of Intellectual Property Law & Practice* 9, no. 9 (September 2014): 721–29, https://doi.org/10.1093/jiplp/jpu117.

[22] Andreas Wiebe and Nico Schur, "Protection of Trade Secrets in a Data-Driven, Networked Environment – Is the Update Already out-Dated?," *Journal of Intellectual Property Law & Practice* 14, no. 10 (October 2019): 814–21, https://doi.org/10.1093/jiplp/jpz119.

[23] Rishma Dzulfania, Sri Karyati, and Ruslan Haerani, "Tinjauan Yuridis Pengaturan Rahasia Dagang Menurut Hukum Positif Di Era Digital Di Indonesia," *Unizar Recht Journal (URJ)* 3, no. 3 (October 2024): 388–96, https://urj.unizar.ac.id/urj/article/view/191.

conducted by Mohapatra and Mishra on India[24] and Matulionyte on Australia.[25] Unfortunately, both are only exploring generalised issues of this discourse and not necessarily calling for or proposing a reform that integrates cybersecurity aspects into trade secret protection.

The literature cited and concisely analysed above shows that discussions regarding this legal issue remain fragmented, with emerging challenges in the form of data theft continuing to evolve and become even more prevalent, significantly threatening the protection of trade secrets worldwide. The gaps within the literature, particularly regarding the integration of cybersecurity threats, such as cyber theft, and the incorporation of cybersecurity standards into the protection of trade secrets, are what this study aims to address. To deepen the analysis, the discourse regarding these two aspects is supported with benchmarking analysis, juxtaposing Indonesian, Indian, and Australian frameworks against the United States Defend Trade Secrets Act (DTSA). This combination of analysis points and depth of normative scrutiny are the main aspects of this study's novelty. A key limitation of this study is that while it analyses the formal legal frameworks for trade secret protection against cyber theft in India, Australia, and Indonesia, it may not fully capture the informal practices, cultural nuances, and inherent differences in their legal systems that also significantly influence the protection of such information.

Research Methods

This study employs the doctrinal legal research method by scrutinising the legal norms of the relevant legal frameworks.[26] On a more specific note, the analysis of doctrinal legal research typically involves the utilisation of secondary

[24] Chinmaya Kumar Mohapatra and Amrita Mishra, "Trade Secret Protection in India," *PalArch's Journal of Archaeology of Egypt / Egyptology* 17, no. 6 (December 2020): 5436–42, https://www.archives.palarch.nl/index.php/jae/article/view/1813.
[25] Rita Matulionyte, "Government Automation, Transparency and Trade Secrets," *Melbourne University Law Review* 47, no. 3 (2024): 679–722, https://doi.org/10.2139/ssrn.4771120.
[26] Hari Sutra Disemadi, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies," *Journal of Judicial Review* 24, no. 2 (2022): 289–304, https://doi.org/10.37253/jjr.v24i2.7280.

data in the form of primary legal sources to provide an adequate legal perspective regarding a particular legal issue.[27] Furthermore, this study also utilises the comparative approach to support the legislative benchmarking of the Indonesian, Indian, and Australian frameworks against the United States' Defend Trade Secrets Act (DTSA). The study also employs the theory of legal positivism to deepen the analysis by focusing on the understanding of legal norms in the form of primary and secondary rules, as popularised by H.L.A Hart.[28] Data were gathered using the literature review technique and analysed descriptively, strictly adhering to the standards of doctrinal legal research. Secondary data were sourced from Indonesia's Law No. 30 of 2000 concerning Trade Secrets, India's Contract Act of 1872, the Information Technology Act of 2000, and relevant sections of the Indian Penal Code (Bharatiya Nyaya Sanhita), as well as Australia's Corporations Act 2001, Privacy Act 1988, and the equitable doctrine of breach of confidence. Additionally, judicial precedents, including Maggbury Pty Ltd v Hafele Australia Pty Ltd, Del Casale v Artedomus (Aust) Pty Ltd, and John Richard Brady & Ors v Chemical Process Equipment P Ltd & Anr, were examined to understand the role of case law in trade secret protection.

Discussion

Normative Connections Between Trade Secret Regimes and Cybersecurity

The digital age, with its boundless connectivity, has presented a double-edged sword for businesses.[29] While it offers unprecedented opportunities for

[27] David Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 2463–78, https://core.ac.uk/download/pdf/490668614.pdf.

[28] Richard Collins, "Taking Legal Positivism Beyond the State: Finding Secondary Rules?," in *Positivism in a Global and Transnational Age*, ed. Luca Siliquini-Cinelli (Cham: Springer International Publishing, 2019), 65–91, https://doi.org/10.1007/978-3-030-24705-8_3.

[29] Yadong Luo, "A General Framework of Digitization Risks in International Business," *Journal of International Business Studies* 53, no. 2 (2022): 344–61, https://doi.org/10.1057/s41267-021-00448-9.

growth and innovation, it also exposes valuable assets to unprecedented risks.[30] Trade secrets, as the lifeblood of many enterprises and a competitive economy, are particularly vulnerable in this landscape.[31] Traditionally, trade secret protection relied on physical security and confidentiality agreements.[32] However, the rise of cyber theft has fundamentally altered the playing field, demanding a re-evaluation of the normative foundations of trade secret law. This can alter the course of many businesses' trajectories, as the loss of their competitive advantage, originally provided by relevant trade secrets, can be acquired by their competitors.[33] Cyber theft in the context of trade secrets extends beyond simple data breaches. It can even encompass a spectrum of malicious activities, from sophisticated hacking operations designed to sensitive information to the deployment of spyware that stays in a targeted system, enabling illegal monitoring.[34] If done on an entirely digital system, this can compromise the security of massive volumes of data, making it practically impossible to estimate the damage.

The requirements for reasonable measures to maintain secrecy, as traditional normative principles of trade secret law, are now being tested in ways unimaginable just a few decades ago.[35] What constitutes "reasonable measures" in a digital environment where sophisticated cyberattacks are commonplace?

---

[30] Xu Haoran, Miao Wenlong, and Zhang Siyu, "Digital Technology Development and Systemic Financial Risks: Evidence from 22 Countries," *Borsa Istanbul Review* 24 (2024): 1–9, https://doi.org/10.1016/j.bir.2024.08.002.

[31] Riccardo Vecellio Segate, "Securitizing Innovation to Protect Trade Secrets Between 'the East' and 'the West': A Neo-Schumpeterian Public Legal Reading," *UCLA Pacific Basin Law Journal* 37, no. 1 (2020): 59–126, https://doi.org/10.5070/p8371048804.

[32] Jason Tanujaya and Vincentius Raymond Wijaya, "Trade Secrets Protection for Blockchain Technology in Indonesia," *Anthology: Inside Intellectual Property Rights* 2, no. 1 (2024): 388–401, https://ojs.uph.edu/index.php/Anthology/article/view/8521.

[33] Sandy Klasa et al., "Protection of Trade Secrets and Capital Structure Decisions," *Journal of Financial Economics* 128, no. 2 (2018): 266–86, https://doi.org/10.1016/j.jfineco.2018.02.008.

[34] Ettredge, Guo, and Li, "Trade Secrets and Cyber Security Breaches."

[35] Hannah E. Brown, "Rethinking 'Reasonableness': Implementation of a National Board to Clarify the Trade Secret Standard Now That the Work-From-Home Culture Has Changed the Rules," *Journal of Intellectual Property Law* 30, no. 2 (2023): 268–304, https://digitalcommons.law.uga.edu/jipl/vol30/iss2/2/.

This fundamental question prompts policymakers to shift their traditional one-dimensional perspective, where trade secrets can be kept safe through non-disclosure agreements and other traditional measures. Most importantly, it forces businesses to delve into the technical aspects of the digital space to implement measures such as firewalls and antivirus software, which, even when implemented, still do not fully guarantee the safety of trade secrets from potential cyber theft.[36] As it is unfair to leave all of these inherent cybersecurity risks to the due diligence of businesses in the digital space, the role of digital system providers becomes a key normative aspect that needs to be explored further. Because they are responsible for collecting, storing, processing, and retaining massive volumes of data every day, it is only fair to demand a high standard of cybersecurity mechanisms through a robust legal framework.[37]

The very concept of confidentiality, which acts as the cornerstone of trade secret protection,[38] is also under siege. Leaked digital information can spread rapidly and uncontrollably, rendering it practically impossible to contain.[39] It is also challenging to accurately assess the extent of damage caused by this leak, primarily because it is difficult to identify all the digital platforms where the leak information has been shared. The traditional remedy of injunctive relief, while

[36] Jason Adler, Eleanor Vaida Gerhards, and Michael J. Lockerby, "Cybersecurity: Putting the Toothpaste Back in the Tube - Best Practices for Responding to a Security Breach," in *ABA Forum on Franchising Annual Meeting* (Nashville: Fox Rothschild, American Bar Association, 2018), 1–60.

[37] Maskun and Rian Nugraha Anwar, "Regulation and Protection of Cloud Computing: Literature Review Perspective," *Jambura Law Review* 3, no. 2 (2021): 336–64, https://doi.org/10.33756/jlr.v3i2.10639.

[38] William H Ross and Danny Franklin, "Characteristics of Effective Trade Secrets and Confi Dential Information Policies: Guidance from Labor Arbitration Cases," *Labor Law Journal* 71, no. 1 (January 2020): 43–57, https://fruehanp1.pythonanywhere.com/bibliography/TYRH2UYC.

[39] This also creates a paradox where even the efforts to handle this leak could risk stopping the free flow of information and knowledge, which serve as the basis for future innovation. *See* Rochelle Cooper Dreyfuss and Orly Lobel, "Economic Espionage as Reality or Rhetoric: Equating Trade Secrecy with National SecuritySecrecy with National Security," *Lewis & Clark Law Review* 20, no. 2 (January 2016): 419–75, https://digital.sandiego.edu/law_fac_works/1/.

still relevant, may prove inadequate in the face of widespread dissemination.[40] Consider, for example, a scenario where a company's proprietary source code is uploaded to a public repository. Even if a court issues an injunction, the information may have already been copied and distributed numerous times, making it exceedingly difficult to reverse the damage. How can a court effectively prevent the use of a trade secret that has already been posted on multiple online forums or shared across peer-to-peer networks? These are not merely hypothetical concerns; they are the tangible obstacles that challenge the core doctrines of trade secret law, requiring a re-evaluation of how we enforce and protect confidential information in the digital realm. Traditional methods are often too slow and limited in scope to address the speed and scale of modern data leaks.

Perhaps the core issue in this discourse is how the traditional IPR-based approach of trade secrets protection can consolidate some of the modern cybersecurity standards without overly leaning toward cybersecurity aspects, hence losing the core aspects of IPR protection. In other words, the normative constructs regarding cybersecurity in the face of cyber theft should focus on supporting the mechanisms of IPR protection rather than replacing them. While trade secret law focuses on protecting the economic value of confidential information, cybercrime law addresses the criminal conduct associated with unauthorised access and data theft. However, there are often gaps and overlaps between these two legal frameworks, leading to potential inconsistencies and inefficiencies. For instance, a hacker who steals a trade secret may be prosecuted under cybercrime laws. However, the victim company may still need to pursue a separate civil action to recover damages under trade secret law. This dual-pronged approach, while theoretically sound, hinges on the coherence and consistency of both legal regimes. If the definitions of offences differ, or if the burden of proof varies significantly, it can create a situation where a wrongdoer

[40] David Bohrer, "Threatened Misappropriation of Trade Secrets: Making a Federal (DTSA) Case Out of It," *Santa Clara High Technology Law Journal* 33, no. 4 (2017): 506–40, https://digitalcommons.law.scu.edu/chtlj/vol33/iss4/3/.

escapes liability or where the victim is unable to obtain adequate redress. The effectiveness of this dual-pronged approach, therefore, depends on a meticulously crafted synergy between these two legal spheres. Therefore, the emphasis on prevention and standardisation of security measures in the digital space can help provide a certain degree of safety in the very complex nature of cyber-related legal issues.[41]

The United States has one of the most developed intellectual property rights (IPR) frameworks, continuously updating its laws to strengthen protections, adapt to technological advancements, and align with global standards.[42] This is evident with the Defend Trade Secrets Act (DTSA), which represents a significant step towards addressing the challenges posed by cyber theft, demonstrating a proactive attempt to reconcile trade secret law with the realities of the digital age.[43] By creating a federal civil remedy for trade secret misappropriation,[44] the DTSA provides businesses with a powerful tool to combat cyber espionage and other forms of digital trade secret theft. This federalisation of trade secret law allows for a more uniform and consistent application of legal principles across state lines, which is particularly important

[41] An argument can even be made that the standardisation of this can significantly improve national security, as consistent protocols for data classification, protection, and cross-border flows prevent unauthorised access to sensitive information that could otherwise pose significant threats when aggregated at scale. As scholar Hong Yanqing noted regarding large data repositories, "the huge amount of user information held by Alibaba, currently covering over 400 million users, is certainly personal information [...] but because of its scale and granularity, it can also match the public security organs' basic national population database and even surpass it in accuracy. For the country, any eventual leak or damage of this scale of basic population data could create a serious threat to national security." *See* Rogier Creemers, "China's Emerging Data Protection Framework," *Journal of Cybersecurity* 8, no. 1 (January 2022): 1–12, https://doi.org/10.1093/cybsec/tyac011.

[42] Geraldine O. Mbah, "US Intellectual Property Law and Its Impact on Business: Recent Developments and Trends," *International Journal of Science and Research Archive* 13, no. 2 (December 2024): 3279–95, https://doi.org/10.30574/ijsra.2024.13.2.2575.

[43] Dan Ciuriak and Maria Ptashkina, "Quantifying Trade Secret Theft: Policy Implications," CIGI Papers (WAterloo, May 2021), https://www.cigionline.org/publications/quantifying-trade-secret-theft-policy-implications/.

[44] Joseph Brees, "Trade Secrets Go Federal – Parade to Follow," *Journal of Business & Technology Law* 12, no. 2 (2017): 277–324, https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/6/.

in the context of cybercrimes that often transcend geographical boundaries. While the DTSA has been lauded for its potential to strengthen trade secret protection, its effectiveness hinges on its implementation and enforcement. The US, in this regard, highlights the importance of specific laws designed to combat digital crimes against trade secrets and how a well-structured federal act can provide a more robust defence than a patchwork of varying state laws. Below is a table listing the normative aspects of the DTSA that can be used to enhance cybersecurity measures and better protect trade secrets from data theft.

Table 1: Key normative points in the DTSA that can serve as the basis of cybersecurity integration in the protection of trade secret

Normative Point	DTSA Provision	Cybersecurity Relevance
***Ex-Parte* Civil Seizure**	Sec. 2(b)(2)	Allows rapid response to prevent digital propagation of stolen trade secrets
Digital Storage Protection	Sec. 2(b)(2)(D)(ii)	Prohibits connecting seized storage media to networks without consent
Technical Expert Involvement	Sec. 2(b)(2)(E)	Permits specialised cybersecurity experts to assist in seizures
Encryption Rights	Sec. 2(b)(2)(H)	Allows encryption of seized digital materials to maintain security
Electronic Espionage Recognition	Sec. 2(b)(6)(A)	Explicitly includes "espionage through electronic means" as improper acquisition
Confidentiality Safeguards	Sec. 2(b)(2)(C)	Protects seized information from unauthorised disclosure
Remedies for Digital Misappropriation	Sec. 2(b)(3)	Allows for comprehensive remedies adaptable to digital trade secret theft

Source: Secondary Data Analysis Results

The rapid pace of technological advancement necessitates a continuous reassessment of the normative foundations of trade secret law in many parts of the world, demanding a level of agility that traditional legal frameworks often struggle to achieve, particularly in countries that still rely upon old frameworks of protection. As cyber threats become increasingly sophisticated and pervasive, legal frameworks worldwide must evolve to ensure that businesses can effectively safeguard their valuable intellectual assets.[45] It is not enough to simply react to emerging threats; proactive measures are needed to anticipate and mitigate future risks. This means fostering a culture of cybersecurity awareness, promoting the adoption of best practices, and investing in research and development to stay ahead of the curve. Therefore, it is fair to say that the success of trade secret protection in the digital age depends on a willingness to embrace change and to recognise that the digital age demands a new paradigm for safeguarding confidential information.

Ultimately, it is essential to recognise that the normative challenges posed by cyber theft are not limited to any single jurisdiction. The globalised nature of digital commerce means that trade secrets are vulnerable to attacks originating from anywhere in the world. This necessitates a coordinated international effort to develop and harmonise legal frameworks for trade secret protection. Therefore, comparative analysis with other countries is crucial in ensuring easier and seamless cooperation, as well as in improving the existing framework within a country through strict legislative benchmarking. Without such collaborative and rigorous legislative efforts, the effectiveness of national trade secret regimes will be significantly undermined, leaving businesses exposed to the ever-present threat of cyber theft while also possibly eroding national security in the long run.

[45] Muhammad Rhogust, "Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia," *Journal of Law, Social Science and Humanities* 1, no. 2 (June 2024): 166–80, https://myjournal.or.id/index.php/JLSSH/article/view/213.

State of The Art in Indonesia, India, and Australia's Framework for Trade Secret

Indonesia's trade secret regime still relies on a rather old legal framework: Law No. 30 of 2000 concerning Trade Secrets.[4647] While the law provides a general framework for protecting undisclosed business information, its enforcement mechanisms do not adequately address modern digital vulnerabilities. Article 3 defines trade secrets based on their confidentiality, economic value, and the owner's efforts to maintain secrecy, making it conceptually broad enough to cover various forms of proprietary information, including digital data. Additionally, Article 13 and Article 14 criminalise unauthorised disclosures and unlawful acquisition, which could, in principle, extend to cyber intrusions. However, the law does not establish clear procedural safeguards for addressing cases involving hacking, unauthorised system access, or AI-driven data extraction, all of which are increasingly common in cyber theft operations.[48] The lack of structured legal mechanisms for handling these risks, coupled with the absence of explicit digital enforcement strategies, results in significant uncertainty when cyber theft cases arise. Without a framework that integrates cybersecurity considerations into trade secret protection, the law remains anchored in traditional conceptions of confidentiality, making its

[46] Lu Sudirman and Hari Sutra Disemadi, "Rahasia Dagang Sebagai Perlindungan Kekayaan Intelektual Usaha Mikro Kecil Dan Menengah Di Era Digitalisasi Dan Globalisasi," *Jurnal Magister Hukum Udayana* 12, no. 1 (2023): 80–98, https://doi.org/10.24843/JMHU.2023.v12.i01.p07.

[47] Adiwibowo, Y. (2013). Technical Barrier To Trade Of Indonesian Clove Cigarettes In The Context Of Measures Affecting The Production And Sale Of Clove Cigarettes United States Of America (Ds-406). *Jurnal Ius Kajian Hukum Dan Keadilan*, 1(2). Https://Doi.Org/10.12345/Ius.V1i2.235

[48] The increasing role of AI and other cutting-edge digital technologies in cybercrime has enabled more sophisticated and automated attacks, allowing cybercriminals to enhance efficiency, scale operations, and exploit security vulnerabilities with minimal human intervention. *See* Murshal Senjaya, "Cyber Crime And Criminal Law In The Era Of Artificial Intelligence," *International Journal of Law and Society* 1, no. 4 (October 2024): 268–76, https://doi.org/10.62951/ijls.v1i4.210.

practical application to digital trade secret misappropriation increasingly ambiguous.[49]

While the law recognises trade secret violations, it lacks explicit provisions addressing cyber theft, which has become a growing threat in the digital economy. Article 14 states that obtaining or controlling a trade secret through unlawful means constitutes a violation; however, it does not specifically mention cyber intrusions, such as hacking, unauthorised system access, or digital espionage. Moreover, Article 16 grants investigative authority to law enforcement and certain government officials, but it does not outline procedures for handling cyber-related trade secrets breaches, such as digital forensics or international cooperation in cross-border cyber theft cases. Additionally, Article 17 sets a relatively lenient maximum penalty of two years in prison or a fine of IDR 300 million, which may not serve as an effective deterrent against large-scale cyber espionage that can result in multimillion-dollar losses. Given these gaps, Indonesia's trade secret law requires modernisation to address digital threats effectively, particularly by incorporating cybersecurity measures and stricter enforcement mechanisms.

India currently lacks a dedicated law governing trade secrets, despite being a signatory to the TRIPS Agreement, which under Article 39 obligates member states to protect "undisclosed information."[50] Instead, trade secret protection in India relies on a combination of legal principles and statutes. The Indian Contract Act 1872 serves as the primary framework through non-disclosure agreements (NDAs) and confidentiality clauses, which courts have upheld as enforceable as long as they do not impose an unreasonable restraint on trade. Additionally, the equitable doctrine of breach of confidence, recognised in common law, allows courts to provide remedies in cases where confidential

[49] Muhammad Syarifuddin, Perspektif Global Penyelesaian Sengketa Investasi di Indonesia, *De Jure: Jurnal Hukum dan Syar'iah* Vol 3, No 1: Juni 2011.

[50] Mohammad Zafar Mahfooz Nomani, Zubair Ahmed, and Mohammad Rauf, "Role of Trade Secret Protection Laws in the Development of Indo-Brazilian Bilateral Trade & Investment," *International Journal of Law* 5, no. 5 (September 2019): 20–24, https://www.lawjournals.org/archives/2019/vol5/issue5/5-4-61.

business information is misused. Judicial precedents, such as John Richard Brady & Ors v. Chemical Process Equipment P Ltd & Anr[51] and Niranjan Shankar Golikari v. Century Spinning and Manufacturing Co. Ltd.,[52] further reinforce the principle that trade secrets can be protected under contractual and common law obligations.

While India's current legal framework provides some level of protection, it lacks explicit provisions addressing digital threats, such as cyber theft and data breaches. The Information Technology Act 2000, particularly Section 66E, offers some protection against unauthorised access to confidential digital information, but its scope is limited. Additionally, the Indian Penal Code (now Bharatiya Nyaya Sanhita) includes provisions for theft and criminal breach of trust, which may be applied in cases of trade secret misappropriation. However, enforcement remains fragmented, relying heavily on contractual agreements rather than a statutory framework.[53] Recognising this gap, the Law Commission of India has proposed the "Protection of Trade Secrets Bill, 2024," which, if enacted, would establish specific rights for trade secret holders, define trade secrets, and designate Commercial Courts to handle misappropriation cases.[54] While the lack of a dedicated law does not leave trade secrets entirely unprotected, the reliance on multiple legal instruments results in ambiguity and inconsistent enforcement, highlighting the need for comprehensive legislation.

---

[51] Veena T. N., "Misappropriation of Trade Secrets Under the Indian Legal Framework: An Analytical Study," *Christ University Law Journal* 12, no. 1 (July 2023): 83–98, https://doi.org/10.12728/culj.22.4.

[52] Raj Aryan, "Protection of Trade Secrets in Light of Business Laws, How Can the Existing Conflict Be Erased?," *International Journal of Advanced Legal Research* 3, no. 4 (May 2023): 1–8, https://ijalr.in/volume-3-issue-4/protection-of-trade-secrets-in-light-of-business-laws-how-can-the-existing-conflict-be-eased-raj-aryan/.

[53] Sood, M. (2018). The Role Of Banking In Payment Of International Trade Contract. *Jurnal IUS Kajian Hukum Dan Keadilan*, *6*(2), 193–207. https://doi.org/10.29303/ius.v6i2.552.

[54] Jeevetha P., "Inadequacy of Legal Framework for Trade Secret Protection in India: A Legal Analysis of Trade Secrets Bill 2024," *International Journal for Research Trends and Innovation* 10, no. 2 (February 2025): a425–41, https://www.ijrti.org/viewpaperforall.php?paper=IJRTI2502046.

Australia, like India, does not have a dedicated statutory regime specifically for trade secrets. Instead, protection is derived from a combination of common law principles, equitable doctrines, contractual obligations, and various legislative provisions that indirectly safeguard confidential business information.[55] The primary legal framework for protecting trade secrets is the equitable doctrine of breach of confidence, which allows courts to impose obligations of confidentiality when information has been shared under circumstances that imply secrecy. Contractual mechanisms such as non-disclosure agreements (NDAs) play a significant role in safeguarding confidential business information. Legislative measures also provide indirect protection, including the Corporations Act 2001, which restricts improper use of confidential information by company officials; the Privacy Act 1988, which regulates the handling of personal and sensitive information; and the Freedom of Information Act 1982, which exempts trade secrets from public disclosure. Judicial precedents, such as Maggbury Pty Ltd v Hafele Australia Pty Ltd[56] and Del Casale v Artedomus (Aust) Pty Ltd,[57] reinforce that trade secret protection is primarily enforced through breach of confidence claims rather than a standalone statutory framework.

While this system provides a foundation for protecting trade secrets, it lacks explicit provisions addressing cyber theft. The absence of a statute specifically designed to combat cyber intrusions such as hacking, unauthorised system access, or digital misappropriation means that legal actions for cyber theft must rely on general breach of confidence principles rather than tailored legislative measures. Although Australian courts offer various remedies, including injunctions, damages, and accounts of profits, these enforcement mechanisms were developed in a pre-digital context. As cyber theft continues to

[55] Suzana Nashkova, "Addressing Criminal Liability for Misuse of Trade Secrets Under Australian Law: Is the Current Legal Framework Adequate to Protect the Interests of Owners of Trade Secrets?," *IIC - International Review of Intellectual Property and Competition Law* 55, no. 8 (2024): 1281–1315, https://doi.org/10.1007/s40319-024-01490-4.
[56] *Maggbury Pty Ltd v Hafele Australia Pty Ltd* (2001) 210 CLR 181.
[57] *Del Casale v Artedomus (Aust) Pty Ltd* [2007] NSWCA 172; (2007) 73 IPR 326.

evolve, the reliance on traditional legal doctrines raises concerns about the adequacy of Australia's framework in addressing the unique challenges of digital trade secret misappropriation.

Despite differences in legal traditions, Indonesia stands out as the only jurisdiction with a dedicated trade secret statute, whereas India and Australia rely on contractual mechanisms, common law doctrines, and scattered statutory provisions for protection. Despite this, Indonesia lacks the procedural mechanisms necessary to address modern cyber threats, leaving enforcement uncertain in the digital realm. India similarly depends on contractual obligations and breach of confidence claims, though the proposed Protection of Trade Secrets Bill 2024 signals an intent to introduce statutory clarity. Australia, despite its sophisticated common law jurisprudence, also faces fragmentation in enforcement, particularly as digital misappropriation challenges outpace traditional equitable remedies. These frameworks, while functional, reveal a pressing need for legislative modernization, particularly as trade secrets become increasingly vulnerable to cyber intrusions, cross-border data theft, and AI-driven exploitation. Without a shift toward structured statutory protection, trade secret holders in these jurisdictions remain reliant on fractional legal instruments that, while adaptable, fail to offer the certainty and efficiency that a dedicated trade secret regime would provide.

Benchmarking Against the US's Defend Trade Secrets Act and Future Legal Developments

The analysis in the previous subsection highlights the normative shortcomings of Indonesia, India, and Australia in protecting trade secrets, particularly in the digital context. Their traditional approach, as previously discussed, is inadequate in addressing the modern-day challenges that businesses face daily. The increasing prevalence of cyber theft, in particular, further complicates this issue and raises the urgency to an unprecedented level. The context of globalisation also needs to be taken into context. Benchmarking serves as a crucial tool for legal analysis, which in turn can provide insights for

future legal developments. As noted previously, the normative spaces opened by the United States' DTSA can fundamentally change the landscape of trade secrets protection. The normative aspects in the DTSA that have been identified as capable of providing a stern basis for the integration of cybersecurity aspects and the protection against the crime of cyber theft, along with the penal provisions against the perpetrators, can serve as a benchmarking tool that can help address the inadequacies of the frameworks that exist within the legal system of Indonesia, India, and Australia. Below is a table benchmarking the legal frameworks for trade secrets in the three countries against the United States' DTSA.

Table 2: Benchmarking of Indonesian, Indian, and Australian trade secret framework against DTSA

DTSA Normative Points (from Table 1)	Indonesia	India	Australia
Ex-Parte Civil Seizure (Sec. 2(b)(2))	Trade Secret Law (Art. 13 & 14) allows action against unauthorised use, but no rapid seizure mechanism	No trade secret law, seizure handled under general civil/criminal procedures	No dedicated statutory provision, but courts may issue injunctions in breach-of-confidence cases
Digital Storage Protection (Sec. 2(b)(2)(D)(ii))	No trade secret-specific restriction on handling	No statutory provision on handling digital evidence in	No explicit trade secret law, general evidence laws apply

	seized digital materials	trade secret cases	
Technical Expert Involvement (Sec. 2(b)(2)(E))	No requirement for expert involvement in trade secret investigations, but cybercrime laws may apply	No trade secret-specific provision, general expert testimony admissible in cybercrime cases	No mandatory requirement; courts may allow expert evidence in breach-of-confidence claims
Encryption Rights (Sec. 2(b)(2)(H))	No mention of encryption in trade secret enforcement; broader IT laws may be relevant	No statutory mention of encryption in trade secret matters	No direct legal mandate for encryption in trade secret enforcement
Electronic Espionage Recognition (Sec. 2(b)(6)(A))	No specific cyber espionage provisions in trade secret law, cybercrime laws may cover some cases	No dedicated statute covering cyber theft of trade secrets, handled under the IT Act	No standalone trade secret law, cyber espionage addressed under general cybercrime laws
Confidentiality Safeguards (Sec. 2(b)(2)(C))	Trade Secret Law protects confidentiality	Courts may impose confidentiality	Confidentiality governed by the breach-of-

	but lacks a mechanism for securing seized materials	measures in breach-of-confidence cases	confidence doctrine and contractual obligations
Remedies for Digital Misappropriation (Sec. 2(b)(3))	Civil and criminal penalties exist under Trade Secret Law but not tailored to cyber theft	Remedies rely on contract enforcement and cybercrime laws	Breach-of-confidence remedies available, but no dedicated legal framework for cyber theft

Source: Secondary Data Analysis Results

The benchmarking results highlight a fundamental gap in the legal frameworks of Indonesia, India, and Australia when addressing cyber theft of trade secrets. While Indonesia has a statutory foundation, its enforcement mechanisms remain outdated and lack procedural safeguards for digital misappropriation. India and Australia rely on contract law, breach of confidence, and general cybercrime statutes, creating fragmented protections that struggle to keep pace with evolving threats. Under the DTSA, *ex parte* civil seizure allows courts to confiscate misappropriated trade secrets without prior notice, thereby preventing their destruction or further dissemination. The act also regulates the handling of seized digital storage, mandates the involvement of technical experts in complex cases, and provides encryption rights to secure sensitive materials. The absence of these mechanisms across all three jurisdictions weakens enforcement and leaves trade secret holders with limited recourse in cyber theft cases.

Applying H.L.A. Hart's legal positivism to Table 2's benchmarking results reveals profound structural deficiencies in the legal systems of Indonesia, India,

and Australia regarding trade secret protection from cyber theft. From a positivist perspective, these jurisdictions exhibit inadequate development of both primary and secondary rules. While primary rules defining trade secrets exist to varying degrees, with Indonesia having statutory definitions but India and Australia relying on common law constructs, all three jurisdictions critically lack the sophisticated secondary rules necessary for effective enforcement in digital contexts. Hart's conception of secondary rules as mechanisms that operationalise primary rules is particularly relevant here; the DTSA provides robust secondary rules through its *ex-parte* seizure provisions, encryption standards, and procedural frameworks for handling digital evidence, whereas the comparative jurisdictions possess minimal or fragmented secondary rules to address cyber misappropriation. This absence of authoritative secondary rules creates what Hart would describe as a "pathology" in these legal systems. It is essentially a condition where valid primary norms exist conceptually but cannot be effectively recognised or enforced in response to emerging digital threats. The benchmarking thus exposes not merely policy gaps but fundamental structural deficiencies in the rule-recognition systems needed to transform abstract trade secret protections into functional legal safeguards against cyber theft.

Conclusion

The legal frameworks protecting trade secrets in Indonesia, India, and Australia remain poorly prepared for the realities of cyber theft, exposing a widening gap between regulation and technological threats. While Indonesia at least possesses a statutory foundation, its outdated enforcement mechanisms fail to address digital vulnerabilities. India and Australia remain tethered to fragmented protections under contract law, breach of confidence, and general cybercrime statutes. The benchmarking results clearly indicate that without procedural safeguards for *ex parte* seizures, encryption, and digital evidence handling, trade secrets will continue to be stolen and exploited with little recourse. Through the lens of Hart's legal positivism, this represents a fundamental failure of the secondary rule structure in these jurisdictions, where

the recognition and adjudication rules necessary for operationalising trade secret protections in the digital domain remain critically underdeveloped. This unchecked legal void not only weakens corporate security but also threatens to undermine national competitiveness, as countries unable to protect innovation will inevitably fall prey to those who can steal it without consequence. Therefore, it is advisable for these countries to modernise their legal frameworks by adopting comprehensive statutory provisions that explicitly address cyber theft, incorporate procedural safeguards for digital evidence handling, and implement stronger enforcement mechanisms like *ex-parte* seizure provisions modelled after the DTSA to adequately protect trade secrets in the digital age.

Future research is recommended to further examine the design and implementation of regulatory frameworks that integrate trade secret protection with comprehensive cybersecurity regimes. Subsequent studies may focus on a comparative analysis of effective protection models adopted in other jurisdictions—such as the United States through the Defend Trade Secrets Act (DTSA)—with the aim of formulating a contextual and applicable legal framework for countries such as Indonesia, India, and Australia. Moreover, empirical research involving legal practitioners, cybercrime investigators, and digital industry stakeholders is crucial for identifying implementation barriers in practice and developing technical guidelines for handling digital evidence in trade secret disputes. Thus, future research should not only be normative in nature but also contribute practically to the development of a legal system that is responsive to the growing challenges of data theft and trade secret misappropriation in the digital era.

Competing Interests

All authors hereby declare that there are no competing interests influencing the writing or publication of this article. The research and findings presented are based solely on academic integrity and objective analysis.

Acknowledgements

We would like to express our sincere gratitude to the editor and anonymous reviewers for their insightful comments and valuable suggestions that greatly improved this article. We are also thankful to the Faculty of Law and the Institute for Research and Community Service (LPPM) at Universitas Internasional Batam, Indonesia, for their moral and financial support. Special thanks to our esteemed collaborator, Upankar Chutia from Alliance School of Law, Alliance University, India, for his kind cooperation in this joint authorship. We are also grateful to Vicko Taniady from the Faculty of Law, Monash University, Australia, a scholarship recipient of the Indonesian Education Fund Management Programme (LPDP) under the Ministry of Finance of the Republic of Indonesia, for his significant contribution to the completion and publication of this paper. This collaborative effort would not have been possible without the dedication and commitment of all parties involved.

References

Abdou Hussien, Abou_el_ela. "Cyber Security Crimes, Ethics and a Suggested Algorithm to Overcome Cyber-Physical Systems Problems (CybSec1)." *Journal of Information Security* 12, no. 1 (2021): 56–78. https://doi.org/10.4236/jis.2021.121003.

Adiwibowo, Y. (2013). Technical Barrier To Trade Of Indonesian Clove Cigarettes In The Context Of Measures Affecting The Production And Sale Of Clove Cigarettes United States Of America (Ds-406). Jurnal Ius Kajian Hukum Dan Keadilan, 1(2). Https://Doi.Org/10.12345/Ius.V1i2.235

Adler, Jason, Eleanor Vaida Gerhards, and Michael J. Lockerby. "Cybersecurity: Putting the Toothpaste Back in the Tube - Best Practices for Responding to a Security Breach." In *ABA Forum on Franchising Annual Meeting*, 1–60. Nashville: Fox Rothschild, American Bar Association, 2018.

Andreicovici, Ionela, Sara Bormann, and Katharina Hombach. "Trade Secret

Protection and the Integration of Information Within Firms." *Management Science* 71, no. 2 (May 2024): 1213–37. https://doi.org/10.1287/mnsc.2021.03484.

Aryan, Raj. "Protection of Trade Secrets in Light of Business Laws, How Can the Existing Conflict Be Erased?" *International Journal of Advanced Legal Research* 3, no. 4 (May 2023): 1–8. https://ijalr.in/volume-3-issue-4/protection-of-trade-secrets-in-light-of-business-laws-how-can-the-existing-conflict-be-eased-raj-aryan/.

Australian Bureau of Statistics. "Digital Activity in the Australian Economy, 2021-22." Australian Bureau of Statistics, October 2023. https://www.abs.gov.au/articles/digital-activity-australian-economy-2021-22.

Australian Cyber Security Centre (ACSC). "ACSC Annual Cyber Threat Report 2021–22." Canberra, July 2022. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2022_0.pdf.

Bohrer, David. "Threatened Misappropriation of Trade Secrets: Making a Federal (DTSA) Case Out of It." *Santa Clara High Technology Law Journal* 33, no. 4 (2017): 506–40. https://digitalcommons.law.scu.edu/chtlj/vol33/iss4/3/.

Brees, Joseph. "Trade Secrets Go Federal – Parade to Follow." *Journal of Business & Technology Law* 12, no. 2 (2017): 277–324. https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/6/.

Brown, Hannah E. "Rethinking 'Reasonableness': Implementation of a National Board to Clarify the Trade Secret Standard Now That the Work-From-Home Culture Has Changed the Rules." *Journal of Intellectual Property Law* 30, no. 2 (2023): 268–304. https://digitalcommons.law.uga.edu/jipl/vol30/iss2/2/.

Chandra, Grace Nadia. "Indonesia to Double the Size of Current SE Asia's Digital Economy 2030." Jakarta Globe, November 2021.

https://jakartaglobe.id/business/indonesia-to-double-the-size-of-current-se-asias-digital-economy-2030.

Chaterine, Rahel Narda, and Dani Prabowo. "Kemenkominfo Duga 279 Juta Data Penduduk Yang Bocor Identik Dengan Data BPJS Kesehatan." Kompas, May 2021. https://nasional.kompas.com/read/2021/05/21/15192491/kemenkominfo-duga-279-juta-data-penduduk-yang-bocor-identik-dengan-data-bpjs.

Ciuriak, Dan, and Maria Ptashkina. "Quantifying Trade Secret Theft: Policy Implications." CIGI Papers. WAterloo, May 2021. https://www.cigionline.org/publications/quantifying-trade-secret-theft-policy-implications/.

CloudSEK Information Security. "CloudSEK Annual Threat Landscape Report 2024." Bengaluru, March 2024. https://www.cloudsek.com/whitepapers-reports/cloudsek-annual-threat-landscape-report-2024.

Collins, Richard. "Taking Legal Positivism Beyond the State: Finding Secondary Rules?" In *Positivism in a Global and Transnational Age*, edited by Luca Siliquini-Cinelli, 65–91. Cham: Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-24705-8_3.

Creemers, Rogier. "China's Emerging Data Protection Framework." *Journal of Cybersecurity* 8, no. 1 (January 2022): 1–12. https://doi.org/10.1093/cybsec/tyac011.

Crittenden, William F, Victoria L Crittenden, and Allison Pierpont. "Trade Secrets: Managerial Guidance for Competitive Advantage." *Business Horizons* 58, no. 6 (2015): 607–13. https://doi.org/10.1016/j.bushor.2015.06.004.

Disemadi, Hari Sutra. "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies." *Journal of Judicial Review* 24, no. 2 (2022): 289–304. https://doi.org/10.37253/jjr.v24i2.7280.

Dreyfuss, Rochelle Cooper, and Orly Lobel. "Economic Espionage as Reality or Rhetoric: Equating Trade Secrecy with National SecuritySecrecy with National Security." *Lewis & Clark Law Review* 20, no. 2 (January 2016): 419–75. https://digital.sandiego.edu/law_fac_works/1/.

Dzulfania, Rishma, Sri Karyati, and Ruslan Haerani. "Tinjauan Yuridis Pengaturan Rahasia Dagang Menurut Hukum Positif Di Era Digital Di Indonesia." *Unizar Recht Journal (URJ)* 3, no. 3 (October 2024): 388–96. https://urj.unizar.ac.id/urj/article/view/191.

Eklund, Lina, Emma von Essen, Fatima Jonsson, and Magnus Johansson. "Beyond a Dichotomous Understanding of Online Anonymity: Bridging the Macro and Micro Level." *Sociological Research Online* 27, no. 2 (June 2021): 486–503. https://doi.org/10.1177/13607804211019760.

Ettredge, Michael, Feng Guo, and Yijun Li. "Trade Secrets and Cyber Security Breaches." *Journal of Accounting and Public Policy* 37, no. 6 (2018): 564–85. https://doi.org/10.1016/j.jaccpubpol.2018.10.006.

Haoran, Xu, Miao Wenlong, and Zhang Siyu. "Digital Technology Development and Systemic Financial Risks: Evidence from 22 Countries." *Borsa Istanbul Review* 24 (2024): 1–9. https://doi.org/10.1016/j.bir.2024.08.002.

Jalil, Juriah Abd, and Halyani Hassan. "Protecting Trade Secret from Theft and Corporate Espionage: Some Legal and Administrative Measures." *International Journal of Business and Society* 21, no. S1 (2020): 205–18. https://openurl.ebsco.com/EPDB%3Agcd%3A11%3A11575179/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A141429605&crl=c&link_origin=www.google.com.

John, Mariah St. "Cybersecurity Stats: Facts And Figures You Should Know – Forbes Advisor." Forbes, August 2024. https://blog.cedsolutions.com/33254/cybersecurity-stats-facts-and-figures-you-should-know/.

Kaka, Noshir, Anu Madgavkar, Alok Kshirsagar, Rajat Gupta, and James

Manyika. "Digital India: Technology to Transform a Connected Nation." Mumbai, 2019. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation.

Klasa, Sandy, Hernán Ortiz-Molina, Matthew Serfling, and Shweta Srinivasan. "Protection of Trade Secrets and Capital Structure Decisions." *Journal of Financial Economics* 128, no. 2 (2018): 266–86. https://doi.org/10.1016/j.jfineco.2018.02.008.

Labadie, Clément, and Christine Legner. "Building Data Management Capabilities to Address Data Protection Regulations: Learnings from EU-GDPR." *Journal of Information Technology* 38, no. 1 (January 2023): 16–44. https://doi.org/10.1177/02683962221141456.

Luo, Yadong. "A General Framework of Digitization Risks in International Business." *Journal of International Business Studies* 53, no. 2 (2022): 344–61. https://doi.org/10.1057/s41267-021-00448-9.

Maskun, and Rian Nugraha Anwar. "Regulation and Protection of Cloud Computing: Literature Review Perspective." *Jambura Law Review* 3, no. 2 (2021): 336–64. https://doi.org/10.33756/jlr.v3i2.10639.

Massa, Silvia, Maria Carmela Annosi, Lucia Marchegiani, and Antonio Messeni Petruzzelli. "Digital Technologies and Knowledge Processes: New Emerging Strategies in International Business. A Systematic Literature Review." *Journal of Knowledge Management* 27, no. 11 (January 2023): 330–87. https://doi.org/10.1108/JKM-12-2022-0993.

Matulionyte, Rita. "Government Automation, Transparency and Trade Secrets." *Melbourne University Law Review* 47, no. 3 (2024): 679–722. https://doi.org/10.2139/ssrn.4771120.

Mavani, Chirag, Hirenkumar Kamleshbhai Mistry, Ripalkumar Patel, and Amit Goswami. "The Role of Cybersecurity in Protecting Intellectual Property." *International Journal on Recent and Innovation Trends in Computing and Communication* 12, no. 2 (February 2024): 529–38.

https://ijritcc.org/index.php/ijritcc/article/view/10935.

Mbah, Geraldine O. "US Intellectual Property Law and Its Impact on Business: Recent Developments and Trends." *International Journal of Science and Research Archive* 13, no. 2 (December 2024): 3279–95. https://doi.org/10.30574/ijsra.2024.13.2.2575.

Mohapatra, Chinmaya Kumar, and Amrita Mishra. "Trade Secret Protection in India." *PalArch's Journal of Archaeology of Egypt / Egyptology* 17, no. 6 (December 2020): 5436–42. https://www.archives.palarch.nl/index.php/jae/article/view/1813.

Nashkova, Suzana. "Addressing Criminal Liability for Misuse of Trade Secrets Under Australian Law: Is the Current Legal Framework Adequate to Protect the Interests of Owners of Trade Secrets?" *IIC - International Review of Intellectual Property and Competition Law* 55, no. 8 (2024): 1281–1315. https://doi.org/10.1007/s40319-024-01490-4.

Nomani, Mohammad Zafar Mahfooz, Zubair Ahmed, and Mohammad Rauf. "Role of Trade Secret Protection Laws in the Development of Indo-Brazilian Bilateral Trade & Investment." *International Journal of Law* 5, no. 5 (September 2019): 20–24. https://www.lawjournals.org/archives/2019/vol5/issue5/5-4-61.

P., Jeevetha. "Inadequacy of Legal Framework for Trade Secret Protection in India: A Legal Analysis of Trade Secrets Bill 2024." *International Journal for Research Trends and Innovation* 10, no. 2 (February 2025): a425–41. https://www.ijrti.org/viewpaperforall.php?paper=IJRTI2502046.

Pervaiz, Hafiz Shahzad, and Shaukat Hussain Bhatti. "Analyses of Cybercrime Regulations Falling behind New Technologies." *Journal of Social Sciences Review* 3, no. 1 (March 2023): 460–69. https://doi.org/10.54183/jssr.v3i1.181.

Rhogust, Muhammad. "Legal Framework for Cybersecurity in the Digital Economy: Challenges and Prospects for Indonesia." *Journal of Law, Social Science and Humanities* 1, no. 2 (June 2024): 166–80.

https://myjournal.or.id/index.php/JLSSH/article/view/213.

Ross, William H, and Danny Franklin. "Characteristics of Effective Trade Secrets and Confi Dential Information Policies: Guidance from Labor Arbitration Cases." *Labor Law Journal* 71, no. 1 (January 2020): 43–57. https://fruehanp1.pythonanywhere.com/bibliography/TYRH2UYC.

Saias, Marco Alexandre. "Unlawful Acquisition of Trade Secrets by Cyber Theft: Between the Proposed Directive on Trade Secrets and the Directive on Cyber Attacks." *Journal of Intellectual Property Law & Practice* 9, no. 9 (September 2014): 721–29. https://doi.org/10.1093/jiplp/jpu117.

Sandeen, Sharon. "Out of Thin Air: Trade Secrets, Cybersecurity, and the Wrongful Acquisition Tort Authors." *Minnesota Journal of Law, Science & Technology* 19, no. 2 (2018): 373–404. https://scholarship.law.umn.edu/mjlst/vol19/iss2/3/.

Senjaya, Murshal. "Cyber Crime And Criminal Law In The Era Of Artificial Intelligence." *International Journal of Law and Society* 1, no. 4 (October 2024): 268–76. https://doi.org/10.62951/ijls.v1i4.210.

Singh, Tripti. "Cybercrime And International Law: Jurisdictional Challenges And Enforcement Mechanisms." *African Journal of Biomedical Research* 27, no. 3S (September 2024): 697–708. https://doi.org/10.53555/AJBR.v27i3S.2101.

Sood, M. (2018). The Role Of Banking In Payment Of International Trade Contract. *Jurnal IUS Kajian Hukum Dan Keadilan*, *6*(2), 193–207. https://doi.org/10.29303/ius.v6i2.552.

Syarifuddin, Muhammad. Perspektif Global Penyelesaian Sengketa Investasi di Indonesia, *De Jure: Jurnal Hukum dan Syar'iah* Vol 3, No 1: Juni 2011.

Sudirman, Lu, and Hari Sutra Disemadi. "Rahasia Dagang Sebagai Perlindungan Kekayaan Intelektual Usaha Mikro Kecil Dan Menengah Di Era Digitalisasi Dan Globalisasi." *Jurnal Magister Hukum Udayana* 12, no. 1 (2023): 80–98. https://doi.org/10.24843/JMHU.2023.v12.i01.p07.

T. N., Veena. "Misappropriation of Trade Secrets Under the Indian Legal Framework: An Analytical Study." *Christ University Law Journal* 12, no. 1 (July 2023): 83–98. https://doi.org/10.12728/culj.22.4.

Tan, David. "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 2463–78. https://core.ac.uk/download/pdf/490668614.pdf.

Tanujaya, Jason, and Vincentius Raymond Wijaya. "Trade Secrets Protection for Blockchain Technology in Indonesia." *Anthology: Inside Intellectual Property Rights* 2, no. 1 (2024): 388–401. https://ojs.uph.edu/index.php/Anthology/article/view/8521.

Ubaydullaeva, Anna. "Know-How and Trade Secrets in Digital Business." *International Journal of Law and Policy* 2, no. 3 (March 2024): 38–52. https://doi.org/10.59022/ijlp.162.

Vecellio Segate, Riccardo. "Securitizing Innovation to Protect Trade Secrets Between 'the East' and 'the West': A Neo-Schumpeterian Public Legal Reading." *UCLA Pacific Basin Law Journal* 37, no. 1 (2020): 59–126. https://doi.org/10.5070/p8371048804.

Wiebe, Andreas, and Nico Schur. "Protection of Trade Secrets in a Data-Driven, Networked Environment – Is the Update Already out-Dated?" *Journal of Intellectual Property Law & Practice* 14, no. 10 (October 2019): 814–21. https://doi.org/10.1093/jiplp/jpz119.

Yaacob, Mohd Noorulfakhri, Syed Zulkarnain Syed Idrus, and Mariam Idris. "Managing Cybersecurity Risks in Emerging Technologies." *International Journal of Business and Technopreneurship (IJBT)* 13, no. 3 (October 2023): 253–70. https://doi.org/10.58915/ijbt.v13i3.297.

Case Laws

Maggbury Pty Ltd v Hafele Australia Pty Ltd (2001) 210 CLR 181.
Del Casale v Artedomus (Aust) Pty Ltd [2007] NSWCA 172; (2007) 73 IPR 326.
John Richard Brady & Ors v Chemical Process Equipment P Ltd & Anr