KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Ekonomi Manajemen Bisnis dan Akuntansi
Vol.3, No.4 Juli 2026
e-ISSN: 3047-6240, p-ISSN: 3047-6232, Hal 1085-1100
DOI : https://doi.org/10.61722/jemba.v3i4.2971

Pengungkapan Keamanan Siber Pada Perusahaan Subsektor Perbankan Yang Terdaftar Di Bursa Efek Indonesia Periode 2025

Dhania Kurnia Putri[1*], Rosalina Pebrica Mayasari[2], Lia Sari[3]
[1]Program Studi Akuntansi, Fakultas Ekonomi Dan Bisnis, Universitas Tridinanti
[2]Program Studi Akuntansi, Fakultas Ekonomi Dan Bisnis, Universitas Tridinanti
[3]Program Studi Akuntansi, Fakultas Ekonomi Dan Bisnis, Universitas Tridinanti
*Penulis Korespondensi: dhaniakurnia4@gmail.com

Abstract. *This study aims to determine the level of cybersecurity disclosure among banking subsector companies listed on the Indonesia Stock Exchange for the 2025 period and to analyze differences in disclosure based on ownership status, bank size, and profitability. This study employed a descriptive quantitative method using secondary data obtained from the annual reports and sustainability reports of banking companies. The sample consisted of 46 banks selected using a saturated sampling technique. Cybersecurity disclosure was measured through content analysis based on 73 disclosure items, with a score of 1 assigned when an item was disclosed and a score of 0 when it was not disclosed. The data were analyzed quantitatively using the cybersecurity disclosure index and difference tests conducted with SPSS. The results showed that the average level of cybersecurity disclosure was 14.38%, indicating that it remained relatively low. The difference test results revealed a significant difference between state-owned banks and non-state-owned banks. However, no significant differences were found based on bank size and profitability. These findings indicate that cybersecurity disclosure in the banking sector still needs to be improved as a form of corporate transparency and accountability to stakeholders.*
Keywords: *Cybersecurity Disclosure; Banking; Ownership Status; Bank Size; Profitability.*

Abstrak. Penelitian ini bertujuan untuk mengetahui tingkat pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025, serta menganalisis perbedaan pengungkapan berdasarkan status kepemilikan, ukuran bank, dan profitabilitas. Penelitian ini menggunakan metode kuantitatif deskriptif dengan sumber data sekunder yang diperoleh dari laporan tahunan dan laporan keberlanjutan perusahaan perbankan. Sampel dalam penelitian ini berjumlah 46 bank yang dipilih menggunakan teknik sampling jenuh. Pengukuran pengungkapan keamanan siber dilakukan dengan metode *content analysis* berdasarkan 73 item pengungkapan, menggunakan skor 1 apabila item diungkapkan dan skor 0 apabila tidak diungkapkan. Teknik analisis data menggunakan pendekatan kuantitatif melalui indeks pengungkapan keamanan siber dan uji beda menggunakan SPSS. Hasil penelitian menunjukkan bahwa rata-rata tingkat pengungkapan keamanan siber sebesar 14,38%, sehingga masih tergolong rendah. Hasil uji beda menunjukkan terdapat perbedaan signifikan antara bank BUMN dan bank non-BUMN, sedangkan berdasarkan ukuran bank dan profitabilitas tidak terdapat perbedaan yang signifikan. Penelitian ini menunjukkan bahwa pengungkapan keamanan siber pada sektor perbankan masih perlu ditingkatkan sebagai bentuk transparansi dan tanggung jawab perusahaan kepada stakeholder.
Kata kunci: Pengungkapan Keamanan Siber; Perbankan; Status Kepemilikan; Ukuran Bank; Profitabilitas.

1. LATAR BELAKANG

Perkembangan teknologi informasi telah mendorong transformasi digital yang sangat pesat dalam berbagai sektor, termasuk sektor perbankan. Perbankan tidak lagi hanya berfungsi sebagai lembaga intermediasi keuangan, tetapi juga sebagai penyedia layanan berbasis teknologi. Namun, di balik kemajuan tersebut, digitalisasi juga membawa berbagai risiko baru yang harus dihadapi oleh perusahaan, khususnya pada sektor perbankan. Ketergantungan bank terhadap sistem teknologi informasi dapat

Naskah Masuk: 01 Juli 2026; Revisi: 05 Juli 2026; Diterima: 06 Juli 2026; ; Terbit: 31 Juli 2026

meningkatkan potensi terjadinya gangguan operasional apabila tidak diimbangi dengan sistem keamanan yang memadai. Risiko keamanan siber pada sektor perbankan dapat berupa penyalahgunaan data, peretasan sistem, pencurian informasi nasabah, *malware, phishing, ransomware*, serta gangguan terhadap sistem layanan digital (Setiawan, 2025).

Transparansi menjadi salah satu aspek penting dalam tata kelola perusahaan modern, khususnya pada sektor perbankan yang memiliki tingkat kepercayaan publik yang tinggi. Salah satu bentuk transparansi tersebut adalah pengungkapan keamanan siber dalam laporan tahunan perusahaan. Informasi ini memberikan gambaran mengenai kesiapan perusahaan dalam menghadapi ancaman digital serta kemampuan dalam mengelola risiko teknologi informasi. Semakin transparan perusahaan dalam mengungkapkan informasi tersebut, semakin tinggi tingkat kepercayaan yang diperoleh dari investor dan *stakeholder*. Oleh karena itu, pengungkapan keamanan siber menjadi bagian penting dalam praktik *Good Corporate Governance* serta diduga memiliki pengaruh terhadap persepsi dan penilaian terhadap Perusahaan (Hendra, 2024).

Dalam praktiknya, tingkat pengungkapan antar perusahaan masih menunjukkan variasi yang signifikan (Kurnia, 2025). Sebagian perusahaan mengungkapkan secara rinci, sementara yang lain masih terbatas. Perbedaan ini menunjukkan adanya variasi kebijakan dalam penyampaian informasi. Hal ini menjadi fenomena yang menarik untuk diteliti lebih lanjut (Healy, 2001).

Dalam perspektif teori *stakeholder*, perusahaan memiliki tanggung jawab untuk memenuhi kebutuhan informasi para pemangku kepentingan. *stakeholder* tidak hanya terdiri dari pemegang saham, tetapi juga mencakup masyarakat dan pemerintah. Pengungkapan keamanan siber menjadi salah satu bentuk tanggung jawab tersebut. Hal ini menunjukkan bahwa perusahaan mampu mengelola risiko dengan baik. Dengan demikian, kepercayaan *stakeholder* dapat tetap terjaga (Freeman & Phillips, 2021).

Pengungkapan keamanan siber berkaitan erat dengan reputasi perusahaan karena informasi yang disampaikan kepada publik mencerminkan bagaimana perusahaan mengelola risiko yang dihadapi. Transparansi dalam pengungkapan memberikan sinyal positif kepada investor dan masyarakat mengenai kesiapan perusahaan dalam menghadapi ancaman siber, sehingga dapat meningkatkan kepercayaan (Zaroh & Purwaningsih, 2026). Salah satu indikator yang dapat digunakan untuk melihat tingkat perhatian perusahaan terhadap teknologi informasi adalah melalui jumlah pengungkapan

terkait teknologi dalam laporan tahunan. Semakin banyak informasi yang disampaikan, maka menunjukkan semakin tinggi tingkat perhatian perusahaan terhadap aspek teknologi, termasuk dalam pengelolaan keamanan siber (Sari, 2025).

Penelitian mengenai pengungkapan keamanan siber di Indonesia masih tergolong terbatas, padahal isu ini semakin penting dalam era digital, khususnya pada sektor perbankan yang memiliki tingkat risiko tinggi terhadap ancaman siber (Hidayah & Ananda, 2025). Penelitian sebelumnya lebih banyak membahas pengungkapan risiko teknologi atau keamanan siber secara umum, serta hanya meneliti faktor tertentu seperti ukuran perusahaan, struktur tata kelola, profitabilitas, atau umur perusahaan (Tri Wahyu & Masiyah, 2024). Dengan demikian, masih terdapat keterbatasan penelitian yang secara spesifik membandingkan tingkat pengungkapan keamanan siber pada perusahaan perbankan berdasarkan status kepemilikan bank, ukuran bank berdasarkan Kelompok Bank berdasarkan Modal Inti, tingkat profitabilitas, dan umur bank secara bersamaan.

Selain itu, penelitian terdahulu belum banyak menggunakan indeks pengungkapan keamanan siber yang lebih komprehensif dan berbasis pada 73 item pengungkapan yang mencakup aspek risiko, tata kelola teknologi informasi, perlindungan data, pengujian keamanan, pemulihan insiden, serta pelaporan insiden keamanan siber. Oleh karena itu, penelitian ini dilakukan untuk mengisi kesenjangan tersebut dengan menganalisis pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025.

Pemilihan periode 2025 dalam penelitian ini didasarkan pada pertimbangan bahwa laporan tahunan tahun 2025 merupakan data terbaru yang dapat digunakan untuk melihat praktik pengungkapan keamanan siber perusahaan perbankan setelah adanya penguatan regulasi terkait teknologi informasi dan keamanan siber. OJK menerbitkan POJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum yang mengatur penyelenggaraan teknologi informasi dalam operasional bank (OJK, 2022). Selain itu, OJK juga menerbitkan SEOJK Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum sebagai pedoman khusus mengenai ketahanan dan keamanan siber perbankan.

Berdasarkan kondisi di atas, terdapat kesenjangan antara teori dan praktik dalam pengungkapan keamanan siber. Secara teori, dalam perspektif teori *stakeholder*, perusahaan diharapkan menyampaikan informasi secara transparan guna memenuhi

kebutuhan informasi para pemangku kepentingan, termasuk terkait pengelolaan risiko keamanan siber. Namun, dalam praktiknya pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia, tingkat pengungkapan keamanan siber masih menunjukkan variasi yang signifikan antar perusahaan.

Dengan demikian, penelitian ini bertujuan untuk menganalisis pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia tahun 2025. Penelitian ini diharapkan dapat memberikan gambaran mengenai praktik pengungkapan keamanan siber pada perusahaan perbankan di Indonesia. Selain itu, penelitian ini juga diharapkan dapat menjadi referensi bagi penelitian selanjutnya dalam bidang pengungkapan informasi perusahaan.

2. KAJIAN TEORITIS

A. *Stakeholder Theory*

Teori *stakeholder* merupakan teori yang menjelaskan bahwa perusahaan tidak hanya bertanggung jawab kepada pemegang saham, tetapi juga kepada seluruh pihak yang memiliki kepentingan terhadap perusahaan. Dalam konteks perbankan, *stakeholder* meliputi investor, nasabah, karyawan, pemerintah, dan masyarakat. Pendekatan ini menunjukkan bahwa perusahaan memiliki tanggung jawab yang luas dalam menjalankan aktivitasnya (Mahajan et al., 2023). Tujuan utama teori *stakeholder* adalah untuk menciptakan keseimbangan antara kepentingan perusahaan dan para pemangku kepentingan. Perusahaan diharapkan tidak hanya berfokus pada keuntungan semata, tetapi juga memperhatikan dampak dari aktivitasnya, termasuk risiko keamanan siber. Dengan memperhatikan kepentingan *stakeholder*, perusahaan dapat meningkatkan kepercayaan dan dukungan dari berbagai pihak (Sundari, 2026).

Hubungan antara perusahaan dan *stakeholder* bersifat saling memengaruhi dan tidak dapat dipisahkan. Perusahaan membutuhkan dukungan dari *stakeholder* untuk menjalankan operasionalnya secara efektif, terutama dalam menjaga keamanan sistem dan data. Sebaliknya, *stakeholder* juga memiliki kepentingan terhadap aktivitas dan kinerja perusahaan. Transparansi informasi merupakan salah satu cara perusahaan dalam memenuhi kebutuhan *stakeholder*. Melalui transparansi, perusahaan perbankan dapat menyampaikan informasi yang akurat dan relevan kepada publik, termasuk terkait keamanan siber. Selain itu, transparansi juga dapat meningkatkan akuntabilitas perusahaan dalam menjalankan operasionalnya (Rajakulanajagam, 2022).

Dalam teori *stakeholder*, pemangku kepentingan dapat diklasifikasikan menjadi *stakeholder* utama (*Primary Stakeholders*) dan *stakeholder* sekunder (*Secondary Stakeholders*). *stakeholder* utama meliputi pihak-pihak yang memiliki hubungan langsung dengan perusahaan seperti investor, nasabah, karyawan, dan regulator, sedangkan *stakeholder* sekunder meliputi pihak yang tidak terlibat secara langsung namun tetap memiliki kepentingan (Freeman & Phillips, 2002).

Teori *stakeholder* juga menekankan pentingnya pengelolaan hubungan antara perusahaan dan pemangku kepentingan melalui penyampaian informasi yang relevan dan transparan. Dalam era digital, kebutuhan akan informasi tidak hanya terbatas pada aspek keuangan, tetapi juga mencakup informasi non-keuangan seperti keamanan siber. Pengungkapan informasi keamanan siber menjadi salah satu bentuk komunikasi perusahaan kepada *stakeholder* mengenai upaya yang dilakukan dalam melindungi data dan sistem. Hal ini penting untuk memberikan keyakinan kepada *stakeholder* bahwa perusahaan mampu mengelola risiko digital secara memadai (Freeman, 2010). Semakin lengkap informasi yang disampaikan, semakin besar pula kemampuan *stakeholder* dalam memahami kondisi perusahaan (Freeman et al., 2018).

3. METODE PENELITIAN

Penelitian ini dilakukan pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia (BEI) pada periode 2025. Penelitian ini dilakukan pada periode Maret hingga Agustus 2026. Data yang digunakan dalam penelitian ini merupakan data sekunder yang diperoleh dari laporan tahunan *(annual report)* dan laporan keberlanjutan *(sustainability report)*. Teknik pengumpulan data dalam penelitian ini menggunakan metode dokumentasi. Populasi dalam penelitian ini adalah seluruh perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia pada periode 2025 sebanyak 46 perusahaan. Teknik pengambilan sampel dalam penelitian ini menggunakan sampel jenuh (census sampling), yaitu seluruh anggota populasi dijadikan sampel penelitian. Teknik pengukuran pengungkapan keamanan siber dalam penelitian ini dilakukan dengan menggunakan metode *content analysis*. Teknik analisis data dalam penelitian ini dilakukan dengan pendekatan kuantitatif dengan bantuan SPSS versi 26. Adapun langkah-langkah yang dilakukan dalam menganalisis data adalah pengukuran indeks pengungkapan keamanan siber, analisis statistik deskriptif, uji normalitas, uji beda (*independent sample t-test* / ANOVA), uji hipotesis, dan penarikan kesimpulan.

4. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

Statistik Deskriptif

Berdasarkan hasil pengolahan SPSS, jumlah data yang dianalisis sebanyak 46 bank. Nilai minimum pengungkapan keamanan siber adalah 0, sedangkan nilai maksimum adalah 20. Nilai rata-rata sebesar 10,50 menunjukkan bahwa secara umum bank mengungkapkan sekitar sepuluh sampai sebelas item dari total 73 item pengungkapan. Dengan demikian, pengungkapan keamanan siber pada bank yang menjadi sampel penelitian masih tergolong terbatas. Nilai minimum sebesar 0 menunjukkan bahwa masih terdapat bank yang belum mengungkapkan item keamanan siber berdasarkan indikator yang digunakan dalam penelitian. Sementara itu, nilai maksimum sebesar 20 menunjukkan bahwa bank dengan pengungkapan tertinggi pun masih belum mencapai setengah dari total 73 item yang digunakan. Kondisi ini menggambarkan bahwa pengungkapan keamanan siber masih perlu diperluas dan diperjelas.

Tabel 1. Hasil Statistik Deskriptif Pengungkapan Keamanan Siber

Variabel	N	Minimum	Maximum	Mean
Pengungkapan Keamanan Siber	46	0	20	10,50

Sumber: Data diolah peneliti menggunakan SPSS, 2026

Berdasarkan Tabel di atas, tingkat pengungkapan keamanan siber pada perusahaan subsektor perbankan memiliki nilai rata-rata sebesar 10,50. Nilai ini menunjukkan bahwa secara umum perusahaan hanya mengungkapkan sebagian kecil dari indikator yang tersedia. Oleh karena itu, pengungkapan keamanan siber masih perlu ditingkatkan agar informasi yang diberikan kepada stakeholder menjadi lebih lengkap dan informatif.

Hasil Berdasarkan Status Kepemilikan Bank

Berdasarkan hasil analisis, bank BUMN memperoleh rata-rata skor sebesar 14,60 item atau 20,00 persen. Sementara itu, bank non-BUMN memperoleh rata-rata skor sebesar 9,36 item atau 12,82 persen. Nilai rata-rata bank BUMN lebih tinggi dibandingkan bank non-BUMN. Hal ini menunjukkan bahwa bank BUMN cenderung mengungkapkan informasi keamanan siber lebih luas dibandingkan bank non-BUMN. Perbedaan rata-rata tersebut dapat disebabkan oleh tingginya tuntutan transparansi pada bank BUMN. Karena berkaitan dengan kepentingan masyarakat luas dan pengawasan pemerintah, bank BUMN cenderung memiliki dorongan lebih besar untuk menyampaikan informasi mengenai tata kelola, pengendalian risiko, dan keamanan sistem.

Tabel 2. Pengungkapan Keamanan Siber Berdasarkan Status Kepemilikan

Status Kepemilikan	Jumlah Bank	Rata-rata Skor	Rata-rata Persentase
BUMN	10	14,60	20,00%
Non-BUMN	36	9,36	12,82%

Sumber: Data diolah peneliti menggunakan SPSS, 2026

Berdasarkan Tabel di atas, bank BUMN memiliki rata-rata pengungkapan yang lebih tinggi dibandingkan bank non-BUMN. Perbedaan ini dapat diartikan bahwa kepemilikan pemerintah berpotensi mendorong perusahaan untuk lebih terbuka dalam mengungkapkan informasi keamanan siber. Walaupun demikian, tingkat pengungkapan kedua kelompok masih berada pada kategori rendah karena nilai rata-rata persentasenya belum mencapai 25 persen. Hasil ini juga menunjukkan bahwa baik bank BUMN maupun bank non-BUMN masih perlu meningkatkan kualitas informasi yang diungkapkan. Pengungkapan tidak cukup hanya menyebutkan keberadaan sistem teknologi informasi, tetapi sebaiknya juga menjelaskan aspek tata kelola, pengujian, pelatihan, rencana pemulihan, dan penanganan insiden secara lebih jelas.

Hasil Berdasarkan Ukuran Bank (KBMI)

Berdasarkan hasil analisis, rata-rata pengungkapan tertinggi terdapat pada bank KBMI 3 dengan skor rata-rata 12,18 item atau 16,69 persen. Selanjutnya, KBMI 1 memperoleh rata-rata 11,67 item atau 15,98 persen, KBMI 4 sebesar 9,58 item atau 13,13 persen, dan KBMI 2 sebesar 8,55 item atau 11,71 persen. Hasil tersebut menunjukkan bahwa rata-rata pengungkapan antar kategori KBMI berbeda, tetapi tidak membentuk pola kenaikan yang tetap dari KBMI 1 sampai KBMI 4.

Perbedaan rata-rata tersebut dapat dipahami karena setiap kelompok KBMI memiliki karakteristik, strategi pengungkapan, serta kebijakan teknologi informasi yang berbeda. Bank dengan ukuran besar belum tentu mengungkapkan seluruh informasi keamanan siber secara lebih luas, sedangkan bank pada kategori yang lebih kecil tetap dapat melakukan pengungkapan apabila memiliki komitmen tata kelola yang baik.

Tabel 3. Pengungkapan Keamanan Siber Berdasarkan KBMI

Kategori KBMI	Jumlah Bank	Rata-rata Skor	Rata-rata Persentase
KBMI 1	12	11,67	15,98%
KBMI 2	11	8,55	11,71%
KBMI 3	11	12,18	16,69%
KBMI 4	12	9,58	13,13%

Sumber: Data diolah peneliti menggunakan SPSS, 2026

Berdasarkan Tabel di atas, rata-rata pengungkapan keamanan siber berbeda pada setiap kategori KBMI. Namun, perbedaan tersebut tidak menunjukkan pola yang sepenuhnya linear. Hal ini menunjukkan bahwa ukuran bank dapat berkaitan dengan pengungkapan keamanan siber, tetapi tidak selalu menjadi satu-satunya faktor yang menentukan luasnya informasi yang disampaikan. Meskipun terdapat perbedaan rata-rata antar kelompok KBMI, pengungkapan pada seluruh kelompok masih tergolong rendah jika dibandingkan dengan total 73 indikator yang digunakan. Hal ini menunjukkan bahwa seluruh kategori bank, baik KBMI 1, KBMI 2, KBMI 3, maupun KBMI 4, masih perlu memperkuat kualitas dan kelengkapan pengungkapan keamanan siber.

Hasil Berdasarkan Profitabilitas Bank

Berdasarkan hasil analisis, bank dengan profitabilitas tinggi memperoleh rata-rata skor sebesar 10,29 item atau 14,09 persen. Bank dengan profitabilitas sedang memperoleh rata-rata skor sebesar 11,53 item atau 15,79 persen. Sementara itu, bank dengan profitabilitas rendah memperoleh rata-rata skor sebesar 9,53 item atau 13,06 persen. Hasil ini menunjukkan bahwa bank dengan profitabilitas sedang memiliki rata-rata pengungkapan yang paling tinggi, tetapi selisih antar kelompok tidak terlalu besar.

Walaupun terdapat perbedaan rata-rata, selisih antar kelompok profitabilitas tidak terlalu besar. Hal ini menunjukkan bahwa profitabilitas mungkin bukan satu-satunya faktor yang menentukan luasnya pengungkapan keamanan siber. Faktor lain seperti kebijakan manajemen, tekanan regulator, struktur tata kelola, ukuran bank, dan tingkat ketergantungan terhadap layanan digital juga dapat memengaruhi pengungkapan.

Tabel 4. Pengungkapan Keamanan Siber Berdasarkan Profitabilitas

Kategori Profitabilitas	Jumlah Bank	Rata-rata Skor	Rata-rata Persentase
Tinggi	14	10,29	14,09%
Sedang	17	11,53	15,79%
Rendah	15	9,53	13,06%

Sumber: Data diolah peneliti menggunakan SPSS, 2026

Berdasarkan Tabel di atas, rata-rata pengungkapan tertinggi terdapat pada kelompok bank dengan profitabilitas sedang. Namun, perbedaan nilai rata-rata antara profitabilitas tinggi, sedang, dan rendah relatif kecil. Hal ini menunjukkan bahwa profitabilitas belum tentu menjadi faktor yang kuat dalam membedakan tingkat pengungkapan keamanan siber. Dalam konteks ini, perusahaan yang memiliki profitabilitas rendah tetap dapat melakukan pengungkapan keamanan siber apabila

memiliki komitmen tata kelola yang baik. Sebaliknya, perusahaan dengan profitabilitas tinggi belum tentu mengungkapkan informasi secara luas apabila kebijakan pengungkapan perusahaan masih terbatas.

Hasil Uji Beda Menggunakan SPSS

Hasil uji beda menunjukkan bahwa nilai signifikansi status kepemilikan sebesar 0,007. Karena nilai tersebut lebih kecil dari 0,05, maka terdapat perbedaan yang signifikan tingkat pengungkapan keamanan siber antara bank BUMN dan bank non-BUMN. Artinya, status kepemilikan dapat menjadi faktor pembeda dalam pengungkapan keamanan siber. Nilai signifikansi ukuran bank berdasarkan KBMI sebesar 0,373. Karena nilai tersebut lebih besar dari 0,05, maka tidak terdapat perbedaan yang signifikan tingkat pengungkapan keamanan siber berdasarkan kategori KBMI. Artinya, ukuran bank belum terbukti menjadi faktor pembeda yang signifikan dalam pengungkapan keamanan siber pada perusahaan perbankan. Nilai signifikansi profitabilitas sebesar 0,603. Karena nilai tersebut lebih besar dari 0,05, maka tidak terdapat perbedaan yang signifikan tingkat pengungkapan keamanan siber berdasarkan kategori profitabilitas. Artinya, profitabilitas tinggi, sedang, dan rendah tidak menunjukkan perbedaan yang cukup kuat secara statistik dalam pengungkapan keamanan siber.

Tabel 5. Ringkasan Hasil Uji Beda Pengungkapan Keamanan Siber

Kelompok yang Diuji	Metode Uji	Nilai Sig.	Kriteria	Kesimpulan
Status kepemilikan (BUMN dan Non-BUMN)	*Independent Sample t-test*	0,007	Sig. < 0,05	Terdapat perbedaan signifikan
Ukuran bank (KBMI 1, KBMI 2, KBMI 3, KBMI 4)	*One Way ANOVA*	0,373	Sig. > 0,05	Tidak terdapat perbedaan signifikan
Profitabilitas (tinggi, sedang, rendah)	*One Way ANOVA*	0,603	Sig. > 0,05	Tidak terdapat perbedaan signifikan

Sumber: Data diolah peneliti menggunakan SPSS versi 26, 2026

Berdasarkan Tabel di atas, kelompok pengujian yang menunjukkan hasil signifikan adalah status kepemilikan. Sementara itu, ukuran bank berdasarkan KBMI dan profitabilitas tidak menunjukkan perbedaan yang signifikan. Hasil ini memberikan gambaran bahwa faktor kepemilikan lebih terlihat dalam membedakan pengungkapan keamanan siber dibandingkan ukuran bank dan kemampuan menghasilkan laba.

B. Pembahasan

Pembahasan Tingkat Pengungkapan Keamanan Siber

Hasil penelitian menunjukkan bahwa tingkat pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025 masih tergolong rendah. Rata-rata pengungkapan sebesar 14,38 persen atau 10,50 item dari total 73 item. Angka tersebut menunjukkan bahwa sebagian besar bank belum menyampaikan informasi keamanan siber secara mendalam dalam laporan tahunan atau laporan keberlanjutan.

Rendahnya tingkat pengungkapan dapat disebabkan oleh beberapa faktor. Pertama, pengungkapan keamanan siber masih dianggap sebagai informasi yang sensitif. Perusahaan mungkin berhati-hati dalam menyampaikan informasi mengenai sistem keamanan, kelemahan, atau insiden karena dapat berpotensi menimbulkan risiko baru. Kedua, belum semua perusahaan memiliki standar pengungkapan yang sama mengenai keamanan siber. Ketiga, informasi keamanan siber sering kali tersebar pada beberapa bagian laporan sehingga tidak selalu disajikan secara terstruktur.

Dalam perspektif *stakeholder theory*, perusahaan seharusnya menyampaikan informasi yang relevan kepada pemangku kepentingan. *Stakeholder* membutuhkan informasi mengenai bagaimana bank mengelola risiko siber, menjaga data nasabah, dan memastikan keberlangsungan layanan digital. Oleh karena itu, pengungkapan keamanan siber dapat dipandang sebagai bentuk tanggung jawab perusahaan kepada *stakeholder* (Mahajan et al., 2023).

Temuan ini menunjukkan adanya kesenjangan antara tuntutan teori stakeholder dan praktik pengungkapan di lapangan. Secara teoritis, *stakeholder* seperti nasabah, investor, regulator, dan masyarakat membutuhkan informasi mengenai perlindungan data, tata kelola teknologi informasi, pengujian keamanan, rencana pemulihan, serta penanganan insiden. Namun, rendahnya rata-rata pengungkapan menunjukkan bahwa sebagian besar bank belum sepenuhnya memenuhi kebutuhan informasi tersebut.

Hasil penelitian ini sejalan dengan penelitian yang menyatakan bahwa pengungkapan risiko teknologi pada perbankan Indonesia masih rendah dan bervariasi antarbank (Naufal & Azmi, 2024). Temuan ini juga mendukung yang menemukan bahwa *cybersecurity disclosure* pada industri perbankan belum dilakukan secara seragam (Firoozi & Mohsni, 2023). Selain itu, hasil ini memperkuat yang menunjukkan bahwa pengungkapan keamanan siber pada bank di Indonesia masih perlu ditingkatkan, khususnya pada aspek tata kelola dan informasi keamanan teknologi (Sari et al., 2024).

Meskipun pengungkapan keamanan siber masih rendah, adanya beberapa item yang diungkapkan menunjukkan bahwa bank mulai menyadari pentingnya isu ini. Informasi yang sering muncul biasanya berkaitan dengan tata kelola teknologi informasi, pengendalian internal, pengamanan data, dan keberadaan sistem manajemen risiko. Namun, informasi mengenai insiden siber, biaya akibat insiden, frekuensi pengujian, dan dampak insiden cenderung masih sangat terbatas.

Pembahasan Berdasarkan Status Kepemilikan

Hasil uji beda menunjukkan bahwa terdapat perbedaan signifikan tingkat pengungkapan keamanan siber antara bank BUMN dan bank non-BUMN. Nilai signifikansi sebesar 0,007 lebih kecil dari 0,05. Dengan demikian, status kepemilikan terbukti menjadi faktor pembeda dalam pengungkapan keamanan siber pada perusahaan subsektor perbankan.

Bank BUMN memiliki rata-rata pengungkapan lebih tinggi dibandingkan bank non-BUMN. Hal ini dapat terjadi karena bank BUMN memiliki tanggung jawab publik yang lebih besar. Sebagai perusahaan yang berhubungan dengan kepentingan pemerintah dan masyarakat, bank BUMN dituntut untuk lebih transparan dalam menyampaikan informasi, termasuk informasi terkait risiko teknologi informasi dan keamanan siber.

Jika dikaitkan dengan *stakeholder theory*, hasil ini menunjukkan bahwa bank BUMN memiliki tekanan akuntabilitas publik yang lebih besar dibandingkan bank non-BUMN. Bank BUMN tidak hanya berorientasi pada kepentingan bisnis, tetapi juga membawa tanggung jawab kepada pemerintah, regulator, nasabah, investor, dan masyarakat luas. Oleh karena itu, bank BUMN lebih terdorong untuk menyampaikan informasi keamanan siber sebagai bentuk transparansi dan pertanggungjawaban publik.

Hasil ini mendukung penelitian Suhendar (2021) yang menyatakan bahwa karakteristik kepemilikan dapat memengaruhi tingkat pengungkapan sukarela perusahaan. Temuan ini juga sejalan dengan Hidayah dan Ananda (2025) dan Sari (2025) yang menegaskan bahwa karakteristik perusahaan dan tata kelola memiliki peran dalam mendorong pengungkapan keamanan siber. Dengan demikian, status kepemilikan bank terbukti menjadi faktor yang membedakan luas pengungkapan keamanan siber pada penelitian ini.

Bank BUMN juga memiliki tingkat eksposur yang tinggi karena memiliki jumlah nasabah besar, jaringan operasional luas, dan layanan digital yang digunakan oleh

masyarakat secara luas. Apabila terjadi gangguan siber, dampaknya tidak hanya dirasakan oleh perusahaan, tetapi juga oleh masyarakat dan sistem keuangan. Oleh sebab itu, bank BUMN cenderung memiliki dorongan lebih besar untuk mengungkapkan informasi keamanan siber. Sementara itu, bank non-BUMN memiliki rata-rata pengungkapan yang lebih rendah. Hal ini bukan berarti bank non-BUMN tidak memperhatikan keamanan siber, tetapi dapat menunjukkan bahwa kebijakan pengungkapan informasi pada bank non-BUMN berbeda-beda. Sebagian bank mungkin lebih fokus pada kepatuhan minimum dan belum menjadikan pengungkapan keamanan siber sebagai bagian utama dalam laporan perusahaan.

Pembahasan Berdasarkan Ukuran Bank

Hasil uji beda berdasarkan KBMI menunjukkan nilai signifikansi sebesar 0,373. Nilai tersebut lebih besar dari 0,05, sehingga dapat disimpulkan bahwa tidak terdapat perbedaan signifikan tingkat pengungkapan keamanan siber berdasarkan ukuran bank. Hasil ini menunjukkan bahwa kategori KBMI belum terbukti menjadi faktor pembeda yang signifikan terhadap luasnya pengungkapan keamanan siber.

Rata-rata pengungkapan tertinggi terdapat pada KBMI 3, sedangkan rata-rata terendah terdapat pada KBMI 2. Pola tersebut menunjukkan bahwa bank dengan ukuran lebih besar belum tentu selalu memiliki pengungkapan keamanan siber yang lebih luas. Kondisi ini dapat terjadi karena pengungkapan tidak hanya dipengaruhi oleh ukuran bank, tetapi juga oleh kebijakan internal, tata kelola, dan komitmen transparansi masing-masing bank. Bank besar memang memiliki tekanan stakeholder yang lebih kuat. Investor, nasabah, regulator, dan masyarakat memiliki perhatian besar terhadap kinerja dan keamanan layanan bank besar. Namun, hasil penelitian ini menunjukkan bahwa tekanan tersebut belum selalu menghasilkan perbedaan pengungkapan yang signifikan antar kategori KBMI.

Sebaliknya, bank dengan KBMI lebih rendah tetap dapat mengungkapkan informasi keamanan siber apabila memiliki perhatian terhadap tata kelola dan kepatuhan regulasi. Dengan demikian, ukuran bank tidak dapat dijadikan satu-satunya dasar untuk menilai luas atau tidaknya pengungkapan keamanan siber dalam laporan perusahaan.

Dalam perspektif *stakeholder theory*, bank berukuran besar seharusnya memiliki tekanan lebih besar untuk mengungkapkan informasi karena memiliki jumlah nasabah yang lebih banyak, aktivitas operasional yang lebih kompleks, dan risiko layanan digital

yang lebih tinggi (Freeman, 1984). Namun, hasil penelitian ini menunjukkan bahwa kategori KBMI belum menjadi faktor pembeda yang signifikan. Artinya, tekanan *stakeholder* pada bank besar belum selalu diikuti dengan pengungkapan keamanan siber yang lebih luas.

Hasil ini berbeda dengan penelitian Hidayah dan Ananda (2025), Sofiani et al. (2024), serta Mazumder dan Hossain (2023) yang menemukan bahwa ukuran perusahaan dapat berhubungan dengan luas pengungkapan risiko atau keamanan siber. Perbedaan hasil ini dapat disebabkan oleh perbedaan objek, periode, indikator ukuran perusahaan, serta kebijakan internal masing-masing bank dalam menyusun laporan tahunan dan laporan keberlanjutan.

Pembahasan Berdasarkan Profitabilitas

Hasil uji beda berdasarkan profitabilitas menunjukkan nilai signifikansi sebesar 0,603. Nilai ini lebih besar dari 0,05, sehingga dapat disimpulkan bahwa tidak terdapat perbedaan signifikan tingkat pengungkapan keamanan siber berdasarkan profitabilitas tinggi, sedang, dan rendah. Dengan demikian, profitabilitas tidak terbukti menjadi faktor pembeda yang signifikan dalam penelitian ini.

Meskipun terdapat perbedaan rata-rata antar kelompok profitabilitas, perbedaannya tidak cukup kuat secara statistik. Hal ini menunjukkan bahwa kemampuan menghasilkan laba belum tentu langsung berhubungan dengan luasnya pengungkapan keamanan siber. Pengungkapan keamanan siber dapat lebih dipengaruhi oleh faktor lain seperti tekanan regulasi, struktur tata kelola, risiko layanan digital, dan kebijakan internal perusahaan.

Hasil ini juga menunjukkan bahwa bank dengan profitabilitas rendah tetap dapat mengungkapkan informasi keamanan siber apabila memiliki kesadaran dan komitmen tata kelola yang baik. Sebaliknya, bank dengan profitabilitas tinggi belum tentu mengungkapkan informasi secara luas apabila perusahaan tidak memiliki kebijakan pengungkapan yang kuat.

Dengan demikian, profitabilitas bukan satu-satunya ukuran untuk menilai kesiapan pengungkapan keamanan siber. Dalam industri perbankan, keamanan siber merupakan kebutuhan dasar yang harus dikelola oleh seluruh bank, baik yang memiliki profitabilitas tinggi maupun rendah. Oleh sebab itu, pengungkapan keamanan siber seharusnya tidak hanya bergantung pada tingkat laba, tetapi juga pada komitmen perusahaan terhadap transparansi dan akuntabilitas.

Berdasarkan *stakeholder theory*, bank dengan profitabilitas tinggi seharusnya memiliki kemampuan sumber daya yang lebih besar untuk mengembangkan sistem keamanan siber dan mengungkapkan informasinya kepada stakeholder (Alsadoun & Albaz, 2025). Akan tetapi, hasil penelitian ini menunjukkan bahwa profitabilitas tidak menjadi faktor pembeda yang signifikan. Hal ini mengindikasikan bahwa pengungkapan keamanan siber lebih dipengaruhi oleh komitmen tata kelola, kebijakan internal, tekanan regulasi, dan kesadaran perusahaan terhadap transparansi daripada hanya oleh kemampuan menghasilkan laba (OJK, 2021).

Hasil ini tidak sepenuhnya sejalan dengan Sofiani et al. (2024) serta Mazumder dan Hossain (2023) yang menyatakan bahwa profitabilitas dapat memengaruhi pengungkapan risiko siber. Namun, perbedaan hasil tersebut dapat dijelaskan karena keamanan siber merupakan kebutuhan dasar bagi seluruh bank, baik bank dengan profitabilitas tinggi, sedang, maupun rendah. Oleh sebab itu, seluruh bank tetap memiliki kewajiban untuk menjaga keamanan data dan menyampaikan informasi yang relevan kepada *stakeholder*.

Secara keseluruhan, hasil penelitian ini memberikan implikasi bahwa perusahaan perbankan perlu meningkatkan kualitas pengungkapan keamanan siber, terutama pada aspek risiko, tata kelola, mitigasi, pengujian keamanan, rencana pemulihan, dan informasi insiden. Bagi investor dan regulator, hasil penelitian ini dapat menjadi bahan pertimbangan dalam menilai transparansi dan kesiapan bank dalam menghadapi risiko digital. Dengan demikian, pembahasan hasil penelitian telah dikaitkan dengan *stakeholder theory* dan diperkuat oleh penelitian terdahulu yang relevan.

5. KESIMPULAN

Tingkat pengungkapan keamanan siber pada perusahaan subsektor perbankan yang terdaftar di Bursa Efek Indonesia periode 2025 masih tergolong rendah. Berdasarkan hasil scoring terhadap 73 item pengungkapan, rata-rata pengungkapan sebesar 14,38 persen atau 10,50 item dari total 73 item. Hal ini menunjukkan bahwa sebagian besar bank belum menyampaikan informasi keamanan siber secara lengkap, terutama terkait risiko, tata kelola teknologi informasi, mitigasi, pengujian, rencana pemulihan, dan insiden keamanan siber. Terdapat perbedaan tingkat pengungkapan keamanan siber antara bank BUMN dan bank non-BUMN. Hasil uji *Independent Sample t-test* menunjukkan nilai signifikansi sebesar 0,007, lebih kecil dari 0,05, sehingga status kepemilikan terbukti menjadi faktor pembeda. Bank BUMN memiliki rata-rata pengungkapan yang lebih

tinggi karena memiliki tanggung jawab publik dan tuntutan transparansi yang lebih besar. Tidak terdapat perbedaan tingkat pengungkapan keamanan siber berdasarkan ukuran bank atau kategori KBMI 1, KBMI 2, KBMI 3, dan KBMI 4. Hasil uji *One Way ANOVA* menunjukkan nilai signifikansi sebesar 0,373, lebih besar dari 0,05. Dengan demikian, kategori KBMI belum terbukti menjadi faktor pembeda utama dalam pengungkapan keamanan siber. Tidak terdapat perbedaan tingkat pengungkapan keamanan siber berdasarkan profitabilitas tinggi, sedang, dan rendah. Hasil uji *One Way ANOVA* menunjukkan nilai signifikansi sebesar 0,603, lebih besar dari 0,05. Dengan demikian, profitabilitas belum terbukti menjadi faktor pembeda dalam pengungkapan keamanan siber, sehingga luas pengungkapan lebih berkaitan dengan kebijakan internal, tata kelola, kepatuhan regulasi, dan komitmen transparansi perusahaan.

DAFTAR REFERENSI

Alsadoun, A. A., & Albaz, M. M. (2025). The impact of cybersecurity risk disclosure and governance on firm value and stock return volatility. *Journal of Governance and Regulation*, *14*(1), 194. https://doi.org/10.22495/jgrv14i1art18

Angelina Septiani Zaroh dan Sri Budi Purwaningsih. (2026). Personal Data Protection in Banking Cybersecurity Breach Cases: Perlindungan Data Pribadi dalam Kasus Pelanggaran Keamanan Siber di Sektor Perbankan. *Indonesian Journal of Law and Economics Review*, *21*(1), 1–13. https://doi.org/10.21070/ijler.v21i1.1533

Freeman, R. E. (2010). *A Stakeholder Approach to Strategic Management*. (01).

Freeman, R. E., & Phillips, R. A. (2002). Stakeholder Theory: A Libertarian Defense. *Business Ethics Quarterly*, *12*(3), 331–349. https://doi.org/10.2307/3858020

Freeman, R. E., & Phillips, R. A. (2021). Stakeholder Theory and the Resource-Based View of the Firm. *Journal of Management*, *47*(7), 1757–1770. https://doi.org/10.1177/0149206321993576

Healy, P. M., & Palepu, K. G. (2001). Information asymmetry , corporate disclosure , and the capital markets : A review of the empirical disclosure literature. *Journal of Accounting and Economics*, *31*, 405–440.

Hendra, M. (2024). Manfaat dan Urgensi Penerapan Good Corporate Governence dalam Perusahaan. *Jurnal Pendidikan Tambusai*, *8*(2), 35477–35485.

Hidayah, E., & Ananda, K. (2025). Cybersecurity Disclosure: Analysis on Banking Companies Listed on the Indonesia Stock Exchange. *International Journal of Economics, Business and Management Research*, *09*(12), 237–254. https://doi.org/10.51505/ijebmr.2025.91212

Mahajan, R., Marc, W., Sareen, M., Kumar, S., & Panwar, R. (2023). Stakeholder theory. *Journal of Business Research*, *166*(June), 1–16. https://doi.org/10.1016/j.jbusres.2023.114104

Muhammad Razan Iftikaar, Ia Kurnia, W. H. (2025). Faktor-Faktor Yang Berpengaruh Terhadap Tingkat Pengungkapan Sukarela Pada Perusahaan Yang Terdaftar di Jakarta Islamic Index. *JIAI (Jurnal Ilmiah Akuntansi Indonesia)*, *10*(2), 1–17.

Naufal, M., & Azmi, A. (2024). Analisa Kasus Kebocoran Data pada Bank Indonesia Dalam Sistem Perbankan. *Jurnal Multidisiplin Ilmu Akademik*, *1*(6), 448–458.

OJK. (2021). *Consultative Paper Manajemen Risiko Keamanan Siber Bank Umum*.

POJK 11/2022. (2022). *Penyelenggaraan Teknologi Informasi Oleh Bank Umum* (p. 33).

R. Edward Freeman, Jeffrey S. Harrison, S. Z. (2018). *Stakeholder Theory*. The British Library.

Rajakulanajagam, R. dan. (2022). Corporate Governance and Corporate Transparency: A Sri Lankan Case. *International Journal of Accountancy*, *2*(2), 1–25.

Sari, L. (2025). Determinan pengungkapan keamanan siber perbankan di indonesia. *Disertasi, Repository Unsri 2025*, 1–28.

Sari, W. F., Saputra, D., Yasmin, Y., Belitung, U. B., & Belitung, B. (2024). Analisis Kinerja Keuangan Bank BUMN dan Bank Swasta Indonesia : Studi Komparatif (Financial Performance Analysis of State-Owned Banks and Private Banks in Indonesia : A Comparative Study). *Studi Ilmu Manajemen Dan Organisasi (SIMO*, *5*(2), 269–283.

Setiawan, R. (2025). Digitalisasi Perbankan dan Ancaman Keamanan Siber : Tantangan dan Strategi Mitigasi Risiko Operasional. *ASEFBA: Advanced Studies in Economic, Finance and Banking*, *1*(1), 73–87.

Suhendar, D. R. H. D. (2021). Pengungkapan Sukarela Berdasarkan Karakteristik Perusahaan dan Kepemilikan Institusional. *Jurnal Akuntansi Berkelanjutan Indonesia*, *4*(1), 16–30.

Sundari, R. (2026). Analisis Perbandingan Teori Keadilan dan Teori Stakeholder dalam Menilai Tanggung Jawab Sosial Syariah Islam. *Scripta Economica: Journal of Economics, Management, and Accounting*, *1*(3), 136–143.

Tri Wahyu, O., & Masiyah, K. (2024). Seberapa Penting Pengungkapan Cybersecurity bagi Nilai Perusahaan? *Jurnal Akuntansi Multiparadigma*, *15*(246), 377–386.