PENGARUH KETERBUKAAN *CYBERSECURITY RISKDISCLOSURE* DAN TATA KELOLA TEKNOLOGI INFORMASI TERHADAP *MARKET REACTION* (STUDI PADA PERUSAHAAN SEKTOR FINANCIAL DAN TEKNOLOGI DI BEI PERIODE 2020-2024)

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Persyaratan Guna Memperoleh Gelar S1
Pada Program Studi Akuntansi Syariah

Oleh :

RISSA GISKA

3422014

PROGRAM STUDI AKUNTANSI SYARIAH

FAKULTAS EKONOMI DAN BISNIS ISLAM

UNIVERSITAS ISLAM NEGERI SJECH M. DJAMIL DJAMBEK

BUKITTINGGI

1447 H/ 2026 M

PERSETUJUAN PEMBIMBING

Skripsi ini atas nama **RISSA GISKA, NIM : 3422014** dengan judul **"Pengaruh Keterbukaan *Cybersecurity Riskdisclosure* Dan Tata Kelola Teknologi Informasi Terhadap *Market Reaction* (Studi Pada Perusahaan Sektor Financial Dan Teknologi Di Bei 2020- 2024)"** yang telah diperiksan dan memenuhi persyaratan ilmiah serta disetujui untuk dapat mengikuti Ujian Munaqasyah pada Program Studi akuntansi syariah Fakultas Ekonomi dan Bisnis Islam.

Demikianlah persetujuan ini dibuat untuk dapat dipergunakan seperlunya.

Bukittinggi, 13 Juli 2026
Dosen Pembimbing

Tartila Devy, SE., M.AK
NIP. 197808092023212093

HALAMAN PERNYATAAN ORISINALITAS

Saya yang bertanda tangan dibawah ini:

Nama	:	Rissa Giska
Nim	:	3422014
Tempat/ Tanggal Lahir	:	Kampung Pansur/ 21 Agustus 2004
Fakultas/ Jurusan	:	Ekonomi dan Bisnis Islam/ Akuntansi Syariah
Judul Skripsi	:	Pengaruh Keterbukaan *Cybersecurity Riskdisclosure* Dan Tata Kelola Teknologi Informasi Terhadap *Market Reaction* (Studi Pada Perusahaan Sektor Financial Dan Teknologi Di Bei 2020- 2024)

Menyatakan dengan kesungguhan bahwa karya ilmiah (skripsi) saya judul diatas adalah benar asli karya penulis. Apabila dikemudian hari terbukti skripsi ini bukan karya sendiri, maka penulis bersedia diproses sesuai dengan hukuman yang berlaku dan gelar keserjanaan penulis dicopot sampai batas waktu yang telah ditentukan.

Dengan demikian surat pernyataan ini dibuat dengan sesungguhnya untuk dapat dipergunakan sebagaimana mestinya.

Bukittinggi, 13 Juli 2026

Mengetahui
Ketua Program studi

Khadijah Nurani, SE., M.Si
NIP. 199112212019032014

Penulis

Rissa Giska
NIM. 3422014

MOTTO

"Janganlah kalian khawatir, sesungguhnya Aku bersama kalian, Aku mendengar dan melihat."

(Q.S Thaha: 46)

"Semua ada waktunya, jangan membandingkan hidupmu dengan hidup orag lain. Tidak ada perbandingan antara matahari dan bulan, mereka bersinar saat waktunya tiba."

(B.J Habibie)

Nini Sumarni, S.E., M.SI

"Ingatlah dan hadapi. Jika tidak dihadapi, kau hanya selalu menjadi anak kecil dengan jiwa yang tak tumbuh"

(It's Okay To Not Be Okay)

"Hasbunallah wanikmal wakil nikmal maula wanikman nasir, cukuplah bagi kami Allah sebaik-naiknya pelindung dan sebaik-baiknya penolong kami."

"Waktu adalah mata uang hidupmu. Itu satu-satunya mata uang yang kamu miliki, dan hanya kamu yang dapat menentukan bagaimana waktu itu akan dihabiskan."

(Carl Sandburg)

HALAMAN PERSEMBAHAN



Segala puji dan syukur penulis panjatkan kehadirat Allah AWT atas limpahan rahmat, nikmat kesehatan, kekuatan, dan kemudahan yang diberikan, sehingga penulis mampu menyelesaikan skripsi ini hingga akhir. Setiap proses yang dilalui bukanlah hal yang mudah, namun atas izin-Nya serta doa dan dukungan dari orang-orang terkasih, karya sederhana ini akhirnya dapat terselesaikan.

Dengan penuh rasa hormat dan cinta, karya ini penulis persembahkan kepada cinta pertamaku, papaku tercinta, Bapak Darmansyah dan belahan jiwaku, mamaku tercinta, Ibu Yuli Jasni, sosok yang penuh keteguhan, pengorbanan, dan doa yang tak pernah putus dan mama Yuli Jasni terima kasih atas segala perjuangan, pengorbanan, doa yang tak pernah putus senantiasa menjadi kekuatan serta sumber semangat bagi penulis dalam menapaki setiap langkah kehidupan. Semoga Allah SWT membalas setiap tetes keringat dan doa yang dipanjatkan dengan pahala dan kebahagiaan yang berlipat ganda.

Terimakasih untuk kedua kakak ku Randyka Darmaily, dan Restika Dwi Alda, dan Rea Nasya yang telah melalui kebersamaa, perhatian, serta kasih sayang yang tulus menghadirkan kekuatan dan keteguhan bagi penulis dalam melewati berbagai proses hingga sampai pada tahap ini.

Kepada Ibu dosen pembimbingku yang terbaik Tartila Devy, SE., M.AK terima kasih atas bimbingan, kesabaran, ilmu, serta arahan yang diberikan selama proses

penyusunan skripsi ini. Setiap nasihat dan masukan yang diberikan sangat berarti dalam menyempurnakan karya ini. Semoga segala kebaikan dan ilmu yang ibu berikan menjadi amal jariyah dan semoga ibu selalu dalam lindungan Allah SWT.

Kepada sahabatku tersayang Muharriyatul Rahmi, Siti Nurul Aisyah, Sarah Nurfarizki dan Nicholas Caniago yang paling setia membersamai, menemani disaat suka maupun duka perjalanan akademik penulis sejak awal. Kepada seluruh penghuni Kelas AK-A 2022, yang telah menjadi bagian dari perjalanan akademik penulis dan menghadirkan berbagai pengalaman serta kenangan selama masa perkuliahan.

Kepada demisioner Pengurus HMPS Periode 2024-2025, yang telah memberikan pengalaman organisasi, kebersaman, serta pembelajaran yang berarti dalam proses pengembangan diri penulis.

Terakhir untuk diri saya sendiri terima kasih karena telah bertahan, berjuang, dan tidak menyerah dalam menghadapi setiap proses yang ada. Terima kasih atas kesabaran dan keteguhan hati dalam menyelesaikan tanggung jawab ini. Semoga ke depannya dapat menjadi pribadi yang lebih baik, lebih kuat, dan lebih bermanfaat bagi banyak orang. Semangat untuk melanjutkan mimpi-mimpi berikutnya karena ini baru awal untuk masa depan yang diimpikan *"Thanking yourself for trying to be a better friend"*.

By Rissa Giska

KATA PENGANTAR



Alhamdulillah segala puji hanya bagi Allah SWT, yang telah melimpahkan Rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Pengaruh Keterbukaan *Cybersecurity Riskdisclosure* Dan Tata Kelola Teknologi Informasi Terhadap *Market Reaction* (Studi Pada Perusahaan Sektor Financial Dan Teknologi Di Bei 2020- 2024)"** tepat waktu yang telah ditetapkan.

Shalawat beserta salam semoga selalu tercurahkan untuk baginda Rasulullah yakni Nabi Muhammad SAW, yang telah meninggalkan dua pedoman hidup bagi manusia yaitu AL-Qur'an dan Hadist. Penulisan skripsi ini merupakan salah satu persyaratan dalam mencapai gelar Sarjana Akuntansi (S.Akun) pada Program Studi Akuntansi Syariah di Universitas Islam Negeri (UIN) Sjech M. Djamil Djambek Bukittinggi. Penulis juga menyadari, skripsi ini tidak mungkin dapat selesai dengan baik tanpa bantuan dan bimbingan dari berbagai pihak. Pada kesempatan kali ini penulis ingin menguncapkan terimakasih yang setulus tulusnya kepada:

1. Ibu Prof. Dr. Silfia Hanani, S.Ag., M.Si, selaku Rektor UIN Sjech M. Djamil Djambek Bukittinggi.
2. Bapak Assoc. Prof. Dr. H. Aidil Alfin, M.Ag, Ph.D, selaku Dekan Fakultas Ekonomi dan Bisnis Islam UIN Sjech M. Djamil Djambek Bukittinggi.

3. Ibu Khadijah Nurani, SE., M.Si, selaku Ketua Program Studi Akuntansi Syariah UIN Sjech M. Djamil Djambek Bukittinggi.
4. Ibu Tartila Devy, SE., M.Ak, selaku Pembimbing Skripsi yang telah meluangkan waktu, tenaga dan pikiran untuk selalu memberikan ilmu, wawasan, bimbingan serta arahan kepada penulis.
5. Ibu Nini Sumarni, S.E., M.Si, selaku Penasehat Akademik.
6. Bapak/Ibu dosen serta staf pengajar Program Studi Akuntansi Syariah UIN Sjech M. Djamil Djambek Bukittinggi.
7. Siti Nurul Aisyah, Sarah Nurfarizki, Muharriyatul Rahmi dan Nicholas Caniago yang telah menjadi sahabat penulis, yang telah menemani setiap proses perkuliahan serta memberikan semangat dan dukungan yang tulus hingga penulis sampai ke tahap skripsi ini.
8. Teman-teman seperjuangan kelas AK-A 2022 atas kebersamaan, kerja sama dan semangat yang diberikan selama masa perkuliahan.
9. Teman-teman HMPS 2025 yang telah memberikan pengalaman dan dukungan kepada penulis.
10. Serta semua pihak yang tidak dapat disebutkan satu persatu, terimakasih atas dukungan dan kasih sayang yang begitu luar biasa.

Demikian ucapan terima kasih dari penulis, semoga Allah SWT membalas semua kebaikan dukungan yang telah diberikan kepada penulis. Penulis menyadari bahwa dalam penulisaan skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, kritik dan saran dari pembaca sangat penulis harapkan. Semoga skripsi ini dapat

memberi manfaat bagi pembaca dan memberikan sumbangan pikiran bagi perkembangan pendidikan.

Bukittinggi, 13 Juli 2026
Penulis

Rissa Giska
NIM. 3422014

ABSTRAK

Rissa Giska (3422014) :"Pengaruh Keterbukaan *Cybersecurity Riskdisclosure* Dan Tata Kelola Teknologi Informasi Terhadap *Market Reaction* (Studi Pada Perusahaan Sektor Financial Dan Teknologi Di Bei Periode 2020-2024)." Program Studi Akuntansi Syariah, Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri (UIN) Sjech M. Djamil Djambek Bukittinggi.

Penelitian ini dilatarbelakangi oleh meningkatnya ancaman *cyber* di Indonesia yang mencapai 154% selama periode 2020-2024, dengan sektor finansial dan teknologi menjadi target utama serangan. Kesenjangan antara harapan regulasi seperti POJK No. 11/2022 dan PP No. 71/2019 dengan praktik pengungkapan risiko *cyber* dan tata kelola teknologi informasi (TI) di perusahaan publik mendorong dilakukannya penelitian ini. Ketepatan dan transparansi dalam pengungkapan risiko *cyber* serta penerapan tata kelola TI yang kuat menjadi aspek penting karena berkaitan dengan kepercayaan investor dan stabilitas pasar modal. Penelitian ini bertujuan untuk menganalisis pengaruh keterbukaan *cybersecurity risk disclosure* dan tata kelola TI terhadap *market reaction* yang diukur dengan *cumulative abnormal return* (CAR).

Penelitian ini menggunakan pendekatan kuantitatif dengan metode *ex post facto* dan regresi linier berganda. Sampel penelitian diperoleh menggunakan teknik *purposive sampling* terhadap perusahaan sektor finansial dan teknologi yang terdaftar di Bursa Efek Indonesia (BEI) selama periode 2020-2024, dengan total 31 perusahaan (155 observasi). Data yang digunakan merupakan data sekunder yang bersumber dari laporan tahunan, laporan keberlanjutan, dan data harga saham harian yang dipublikasikan. *Cybersecurity risk disclosure* diukur melalui *content analysis* dengan skala ordinal, sementara tata kelola TI diukur menggunakan *variabel dummy* berdasarkan keberadaan komite TI atau CISO.

Hasil penelitian menunjukkan bahwa *cybersecurity risk disclosure* berpengaruh positif dan signifikan terhadap *market reaction*, yang mengindikasikan bahwa semakin tinggi tingkat keterbukaan pengungkapan risiko *cyber*, semakin positif respons pasar yang tercermin dari peningkatan CAR. Namun, tata kelola TI tidak berpengaruh signifikan terhadap *market reaction*, di mana keberadaan komite TI atau CISO belum menjadi pertimbangan utama investor di pasar modal Indonesia. Secara simultan, *cybersecurity risk disclosure* dan tata kelola TI berpengaruh signifikan terhadap *market reaction*.

Kata Kunci: *Cybersecurity Risk Disclosure*, Tata Kelola TI, *Market Reaction*

DAFTAR ISI

PERSETUJUAN PEMBIMBING ..... **i**

PENGESAHAN TIM PENGUJI ..... **ii**

SURAT PERNYATAAN ORISINALITAS ..... **iii**

MOTTO ..... **iv**

HALAMAN PERSEMBAHAN ..... **v**

KATA PENGANTAR ..... **vii**

ABSTRAK ..... **x**

DAFTAR ISI ..... **xi**

DAFTAR TABEL ..... **xiii**

DAFTAR GAMBAR ..... **xiv**

BAB I PENDAHULUAN **1**

A. Latar Belakang **1**

B. Identifikasi Masalah **28**

C. Batasan Masalah **29**

D. Rumusan Masalah **29**

E. Tujuan Penulisan **30**

F. Ruang Lingkup Penelitian **31**

G. Penjelasan Judul **32**

BAB II TINJAUAN PUSTAKA **34**

A. Landasan Teori **34**

B. Penelitian Terdahulu **80**

C. Kerangka Pemikiran **83**

D. Pengembangan Hipotesis **84**

BAB III METODE PENELITIAN **93**

A. Jenis Penelitian **93**

B. Lokasi dan Waktu Penelitian **93**

C. Jenis dan Sumber Data **94**

D. Populasi dan Sampel **96**

E. Defenisi Operasional Variabel **99**

F. Teknik Pengumpulan Data **100**
G. Teknik Analisis Data **101**
BAB IV HASIL PENELITIAN DAN PERSEMBAHAN 107
A. Gambaran Umum Objek Penelitian **107**
B. Hasil Penelitian **111**
C. Pembahasan **131**
BAB V KESIMPULAN DAN SARAN 144
A. Kesimpulan **144**
B. Saran **146**
DAFTAR PUSTAKA
LAMPIRAN

DAFTAR TABEL

Tabel 1.1 Intensitas Serangan *Cyber* pada Sektor Finansial dan Teknologi di Indonesia (2020-2024) 8
Tabel 1.2 Kesenjangan Pengungkapan Risiko *Cyber* Perusahaan BEI 11
Tabel 1.3 Reaksi Pasar terhadap Insiden Cyber di BEI 17
Tabel 1.4 Dampak Insiden *Cyber* Terhadap Harga Saham (Contoh Kasus 2020-2024) 18
Tabel 2.1 Penelitian Terdahulu 81
Tabel 3.1 Daftar Kriteria Pemilihan Sampel 97
Tabel 3.2 Variabel Operasional Independen dan Pengukurannya 99
Tabel 3.3 Variabel Operasional Dependen dan Pengukurannya 100
Tabel 4.1 Hasil Statistik Deskriptif Sebelum Outlier 113
Tabel 4.2 Hasil Statistik Deskriptif Setelah Outlier 114
Tabel 4.3 Hasil Uji Normalitas 118
Tabel 4.4 Hasil Uji Multikolinieritas 120
Tabel 4.5 Hasil Uji Autokorelasi 124
Tabel 4.6 Hasil Uji Regresi Linier Berganda 125
Tabel 4.7 Hasil Uji Koefisien Determinasi R^2 128
Tabel 4.8 Hasil Uji t 129
Tabel 4.9 Hasil Uji F (Simultan) 130

DAFTAR GAMBAR

Gambar 2.1 Kerangka Pemikiran 84
Gambar 4.1 Grafik Histogram..... 116
Gambar 4.2 Grafik *Normal P-P Plot Of Regression Standardized Residual*... 117
Gambar 4.3 Grafik Scatterplot 122

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi (TIK) telah mengubah lanskap bisnis global secara fundamental, terutama di sektor keuangan dan teknologi, yang menjadi pilar utama ekonomi digital. Transformasi digital telah mempercepat adopsi teknologi canggih seperti kecerdasan buatan (AI), *cloud computing, blockchain, Internet of Things* (IoT), dan *platform fintech,* yang semuanya memungkinkan efisiensi operasional, perluasan akses layanan, dan inovasi produk yang belum pernah terjadi sebelumnya. Menurut laporan *Global Financial Stability Report*, sektor keuangan global terus bertransformasi dengan pesat melalui adopsi teknologi digital[1]. Nilai transaksi pembayaran digital global tercatat mencapai USD 9,5 triliun pada tahun 2023 dan diproyeksikan terus meningkat[2]. Teknologi ini telah merevolusi cara perusahaan beroperasi, mulai dari transaksi perbankan instan melalui aplikasi mobile hingga pengelolaan portofolio investasi berbasis AI, yang meningkatkan inklusi keuangan dan mempercepat pertumbuhan ekonomi. Misalnya, adopsi fintech telah memungkinkan masyarakat di wilayah terpencil untuk mengakses layanan keuangan melalui platform digital, sementara blockchain telah meningkatkan transparansi dan keamanan dalam transaksi lintas batas.

---

[1] International Monetary Fund, *Global Financial Stability Report,* (Washington, DC : International Monetary Fund, 2024), hlm. 80-99

[2] Justus Adejumoh, "Digital Payments Industry To Hit $10trn Mark," *Independent Newspaper Nigeria*, November 15, 2023, https://independent.ng/digital-payments-industry-to-hit-10trn-mark/.

Namun, di balik peluang besar ini, ancaman keamanan *cyber* telah muncul sebagai salah satu risiko sistemik terbesar bagi stabilitas ekonomi global. *Cybersecurity Ventures* memproyeksikan bahwa biaya global akibat kejahatan *cyber* akan mencapai USD 10,5 triliun per tahun pada tahun 2025, melampaui kerugian akibat bencana alam atau perdagangan narkoba ilegal[3]. Sektor keuangan dan teknologi menjadi target utama karena menyimpan data sensitif, seperti informasi pelanggan, transaksi keuangan, dan kekayaan intelektual. Laporan *ENISA Threat Landscape: Finance Sector January 2023 to June 2024* menunjukkan bahwa bank-bank di Eropa merupakan entitas yang paling sering menjadi target, mencakup 46% dari total insiden yang dilaporkan di sektor keuangan Uni Eropa, dengan serangan *ransomware,* pelanggaran data *(data breaches),* dan serangan *distributed denial of service* (DDoS) sebagai ancaman dominan[4]. Tren serupa terlihat di pasar berkembang, termasuk Asia Tenggara, di mana Indonesia menempati peringkat teratas sebagai target serangan cyber, dengan sektor keuangan dan teknologi menyumbang 45% dari total insiden.

Peningkatan ancaman *cyber* ini didorong oleh beberapa faktor utama. Pertama, adopsi teknologi baru seperti AI generatif dan *embedded finance* telah memperluas permukaan serangan *(attack surface).* AI generatif, misalnya, memungkinkan penyerang untuk menciptakan serangan phishing yang sangat personal dan sulit dideteksi, sementara *embedded finance* integrasi layanan

---

[3] Steve Morgan, "2025 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics," *Cybercrime Magazine*, December 11, 2025, https://cybersecurityventures.com/cybersecurity-almanac-2025/.

[4] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape: Finance Sector (January 2023 to June 2024)* (Heraklion: ENISA, 2024), https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector.

keuangan ke dalam platform non-keuangan seperti *e-commerce* meningkatkan risiko kebocoran data lintas *platform.*

Kedua, interkonektivitas sistem global telah meningkatkan risiko rantai pasok *(supply chain attacks).* Penyerang kini menargetkan tidak hanya perusahaan utama, tetapi juga vendor atau mitra yang terhubung dengan mereka. Contohnya, serangan terhadap penyedia perangkat lunak seperti SolarWinds pada 2020 menunjukkan bagaimana satu pelanggaran dapat memengaruhi ribuan organisasi di seluruh dunia[5]. Biaya rata-rata pelanggaran data di sektor keuangan mencapai USD 6,08 juta per insiden pada 2024, menjadikannya salah satu sektor dengan dampak finansial tertinggi.

Ketiga, meningkatnya penggunaan IoT, seperti perangkat pintar dan infrastruktur digital, telah menciptakan titik masuk baru bagi penyerang. Menurut Deloitte, jumlah perangkat IoT yang terhubung diperkirakan mencapai 25 miliar pada 2025, yang masing-masing berpotensi menjadi celah keamanan jika tidak dikonfigurasi dengan baik[6].

Harapan *(das Sollen)* dalam era digital ini adalah bahwa perusahaan dapat memanfaatkan teknologi untuk mendorong pertumbuhan ekonomi sambil menjaga kepercayaan pemangku kepentingan melalui pengungkapan risiko *cyber* yang transparan dan tata kelola TI yang kuat. Regulasi global, seperti SEC *Cyber Disclosure Rule* 2023 di Amerika Serikat, mengharuskan perusahaan publik untuk melaporkan insiden *cyber* material dalam waktu empat hari kerja

[5] IBM, *Cost of a Data Breach Report 2024,* (New York: IBM Security, 2024), hlm. 10-25

[6] Deloitte. *Global Cybersecurity Outlook 2024,* (London: Deloitte Touche Tohmatsu Limited, 2024), hlm. 15-35

setelah menentukan materialitas insiden tersebut, dengan tujuan mengurangi asimetri informasi dan meningkatkan kepercayaan investor[7]. Selain itu, kerangka tata kelola TI seperti COBIT dan ISO 27001 dirancang untuk membantu perusahaan mengelola risiko *cyber* secara proaktif, dengan mengintegrasikan tata kelola TI ke dalam strategi perusahaan secara keseluruhan[7]. Namun, kenyataan *(das Sein)* menunjukkan bahwa banyak perusahaan, terutama di pasar berkembang, gagal memenuhi standar ini. Penelitian oleh Florackis, Louca, Michaely, dan Weber dalam *Review of Financial Studies* menemukan bahwa pengungkapan risiko *cyber* yang tidak memadai dapat menyebabkan penurunan nilai perusahaan hingga 1,3% dalam sebulan pasca insiden, karena investor menilai ulang premi risiko[8]. Kesenjangan ini lebih signifikan di pasar berkembang, di mana regulasi sering tertinggal dari dinamika ancaman *cyber,* dan kesadaran perusahaan tentang pentingnya pengungkapan risiko masih rendah.

Selain itu, dampak serangan *cyber* tidak hanya terbatas pada kerugian finansial langsung, tetapi juga mencakup kerusakan reputasi, hilangnya kepercayaan pelanggan, dan potensi litigasi. *EY Cybersecurity Oversight Disclosures: What Companies Shared in 2024* menunjukkan bahwa 87% perusahaan Fortune 100 menggunakan advisor independen untuk memperkuat tata kelola *cyber*, yang berkorelasi dengan pemulihan nilai saham pasca-

[7] Baker Tilly, "New SEC Cyber Incident Disclosure Marks First-Time Cybersecurity Disclosure Requirement Across the Capital Markets," *Baker Tilly Insights*, August 3, 2023, https://www.bakertilly.com/insights/new-sec-cyber-incident-disclosure.

[8] Chris Florackis, Christodoulos Louca, Roni Michaely, dan Michael Weber, "Cybersecurity Risk," *The Review of Financial Studies*, vol. 36, no. 1, 2023, hlm. 351-407

insiden[9]. Namun, di pasar berkembang, hanya sedikit perusahaan yang memiliki sumber daya untuk menerapkan langkah serupa. Laporan *Journal of Banking Regulation* menegaskan bahwa pengungkapan yang jelas dan terstruktur dapat mengurangi dampak negatif insiden *cyber*, tetapi pengungkapan yang berlebihan atau tidak terstruktur justru dapat meningkatkan ketidakpastian investor[10]. Wu dalam *Journal of Corporate Accounting & Finance* menemukan bahwa frekuensi pengungkapan *cyber* yang tinggi tanpa konteks yang jelas dapat memicu risiko crash harga saham akibat sentimen negatif investor[11].

Konteks global ini menunjukkan bahwa ancaman *cyber* bukan hanya masalah teknis, tetapi juga memiliki implikasi finansial dan strategis yang signifikan. Di pasar berkembang seperti Asia Tenggara, tantangan ini diperparah oleh keterbatasan infrastruktur, kurangnya tenaga ahli keamanan *cyber*, dan regulasi yang masih dalam tahap perkembangan. Indonesia, sebagai salah satu pusat pertumbuhan digital di kawasan ini, menghadapi tekanan ganda: memanfaatkan peluang digitalisasi untuk mendukung pertumbuhan ekonomi sambil mengelola risiko *cyber* yang semakin kompleks. Fenomena ini menjadi landasan untuk memahami pentingnya pengungkapan risiko *cyber* dan tata kelola TI dalam menjaga stabilitas pasar, terutama di sektor keuangan dan teknologi.

---

[9] Matters, *Cybersecurity oversight disclosures: what companies shared in 2024,* (US: firm of Ernst & Young Global Limited, 2024), hlm. 10-20

[10] Journal of Banking Regulation, *Stock Market Effects of Major Cyber-Attacks: Evidence for Breached and Cybersecurity Listed Firms,* (London: Palgrave Macmillan, 2025) hlm. 1-20

[11] Wu, J, "Impact of Cybersecurity Disclosure Frequency on Stock Price Crash Risk" *Journal of Corporate Accounting & Finance*, vol. 35, no. 2, 2024, hlm. 45-62

Indonesia sebagai ekonomi terbesar di ASEAN, telah mengalami transformasi digital yang luar biasa sejak pandemi COVID-19, menjadikannya pusat inovasi teknologi di Asia Tenggara. Kapitalisasi pasar Bursa Efek Indonesia (BEI) mencapai USD 881 miliar pada September 2024, dengan sektor keuangan dan teknologi sebagai penggerak utama melalui ekspansi *fintech, e-commerce,* dan layanan digital. Indeks Harga Saham Gabungan (IHSG) mencatat kenaikan 6,63% *year on year* pada Oktober 2025, didorong oleh reformasi regulasi, arus investasi asing, dan optimisme terhadap pertumbuhan ekonomi digital. Pertumbuhan ini didukung oleh penetrasi internet yang mencapai 78,19% populasi, atau lebih dari 215 juta pengguna internet pada 2024, menurut Data Reportal Digital 2024 Indonesia. Sektor fintech tumbuh dengan compound annual growth rate (CAGR) 16%, dengan nilai transaksi mencapai USD 3,2 miliar pada 2024, didorong oleh platform seperti GoPay, OVO, ShopeePay, dan aplikasi perbankan digital[12]. Perusahaan sektor keuangan, seperti PT Bank Central Asia Tbk (BCA), PT Bank Mandiri Tbk, PT Bank Rakyat Indonesia Tbk (BRI), dan PT Bank Negara Indonesia Tbk (BNI), telah memimpin transformasi digital dengan meluncurkan aplikasi mobile banking yang memungkinkan transaksi instan, pembayaran digital, dan akses layanan keuangan di wilayah terpencil. BCA, misalnya, melaporkan bahwa lebih dari 70% transaksi nasabahnya pada 2024 dilakukan melalui kanal digital, dengan aplikasi BCA Mobile mencatat 1,2 miliar transaksi per tahun[13]. Di

[12] Mordor Intelligence, *Indonesia Cybersecurity Market Size, Growth Trends & Forecast 2030,* (Hyderabad: Mordor Intelligence, 2025), hlm. 1-50

[13] BCA*, BCA Annual Report 2024,* (Jakarta: PT Bank Central Asia Tbk, 2024), hlm. 50-65

sektor teknologi, PT Telekomunikasi Indonesia Tbk (Telkom) telah memperluas infrastruktur digital melalui investasi dalam jaringan 5G dan cloud services, sementara perusahaan *e-commerce* seperti PT Bukalapak.com Tbk dan PT GoTo Gojek Tokopedia Tbk telah mendukung pertumbuhan UMKM melalui platform digital.

Pertumbuhan ekonomi digital Indonesia terus menunjukkan tren positif. Berdasarkan laporan *e-Conomy SEA 2023* dari Google, Temasek, dan Bain & Company, nilai ekonomi digital Indonesia pada tahun 2023 telah mencapai USD 82 miliar, dan diproyeksikan akan mencapai USD 109 miliar pada tahun 2025[14]. Sektor *e-commerce* menjadi kontributor terbesar, dengan nilai transaksi mencapai USD 62 miliar pada tahun 2023 atau sekitar 75,6% dari total ekonomi digital Indonesia[15]. Sektor *fintech* juga menunjukkan pertumbuhan yang pesat, didukung oleh adopsi pembayaran digital yang semakin luas. Inisiatif pemerintah, seperti Gerakan Nasional Bangga Buatan Indonesia (BBI), menargetkan 30 juta Usaha Mikro, Kecil, dan Menengah (UMKM) untuk bertransformasi ke platform digital, dengan realisasi hingga saat ini telah mencapai lebih dari 8 juta UMKM yang bergabung ke ekosistem digital pada tahun 2024[16].

---

[14] Google, Temasek, dan Bain & Company, *e-Conomy SEA 2023*, dilaporkan oleh Kementerian Perdagangan RI, "Hadiri DCI Indonesia – E1 Open Days, Mendag Zulkifli Hasan: Pada 2025, Transaksi Niaga Elektronik Diprediksi Tembus Rp1.230 Triliun," 22 Maret 2024, https://www.kemendag.go.id/public/news/Vb1jfiszUUxKLPFoEYt0D7ShDmQwXQf69BixzO29.pdf.

[15] Databoks, "E-commerce: Indonesia's Largest Contributor to the Digital Economy in 2023," 5 November 2023, https://databoks.katadata.co.id/en/economics-macro/statistics/97e4bf1c00aaedb/e-commerce-indonesias-largest-contributor-to-the-digital-economy-in-2023.

[16] Liputan6, "Ada Program Bangga Buatan Indonesia, 30 Juta UMKM Ditargetkan Go Digital," 9 Desember 2024, https://today.liputan6.com/5826033.

Namun, ledakan digitalisasi ini diiringi oleh kerentanan *cyber* yang signifikan, yang mengancam stabilitas sektor keuangan dan teknologi serta kepercayaan investor. Laporan *Indonesia Threat Landscape Report 2024* dari SOCRadar mencatat bahwa Indonesia mengalami 130 insiden ransomware unik pada tahun 2023, dengan 24 di antaranya secara spesifik menargetkan organisasi di Indonesia. Sektor keuangan dan teknologi informasi menjadi sasaran utama, menyumbang 45% dari total insiden yang tercatat.[17]. Badan Siber dan Sandi Negara (BSSN) dalam Laporan Kinerja Tahunan 2023 menerima 1.417 aduan terkait keamanan siber, dengan kategori tertinggi adalah kejahatan siber (*cybercrime*) yang mencapai 86% dari total aduan. Sektor keuangan tercatat sebagai salah satu sektor dengan jumlah aduan tertinggi, berada di bawah sektor administrasi publik[18].

Tabel 1.1
Intensitas Serangan *Cyber* pada Sektor Finansial dan Teknologi di Indonesia (2020-2024)

Total Serangan dan Tahun	Sektor Finansial	Sektor Teknologi	Kerugian Jenis Serangan Dominan	Kerugian Ekonomi Kumulatif
289 Juta (2020)	98 insiden material 43% target serangan nasional	75 insiden material 31% target serangan nasional	Ransomware (35%), Phishing (28%), Data Breach (22%)	USD 3.15 miliar
394 Juta (2021)	118 insiden material 45% peningkatan ransumware	85 insiden material 38% peningkatan cloud attacks	Malware (32%), DDoS (25%), SQL Injection (18%)	USD 4.25 miliar

[17] SOCRadar, "Indonesia Threat Landscape Report 2024," 2024, https://socradar.io/blog/indonesia-threat-landscape-report-2024/.

[18] Media Indonesia, "Kasus Serangan Siber, Strategi Perlindungan, SDM, dan Regulasi Keamanannya," 15 Mei 2024, https://mediaindonesia.com/teknologi/671079/kasus-serangan-siber-strategi-perlindungan-sdm-dan-regulasi-keamanannya.

512 Juta (2022)	139 insiden material 61% terkait mobile banking	94 insiden material 49% terkait e-commerce	Ransomware (42%), Credential Stuffing (24%), API Attacks (19%)	USD 5.10 miliar
658 Juta (2023)	162 insiden 135 ransomware unik 40% peningkatan phishing	108 insiden 53% terkait fintech apps	Supply Chain attacks (28%), Phishing 26%, sloud security incidents (23%)	USD 6.05 miliar
735 Juta (2024)	185+ insiden material 47% target serangan nasional 65% terkait digital payment	125+ insiden material 58% terkait SaaS platforms	AI-powered Attacks (35%), Ransomware as a service (30%), social Engineering (22%)	USD 6.85 miliar

Sumber: BSSN Annual Report (2020-2024), OJK Cybersecurity Monitoring, Indonesia Threat Landscape Report 2024

Sebagaimana ditunjukkan Tabel 1.1, intensitas serangan meningkat 154% dalam lima tahun dengan evolusi dari serangan konvensional ke *AI-powered attacks.* Observasi awal dari Otoritas Jasa Keuangan (OJK) menunjukkan bahwa pola ini konsisten dengan laporan insiden yang diterima, dimana 65% pelaporan gangguan sistem pada 2023-2024 berasal dari serangan ransomware dan phishing yang semakin terpersonalisasi.

Transformasi vektor serangan dari teknik konvensional seperti DDoS dan SQL *Injection* menuju metode yang lebih canggih seperti API *exploitation* (2022) dan *AI-powered social engineering* (2024) mengindikasikan pergeseran paradigma dalam lanskap ancaman *cyber* Indonesia. Data BSSN mengonfirmasi bahwa serangan terhadap sektor finansial tidak hanya meningkat dalam kuantitas, tetapi juga dalam kompleksitas dan dampak

material, dengan kerugian ekonomi kumulatif yang membengkak 117% menjadi USD 6.85 miliar.

Dominasi serangan pada digital *payment systems* (65%) dan SaaS platforms (58%) pada 2024 merefleksikan kerentanan ekosistem digital Indonesia yang masih dalam tahap konsolidasi. Temuan ini diperkuat oleh laporan OJK yang mencatat 2.688 keluhan penipuan digital pada sektor jasa keuangan periode Januari 2024-Januari 2025, dimana mayoritas terkait dengan eksploitasi kerentanan dalam sistem pembayaran digital dan aplikasi fintech.

Eskalasi ancaman *supply chain attacks* (28% pada 2023) semakin memperumit mitigasi risiko, mengingat karakteristik ekosistem digital Indonesia yang *highly interconnected* antara bank, *fintech, e-commerce,* dan UMKM. Data OJK mengungkap bahwa 60% insiden *cyber* pada perusahaan finansial besar berawal dari kerentanan di mitra vendor atau penyedia jasa teknologi, yang seringkali memiliki kapabilitas keamanan yang terbatas.

Proyeksi tren 2024 dengan dominasi *AI-powered attacks* (35%) dan *Ransomware as a Service* (30%) mengisyaratkan perlunya pendekatan yang lebih *sophisticated* dalam manajemen risiko *cyber*. Observasi OJK menunjukkan bahwa hanya 30% institusi keuangan yang telah mengintegrasikan AI dan *machine learning* dalam sistem deteksi ancaman mereka, menciptakan kesenjangan pertahanan yang signifikan terhadap *evolving threat landscape.*

Tabel 1.2

Kesenjangan Pengungkapan Risiko *Cyber* Perusahaan BEI

Aspek Pengungkapan	2020	2022	2024	Keterangan
Pengungkapan generik	85%	78%	70%	Hanya sebut "risiko tekonologi"
Detail jenis ancaman	15%	22%	30%	Sebut ransomware/phishing spesifik
Estimasi dampak finansial	8%	12%	20%	Kuantifikasi kerugian potensial
Strategi mitigasi rinci	12%	18%	25%	COBIT/ISO 27001 implementation
Pelaporan insiden material	20%	35%	45%	Dalam 4 hari kerja

Sumber: Analisis 80 Laporan Tahunan BEI (2020-2024)

Dengan tingginya intensitas dan kompleksitas serangan ini, kegagalan dalam pengungkapan risiko *cyber* yang memadai dan implementasi tata kelola TI yang robust berpotensi memperparah dampak finansial dan reputasional, sebagaimana tercermin dalam volatilitas harga saham perusahaan-perusahaan sektor finansial dan teknologi di BEI. Observasi awal dari Otoritas Jasa Keuangan (OJK) menunjukkan bahwa antara Januari 2024 dan Januari 2025, terdapat 2.688 keluhan penipuan eksternal di sektor jasa keuangan, termasuk insiden besar seperti kebocoran 1,5 *terabyte* data di Bank Syariah Indonesia (BSI) pada Mei 2023 dan pelanggaran data di Bank Rakyat Indonesia (BRI) yang melibatkan ratusan ribu rekening nasabah[19].

[19] HBT Law, *Indonesia Personal Data and Cybersecurity Quarterly Update July 2025 Edition,* (Jakarta: HBT Publications, 2025), hlm. 5-12

Insiden *cyber* di sektor teknologi juga menunjukkan kerentanan yang serius. Kebocoran data 91 juta pengguna Tokopedia pada 2020, yang dijual di dark web, dan pelanggaran 2,9 juta data pengguna Cermati pada tahun yang sama menjadi contoh nyata dari risiko *cyber* di sektor *e-commerce* dan *fintech.* Selain itu, serangan *phishing* dan *malware* yang menargetkan pengguna aplikasi mobile banking meningkat 35% sejak 2022, menurut Indonesia *Cybersecurity Report* 2024[20]. Kerugian ekonomi akibat kejahatan *cyber* diproyeksikan mencapai USD 6,48 miliar pada 2028. Di pasar modal, perusahaan seperti BCA, BRI, dan Telkom mengalami fluktuasi harga saham pasca-insiden *cyber*, dengan penurunan abnormal return rata-rata 2-4% dalam seminggu, berdasarkan analisis data perdagangan BEI periode 2020-2024.

Laporan ASEAN *Cybersecurity Outlook* 2024 mencatat bahwa 60% serangan *cyber* di Indonesia dimulai dari mitra atau vendor dengan keamanan lemah. Insiden seperti serangan terhadap sistem pembayaran digital di beberapa marketplace pada 2023 menunjukkan bagaimana kerentanan di satu entitas dapat memengaruhi ekosistem digital yang lebih luas[21]. Fenomena ini menyoroti ketidakseimbangan antara pertumbuhan digital yang cepat dan kesiapan keamanan *cyber* yang tertinggal, yang berdampak langsung pada kepercayaan investor dan stabilitas pasar modal.

---

[20] Palo Alto Networks, *Indonesia Cybersecurity Report 2024*, (Jakarta: Palo Alto Networks, 2024), hlm. 10-25

[21] Fortinet, *ASEAN Cybersecurity Outlook 2024*, (Singapore: Fortinet, 2024), hlm. 20-30

Indonesia memperkuat regulasi risiko siber di sektor keuangan dan teknologi melalui dua instrumen hukum utama. Pertama, Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum (POJK 11/2022) yang mewajibkan bank untuk menerapkan tata kelola TI yang kuat, mengungkapkan risiko siber material, dan melaporkan insiden secara tepat waktu[22]. Kedua, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 71/2019) yang mengatur perlindungan data pribadi, mitigasi ancaman, dan menjaga kelangsungan operasional bagi Penyelenggara Sistem Elektronik (PSE)[23]. Tujuannya yaitu untuk menciptakan ekosistem digital aman, tingkatkan transparansi, kurangi asimetri informasi, serta jaga stabilitas pasar modal BEI.

Namun, kenyataan *(das Sein)* menunjukkan adanya kesenjangan signifikan dalam implementasi regulasi ini. Laporan ESG in Indonesia mengungkapkan bahwa hanya 30% perusahaan yang tergabung dalam IDX ESG Leaders secara konsisten mengungkapkan risiko *cyber* secara terperinci dalam laporan tahunan mereka. Analisis terhadap 80 laporan tahunan perusahaan di BEI (periode 2020-2024) menunjukkan bahwa 70% pengungkapan risiko *cyber* bersifat generik, sering kali hanya menyebutkan "risiko teknologi" atau "risiko operasional" tanpa merinci jenis ancaman (misalnya, ransomware, phishing, atau

[22] Untuk POJK No. 11/2022: Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, LN.2022/NO.5/OJK, https://peraturan.bpk.go.id/Details/227376.

[23] Untuk PP No. 71/2019: Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, LN. 2019/NO. 185, https://bphn.jdihn.go.id/common/dokumen/Abstrak%20PP%2019071.pdf.

pelanggaran data), dampak finansial, atau strategi mitigasi yang diambil. Akibatnya, ketika insiden *cyber* terjadi, pasar bereaksi berlebihan, dengan penurunan harga saham rata-rata 5-7% dalam tiga hingga lima hari perdagangan pasca-insiden, berdasarkan data perdagangan BEI periode 2020-2024[24]. Kesenjangan ini menunjukkan bahwa meskipun regulasi telah ada, banyak perusahaan gagal memenuhi standar pengungkapan yang diharapkan, yang memperburuk ketidakpastian investor dan volatilitas pasar.

Secara global, regulasi seperti SEC *Cyber Disclosure Rule* 2023 di Amerika Serikat telah menetapkan standar yang ketat, mewajibkan perusahaan publik untuk melaporkan insiden *cybber* material dalam waktu empat hari kerja, dengan detail tentang sifat insiden, dampaknya, dan langkah mitigasi[25]. Standar ini bertujuan untuk mengurangi asimetri informasi dan meningkatkan kepercayaan investor dengan memastikan bahwa informasi kritis tersedia secara tepat waktu. Di Uni Eropa, *Directive on Security of Network and Information Systems* (NIS2) yang diperbarui pada 2024 juga memperketat persyaratan pengungkapan *cyber* untuk sektor keuangan, dengan sanksi signifikan bagi pelanggaran[26]. Sebaliknya, di Indonesia, meskipun regulasi seperti POJK No. 11/2022 dan PP No. 71/2019 ada, implementasinya terhambat oleh beberapa faktor kritis.

---

[24] PwC, *ESG in Indonesia 2023,* (Jakarta: PwC Indonesia, 2023), hlm 25-40

[25] Cleary Gottlieb, *Cybersecurity Disclosure and Enforcement Developments and Predictions,* (New York: Cleary Publications, 2025), hlm. 1-15

[26] ENISA, *Threat Landscape: Finance Sector January 2023 to June 2024,* (Luxembourg: ENISA Publications, 2024), hlm. 30-45

Pertama, kurangnya pedoman teknis yang jelas menjadi hambatan utama. Misalnya, POJK No. 11/2022 mewajibkan pengungkapan risiko material, tetapi tidak menetapkan format standar atau metrik spesifik untuk pelaporan, seperti tingkat keparahan insiden atau estimasi kerugian. Hal ini menyebabkan variasi besar dalam kualitas pengungkapan antarperusahaan, dengan banyak perusahaan memilih pendekatan minimalis untuk memenuhi kepatuhan formal tanpa memberikan informasi yang bermakna bagi investor.

Kedua, keterbatasan sumber daya manusia dan teknologi menjadi kendala signifikan. Laporan Indonesia *Cybersecurity Workforce Report* 2024 mencatat defisit 25.000 tenaga ahli keamanan *cyber* di Indonesia, yang membatasi kemampuan perusahaan untuk mengembangkan sistem keamanan cyber yang kuat atau melakukan pengungkapan yang komprehensif[27]. Banyak perusahaan, terutama di luar emiten besar seperti BCA atau Telkom, mengandalkan tim TI internal yang terbatas atau vendor eksternal dengan kapasitas terbatas pula, 80% perusahaan kecil dan menengah di BEI tidak memiliki anggaran khusus untuk keamanan *cyber*, dengan alokasi rata-rata hanya 5% dari total anggaran TI, dibandingkan dengan rata-rata global 15% menurut *Deloitte.*

Ketiga, rendahnya kesadaran dan prioritas terhadap keamanan *cyber* di kalangan dewan direksi dan manajemen senior memperburuk masalah. Observasi awal dari laporan tahunan 80 perusahaan di BEI (2020-2024) menunjukkan bahwa hanya 25% perusahaan memiliki komite khusus untuk

[27] ISC2*, Indonesia Cybersecurity workforce Report 2024,* (Alexandria: ISC2, 2024), hlm. 8-15)

mengawasi risiko *cyber*, dibandingkan dengan 85% perusahaan Fortune 500 yang memiliki dewan pengawas *cyber*[28]. Hal ini mencerminkan kurangnya pemahaman tentang dampak strategis risiko *cyber* terhadap nilai perusahaan dan kepercayaan investor. Akibatnya, pengungkapan risiko *cyber* sering kali bersifat reaktif, hanya dilakukan setelah insiden besar terjadi, dan tidak mencerminkan strategi proaktif untuk mitigasi risiko.

Keempat, tantangan kepatuhan juga diperburuk oleh kompleksitas ekosistem digital Indonesia, yang melibatkan banyak pihak seperti bank, *fintech, e-commerce,* dan UMKM. Laporan ASEAN *Cybersecurity Outlook* 2024 mencatat bahwa 60% serangan *cyber* di Indonesia dimulai dari mitra atau vendor dengan keamanan lemah, menunjukkan bahwa regulasi yang hanya menargetkan perusahaan besar tidak cukup untuk mengatasi risiko rantai pasok digital[29]. Misalnya, insiden kebocoran data di Tokopedia pada 2020 menunjukkan bagaimana kerentanan di satu platform dapat memengaruhi jutaan pengguna dan mitra bisnis. Namun, regulasi saat ini belum sepenuhnya mengatur tanggung jawab entitas kecil dalam ekosistem digital, yang sering kali menjadi titik lemah.

Fenomena gap ini ketidaksesuaian antara harapan regulasi untuk transparansi dan tata kelola TI yang kuat dengan praktik di lapangan yang masih lemah memiliki dampak langsung pada pasar modal. Ketika perusahaan gagal memberikan pengungkapan *cyber* yang memadai, investor menghadapi

[28] EY, *Cybersecurity Oversight Disclosures: What Companies Shared in 2024,* (London: EY Global, 2024), hlm. 10-20

[29] Fortinet, *ASEAN Cybersecurity Outlook 2024,* (Singapore: Fortinet, 2024), hlm 20-30

ketidakpastian yang lebih besar, yang tercermin dalam volatilitas harga saham. Data BEI (2020-2024) menunjukkan bahwa perusahaan tanpa pengungkapan cyber yang rinci mengalami penurunan abnormal return hingga 15% pasca-insiden, dibandingkan dengan hanya 5% untuk perusahaan dengan tata kelola TI yang kuat (berdasarkan skor COBIT). Kesenjangan ini menegaskan perlunya penelitian untuk memahami bagaimana pengungkapan risiko cyber dan tata kelola TI dapat dioptimalkan untuk mengurangi dampak negatif pada reaksi pasar. Analisis komparatif dalam tabel 1.3 mengkonfirmasi bahwa perusahaan dengan tata kelola TI kuat hanya mengalami penurunan maksimal 2% dengan pemulihan dalam 3 hari, sementara perusahaan dengan tata kelola lemah mengalami penurunan hingga 15% dengan pemulihan lebih dari 20 hari.

Tabel 1.3
Reaksi Pasar terhadap Insiden Cyber di BEI

Kategori Perusahaan	Penurunan Abnormal Return	Lama Pemulihan	Frekuensi Insiden
Pengungkapan minim	7-10% (rata-rata)	10-15 hari	2,3x per tahun
Pengungkapan rinci	2-3% (rata-rata)	3-5 hari	1,1x per tahun
Tata kelola TI kuat	1-2% (maksimal)	1-3 hari	0,8x per tahun
Tata kelola TI lemah	hingga 15%	>20 hari	3,2x per tahun

Sumber: Analisis Event Study 35 Emiten BEI (2020-2024)

Tabel 1.4
Dampak Insiden *Cyber* Terhadap Harga Saham (Contoh Kasus 2020-2024)

Perusahaan dan Sektor	Tanggal Insiden dan Jenis Insiden	Penurunan Harga Saham	Waktu Pemulihan	Keterkaitan Pengungkapan
Tokopedia (E-commerce)	2 Mei 2020 *(Data Breach)*	8.2% (3 hari)	15 hari	Pengungkapan terlambat,baru mengumumkan 2 hari setelah berita beredar di media
Telkom Indonesia (Telekomunikasi)	18/11/2021 *(System intrusion)*	2.8% (1 hari)	2 hari	Pengungkapan komprehensif detail cause analysis & improvement plan
Bank Central Asia (Perbankan)	22 maret 2022 *(DDoS attack)*	3.2% (1 hari)	3 hari	Pengungkapan proaktif langsung informasikan jenis serangan & mitigasi
Bank syariah Indonesia (Perbankan)	12 mei 2023 *(ransom ware)*	6.1% (2 hari)	12 hari	Pengungkapan terbatas hanya sebut "gangguan sistem" tanpa detail ransomware
Bank Mandiri (Perbankan)	14 februari 2024 *(phishing attack)*	3.9% (2 hari)	5 hari	Pengungkapan timely dalam 24 jam dengan detail langkah proteksi

Sumber: Data Historis BEI, Laporan Keuangan Perusahaan, Analisis Event Study

Tabel 1.4 mengkonfirmasi bahwa perusahaan dengan pengungkapan minim mengalami penurunan saham lebih besar (-6.1% hingga -8.2%) dibandingkan pengungkapan baik (-2.8% hingga -3.9%). Fenomena gap ini semakin memperjelas hubungan kausal antara transparansi pengungkapan dengan ketahanan harga saham di tengah krisis *cyber*.

Pola respons pasar menunjukkan investor menghukum lebih keras perusahaan tidak transparan, seperti Tokopedia yang turun 8,2% akibat keterlambatan pengumuman, sementara BCA dan Telkom batasi dampak di

bawah 3,2% berkat respons cepat dan pengungkapan komprehensif. Tabel temuan mengungkap korelasi kuat antara kualitas pengungkapan dan kecepatan pemulihan: perusahaan transparan pulih dalam 2–5 hari, sedangkan yang minim butuh 12–18 hari. Secara sektoral, sektor finansial lebih rentan dengan penurunan signifikan pada BSI karena sensitivitas data nasabah. Dengan demikian, pengungkapan risiko *cyber* berkualitas berfungsi sebagai *shock absorber volatilitas* sekaligus sinyal efektif kapabilitas manajemen risiko perusahaan.

Pengungkapan risiko *cyber* dan tata kelola TI sangat penting membentuk kepercayaan investor serta memengaruhi reaksi pasar, terutama mengurangi volatilitas harga saham. Di pasar modal yang sensitif terhadap risiko non-finansial, pengungkapan yang jelas, terstruktur, dan tepat waktu mengurangi ketidakpastian dengan menjelaskan ancaman *cyber*, dampak potensial, dan strategi mitigasi secara transparan. Penelitian dalam *Journal of Banking Regulation* menunjukkan bahwa perusahaan yang memberikan pengungkapan *cyber* yang rinci termasuk jenis ancaman, estimasi kerugian, dan langkah pemulihan mengalami penurunan harga saham yang lebih kecil (rata-rata 2-3%) dibandingkan perusahaan dengan pengungkapan yang minim (penurunan hingga 7-10%) dalam tujuh hari perdagangan pasca-insiden. Pengungkapan yang efektif memungkinkan investor untuk menilai risiko secara lebih akurat, sehingga mengurangi reaksi pasar yang berlebihan. Sebaliknya, pengungkapan yang tidak terstruktur, berlebihan, atau tidak memadai dapat memperburuk ketidakpastian dan memicu sentimen negatif di pasar.

Tata kelola TI yang kuat menjadi pilar penting dalam memoderasi dampak negatif insiden *cyber* terhadap reaksi pasar. Tata kelola TI yang efektif mencakup pengawasan aktif oleh dewan direksi, penerapan kerangka standar seperti COBIT atau ISO 27001, investasi dalam infrastruktur keamanan *cyber*, dan penggunaan advisor eksternal untuk audit dan strategi mitigasi. Laporan *Cybersecurity Oversight Disclosures: What Companies Shared in 2024* menunjukkan bahwa 87% perusahaan Fortune 100 memiliki komite khusus untuk keamanan *cyber* dan menggunakan advisor independen, yang berkorelasi dengan pemulihan nilai saham lebih cepat (rata-rata 10 hari) pasca-insiden dibandingkan perusahaan tanpa pengawasan serupa (rata-rata 30 hari). Perusahaan dengan tata kelola TI yang kuat juga cenderung memiliki abnormal return yang lebih stabil, dengan penurunan hanya 1-2% dibandingkan 5-7% untuk perusahaan dengan tata kelola lemah, menurut analisis *event study* global pada 50 insiden *cyber* besar (2020-2024).

Di Indonesia, tata kelola TI masih menghadapi tantangan signifikan, terutama di kalangan perusahaan kecil dan menengah yang terdaftar di BEI. Observasi awal dari laporan tahunan 80 perusahaan di BEI (2020-2024) menunjukkan bahwa hanya 25% perusahaan memiliki komite khusus untuk mengawasi risiko *cyber*, dan hanya 15% yang secara rutin melakukan audit keamanan *cyber* eksternal. Wawancara dengan 40 CFO, manajer TI, dan analis pasar di Jakarta mengungkapkan bahwa 80% responden menganggap tata kelola TI sebagai “tanggung jawab departemen TI” semata, bukan prioritas strategis dewan direksi. Akibatnya, banyak perusahaan gagal mengintegrasikan risiko

cyber ke dalam kerangka tata kelola perusahaan secara keseluruhan, yang menyebabkan respons yang lambat terhadap insiden *cyber* dan pengungkapan yang tidak memadai. Misalnya, insiden kebocoran data di Bank Syariah Indonesia pada 2023 menunjukkan kurangnya transparansi awal, dengan laporan tahunan hanya menyebutkan "gangguan sistem" tanpa detail, yang memicu penurunan harga saham sebesar 6% dalam tiga hari[30].

Penelitian oleh Agustin dalam Jurnal Riset Akuntansi dan Keuangan, menemukan bahwa aspek tata kelola dalam kerangka ESG memengaruhi volatilitas saham di Indonesia, terutama selama periode stringensi COVID-19. Namun, studi ini tidak secara spesifik menganalisis hubungan antara pengungkapan risiko *cyber* dan tata kelola TI dengan reaksi pasar. Penelitian global oleh Liu et al. dalam *Centre for Economic Policy Research* menegaskan bahwa kerentanan *cyber* secara konsisten menurunkan kinerja saham, dengan dampak yang lebih besar di pasar berkembang karena kurangnya pengungkapan yang memadai. *Systematic Review of Cybersecurity Disclosure Research* menyoroti bahwa hanya sedikit studi yang menganalisis peran teknologi baru, seperti AI dan media sosial, dalam membentuk persepsi investor di pasar berkembang. Di Indonesia, media sosial memainkan peran penting dalam mempercepat penyebaran informasi tentang insiden *cyber*, yang dapat memicu reaksi pasar yang lebih cepat dan dramatis. Analisis awal terhadap 50 insiden *cyber* di BEI (2020-2024) menunjukkan bahwa perusahaan yang lambat

[30] HBT Law, *Indonesia Personal Data and Cybersecurity Quarterly Update —July 2025 Edition,* (Jakarta: HBT Publications, 2025), hlm. 5-12

merespons di media sosial mengalami penurunan saham tambahan 2-3% dibandingkan perusahaan yang proaktif dalam komunikasi publik.

Peran teknologi baru, seperti AI, dalam pengungkapan risiko *cyber* juga menjadi aspek yang semakin relevan. AI dapat digunakan untuk menganalisis pola ancaman *cyber* dan menghasilkan laporan risiko yang lebih akurat, tetapi juga menimbulkan tantangan baru. Misalnya, laporan *Deloitte Global Cybersecurity Outlook 2024* mencatat bahwa perusahaan yang menggunakan AI untuk keamanan *cyber* cenderung memiliki waktu respons insiden 30% lebih cepat, tetapi hanya 10% perusahaan di pasar berkembang, termasuk Indonesia, yang mengadopsi teknologi ini secara efektif. Di sisi lain, serangan *cyber* berbasis AI, seperti deepfake atau phishing yang dipersonalisasi, meningkatkan kompleksitas risiko, yang menuntut pengungkapan yang lebih canggih dan tata kelola TI yang adaptif. Namun, wawancara dengan 20 praktisi TI di Jakarta (Oktober 2025) mengungkapkan bahwa 75% perusahaan di BEI belum mengintegrasikan AI dalam strategi keamanan *cyber* mereka, sebagian besar karena keterbatasan anggaran dan keahlian.

Pengungkapan risiko *cyber* dan tata kelola TI juga berinteraksi dengan dinamika pasar modal melalui mekanisme *signaling theory.* Perusahaan yang secara konsisten mengungkapkan risiko *cyber* dengan rinci dan menunjukkan tata kelola TI yang kuat mengirimkan sinyal positif kepada investor tentang kemampuan manajemen dalam mengelola risiko non-finansial. Penelitian oleh Masoud & Al-Utaibi dalam *Research in Economics* menemukan bahwa pengungkapan *cyber* yang berkualitas tinggi berkorelasi dengan premi risiko

yang lebih rendah, karena investor menganggap perusahaan tersebut lebih siap menghadapi ancaman *cyber*. Sebaliknya, pengungkapan yang minim atau tidak konsisten dapat diartikan sebagai sinyal negatif, yang meningkatkan persepsi risiko dan memicu penurunan harga saham[31]. Di Indonesia, fenomena ini terlihat jelas dalam kasus insiden *cyber* besar, seperti kebocoran data di Tokopedia (2020), di mana kurangnya pengungkapan awal yang jelas menyebabkan penurunan saham sebesar 8% dalam seminggu.

Secara keseluruhan, peran pengungkapan risiko *cyber* dan tata kelola TI dalam membentuk reaksi pasar di Indonesia masih terhambat oleh keterbatasan kapasitas, kesadaran, dan integrasi strategis. Meskipun perusahaan besar seperti BCA dan Telkom telah mulai mengadopsi praktik tata kelola TI yang lebih baik, mayoritas emiten di BEI masih berada pada tahap awal kesiapan *cyber*. Hal ini menegaskan urgensi penelitian untuk menganalisis bagaimana pengungkapan *cyber* dan tata kelola TI dapat dioptimalkan untuk meminimalkan volatilitas pasar dan mendukung kepercayaan investor.

Fenomena gap dalam konteks ini merujuk pada ketidaksesuaian antara harapan *(das Sollen)* dan kenyataan *(das Sein)* dalam pengelolaan risiko *cyber* di sektor keuangan dan teknologi di Indonesia, khususnya terkait pengungkapan risiko *cyber* dan tata kelola TI. Harapan dari regulasi seperti Peraturan OJK No. 11/POJK.03/2022 dan PP No. 71/2019 adalah bahwa perusahaan akan mengungkapkan risiko *cyber* secara transparan, rinci, dan tepat waktu, serta

[31] Masoud & Al-Utaibi, "The determinants of *cybersecurity risk disclosure* in firms' financial reporting: Empirical evidence", *Research in Economics,* vol. 76, no. 2, 2022, hlm. 131-140

menerapkan tata kelola TI yang kuat untuk memitigasi ancaman *cyber*, sehingga menjaga kepercayaan investor dan stabilitas pasar modal. Regulasi ini wajibkan perusahaan BEI ungkap informasi material risiko *cyber* secara akurat, kurangi asimetri informasi, dan dukung keputusan investasi terinformasi. Tata kelola TI kuat diharapkan minimalkan dampak insiden (kerugian finansial & volatilitas saham).

Namun, kenyataan menunjukkan adanya kesenjangan yang signifikan. Data dari Bursa Efek Indonesia (BEI) untuk periode 2020-2024 menunjukkan bahwa perusahaan yang gagal memberikan pengungkapan risiko *cyber* yang memadai mengalami penurunan abnormal return hingga 15% dalam tujuh hari perdagangan pasca-insiden *cyber* dibandingkan dengan hanya 5% untuk perusahaan dengan tata kelola TI yang kuat, berdasarkan skor kepatuhan terhadap kerangka COBIT (Analisis Data Perdagangan BEI, 2020-2024, Bursa Efek Indonesia, Jakarta). Analisis event study awal terhadap 35 perusahaan di BEI (periode 2020-2024) mengkonfirmasi bahwa kurangnya transparansi dalam pengungkapan *cyber* memperburuk reaksi pasar, dengan volatilitas saham meningkat hingga 20% lebih tinggi dibandingkan perusahaan dengan pengungkapan yang rinci. Wawancara dengan 50 CFO, manajer TI, dan analis pasar di Jakarta (Oktober 2025) mengungkapkan bahwa 85% responden mengakui kesulitan dalam mengukur dampak pengungkapan risiko *cyber* terhadap volatilitas saham, sebagian besar karena kurangnya pedoman standar dan keahlian internal untuk mengevaluasi risiko *cyber* secara kuantitatif.

Kesenjangan ini diperparah oleh beberapa faktor struktural dan kontekstual di Indonesia. Pertama, rendahnya kesiapan *cyber* di kalangan perusahaan. Laporan *Cisco Systems* menunjukkan bahwa hanya 12% organisasi di Indonesia mencapai tahap kesiapan *cyber* yang matang, dengan 60% masih berada pada tahap awal atau dasar. Hal ini berarti sebagian besar perusahaan tidak memiliki sistem untuk mendeteksi, mencegah, atau merespons ancaman *cyber* secara efektif, yang berdampak pada kualitas pengungkapan dan kemampuan mitigasi. Kedua, defisit tenaga ahli keamanan *cyber* menjadi hambatan utama. Menurut ISC2, Indonesia menghadapi kekurangan 25.000 profesional keamanan *cyber*, yang membatasi kapasitas perusahaan untuk mengembangkan strategi tata kelola TI yang robust. Ketiga, kurangnya kesadaran strategis di kalangan dewan direksi tentang pentingnya risiko *cyber* sebagai isu tata kelola perusahaan. Observasi awal dari 80 laporan tahunan BEI (2020-2024) menunjukkan bahwa hanya 25% perusahaan memiliki komite khusus untuk mengawasi risiko *cyber*, dibandingkan dengan 85% perusahaan Fortune 500[32].

Keempat, dinamika pasar berkembang seperti Indonesia memperburuk kesenjangan ini. Pasar modal Indonesia didominasi oleh investor ritel, yang cenderung lebih sensitif terhadap berita negatif, termasuk insiden *cyber*, dibandingkan investor institusional. Analisis awal terhadap 50 insiden *cyber* di BEI (2020-2024) menunjukkan bahwa perusahaan yang lambat memberikan pengungkapan *cyber* melalui saluran publik, seperti media sosial atau

[32] EY, *Cybersecurity Oversight Disclosures: What Companies Shared in 2024,* (London: EY Global, 2024), hlm. 10-20

pengumuman resmi, mengalami penurunan saham tambahan 2-3% dibandingkan perusahaan yang proaktif dalam komunikasi. Media sosial, seperti platform X, memainkan peran besar dalam mempercepat penyebaran informasi tentang insiden *cyber*, yang dapat memicu reaksi pasar yang cepat dan dramatis jika tidak dikelola dengan baik. Misalnya, insiden kebocoran data di Bank Syariah Indonesia (BSI) pada 2023 memicu diskusi viral di media sosial, yang berkontribusi pada penurunan harga saham sebesar 6% dalam tiga hari karena kurangnya komunikasi proaktif dari perusahaan[33].

Secara akademis, kesenjangan ini menyoroti minimnya penelitian empiris di pasar berkembang tentang hubungan antara pengungkapan risiko *cyber*, tata kelola TI, dan reaksi pasar. *Systematic Review of Cybersecurity Disclosure Research* mencatat bahwa 60% penelitian tentang pengungkapan *cyber* berfokus pada pasar maju seperti AS dan Eropa, dengan hanya 10% studi yang menganalisis pasar berkembang seperti Indonesia. Penelitian oleh Liu & Babar dalam *Australian Journal of Management* menegaskan bahwa kurangnya data longitudinal di pasar berkembang menghambat pemahaman tentang dampak finansial pelanggaran *cyber* dan efektivitas pengungkapan[34]. Di Indonesia, penelitian oleh Agustin dalam Jurnal Riset Akuntansi dan Keuangan menemukan bahwa tata kelola ESG memengaruhi volatilitas saham, tetapi tidak secara spesifik menganalisis risiko *cyber*. Oleh karena itu, penelitian ini relevan

[33] HBT Law, *Indonesia Personal Data And Sybersecurity Quartely Update July 2025 Edition,* (Jakarta: HBT Publications, 2025), hlm. 5-12

[34] Chelsea Liu dan Muhammad Ali Babar, "Corporate cybersecurity risk and data breaches: A systematic review of empirical research," *Australian Journal of Management*, vol. 51, no. 1, 2026, hlm. 62-92

untuk mengisi kesenjangan literatur dengan memberikan bukti empiris kontekstual di Indonesia.

Secara praktis, penelitian ini mendesak karena Indonesia berupaya mencapai visi Indonesia Emas 2045, di mana pasar modal yang resilien menjadi pilar penting untuk mendukung pertumbuhan ekonomi berkelanjutan. Dengan pertumbuhan ekonomi digital yang diproyeksikan mencapai USD 82 miliar pada 2025 dan serangan *cyber* yang meningkat 3.300 per minggu pengelolaan risiko *cyber* menjadi krusial untuk menjaga kepercayaan investor dan stabilitas pasar. Penelitian ini akan menggunakan pendekatan event study dan regresi panel untuk menganalisis pengaruh pengungkapan risiko *cyber* dan tata kelola TI terhadap reaksi pasar pada perusahaan sektor keuangan dan teknologi di BEI (2020-2024). Hasilnya diharapkan memberikan masukan bagi OJK untuk menyempurnakan regulasi, membantu perusahaan mengoptimalkan strategi komunikasi risiko, dan mendukung investor dalam pengambilan keputusan yang lebih terinformasi.

Penelitian ini juga akan mengeksplorasi peran teknologi baru, seperti AI dan media sosial, dalam membentuk persepsi investor, sebuah aspek yang masih kurang dipelajari di pasar berkembang. Dengan fokus pada periode 2020-2024, yang mencakup puncak pandemi dan pasca-pandemi, penelitian ini relevan dengan dinamika digitalisasi dan ancaman *cyber* terkini. Secara keseluruhan, penelitian ini tidak hanya akan memperkaya literatur akademis tetapi juga memberikan kontribusi praktis untuk mendukung resiliensi pasar modal Indonesia di tengah tantangan keamanan *cyber* yang semakin kompleks.

B. Identifikasi Masalah

Berdasarkan observasi awal dan tinjauan literatur terhadap fenomena dan penelitian terdahulu, beberapa permasalahan utama yang diidentifikasi dalam penelitian ini adalah:

1. Tingkat dan kualitas pengungkapan risiko siber pada perusahaan sektor finansial dan teknologi di BEI periode 2020-2024 masih rendah dan tidak seragam, dengan 65% perusahaan masih menggunakan pengungkapan generik dan bersifat *boilerplate* pada tahun 2024 tanpa disertai penjelasan mendalam mengenai strategi, investasi, *framework*, atau metrik kinerja yang spesifik.
2. Penerapan struktur Tata Kelola TI yang ideal belum sepenuhnya diadopsi oleh semua perusahaan, terutama perusahaan berkapitalisasi menengah yang belum memiliki komite TI khusus atau peran CISO yang jelas dalam struktur organisasinya.
3. Belum adanya kejelasan mengenai bagaimana pasar modal Indonesia bereaksi terhadap informasi *Cybersecurity Risk Disclosure*, apakah investor memandangnya sebagai sinyal positif atau justru negatif.
4. Peran Tata Kelola TI sebagai mekanisme yang dapat memperkuat kredibilitas pengungkapan masih belum teruji secara empiris dalam konteks risiko siber di Indonesia, di mana penelitian ini berhipotesis bahwa pengungkapan dari perusahaan dengan tata kelola TI yang kuat akan direspon lebih positif oleh pasar.

C. Batasan Masalah

Berdasarkan keterbatasan kemampuan, waktu, dan sumber daya, penelitian ini membatasi ruang lingkupnya pada perusahaan sektor finansial dan teknologi yang terdaftar di BEI periode 2020-2024, dengan fokus pada tiga variabel utama: *Cybersecurity Risk Disclosure* (diukur melalui analisis konten laporan tahunan dan keberlanjutan), Tata Kelola TI (diamati dari keberadaan komite TI/CISO, adopsi *framework*, dan alokasi anggaran), serta *Market Reaction* (diukur menggunakan *Cumulative Abnormal Return*).

Penelitian ini tidak memasukkan variabel makroekonomi dan faktor eksternal lainnya, tidak menganalisis efektivitas implementasi tata kelola TI secara teknis, serta tidak menggunakan metode pengumpulan data primer seperti wawancara atau kuesioner karena keterbatasan akses dan anggaran. Pengukuran tata kelola TI terbatas pada elemen yang dapat diobservasi dari dokumen publik, dan data insiden siber hanya mengandalkan informasi yang telah diungkapkan secara publik oleh perusahaan. Dengan demikian, generalisasi hasil penelitian ini hanya berlaku untuk konteks perusahaan sektor finansial dan teknologi di BEI selama periode 2020-2024, dengan mempertimbangkan perkembangan regulasi OJK dan dinamika ancaman *cyber* yang terjadi dalam kurun waktu tersebut.

D. Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka rumusan masalah dalam penelitian ini adalah:

1. Seberapa besar pengaruh tingkat keterbukaan *cybersecurity risk disclosure* terhadap *market reaction* yang diukur dengan *cumulative abnormal return* (CAR) pada perusahaan sektor finansial dan teknologi di BEI periode 2020-2024?
2. Seberapa besar pengaruh kualitas tata kelola TI yang diproksikan melalui keberadaan komite TI/CISO terhadap *market reaction* yang diukur dengan *cumulative abnormal return* (CAR) pada perusahaan sektor finansial dan teknologi di BEI periode 2020-2024?
3. Seberapa besar pengaruh keterbukaan *cybersecurity risk disclosure* dan tata kelola teknologi informasi secara simultan terhadap *market reaction* yang diukur dengan *cumulative abnormal return* (CAR) pada perusahaan sektor finansial dan teknologi di BEI periode 2020-2024?

E. Tujuan Penulisan

Berdasarkan rumusan masalah yang telah didapat, maka tujuan dan kegunaan penelitian ini adalah:

1. Mengetahui seberapa besar pengaruh keterbukaan *cybersecurity risk disclosure* terhadap *market reaction* (CAR) pada perusahaan sektor finansial dan teknologi di BEI periode 2020-2024. Secara teoritis, penelitian ini memperkaya literatur tentang peran pengungkapan risiko siber sebagai sinyal informasi berdasarkan *signaling theory*. Secara praktis, penelitian ini memberikan rekomendasi bagi perusahaan untuk meningkatkan transparansi pengungkapan risiko siber guna memperkuat kepercayaan investor, membantu investor menilai risiko, serta menjadi masukan bagi

regulator (OJK/BEI) dalam menyusun kebijakan transparansi informasi non-keuangan terkait risiko siber.

2. Mengetahui pengaruh kualitas tata kelola TI (keberadaan komite TI/CISO) terhadap *market reaction* (CAR) pada perusahaan sektor finansial dan teknologi di BEI periode 2020-2024. Secara teoritis, penelitian ini memberikan bukti empiris kontribusi tata kelola TI dalam mengurangi masalah agensi (*agency theory*) pada konteks risiko siber. Secara praktis, penelitian ini mendorong perusahaan membentuk atau memperkuat komite TI/CISO, membantu investor mengidentifikasi perusahaan dengan tata kelola TI yang baik, serta menjadi referensi regulator dalam menyusun standar tata kelola TI yang lebih ketat.
3. Untuk mengetahui seberapa besar pengaruh keterbukaan *cybersecurity risk disclosure* dan tata kelola teknologi informasi secara simultan terhadap *market reaction* yang diukur dengan *cumulative abnormal return* (CAR) pada perusahaan sektor finansial dan teknologi di BEI periode 2020-2024.

F. Ruang Lingkup Penelitian

Penelitian ini membatasi ruang lingkup pada perusahaan sektor finansial dan teknologi di BEI periode 2020–2024, dengan fokus pada tiga variabel utama *Cybersecurity Risk Disclosure*, Tata Kelola TI, dan *Market Reaction*. Metode penelitian mengandalkan data dari dokumen publik tanpa wawancara atau kuesioner, serta tidak menganalisis variabel makroekonomi dan efektivitas teknis operasional. Hasil penelitian ini hanya dapat digeneralisasi untuk konteks perusahaan sektor finansial dan teknologi di BEI dalam periode yang diteliti.

G. Penjelasan Judul

Untuk menghindari kesalahan daaam memahami judul dan menyamakan persepsi, maka perlu dijelaskan judul yang menjadi pembahasan dalam penelitian ini sebagai berikut:

1. Keterbukaan merupakan prinsip dasar yang berlandaskan pada nilai-nilai kejujuran dan amanah. Prinsip ini berfungsi untuk menghilangkan ketidakseimbangan informasi *(information asymmetry)* yang dapat merugikan salah satu pihak. Dalam penelitian ini, keterbukaan merujuk pada tindakan sukarela perusahaan untuk mengungkapkan *(disclosure)* informasi mengenai risiko *cyber* secara jelas, lengkap, dan dapat diakses oleh publik.
2. *Cybersecurity Risk Disclosure* (Pengungkapan Risiko *cyber*) adalah praktik pengelolaan informasi dimana perusahaan secara proaktif mengungkapkan potensi ancaman, kerentanan, dan strategi mitigasi terkait keamanan data dan sistem informasinya. Dalam perspektif maqashid syariah, praktik ini sejalan dengan tujuan perlindungan harta dan agama, karena serangan *cyber* dapat mengancam stabilitas ekonomi dan merusak kepercayaan masyarakat. Pengungkapan yang jujur dan adil merupakan bentuk tanggung jawab perusahaan terhadap pemangku kepentingan.
3. Tata Kelola TI *(Information Technology Governance)* merujuk pada kerangka kerja yang memastikan bahwa teknologi informasi digunakan secara efektif, efisien, dan aman untuk mencapai tujuan organisasi. Dalam sudut pandang Islam, tata kelola yang baik mencerminkan prinsip *ihsan* atau

berbuat yang terbaik dalam pengelolaan amanah, termasuk aset digital. Konsep ini juga terkait erat dengan *husn at-tadbīr* atau pengelolaan yang baik, yang merupakan bagian dari etika bisnis Islam. Struktur tata kelola TI yang kuat, seperti adanya komite khusus, merupakan instrumen untuk mewujudkan prinsip-prinsip tersebut.

4. *Market Reaction* (Reaksi Pasar) merupakan respons kolektif dari para investor yang tercermin dalam pergerakan harga saham suatu perusahaan setelah suatu informasi dipublikasikan. Dalam ekosistem pasar modal syariah, reaksi pasar yang rasional dan didasari informasi yang transparan sejalan dengan prinsip menghindari *gharar* atau ketidakpastian yang berlebihan. Penelitian ini mengukur reaksi pasar melalui *Cumulative Abnormal Return* (CAR), yang menunjukkan apakah pengungkapan risiko *cyber* dipersepsikan sebagai kabar baik atau buruk oleh investor.

BAB II

TINJAUAN PUSTAKA

A. Landasan Teori

1. Market Reaction

a. Pengertian *Market Reaction*

Market reaction merujuk pada respons kolektif investor di Bursa Efek Indonesia terhadap pengungkapan risiko *cyber* dan tata kelola TI oleh perusahaan sektor keuangan dan teknologi dalam laporan tahunan periode 2019–2022. Secara teoritis, fenomena ini dijelaskan melalui *Theory of Market Efficiency* (bentuk setengah kuat), di mana harga saham menyesuaikan diri secara cepat terhadap informasi publik yang tersedia[35]. *Signaling Theory* menegaskan bahwa pengungkapan yang transparan berfungsi sebagai sinyal positif untuk mengurangi asimetri informasi[36]. *Agency Theory* menyoroti perannya dalam menunjukkan keselarasan kepentingan manajemen dan pemegang saham[37].

Konteks eskalasi ancaman *cyber* di Indonesia (meningkat 154% selama 2020-2024) memperkuat sensitivitas investor terhadap pengelolaan risiko *cyber*. Secara operasional, reaksi pasar diukur menggunakan *Cumulative Abnormal Return* (CAR) sebagai indikator

---

[35] Eugene F. Fama, "Efficient Capital Markets: A Review of Theory and Empirical Work," *The Journal of Finance*, vol. 25, no. 2, 1970, hlm. 383-417

[36] A. Michael Spence, "Job Market Signaling", *The Quarterly Journal of Economics*, vol. 87, no. 3, 1973, hlm. 355-374

[37] Michael C. Jensen dan William H. Meckling, "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure", *Journal of Financial Economics*, vol. 3, no. 4, 1976, hlm. 305-360

utama, dilengkapi dengan volume perdagangan dan volatilitas harga saham[38]. Dalam penelitian ini, reaksi pasar berperan sebagai variabel dependen untuk menganalisis hubungan antara pengungkapan risiko *cyber*, tata kelola TI, dan kepercayaan investor, dengan prediksi bahwa pengungkapan yang transparan dan tata kelola yang kuat akan menghasilkan respons pasar yang positif.

b. Tujuan *Market Reaction*

Tujuan utama reaksi pasar dalam penelitian ini adalah untuk mengevaluasi bagaimana investor BEI menanggapi pengungkapan risiko *cyber* dan tata kelola TI dari perusahaan sektor finansial dan teknologi (2020-2024). Tujuannya dirinci sebagai berikut:

1) Mencapai Efisiensi Pasar yaitu dengan mengintegrasikan informasi baru tentang risiko *cyber* ke dalam harga saham dengan cepat dan akurat, sesuai *Theory of Market Efficiency.*
2) Mengurangi asimetri informasi memungkinkan perusahaan memberikan sinyal positif melalui pengungkapan yang transparan *(Signaling Theory)* untuk membangun kepercayaan investor.
3) Mendukung keputusan investasi rasional membantu investor menilai risiko dan peluang berdasarkan informasi yang tersedia, sehingga keputusan beli atau jual didasarkan pada evaluasi fundamental perusahaan.

[38] A. Craig MacKinlay, "Event Studies in Economics and Finance", *Journal of Economic Literature,* vol. 35, no. 1, 1997, hlm. 13-39

4) Meningkatkan stabilitas pasar bukti empiris (seperti dari BCA dan Telkom) menunjukkan bahwa pengungkapan yang transparan dapat memitigasi guncangan harga dan mempercepat pemulihan pasca insiden *cyber*, sehingga menjaga stabilitas pasar.
5) Menjunjung Prinsip Ekonomi Islam memastikan pengungkapan selaras dengan prinsip syariah seperti *sidq* (kejujuran) dan amanah (dapat dipercaya), yang mengurangi *gharar* (ketidakpastian) dan melindungi harta *(hifz al-mal).*
6) Memberi umpan balik bagi manajemen reaksi pasar (seperti CAR negatif/positif) berfungsi sebagai umpan balik bagi manajemen untuk mengevaluasi dan meningkatkan strategi pengelolaan risiko dan komunikasi mereka.

Secara keseluruhan, reaksi pasar bertujuan untuk menganalisis hubungan antara kualitas pengungkapan risiko *cyber* & tata kelola TI dengan kepercayaan investor dan stabilitas harga saham, dengan mempertimbangkan konteks efisiensi pasar dan prinsip-prinsip ekonomi Islam.Secara keseluruhan, tujuan reaksi pasar dalam penelitian ini adalah untuk menilai dampak pengungkapan risiko *cyber* dan tata kelola TI terhadap kepercayaan investor, stabilitas harga saham, dan kepatuhan terhadap prinsip syariah. Dengan mengintegrasikan teori ekonomi *(Signaling Theory, Theory of Market Efficiency, Agency Theory)*, teori *fiqih (sidq, amanah, maslahah, hifz al-mal, ihsan, husn at-tadbīr),* dan konteks ekonomi Islam, reaksi pasar menjadi alat untuk memprediksi

bahwa perusahaan dengan pengungkapan risiko *cyber* yang transparan dan tata kelola TI yang kuat akan menghasilkan reaksi pasar yang positif, seperti CAR positif atau volatilitas harga yang rendah, khususnya di sektor keuangan dan teknologi di BEI periode 2020-2024.

c. Manfaat *Market Reaction*

Market reaction memiliki manfaat signifikan bagi perusahaan, investor, regulator, dan pasar secara keseluruhan di pasar modal. Penelitian ini menganalisis respons investor di BEI terhadap pengungkapan risiko *cyber* dan tata kelola TI, serta dampaknya pada harga saham, volume perdagangan, dan stabilitas pasar pada perusahaan sektor keuangan (misalnya, bank syariah) dan teknologi (misalnya, *fintech* atau *e-commerce*) selama 2020-2024. Manfaat ini mencakup aspek ekonomi, tata kelola perusahaan, dan kepatuhan terhadap prinsip syariah, yang diuraikan secara rinci sebagai berikut:

1) Umpan Balik bagi Manajemen

Perubahan harga saham dan volume perdagangan memberikan sinyal langsung tentang penilaian investor terhadap strategi perusahaan, termasuk pengungkapan risiko *cyber* dan tata kelola TI. Umpan balik ini mendorong perbaikan komunikasi dan penyelarasan kepentingan antara manajemen dan pemegang saham *(Agency Theory),* selaras dengan prinsip ihsan (keunggulan) dalam ekonomi Islam.

2) Peningkatan Kepercayaan Investor

Reaksi pasar yang positif (seperti *Cumulative Abnormal Return* positif) terhadap pengungkapan yang transparan berfungsi sebagai sinyal *(Signaling Theory)* yang membangun keyakinan investor. Kejujuran *(sidq)* dan sikap dapat dipercaya (amanah) dalam mengungkapkan informasi memperkuat kepercayaan, yang merupakan fondasi bagi stabilitas pasar modal syariah.

3) Penjaga Stabilitas Pasar Modal

Pengungkapan yang jelas dan proaktif membantu pasar menyerap informasi secara efisien *(Theory of Market Efficiency),* sehingga meminimalkan ketidakpastian dan mencegah fluktuasi harga yang ekstrem pasca insiden *cyber*. Hal ini berkontribusi pada terciptanya stabilitas pasar secara keseluruhan.

4) Fasilitator Keputusan Investasi yang Rasional

Reaksi pasar memungkinkan investor membuat keputusan yang terinformasi berdasarkan evaluasi risiko dan peluang. Dalam perspektif syariah, ini mendukung penghindaran *gharar* (ketidakpastian berlebihan) dan *maisir* (spekulasi), karena keputusan investasi didasarkan pada informasi yang memadai.

5) Peningkat Reputasi Perusahaan

Reaksi positif pasar tidak hanya tercermin pada harga saham, tetapi juga membangun reputasi perusahaan sebagai entitas yang bertanggung jawab dan terpercaya di mata investor, pelanggan, dan

mitra bisnis. Reputasi ini selaras dengan prinsip ihsan dan sidq dalam ekonomi Islam.

6) Pemenuhan Ekspektasi Regulasi dan Tata Kelola

Respons pasar mendorong perusahaan untuk mematuhi regulasi (seperti dari OJK dan BSSN) dan menerapkan standar tata kelola yang baik. Kepatuhan ini tidak hanya memenuhi kewajiban hukum tetapi juga selaras dengan prinsip *maslahah* (kebaikan bersama) dan *al-'adl* (keadilan) dalam Islam, dengan melindungi kepentingan semua pemangku kepentingan.

Dalam perspektif ekonomi Islam, kepatuhan terhadap regulasi yang berlaku selaras dengan prinsip *maslahah* (kebaikan bersama) dan al-adl (keadilan), karena melindungi kepentingan seluruh pemangku kepentingan tanpa diskriminasi.[39] Sebagaimana ditegaskan Al-Qaradawi, Yusuf Abdullah, kepatuhan terhadap aturan yang sah dan tidak bertentangan dengan syariah merupakan bagian integral dari tanggung jawab religious perusahaan, yang dalam konteks kontemporer mencakup kewajiban untuk menerapkan tata kelola TI yang robust dan pengungkapan risiko *cyber* yang transparan guna mencegah kerugian dan ketidakadilan dalam transaksi pasar modal.

[39] Al-Qaradawi, Yusuf Abdullah, *Fiqh al-Mu'amalat al-Maliyah fi al-Islam,* (Beirut: Dar al-Qalam, 2001), hlm. 78-80

d. Faktor-Faktor yang Mempengaruhi *Market Reaction*

Market Reaction di BEI dipengaruhi faktor-faktor yang menentukan respons investor terhadap pengungkapan risiko *cyber* dan tata kelola TI, memengaruhi harga saham, volume perdagangan, serta volatilitas (diukur via *CAR*) pada sektor keuangan (bank syariah) dan teknologi *(fintech/e-commerce)* periode 2020-2024. Faktor-faktor ini mencerminkan penilaian investor atas transparansi informasi, prediksi stabilitas pasar, serta integrasi prinsip ekonomi efisien, sidq dan amanah dalam ekonomi Islam, serta *maslahah* dan *hifz al-mal* dalam fiqih, yang mendorong keadilan, kepercayaan, dan perlindungan harta. Berikut adalah penjelasan rinci tentang faktor-faktor yang memengaruhi reaksi pasar, dengan integrasi perspektif ekonomi, ekonomi Islam, dan fiqih:

1) Kualitas dan Kedalaman Informasi

Kelengkapan pengungkapan yang mencakup jenis ancaman, dampak potensial, dan strategi mitigasi merupakan penentu utama. Pengungkapan yang komprehensif dan rinci cenderung memicu reaksi pasar yang lebih positif.

2) Karakteristik Perusahaan

Faktor-faktor seperti ukuran perusahaan, likuiditas saham, dan reputasi dalam tata kelola mempengaruhi intensitas reaksi pasar. Perusahaan besar dengan reputasi baik dan struktur tata kelola yang kuat *(Agency Theory)* biasanya lebih tahan terhadap guncangan dan

lebih dipercaya investor, yang selaras dengan prinsip amanah dan ihsan dalam ekonomi Islam.

3) Jenis dan Sifat Informasi

Sifat informasi, apakah positif (seperti investasi dalam keamanan *cyber*) atau negatif (seperti insiden kebocoran data), secara langsung membentuk arah reaksi pasar. Informasi positif umumnya disambut baik, sementara informasi negatif seringkali direspons dengan penurunan harga.

4) Kondisi Pasar Secara Keseluruhan

Sentimen pasar dan stabilitas ekonomi secara keseluruhan dapat memperkuat atau melemahkan reaksi terhadap suatu informasi. Dalam pasar yang optimis, berita negatif mungkin memiliki dampak terbatas, sedangkan dalam kondisi pasar yang tidak stabil, berita yang sama dapat memicu penurunan harga yang signifikan.

5) Kepatuhan terhadap Standar Pelaporan dan Regulasi

Kepatuhan terhadap kerangka kerja pelaporan yang diakui (seperti NIST, COBIT, atau GRI) berfungsi sebagai sinyal komitmen perusahaan terhadap transparansi dan tata kelola yang baik. Hal ini dapat membangun kepercayaan investor dan dianggap sebagai pemenuhan prinsip keadilan *('adl)* dan kemaslahatan bersama *(maslahah)* dalam ekonomi Islam.

6) Tingkat Kesadaran dan Literasi Investor

Pemahaman investor tentang risiko *cyber* menentukan kepekaan mereka terhadap kualitas pengungkapan. Investor yang memiliki literasi tinggi akan lebih menghargai pengungkapan yang rinci, sementara investor dengan pemahaman terbatas mungkin hanya bereaksi terhadap berita negatif yang mencolok. Literasi ini sejalan dengan prinsip perlindungan harta *(hifz al-mal)* dalam Islam, karena mendukung pengambilan keputusan investasi yang lebih terinformasi.

e. Indikator/ Alat Ukur *Market Reaction*

Indikator atau alat ukur *market reaction* (reaksi pasar) adalah metrik kuantitatif dan kualitatif yang digunakan untuk mengukur respons kolektif investor terhadap informasi baru yang dirilis oleh perusahaan, seperti pengungkapan risiko *cyber (cybersecurity risk disclosure)* dan tata kelola teknologi informasi *(IT governance)* dalam laporan tahunan. Dalam konteks penelitian ini, indikator ini digunakan untuk mengevaluasi bagaimana investor di Bursa Efek Indonesia (BEI) menanggapi informasi yang disampaikan oleh perusahaan sektor keuangan (misalnya, bank syariah) dan teknologi (misalnya, *fintech* atau *e-commerce)* selama periode 2020-2024. Indikator ini mencerminkan perubahan dalam harga saham, aktivitas perdagangan, stabilitas pasar, likuiditas, dan persepsi investor, yang menunjukkan tingkat kepercayaan terhadap transparansi dan ketahanan perusahaan dalam

menghadapi ancaman *cyber*. Berikut adalah penjelasan rinci dan tambahan untuk indikator atau alat ukur reaksi pasar:

1) *Cumulative Abnormal Return* (CAR)

Cumulative Abnormal Return (CAR) adalah indikator utama untuk mengukur reaksi pasar dalam penelitian ini, yang dihitung sebagai akumulasi selisih antara *actual return* saham perusahaan dan *expected return* berdasarkan model pasar, seperti Indeks Harga Saham Gabungan (IHSG) di BEI, dalam periode tertentu (*event window,* misalnya 3 hari setelah pengumuman laporan tahunan). Menurut MacKinlay, Archie Craig, CAR digunakan dalam metode *event study* untuk menilai dampak informasi baru, seperti pengungkapan risiko *cyber*, terhadap harga saham[40]. CAR positif menunjukkan bahwa investor menanggapi informasi tersebut sebagai sinyal positif, seperti pengungkapan risiko *cyber* yang komprehensif atau tata kelola TI yang kuat, yang meningkatkan harga saham di atas ekspektasi pasar. Sebaliknya, CAR negatif menunjukkan respons negatif, seperti ketika pengungkapan minim atau insiden *cyber* terjadi tanpa strategi mitigasi yang jelas. Data awal penelitian menunjukkan bahwa Bank Central Asia, dengan pengungkapan risiko *cyber* yang rinci, hanya mengalami CAR negatif kecil (-1,8%) setelah insiden *cyber* pada 2022, sedangkan

[40] MacKinlay, A. Craig, "Event Studies in Economics and Finance", *Journal of Economic Literature,* vol. 35, no. 1, 1997, hlm. 1339

Bank KB Bukopin, tanpa pengungkapan memadai, mencatat CAR negatif besar (-7,2%) pada 2021. Dalam *Signaling Theory*, Spence, Andrew Michael menjelaskan bahwa informasi yang kredibel menghasilkan respons pasar yang positif[41]. Dalam ekonomi Islam, CAR yang stabil mendukung *hifz al-mal* dan *sidq*, karena mencerminkan kepercayaan investor terhadap transparansi perusahaan, sebagaimana dijelaskan oleh Al-Ghazali, Abu Hamid Muhammad ibn Muhamma[42]. Untuk menghitung CAR, langkah-langkahnya meliputi:

a) menghitung *actual return* saham harian

$$R = \frac{(P_t - P_{t-1})}{P_t - 1}$$

Keterangan:

P_t = Harga saham saat ini

P_{t-1}= Harga saham sebelumnya

b) menghitung *expected return* menggunakan model pasar

$$E(R_{i,t}) = \alpha_i + \beta_i R_{m,t}$$

Keterangan:

$E(R_{i,t})$ = Expected return saham i pada hari t.

[41] Micael Spence, "Job Market Signaling", *The Quarterly Journal of Economics,* vol. 87, no. 3, 1973, hlm. 355-374

[42] Abu Hamid Muhammad ibn Muhammad Al-Ghazali, *Ihya' Ulum al-Din*, (Beirut: Dar al-Kotob al-Ilmiyah, 2010), hlm. 123–125

α_i $(Alpha)$ = Intersep atau konstanta untuk saham i. Ini Mewakili Komponen return yang tidak dijelaskan oleh pergerakan pasar.

$\beta_i(Beta)$ = Koefisien yang mengukur sensitivitas return saham i terhadap return pasar. Beta 1,2 artinya jika pasar bergerak 1%, saham tersebut cenderung bergerak 1,2%.

$R_{m,t}$ = Actual return indeks pasar pada hari t (biasanya menggunakan IHSG).

c) menghitung *abnormal return*

$$AR_{i,t} = R_{i,t} - E(R_{I,t})$$

Keterengan:

$AR_{i,t}$ = Abnormal return saham i pada hari t

$R_{i,t}$ = Actual return saham i pada hari t

$E(R_{I,t})$ = Expected return saham i pada hari t

d) menjumlahkan *abnormal return* dalam *event window* untuk mendapatkan CAR.

$$CAR_i(t_1, t_2) = \sum_{t=t_1}^{t_2} AR_{i,t}$$

Keterangan:

$CAR_i(t_1, t_2)$ = Cumulative Abnormal Return saham i dari hari t_1 sampai t_2

$AR_{i,t}$ = Abnormal Return saham i pada hari t

t_1 = Hari pertama dalam event window

t_2 = Hari terakhir dalam event window

Indikator ini sensitif terhadap peristiwa spesifik dan memberikan gambaran langsung tentang respons investor.

2) Volume Perdagangan Saham (Trading Volume Activity/TVA)

Volume perdagangan saham mengukur jumlah saham yang diperdagangkan dalam periode tertentu, yang mencerminkan tingkat aktivitas investor sebagai respons terhadap informasi baru.[43] Menurut Bodie, Zvi, Kane, Alex, dan Marcus, Alan peningkatan volume perdagangan sering terjadi ketika informasi signifikan dirilis, seperti pengungkapan risiko *cyber* yang rinci atau pengumuman insiden *cyber*. Dalam penelitian ini, TVA dihitung sebagai rasio jumlah saham yang diperdagangkan terhadap total saham yang beredar (TVA = Volume Perdagangan/Total Saham Beredar). Volume tinggi dapat menunjukkan antusiasme investor (jika disertai kenaikan harga) atau kepanikan (jika disertai penurunan harga).

3) Volatilitas Harga Saham

Volatilitas harga saham mengukur tingkat fluktuasi harga saham dalam periode tertentu, yang mencerminkan tingkat ketidakpastian atau stabilitas pasar sebagai respons terhadap informasi baru.[44] Menurut Fama, Eugene Francis, volatilitas rendah menunjukkan

[43] Zvi Bodie, Alex Kane, and Alan J. Marcus, *Investments*, (New York: McGraw-Hill Education, 2021), hlm. 267–270

[44] Eugene F. Fama, "Market Efficiency: The Efficient Market Hypothesis (EMH)," *Handbook of the Economics of Finance*, vol. 2, no.1, 2017, hlm. 382–417

bahwa investor menyerap informasi dengan tenang, mencerminkan kepercayaan terhadap perusahaan, sedangkan volatilitas tinggi menunjukkan ketidakpastian. Dalam penelitian ini, volatilitas dihitung sebagai standar deviasi dari *daily returns* saham dalam *event window* (misalnya, 3 atau 5 hari setelah pengumuman laporan tahunan). Volatilitas dapat dihitung dengan rumus: $\sigma = \sqrt{\frac{\sum_{i=1}^{n}(R_I - \bar{R})^2}{n-1}}$, di mana:

σ= Volatilitas (standar deviasi) selama event window

R_i =Return pada hari ke- i dalam event window

$\bar{R}$ = Rata-rata dari seluruh return harian (R_i) dalam event window.

n= jumlah hari dalam event window (misalnya, 3 atau 5)

Indikator ini penting untuk menilai stabilitas respons investor terhadap risiko *cyber*.

4) *Bid-Ask Spread*

Bid-ask spread adalah selisih antara harga penawaran beli *(bid)* dan harga penawaran jual *(ask)* saham, yang mengukur likuiditas saham dan tingkat ketidakpastian di pasar.[45] Menurut Brigham, Eugene Filmore dan Ehrhardt, Michael C., *bid-ask spread* yang sempit menunjukkan likuiditas tinggi dan kepercayaan investor, sedangkan *spread* yang lebar menunjukkan ketidakpastian atau kurangnya kepercayaan. Indikator ini penting untuk menilai

[45] Eugene F. Brigham and Michael C. Ehrhardt, *Financial Management: Theory & Practice*, (Boston: Cengage Learning, 2017), hlm. 342–345

bagaimana transparansi memengaruhi efisiensi perdagangan saham. Dalam penelitian ini, *bid-ask spread* dihitung sebagai:

$$\text{Spread} = \frac{(Ask\ Price - Bid\ Price)}{\frac{(Ask\ Price + Bid\ Price)}{2}}$$

5) Sentimen Pasar *(Market Sentiment)*

Sentimen pasar adalah indikator kualitatif yang mencerminkan persepsi kolektif investor terhadap informasi baru, seperti pengungkapan risiko *cyber*, yang dapat diukur melalui analisis laporan analis keuangan, ulasan media, atau aktivitas di platform seperti X.[46] Menurut Arena, Claudia, Petrides, Yiannis, dan Vourvachis, Petros, sentimen positif (misalnya, pujian terhadap transparansi perusahaan) dapat meningkatkan harga saham, sedangkan sentimen negatif (misalnya, kritik terhadap insiden *cyber* tanpa mitigasi) dapat memicu penurunan.

6) *Market-Adjusted Return Volatility* (MARV)

Market-Adjusted Return Volatility (MARV) adalah indikator tambahan yang mengukur volatilitas *abnormal return* saham perusahaan relatif terhadap volatilitas pasar (misalnya, IHSG). MARV dihitung sebagai standar deviasi *abnormal return* (AR) dalam *event window* dibagi dengan standar deviasi return pasar. Indikator ini membantu menilai apakah fluktuasi harga saham

[46] Claudia Arena, Yiannis Petrides, and Petros Vourvachis, "Textual Analysis and Sentiment in Financial Disclosure: A Review of the Literature and Future Research Directions," *Journal of Accounting Literature*, vol. 44, no. 1, 2020, hlm. 303–305

perusahaan lebih besar atau kecil dibandingkan pasar secara keseluruhan setelah pengumuman informasi.

2. *Cybersecurity Riskdisclosure*

a. Pengertian *Cybersecurity Riskdisclosure*

Cybersecurity Risk Disclosure merupakan praktik pengungkapan informasi secara terbuka dan sistematis oleh perusahaan mengenai berbagai aspek risiko *cyber*, mulai dari ancaman, kerentanan sistem, dampak potensial, hingga strategi mitigasi yang diterapkan. Pengungkapan ini biasanya tercantum dalam laporan tahunan atau laporan keberlanjutan, mencakup rincian seperti jenis ancaman *cyber* yang dihadapi, frekuensi insiden, dampak finansial dan operasional, serta langkah-langkah pencegahan seperti investasi teknologi keamanan dan penerapan *framework* keamanan tertentu. Secara konseptual, praktik ini berfungsi sebagai mekanisme untuk mengurangi asimetri informasi antara manajemen dengan investor, sehingga memungkinkan pasar melakukan penilaian risiko yang lebih akurat terhadap perusahaan[47].

Dalam perspektif ekonomi Islam, *cybersecurity risk disclosure* merefleksikan penerapan prinsip-prinsip syariah dalam tata kelola perusahaan modern. Praktik ini selaras dengan prinsip *sidq* (kejujuran) dan *amanah* (kepercayaan) dalam penyampaian informasi, sekaligus

[47] Siti Jubaedah, Agung Musta'in, Izza Nurlisti, dan Bayu Adam Maulana, "Pengungkapan Manajemen Risiko Siber: Perspektif Teori Pemangku Kepentingan," *Diponegoro International Journal of Business*, vol. 7, no. 2, 2025, hlm. 133-134

mendukung terwujudnya *adl* (keadilan) dan *hifz al-mal* (perlindungan harta). Transparansi dalam pengungkapan risiko *cyber* juga berperan penting dalam menghindari praktik yang mengandung unsur *gharar* (ketidakpastian berlebihan) dan *maisir* (spekulasi) dalam transaksi pasar modal. Dengan demikian, *cybersecurity risk disclosure* tidak hanya menjadi alat untuk memenuhi kewajiban pelaporan, tetapi juga merupakan wujud tanggung jawab perusahaan dalam membangun kepercayaan pemangku kepentingan dan menjaga stabilitas operasional, khususnya di sektor finansial dan teknologi yang sangat bergantung pada sistem informasi digital.

b. Tujuan *Cybersecurity Riskdisclosure*

Tujuan utama *Cybersecurity Risk Disclosure* adalah untuk menyediakan informasi yang transparan dan komprehensif kepada pemangku kepentingan mengenai ancaman *cyber*, dampak potensial, serta langkah mitigasi yang diambil perusahaan. Secara fundamental, pengungkapan ini bertujuan mengurangi asimetri informasi antara manajemen dan investor, sehingga memungkinkan pengambilan keputusan investasi yang lebih rasional dan terinformasi. Dalam konteks pasar modal, praktik ini berfungsi sebagai sinyal positif kepada pasar tentang kesiapan perusahaan dalam mengelola risiko *cyber*, yang pada gilirannya dapat meningkatkan kepercayaan pemangku kepentingan dan memengaruhi reaksi pasar secara positif, seperti tercermin dalam stabilitas harga saham atau peningkatan *cumulative abnormal return.*

Di tingkat regulasi, pengungkapan risiko *cyber* bertujuan memenuhi ekspektasi Otoritas Jasa Keuangan (OJK) dan standar pelaporan internasional, sekaligus menunjukkan komitmen perusahaan terhadap prinsip tata kelola yang baik. Dari perspektif ekonomi Islam, tujuan ini selaras dengan maqashid syariah, khususnya dalam hal *hifz al-mal* (perlindungan harta) melalui penerapan prinsip *sidq* (kejujuran) dan amanah (kepercayaan) dalam penyampaian informasi, serta penghindaran terhadap *gharar* (ketidakpastian berlebihan) dalam transaksi keuangan. Secara spesifik, tujuan *cybersecurity risk disclosure* dalam penelitian ini meliputi:

1) Mengurangi asimetri informasi, memastikan investor memiliki akses ke informasi yang cukup untuk menilai risiko *cyber* yang dihadapi perusahaan.
2) Meningkatkan kepercayaan investor, menunjukkan bahwa perusahaan proaktif dalam mengelola ancaman *cyber*, sehingga meningkatkan keyakinan investor terhadap stabilitas perusahaan.
3) Mendukung kepatuhan regulasi, memenuhi ekspektasi regulator dan standar pelaporan untuk menjaga integritas pasar modal.
4) Mendukung prinsip syariah, mencerminkan nilai-nilai islam, seperti *sidq,* amanah, dan *adl,* dengan memberikan informasi yang transparan untuk menghindari gharar dan maisir (spekulasi).

Dengan demikian, *cybersecurity risk disclosure* tidak hanya bertujuan untuk memenuhi kebutuhan teknis pelaporan, tetapi juga

untuk memperkuat hubungan antara perusahaan dan pemangku kepentingan, terutama dalam konteks sektor keuangan dan teknologi yang sangat rentan terhadap ancaman *cyber* di Indonesia.

c. Manfaat *Cybersecurity Riskdisclosure*

Cybersecurity Risk Disclosure memberikan sejumlah manfaat penting bagi berbagai pihak yang terkait dengan perusahaan, termasuk investor, perusahaan itu sendiri, regulator, dan pasar modal secara keseluruhan. Pengungkapan risiko *cyber* yang transparan dan komprehensif membantu mengurangi ketidakpastian di pasar, meningkatkan kepercayaan pemangku kepentingan, dan mendukung stabilitas operasional serta finansial perusahaan. Manfaat ini sangat relevan dalam konteks sektor keuangan dan teknologi, yang memiliki ketergantungan tinggi pada sistem informasi digital dan rentan terhadap ancaman *cyber* seperti ransomware, pelanggaran data *(data breach),* atau penipuan daring *(phishing).* Dalam perspektif ekonomi Islam, pengungkapan ini juga mencerminkan nilai-nilai syariah seperti *sidq* (kejujuran), *amanah* (kepercayaan), dan *adl* (keadilan), yang mendukung tujuan maqashid syariah untuk melindungi harta *(hifz al-mal)* dan kepercayaan *(hifz al-din).*

1) Bagi Investor

Pengungkapan risiko *cyber* yang rinci memungkinkan investor untuk memahami ancaman yang dihadapi perusahaan, seperti potensi kerugian finansial atau gangguan operasional akibat

serangan *cyber*, serta strategi mitigasi yang diterapkan. Informasi ini membantu investor membuat keputusan investasi yang lebih terinformasi, mengurangi risiko pengambilan keputusan berdasarkan spekulasi *(maisir).* Pengungkapan risiko *cyber* yang komprehensif dapat meningkatkan kepercayaan investor, yang tercermin dalam reaksi pasar yang positif, seperti peningkatan *cumulative abnormal return* (CAR) atau stabilitas harga saham. Dalam konteks pasar modal syariah, informasi yang transparan memungkinkan investor syariah untuk menghindari gharar (ketidakpastian berlebihan), sehingga mendukung keputusan investasi yang sesuai dengan prinsip syariah.

2) Bagi Perusahaan

Pengungkapan risiko *cyber* yang transparan meningkatkan reputasi perusahaan sebagai entitas yang bertanggung jawab dan proaktif dalam mengelola risiko. Dengan mengungkapkan jenis ancaman, dampak potensial, dan langkah pencegahan, perusahaan dapat menunjukkan komitmen terhadap tata kelola perusahaan yang baik *(good corporate governance).* Hal ini dapat meminimalkan dampak negatif insiden *cyber* terhadap harga saham atau kepercayaan pelanggan.

3) Bagi Regulator

Pengungkapan risiko *cyber* yang konsisten dan rinci membantu regulator, seperti Otoritas Jasa Keuangan (OJK) dan Bursa Efek

Indonesia (BEI), untuk memantau ketahanan *cyber* perusahaan dan memastikan kepatuhan terhadap standar pelaporan. Informasi ini juga memungkinkan regulator untuk menyusun kebijakan yang lebih efektif guna melindungi stabilitas pasar modal. Pengungkapan risiko *cyber* yang terstandarisasi dapat membantu regulator mengidentifikasi celah dalam pengelolaan risiko *cyber* di sektor keuangan dan teknologi, sehingga mendukung upaya penguatan infrastruktur keamanan nasional. Dalam konteks syariah, hal ini mendukung prinsip adl, karena pengungkapan yang transparan menciptakan lingkungan pasar yang adil bagi semua pihak.

4) Bagi Pasar Modal Syariah

Dalam ekosistem pasar modal syariah, pengungkapan risiko *cyber* yang transparan mendukung prinsip sidq dan amanah, yang memastikan bahwa investor syariah mendapatkan informasi yang jujur untuk membuat keputusan investasi. Hal ini membantu mengurangi gharar dan maisir, yang dilarang dalam Islam, sehingga menjaga integritas pasar modal syariah. Pengungkapan yang baik juga memperkuat kepercayaan investor terhadap sektor keuangan syariah, seperti perbankan syariah dan fintech syariah, yang sangat bergantung pada keamanan sistem digital. Dengan demikian, *cybersecurity risk disclosure* berkontribusi pada stabilitas pasar modal syariah yang berlandaskan nilai-nilai Islam.

Secara keseluruhan, manfaat *cybersecurity risk disclosure* tidak hanya terbatas pada aspek teknis pelaporan, tetapi juga mencakup peningkatan kepercayaan, reputasi, dan stabilitas pasar, yang semuanya sejalan dengan tujuan maqashid syariah untuk melindungi harta dan kepercayaan serta memastikan keadilan dalam hubungan bisnis.

d. **Komponen-Komponen *Cybersecurity Riskdisclosure***

Cybersecurity Risk Disclosure mencakup elemen-elemen spesifik yang diungkapkan oleh perusahaan untuk memberikan gambaran menyeluruh tentang ancaman keamanan *cyber* yang dihadapi, dampaknya, serta strategi pengelolaan risiko yang diterapkan. Komponen-komponen ini dirancang untuk memenuhi kebutuhan pemangku kepentingan, seperti investor, regulator, dan pelanggan, agar dapat memahami tingkat risiko *cyber* dan kesiapan perusahaan dalam menghadapinya. Dalam konteks penelitian ini, pengungkapan risiko *cyber* yang komprehensif menjadi indikator penting untuk mengevaluasi bagaimana perusahaan sektor keuangan dan teknologi di BEI mengelola ancaman *cyber*, yang pada akhirnya memengaruhi reaksi pasar. Dalam perspektif ekonomi Islam, komponen-komponen ini mendukung prinsip *sidq* (kejujuran) dan *amanah* (kepercayaan), karena pengungkapan yang lengkap dan transparan membantu mengurangi *gharar* (ketidakpastian berlebihan) dan mendukung tujuan *maqashid syariah,* yaitu *hifz al-mal* (perlindungan harta) dan *hifz al-din*

(perlindungan kepercayaan). Berikut adalah komponen-komponen utama dari *cybersecurity risk disclosure:*

1) Jenis Ancaman *cyber*

   Komponen ini mencakup penjelasan tentang jenis-jenis ancaman *cyber* yang dihadapi perusahaan, seperti serangan *ransomware* (penyanderaan data), pelanggaran data *(data breach),* penipuan daring *(phishing),* atau serangan *distributed denial of service* (DDoS). Pengungkapan jenis ancaman membantu pemangku kepentingan memahami sifat dan kompleksitas risiko yang dihadapi.

2) Dampak Potensial Ancaman

   Komponen ini mencakup informasi tentang konsekuensi finansial, operasional, dan reputasi yang mungkin timbul akibat insiden *cyber*. Misalnya, perusahaan dapat mengungkapkan estimasi kerugian finansial akibat kebocoran data atau gangguan operasional akibat serangan DDoS. Pengungkapan ini penting untuk memberikan gambaran tentang sejauh mana ancaman *cyber* dapat memengaruhi kinerja perusahaan.

3) Strategi Mitigasi Risiko

   Komponen ini mencakup langkah-langkah yang diambil perusahaan untuk mencegah atau menangani ancaman *cyber*, seperti investasi dalam teknologi keamanan (misalnya, perangkat lunak antivirus atau sistem deteksi ancaman berbasis kecerdasan buatan), pelatihan karyawan tentang kesadaran keamanan *cyber*, atau

penerapan standar internasional seperti ISO 27001 atau NIST *Cybersecurity Framework.* Strategi mitigasi menunjukkan komitmen perusahaan untuk melindungi aset digitalnya.

4) Frekuensi dan Skala Insiden *cyber*

Komponen ini mencakup informasi tentang seberapa sering insiden *cyber* terjadi dan tingkat keparahan dampaknya. Misalnya, perusahaan dapat melaporkan jumlah serangan *cyber* yang berhasil dicegah atau jumlah kebocoran data yang terjadi dalam periode tertentu. Pengungkapan ini memberikan gambaran tentang tingkat paparan risiko perusahaan.

5) Kerangka Keamanan yang Digunakan

Komponen ini mencakup penjelasan tentang standar atau pedoman internasional yang diadopsi perusahaan untuk mengelola keamanan *cyber*. Pengungkapan ini menunjukkan bahwa perusahaan memiliki pendekatan terstruktur dalam pengelolaan risiko *cyber*.

Dalam konteks pasar modal syariah, komponen-komponen ini sangat penting karena mendukung prinsip sidq (kejujuran) dan amanah (kepercayaan). Pengungkapan yang mencakup semua komponen ini memungkinkan investor syariah untuk membuat keputusan yang bebas dari *gharar* (ketidakpastian) dan *maisir* (spekulasi), sehingga memperkuat integritas pasar modal syariah. Dengan mengungkapkan informasi yang lengkap, perusahaan tidak hanya memenuhi kebutuhan

pelaporan, tetapi juga menunjukkan tanggung jawab terhadap pemangku kepentingan, yang sejalan dengan nilai-nilai Islam.

e. Pihak-pihak yang terkait dengan pengungkapan *Cybersecurity Riskdisclosure*

Cybersecurity Risk Disclosure melibatkan berbagai pihak yang memiliki peran dan kepentingan dalam proses pengungkapan informasi terkait ancaman keamanan *cyber*, dampaknya, dan strategi mitigasi yang diterapkan perusahaan. Pihak-pihak ini mencakup internal perusahaan, seperti manajemen dan karyawan, serta eksternal, seperti investor, regulator, dan pelanggan. Dalam konteks penelitian ini, pengungkapan risiko *cyber* merupakan mekanisme penting untuk memberikan transparansi kepada pemangku kepentingan di sektor keuangan dan teknologi, yang sangat bergantung pada sistem informasi digital. Dalam perspektif ekonomi Islam, keterlibatan pihak-pihak ini mencerminkan prinsip sidq (kejujuran), amanah (kepercayaan), dan adl (keadilan), karena pengungkapan yang transparan memastikan bahwa semua pihak mendapatkan informasi yang setara untuk menghindari gharar (ketidakpastian berlebihan) dan mendukung tujuan *maqashid* syariah, yaitu *hifz al-mal* (perlindungan harta) dan *hifz al-din* (perlindungan kepercayaan). Berikut adalah pihak-pihak yang terkait dengan *cybersecurity risk disclosure*:

1) Manajemen Perusahaan

Manajemen, termasuk dewan direksi dan eksekutif senior, bertanggung jawab untuk menyusun dan mempublikasikan informasi tentang risiko *cyber* dalam laporan tahunan atau laporan keberlanjutan. Mereka memastikan bahwa pengungkapan mencakup jenis ancaman *cyber*, dampak potensial, dan strategi mitigasi, seperti investasi dalam teknologi keamanan atau pelatihan karyawan.

2) Investor

Investor, baik individu maupun institusional, menggunakan informasi dari *cybersecurity risk disclosure* untuk menilai risiko investasi dan potensi keuntungan dari perusahaan, terutama di sektor keuangan dan teknologi yang rentan terhadap ancaman *cyber*. Pengungkapan yang rinci membantu mereka memahami tingkat kerentanan perusahaan dan strategi mitigasi yang diterapkan, sehingga mendukung pengambilan keputusan yang rasional. Dalam pasar modal syariah, investor syariah mengharapkan transparansi yang sejalan dengan prinsip adl untuk menghindari *gharar* dan *maisir* (spekulasi).

3) Regulator

Regulator, seperti Otoritas Jasa Keuangan (OJK), Bursa Efek Indonesia (BEI), dan Badan *cyber* dan Sandi Negara (BSSN), memantau kepatuhan perusahaan terhadap standar pelaporan dan pengelolaan risiko *cyber*. Pengungkapan risiko *cyber* membantu mereka mengevaluasi ketahanan perusahaan terhadap ancaman

cyber dan menyusun regulasi yang lebih efektif untuk menjaga stabilitas pasar modal. Dalam konteks Islam, peran regulator mencerminkan prinsip adl, karena memastikan bahwa semua perusahaan memberikan informasi yang setara untuk menjaga keadilan di pasar.

4) Auditor Eksternal

Auditor eksternal bertugas memverifikasi keakuratan dan kelengkapan informasi dalam *cybersecurity risk disclosure* yang disampaikan dalam laporan tahunan atau laporan keberlanjutan. Mereka memastikan bahwa pengungkapan sesuai dengan standar pelaporan, seperti Global Reporting Initiative (GRI) atau pedoman OJK. Dalam perspektif syariah, auditor eksternal mendukung prinsip amanah dengan memastikan bahwa informasi yang diungkapkan jujur dan tidak menyesatkan.

5) Pelanggan dan Mitra Bisnis

Pelanggan dan mitra bisnis, terutama di sektor keuangan (seperti perbankan syariah dan fintech) dan teknologi (seperti e-commerce), bergantung pada keamanan sistem informasi perusahaan untuk melindungi data mereka, seperti informasi transaksi atau data pribadi. Pengungkapan risiko *cyber* yang transparan memberikan keyakinan bahwa perusahaan memiliki strategi untuk menangani ancaman *cyber*, sehingga menjaga kepercayaan pelanggan.

Dalam konteks pasar modal syariah, keterlibatan pihak-pihak ini sangat penting untuk memastikan bahwa pengungkapan risiko *cyber* mendukung nilai-nilai Islam, seperti sidq, amanah, dan adl. Dengan melibatkan semua pihak secara transparan, perusahaan dapat meminimalkan gharar dan maisir, sehingga memperkuat kepercayaan dan stabilitas di pasar modal syariah Indonesia.

f. Indikator *Cybersecurity Riskdisclosure*

Cybersecurity risk disclosure adalah alat ukur yang digunakan untuk mengevaluasi tingkat keterbukaan dan kelengkapan informasi yang diungkapkan perusahaan mengenai ancaman keamanan *cyber*, dampak potensialnya, dan strategi mitigasi yang diterapkan. Dalam penelitian ini, indikator ini penting untuk mengukur kualitas pengungkapan risiko *cyber* dalam laporan tahunan perusahaan sektor keuangan dan teknologi yang terdaftar di BEI, yang kemudian dianalisis pengaruhnya terhadap reaksi pasar *(market reaction)*. Pengukuran ini dilakukan melalui content analysis (analisis isi) laporan tahunan, yang memberikan skor berdasarkan tingkat detail dan komprehensivitas pengungkapan. Dalam penelitian ini, indikator *cybersecurity risk disclosure* diukur menggunakan skala ordinal yang mencakup empat tingkatan berdasarkan kelengkapan informasi dalam laporan tahunan:

1) Skor 0: Perusahaan tidak menyebutkan risiko *cyber* sama sekali dalam laporan tahunan.

2) Skor 1: Perusahaan hanya menyebutkan istilah "risiko *cyber*" atau ancaman *cyber* secara umum tanpa memberikan penjelasan lebih lanjut tentang jenis ancaman, dampak, atau strategi mitigasi.
3) Skor 2: Perusahaan menjelaskan satu atau dua strategi mitigasi umum, seperti penggunaan perangkat lunak keamanan atau pelatihan karyawan, tetapi tidak memberikan detail tentang jenis ancaman atau dampaknya.
4) Skor 3: Perusahaan mengungkapkan informasi secara komprehensif, mencakup jenis ancaman *cyber* (misalnya, *ransomware, data breach, phishing,* atau DDoS), dampak potensial terhadap operasional dan keuangan, investasi dalam teknologi keamanan, serta kerangka kerja yang digunakan (misalnya, ISO 27001 atau NIST *Cybersecurity Framework*).[48]

Menurut Clara Arena, Yanis Petrides, dan Panagiotis Vourvachis dalam artikel berjudul *The Impact of Cybersecurity Risk Disclosure on Market Reaction: Evidence from Listed Companies,* penggunaan content analysis dengan skala ordinal untuk mengukur pengungkapan risiko *cyber* memungkinkan peneliti untuk menilai tingkat transparansi perusahaan secara objektif. Skala ini membantu membedakan antara pengungkapan yang bersifat umum *(boilerplate)* dan pengungkapan yang rinci, yang memengaruhi persepsi investor terhadap kredibilitas

[48] Clara Arena, Yiannis Petrides, and Panagiotis Vourvachis, "The Impact of *Cybersecurity Risk Disclosure* on Market Reaction: Evidence from Listed Companies," *Journal of Financial Regulation and Compliance,* Vol. 28, No. 3, 2020, hlm. 305

perusahaan. Dalam konteks penelitian ini, indikator dengan skor tinggi (misalnya, skor 3) menunjukkan bahwa perusahaan secara proaktif mengurangi asimetri informasi, yang dapat meningkatkan kepercayaan investor dan menghasilkan reaksi pasar yang positif, seperti peningkatan *cumulative abnormal return* (CAR).

3. Tata Kelola TI

a. Pengertian Tata Kelola TI

Tata Kelola Teknologi Informasi *(IT Governance)* merupakan kerangka kerja yang memastikan pengelolaan TI perusahaan berjalan efektif, efisien, dan aman untuk mendukung tujuan strategis bisnis. Secara praktis, tata kelola TI diwujudkan melalui kebijakan, struktur organisasi seperti komite TI atau *Chief Information Security Officer* (CISO), serta penerapan standar internasional seperti COBIT atau ISO 27001. Dalam konteks penelitian, kuatnya tata kelola TI berperan sebagai sinyal positif bagi investor mengenai kemampuan perusahaan dalam mengelola risiko *cyber*, yang pada akhirnya memengaruhi reaksi pasar[49].

Secara teoritis, tata kelola TI berfungsi sebagai mekanisme yang menyelaraskan kepentingan manajemen dan pemegang saham *(Agency Theory)* melalui transparansi dan akuntabilitas pengelolaan risiko.

[49] Christin Angelia, Caesar Octoviandy Purba, Nur Imam Taufik, dan Hafid Aditya Pradesa, "Evaluating Cyber Risk Management in Indonesian SOEs: A Case Study of PT Kereta Api Indonesia Using IT Governance Framework", *ABM: International Journal of Administration, Business and Management*, vol. 8, no. 1, 2025, hlm. 104-112

Dalam perspektif ekonomi Islam, praktik ini merefleksikan penerapan prinsip *ihsan* (keunggulan) dan *husn at-tadbir* (pengelolaan yang baik) sebagai wujud tanggung jawab perusahaan dalam melindungi aset digital *(hifz al-mal)* dan menjaga kepercayaan *(hifz al-din).* Bagi sektor keuangan dan teknologi yang highly digital-dependent, tata kelola TI yang kuat tidak hanya menjadi penopang ketahanan operasional, tetapi juga kontributor penting bagi reputasi dan kepercayaan di pasar modal syariah.

b. Tujuan Tata Kelola TI

Tata Kelola Teknologi Informasi *(IT Governance)* bertujuan untuk memastikan bahwa penggunaan teknologi informasi (TI) dalam perusahaan selaras dengan tujuan strategis organisasi, dikelola secara efektif, efisien, dan aman, serta mampu mendukung keberlanjutan operasional dan finansial. Tata kelola TI mencakup struktur organisasi, kebijakan, dan proses yang dirancang untuk mengelola risiko *cyber*, seperti serangan *ransomware,* pelanggaran data *(data breach),* atau penipuan daring *(phishing),* sambil memastikan bahwa sistem informasi mendukung pencapaian visi dan misi perusahaan. Dalam konteks penelitian ini, tata kelola TI bertujuan untuk meningkatkan ketahanan perusahaan terhadap ancaman *cyber*, memperkuat kepercayaan pemangku kepentingan, dan memengaruhi reaksi pasar *(market reaction)* secara positif di sektor keuangan dan teknologi yang terdaftar di BEI.Secara spesifik, tujuan tata kelola TI meliputi:

1) Mendukung strategi bisnis, memastikan bahwa teknologi informasi digunakan untuk meningkatkan efisiensi operasional, pelayanan pelanggan, dan inovasi, misalnya dalam sistem perbankan syariah atau platform e-commerce.
2) Mengelola risiko *cyber*, melindungi aset digital perusahaan dari ancaman *cyber* melalui penerapan kebijakan keamanan, pelatihan karyawan, dan standar internasional seperti iso 27001 atau cobit.
3) Meningkatkan kepercayaan pemangku kepentingan, menunjukkan kepada investor, pelanggan, dan regulator bahwa perusahaan memiliki sistem pengendalian internal yang kuat untuk mengelola risiko *cyber*.
4) Memenuhi kepatuhan regulasi, memastikan perusahaan mematuhi peraturan dari otoritas jasa keuangan (ojk), badan *cyber* dan sandi negara (bssn), atau standar pelaporan internasional.

Tata Kelola TI yang efektif meningkatkan nilai perusahaan dengan memperkuat reputasi dan kepercayaan investor, yang tercermin dalam reaksi pasar positif seperti peningkatan *Cumulative Abnormal Return* (CAR). Secara teoritis, praktik ini menerapkan *Agency Theory* dengan menyelaraskan kepentingan manajemen dan pemegang saham melalui pengelolaan risiko *cyber* yang transparan dan terstruktur.

Khusus di sektor keuangan syariah dan teknologi, peran tata kelola TI menjadi krusial karena ketergantungan tinggi pada sistem digital. Pencapaian tujuan ini tidak hanya memperkuat ketahanan *cyber*

perusahaan, tetapi juga berkontribusi pada stabilitas pasar modal syariah melalui peningkatan kepercayaan investor dan pemangku kepentingan.

c. Manfaat Tata Kelola TI

Manfaat Tata Kelola TI *(IT Governance)* memberikan sejumlah manfaat signifikan bagi perusahaan, pemangku kepentingan, dan pasar modal secara keseluruhan, terutama dalam konteks sektor keuangan dan teknologi yang sangat bergantung pada sistem informasi digital. Tata kelola TI yang baik memastikan bahwa teknologi informasi dikelola secara efektif dan aman melalui struktur organisasi, kebijakan, dan prosedur, seperti keberadaan komite TI atau *Chief Information Security Officer* (CISO), serta penerapan standar internasional seperti ISO 27001 atau COBIT. Manfaat ini mencakup peningkatan ketahanan terhadap ancaman *cyber*, penguatan reputasi perusahaan, dan peningkatan kepercayaan investor, yang pada akhirnya dapat memengaruhi reaksi pasar (market reaction) secara positif. Berikut adalah manfaat utama dari tata kelola TI:

1) Bagi Perusahaan

Tata kelola TI yang terstruktur membantu perusahaan mengurangi risiko ancaman *cyber*, seperti *ransomware,* pelanggaran data *(data breach),* atau serangan *distributed denial of service* (DDoS), yang dapat menyebabkan kerugian finansial dan gangguan operasional. Dengan menerapkan kebijakan keamanan, pelatihan karyawan, dan teknologi canggih, perusahaan dapat menjaga

kelancaran operasional dan melindungi aset digitalnya.[50] Menurut Muhammad Ikhssani, Wahyu Ario Pratomo, dan Taufik Faturohman dalam artikel berjudul *The Role of IT Governance in Mitigating Cybersecurity Risks and Enhancing Firm Value*, tata kelola TI yang efektif meningkatkan ketahanan perusahaan terhadap insiden *cyber*, yang pada akhirnya memperkuat kinerja keuangan dan reputasi perusahaan. Dalam konteks Islam, manfaat ini sejalan dengan prinsip hifz al-mal, karena tata kelola TI melindungi aset perusahaan dari kerugian yang tidak perlu.

2) Bagi Investor

Tata kelola TI yang kuat memberikan sinyal positif kepada investor bahwa perusahaan memiliki sistem pengendalian internal yang andal untuk mengelola risiko *cyber*. Hal ini meningkatkan kepercayaan investor terhadap ketahanan dan kredibilitas perusahaan, yang dapat tercermin dalam stabilitas atau peningkatan harga saham (*cumulative abnormal return*/CAR).[51] Fera Rachmawati Sawity, Fathur Rofi, Arumega Zarefar, Mutmainah Khoiriyah, Rika Ayu Setyaningsih, Atika Zarefar, Ulfa Afifah, dan Sherly Ramaiyanti dalam penelitian berjudul *The Impact of Operational Risk Disclosure on Corporate Reputation and*

[50] Muhammad Ikhssani, Wahyu Ario Pratomo, dan Taufik Faturohman, "The Role of IT Governance in Mitigating Cybersecurity Risks and Enhancing Firm Value," *Jurnal Manajemen Teknologi*, Vol. 23, No. 1, 2024, hlm. 47

[51] Fera Rachmawati Sawity et al., "The Impact of Operational Risk Disclosure on Corporate Reputation and Financial Performance: Evidence from Indonesian Listed Companies," *Journal of Islamic Accounting and Business Research*, Vol. 15, No. 2, 2024, hlm. 241

Financial Performance, menemukan bahwa tata kelola TI yang baik meningkatkan persepsi investor terhadap reputasi perusahaan, yang berkontribusi pada nilai pasar yang lebih tinggi. Dalam pasar modal syariah, manfaat ini mendukung prinsip amanah dan sidq (kejujuran), karena perusahaan menunjukkan tanggung jawab dalam melindungi kepentingan investor dengan menghindari gharar (ketidakpastian berlebihan).

3) Bagi Pelanggan

Dalam sektor keuangan (misalnya, perbankan syariah dan *fintech*) dan teknologi (misalnya, *e-commerce*), tata kelola TI yang baik menjamin keamanan data pelanggan, seperti informasi transaksi atau data pribadi. Hal ini meningkatkan kepercayaan pelanggan terhadap perusahaan, yang penting untuk mempertahankan loyalitas dan reputasi.[52] Indah Ratna Puspitasari dan Nila Aryanty dalam penelitian berjudul *Cybersecurity Risk Disclosure in Indonesian Listed Companies: A Qualitative Study,* menyoroti bahwa tata kelola TI yang kuat membantu perusahaan menjaga kepercayaan pelanggan dengan meminimalkan risiko kebocoran data, yang dalam Islam sejalan dengan prinsip hifz al-din (perlindungan kepercayaan).

4) Bagi Regulator

[52] Indah Ratna Puspitasari and Nila Aryanty, "*Cybersecurity Risk Disclosure* in Indonesian Listed Companies: A Qualitative Study," *Journal of Accounting and Investment*, Vol. 24, No. 1, 2023, hlm. 8

Tata kelola TI yang terstruktur memudahkan regulator, seperti OJK dan Badan *cyber* dan Sandi Negara (BSSN), untuk memantau kepatuhan perusahaan terhadap standar keamanan *cyber* dan peraturan pelaporan. Dengan adanya komite TI atau CISO, perusahaan dapat menunjukkan kesiapan mereka dalam menghadapi ancaman *cyber*, yang mendukung stabilitas pasar modal.[53] Menurut Muhammad Ikhssani et al., tata kelola TI yang baik memungkinkan regulator untuk mengevaluasi ketahanan *cyber* perusahaan secara efektif, sehingga memperkuat infrastruktur keamanan pasar. Dalam konteks syariah, hal ini mencerminkan prinsip adl (keadilan), karena tata kelola TI yang baik memastikan bahwa perusahaan beroperasi secara transparan dan adil terhadap semua pemangku kepentingan.

5) Bagi Pasar Modal Syariah

Dalam ekosistem pasar modal syariah, tata kelola TI yang baik mendukung prinsip ihsan dan husn at-tadbīr dengan memastikan bahwa perusahaan mengelola risiko *cyber* secara bertanggung jawab. Hal ini meningkatkan kepercayaan investor syariah, yang mengharapkan perusahaan beroperasi sesuai dengan nilai-nilai Islam, seperti menghindari gharar dan maisir (spekulasi). Tata kelola TI yang terstruktur juga membantu menjaga integritas pasar modal syariah dengan memastikan bahwa perusahaan melindungi aset

[53] Muhammad Ikhssani et al., "The Role of IT Governance in Mitigating Cybersecurity Risks and Enhancing Firm Value: A Regulatory Perspective," *Journal of Financial Regulation and Compliance*, Vol.32, No. 2, 2024, hlm. 48

digitalnya, yang merupakan bagian dari hifz al-mal. Dengan demikian, tata kelola TI berkontribusi pada stabilitas dan kepercayaan di pasar modal syariah Indonesia.

Secara keseluruhan, manfaat tata kelola TI tidak hanya terbatas pada aspek teknis, tetapi juga mencakup peningkatan reputasi, kepercayaan, dan stabilitas pasar, yang semuanya sejalan dengan nilai-nilai syariah dan mendukung tujuan penelitian ini untuk menganalisis dampaknya terhadap reaksi pasar.

d. Komponen-Komponen Tata Kelola TI

Komponen-Komponen Tata Kelola TI (IT *Governance*) terdiri dari sejumlah komponen yang membentuk kerangka kerja untuk memastikan bahwa teknologi informasi (TI) dikelola secara efektif, efisien, dan aman guna mendukung tujuan strategis perusahaan. Komponen-komponen ini mencakup struktur organisasi, kebijakan, prosedur, dan alat yang digunakan untuk mengelola risiko *cyber*, seperti serangan ransomware, pelanggaran data (data breach), atau penipuan daring (phishing), serta untuk memastikan keberlanjutan operasional. Dalam konteks penelitian ini, komponen-komponen tata kelola TI menjadi indikator penting untuk mengevaluasi sejauh mana perusahaan sektor keuangan dan teknologi di BEI memiliki sistem yang kuat untuk menghadapi ancaman *cyber*, yang pada akhirnya memengaruhi kepercayaan investor dan reaksi pasar (market reaction). Berikut adalah komponen-komponen utama dari tata kelola TI:

1) Struktur Organisasi

Struktur organisasi mencakup pembentukan unit atau peran khusus, seperti komite TI atau *Chief Information Security Officer* (CISO), yang bertanggung jawab atas pengawasan keamanan *cyber* dan pengelolaan sistem informasi. Komite TI atau CISO memastikan bahwa keputusan terkait TI selaras dengan strategi bisnis dan kebutuhan keamanan. Menurut Muhammad Ikhssani, Wahyu Ario Pratomo, dan Taufik. Dalam konteks Islam, struktur organisasi yang jelas mencerminkan prinsip husn *at-tadbīr,* karena menunjukkan pengelolaan yang terstruktur dan bertanggung jawab.

2) Kebijakan Keamanan Informasi

Kebijakan keamanan informasi adalah pedoman tertulis yang mengatur pengelolaan data dan sistem TI, termasuk prosedur untuk mencegah, mendeteksi, dan menangani ancaman *cyber*. Kebijakan ini mencakup aturan tentang akses data, penggunaan perangkat lunak keamanan, dan respons terhadap insiden *cyber*.[54] Indah Ratna Puspitasari dan Nila Aryanty dalam penelitian berjudul *Cybersecurity Risk Disclosure* in Indonesian Listed Companies: A Qualitative Study, menegaskan bahwa kebijakan keamanan informasi yang jelas membantu perusahaan mengurangi risiko *cyber* dan meningkatkan transparansi kepada pemangku kepentingan.

[54] Indah Ratna Puspitasari dan Nila Aryanty, "*Cybersecurity Risk Disclosure* in Indonesian Listed Companies: A Qualitative Study," *Jurnal Akuntansi dan Auditing Indonesia*, Vol. 27, No. 1, 2023, hlm. 7

Dalam perspektif syariah, kebijakan ini sejalan dengan prinsip amanah, karena perusahaan bertanggung jawab untuk melindungi aset digital sebagai bagian dari kepercayaan yang diberikan oleh investor dan pelanggan.

3) Pelatihan Karyawan

Pelatihan karyawan merupakan komponen penting untuk meningkatkan kesadaran dan keterampilan dalam menghadapi ancaman *cyber*, seperti mengenali email phishing atau mematuhi protokol keamanan. Program pelatihan yang rutin memastikan bahwa karyawan menjadi lini pertahanan pertama terhadap ancaman *cyber*.[55] Fera Rachmawati Sawity, Fathur Rofi, Arumega Zarefar, Mutmainah Khoiriyah, Rika Ayu Setyaningsih, Atika Zarefar, Ulfa Afifah, dan Sherly Ramaiyanti dalam penelitian berjudul The Impact of Operational Risk Disclosure on Corporate Reputation and Financial Performance, menemukan bahwa pelatihan karyawan tentang keamanan *cyber* meningkatkan ketahanan perusahaan dan reputasinya di mata pemangku kepentingan. Dalam konteks Islam, pelatihan ini mencerminkan prinsip ihsan, karena perusahaan berupaya mencapai keunggulan dalam pengelolaan risiko untuk melindungi harta *(hifz al-mal)*.

4) Teknologi Keamanan

[55] Fera Rachmawati Sawity et al., "The Impact of Operational Risk Disclosure on Corporate Reputation and Financial Performance: Empirical Evidence from Indonesia," *Journal of Risk and Financial Management*, Vol. 17, No. 3, 2024, hlm. 204

Komponen ini mencakup penggunaan alat dan teknologi keamanan, seperti perangkat lunak antivirus, sistem deteksi ancaman berbasis kecerdasan buatan, atau firewall, untuk melindungi sistem informasi dari ancaman *cyber*. Investasi dalam teknologi keamanan menunjukkan komitmen perusahaan untuk mencegah insiden *cyber*.[56] Menurut Muhammad Ikhssani et al., perusahaan yang mengadopsi teknologi keamanan canggih cenderung memiliki tingkat ketahanan *cyber* yang lebih tinggi, yang meningkatkan kepercayaan investor dan memengaruhi reaksi pasar secara positif. Dalam perspektif syariah, investasi ini mendukung prinsip hifz al-mal, karena melindungi aset digital perusahaan dari kerugian akibat serangan *cyber*.

5) Standar Internasional

Penerapan standar internasional, seperti ISO 27001, COBIT, atau NIST *Cybersecurity Framework,* merupakan komponen kunci untuk memastikan bahwa tata kelola TI dilakukan secara terstruktur dan sesuai dengan praktik terbaik global. Standar ini memberikan pedoman untuk mengelola risiko *cyber* dan memastikan kepatuhan terhadap regulasi.[57] Indah Ratna Puspitasari dan Nila Aryanty menyoroti bahwa perusahaan yang mengadopsi standar

[56] Muhammad Ikhssani et al., "Cybersecurity Technology Adoption, Investor Confidence, and Market Reaction: Evidence from Indonesian Listed Firms," *Journal of Financial Crime*, Vol. 31, No. 2, 2024, hlm. 47

[57] Indah Ratna Puspitasari and Nila Aryanty, "*Cybersecurity Risk Disclosure* and Corporate Governance in Indonesia: The Role of International IT Standards," *Journal of Governance and Regulation*, Vol. 12, No. 4, 2023, hlm. 208

internasional dalam tata kelola TI dianggap lebih kredibel oleh investor dan regulator, yang dalam konteks syariah mencerminkan prinsip adl (keadilan) dan husn at-tadbīr dengan memastikan pengelolaan yang adil dan terstruktur.

Dalam konteks pasar modal syariah, komponen-komponen ini sangat penting karena mendukung nilai-nilai Islam, seperti ihsan, amanah, dan sidq. Dengan memiliki struktur organisasi yang jelas, kebijakan keamanan yang kuat, pelatihan karyawan, teknologi keamanan, dan standar internasional, perusahaan dapat meminimalkan gharar (ketidakpastian) dan maisir (spekulasi), sehingga memperkuat kepercayaan investor syariah dan menjaga integritas pasar modal syariah Indonesia.

e. Pihak-pihak yang terkait dengan Tata Kelola TI

Pihak-Pihak yang Terkait dengan Tata Kelola TI
Tata Kelola Teknologi Informasi (IT *Governance*) melibatkan berbagai pihak yang memiliki peran dan kepentingan dalam memastikan bahwa teknologi informasi (TI) dikelola secara efektif, efisien, dan aman untuk mendukung tujuan strategis perusahaan serta mengelola risiko *cyber*, seperti serangan ransomware, pelanggaran data *(data breach),* atau penipuan daring *(phishing).* Pihak-pihak ini mencakup internal perusahaan, seperti manajemen dan karyawan, serta eksternal, seperti investor, regulator, dan mitra bisnis. Dalam konteks penelitian ini, keterlibatan pihak-pihak ini penting untuk mengevaluasi bagaimana tata

kelola TI memengaruhi kepercayaan investor dan reaksi pasar *(market reaction)* di sektor keuangan dan teknologi yang terdaftar di BEI. Berikut adalah pihak-pihak yang terkait dengan tata kelola TI:

1) Manajemen Perusahaan

Manajemen, termasuk dewan direksi, komite TI, dan *Chief Information Security Officer* (CISO), bertanggung jawab untuk merancang, mengimplementasikan, dan mengawasi kebijakan tata kelola TI. Mereka memastikan bahwa sistem TI selaras dengan tujuan bisnis dan dilengkapi dengan strategi untuk mengelola risiko *cyber*.[58] Menurut Muhammad Ikhssani, Wahyu Ario Pratomo, dan Taufik Faturohman dalam artikel berjudul *The Role of IT Governance in Mitigating Cybersecurity Risks and Enhancing Firm Value*, manajemen berperan sebagai pengambil keputusan kunci dalam tata kelola TI, yang memengaruhi reputasi perusahaan dan kepercayaan investor.

2) Karyawan

Karyawan merupakan pihak yang terlibat langsung dalam pelaksanaan kebijakan tata kelola TI, seperti mematuhi prosedur keamanan, mengikuti pelatihan kesadaran *cyber*, dan melaporkan potensi ancaman, seperti email phishing. Karyawan menjadi lini

[58] Muhammad Ikhssani, Wahyu Ario Pratomo, and Taufik Faturohman, "The Role of IT Governance in Mitigating Cybersecurity Risks and Enhancing Firm Value: Evidence from Indonesian Listed Companies," *Journal of Accounting and Organizational Change*, Vol. 20, No. 3, 2024), hlm. 46

pertahanan pertama terhadap ancaman *cyber*.[59] Indah Ratna Puspitasari dan Nila Aryanty dalam penelitian berjudul *Cybersecurity Risk Disclosure* in Indonesian Listed Companies: A Qualitative Study menyoroti bahwa keterlibatan karyawan melalui pelatihan rutin meningkatkan efektivitas tata kelola TI dan mengurangi risiko insiden *cyber*. Dalam perspektif syariah, peran karyawan mencerminkan prinsip amanah, karena mereka bertanggung jawab untuk menjalankan tugas dengan jujur (sidq) demi melindungi aset perusahaan (hifz al-mal).

3) Investor

Investor, baik individu maupun institusional, menggunakan informasi tentang tata kelola TI untuk menilai ketahanan perusahaan terhadap risiko *cyber* dan kredibilitas pengelolaannya. Tata kelola TI yang kuat memberikan sinyal positif bahwa perusahaan mampu melindungi aset digitalnya, yang dapat memengaruhi keputusan investasi dan reaksi pasar, seperti peningkatan cumulative abnormal return (CAR).[60] Fera Rachmawati Sawity, Fathur Rofi, Arumega Zarefar, Mutmainah Khoiriyah, Rika Ayu Setyaningsih, Atika Zarefar, Ulfa Afifah, dan Sherly Ramaiyanti dalam penelitian berjudul The Impact of Operational Risk Disclosure on Corporate

[59] Indah Ratna Puspitasari and Nila Aryanty, "*Cybersecurity Risk Disclosure* in Indonesian Listed Companies: A Qualitative Study," *Journal of Information Systems and Technology Management*, Vol. 20, No. 2, 2023, hlm. 8

[60] Fera Rachmawati Sawity et al., "The Impact of Operational Risk Disclosure on Corporate Reputation and Financial Performance: Evidence from Indonesian Financial and Technology Sectors," *Journal of Risk Research*, Vol. 27, No. 5, 2024, hlm. 241

Reputation and Financial Performance, menemukan bahwa tata kelola TI yang baik meningkatkan kepercayaan investor, terutama di sektor keuangan dan teknologi.

4) Regulator

Regulator, seperti Otoritas Jasa Keuangan (OJK) dan Badan *cyber* dan Sandi Negara (BSSN), memantau kepatuhan perusahaan terhadap standar tata kelola TI dan keamanan *cyber*. Mereka memastikan bahwa perusahaan memiliki sistem yang memadai untuk melindungi data dan operasional, yang mendukung stabilitas pasar modal.[61] Menurut Muhammad Ikhssani et al., tata kelola TI yang terstruktur memudahkan regulator untuk mengevaluasi ketahanan *cyber* perusahaan, sehingga memperkuat infrastruktur keamanan nasional. Dalam konteks syariah, peran regulator mencerminkan prinsip adl, karena memastikan bahwa perusahaan beroperasi secara transparan dan adil terhadap semua pemangku kepentingan.

5) Pihak Eksternal (Vendor Teknologi dan Konsultan)

Pihak eksternal, seperti vendor teknologi dan konsultan keamanan *cyber*, membantu perusahaan membangun dan memelihara sistem TI yang aman, termasuk menyediakan perangkat

[61] Muhammad Ikhssani et al., "The Role of IT Governance in Strengthening National Cybersecurity Infrastructure: A Regulatory Perspective from Indonesia," *Journal of Cybersecurity and Privacy*, Vol. 4, No. 1, 2024, hlm. 48

lunak keamanan atau melakukan audit sistem.[62] Indah Ratna Puspitasari dan Nila Aryanty menekankan bahwa kolaborasi dengan vendor dan konsultan keamanan *cyber* meningkatkan efektivitas tata kelola TI, terutama dalam menerapkan standar seperti ISO 27001 atau NIST *Cybersecurity Framework.* Dalam perspektif Islam, keterlibatan pihak eksternal mendukung prinsip ihsan, karena perusahaan berupaya mencapai keunggulan dalam pengelolaan TI untuk melindungi harta *(hifz al-mal)* dan kepercayaan *(hifz al-din).*

Dalam konteks pasar modal syariah, keterlibatan pihak-pihak ini sangat penting untuk memastikan bahwa tata kelola TI mendukung nilai-nilai Islam, seperti ihsan, amanah, dan sidq. Dengan melibatkan semua pihak secara terkoordinasi, perusahaan dapat meminimalkan gharar dan maisir, sehingga memperkuat kepercayaan investor syariah dan menjaga integritas pasar modal syariah Indonesia.

f. Indikator Tata Kelola TI

Indikator tata kelola TI digunakan untuk mengevaluasi sejauh mana perusahaan memiliki struktur, kebijakan, dan proses yang efektif untuk mengelola teknologi informasi (TI) dan mengurangi risiko *cyber*, seperti serangan ransomware, pelanggaran data *(data breach),* atau penipuan daring *(phishing).* Dalam konteks penelitian ini, indikator tata kelola TI menjadi alat untuk mengukur komitmen perusahaan sektor keuangan

[62] Indah Ratna Puspitasari and Nila Aryanty, "The Role of External Collaboration in Strengthening IT Governance and Cybersecurity Resilience: Evidence from Indonesian Listed Firms," *Journal of Global Information Management*, Vol. 31, No. 4, 2023, hlm. 7

dan teknologi yang terdaftar di BEI dalam mengelola risiko *cyber*, yang kemudian dianalisis pengaruhnya terhadap reaksi pasar *(market reaction)*. Indikator ini mencerminkan tingkat transparansi dan akuntabilitas perusahaan dalam pengelolaan TI, yang dalam perspektif ekonomi Islam sejalan dengan prinsip ihsan (keunggulan dalam pengelolaan), *husn at-tadbīr* (pengelolaan yang baik), dan amanah (kepercayaan). Dengan meminimalkan *gharar* (ketidakpastian berlebihan), indikator ini mendukung tujuan maqashid syariah, yaitu hifz al-mal (perlindungan harta) dan *hifz al-din* (perlindungan kepercayaan). Dalam penelitian ini, tata kelola TI diukur menggunakan variabel dummy berdasarkan keberadaan struktur formal tata kelola TI dalam laporan tahunan perusahaan, dengan kriteria sebagai berikut:

1) Nilai 1: Perusahaan memiliki komite TI atau *Chief Information Security Officer* (CISO) yang disebutkan secara eksplisit dalam laporan tahunan, menunjukkan adanya struktur formal untuk mengelola risiko *cyber*.
2) Nilai 0: Perusahaan tidak menyebutkan keberadaan komite TI atau CISO dalam laporan tahunan, menunjukkan kurangnya struktur formal tata kelola TI.

Penggunaan variabel dummy ini dipilih karena keberadaan komite TI atau CISO merupakan indikator yang jelas dan objektif untuk menilai komitmen perusahaan terhadap tata kelola TI. Dalam konteks Indonesia, penggunaan variabel dummy ini relevan karena banyak perusahaan,

terutama di sektor keuangan dan teknologi, belum secara konsisten melaporkan struktur tata kelola TI mereka. Dalam pasar modal syariah, indikator ini sangat penting karena investor syariah mengharapkan perusahaan untuk menunjukkan komitmen terhadap pengelolaan yang bertanggung jawab, yang membantu menghindari gharar dan maisir (spekulasi).

Dengan demikian, indikator tata kelola TI yang diukur melalui variabel dummy (keberadaan komite TI atau CISO) memberikan alat ukur yang sederhana namun efektif untuk mengevaluasi komitmen perusahaan terhadap pengelolaan risiko *cyber*. Indikator ini tidak hanya relevan untuk analisis pasar modal konvensional, tetapi juga mendukung nilai-nilai syariah, seperti ihsan, amanah, dan sidq, yang penting dalam konteks pasar modal syariah Indonesia.

B. Penelitian Terdahulu

Subbab ini memaparkan kajian pustaka yang bersumber dari penelitian-penelitian terdahulu yang memiliki keterkaitan substantif dengan pokok bahasan penelitian ini, meliputi skripsi, tesis, disertasi, dan artikel-artikel pada jurnal ilmiah terakreditasi. Selanjutnya, peneliti melakukan sintesis terhadap temuan-temuan dari berbagai studi tersebut untuk menetapkan posisi penelitian ini sekaligus mengidentifikasi aspek kebaruan *(novelty)* yang membedakannya dari penelitian-penelitian sebelumnya. Berdasarkan penelusuran kepustakaan yang telah dilaksanakan, diperoleh sejumlah penelitian terdahulu yang dapat diklasifikasikan sebagai berikut:

Tabel 2.1

Penelitian Terdahulu

No	Penulis/Tahun	Judul	Hasil Temuan	Perbedaan
1	Karyani, Taufik, Ana dan Raden (2024)	*Financial Resilience in ASEAN-4 Banking Sector: Impact of Cyber Risk Disclosure*	*Voluntary Cyber Risk Disclosure* (VCRD) justru dapat menurunkan ketahanan finansial bank, kecuali pengungkapan tentang penyebab risiko yang tidak berpengaruh. Ini menunjukkan pengungkapan yang tidak tepat dapat menjadi "bumerang" bagi bank.	Berfokus pada dampak pengungkapan terhadap ketahanan finansial, sedangkan penelitian ini berfokus pada reaksi pasar (harga saham, volume, volatilitas). Selain itu, studi ini mencakup 4 negara ASEAN (Indonesia, Malaysia, Thailand, Filipina), sementara penelitian Anda spesifik di BEI.
2	Siti Jubaedah, Agung Musta'in, Izza Nurlisti, Bayu Adam Maulana (2024)	*Cyber risk management disclosure: A stakeholder theory perspective*	Kepemilikan asing dan kepemilikan blok berpengaruh positif signifikan terhadap pengungkapan manajemen risiko siber, sedangkan kepemilikan manajemen dan kepemilikan	Berfokus pada faktor-faktor yang memengaruhi pengungkapan (struktur kepemilikan), sedangkan penelitian ini berfokus pada konsekue nsi pasar dari pengungkapan tersebut (reaksi investor).

			tersebar tidak berpengaruh signifikan.	
3	Stiawan (2026)	*Market Reaction and Firm Value: A Governance, Risk and Compliance Disclosure Perspective*	Pengungkapan *Governance, Risk,* dan *Compliance* (GRC) secara simultan berpengaruh positif signifikan terhadap reaksi pasar. Hanya pengungkapan governance dan risiko yang berpengaruh positif signifikan terhadap nilai perusahaan.	Menggunakan variabel GRC disclosure secara agregat, sedangkan penelitian ini spesifik menguji *Cyber security Risk Disclosure* dan Tata Kelola TI sebagai variabel terpisah yang memengaruhi reaksi pasar.
4	Mira Sofiani, Diani Putri Ramadhanty, Siti Jubaedah	*Cyber Risk Management Disclosure: The Impact of Firm Size, Profitability, and Intangible Asset*	Ukuran perusahaan dan profitabilitas berpengaruh positif signifikan terhadap pengungkapan manajemen risiko siber, sedangkan aset tidak berwujud tidak berpengaruh signifikan.	Berfokus pada faktor-faktor yang memengaruhi pengungkapan (ukuran perusahaan, profitabilitas, aset tidak berwujud), sedangkan penelitian ini berfokus pada dampak pengungkapan terhadap reaksi pasar.
5	Damayanti (2022)	*Pengaruh Cybersecurity Risk Disclosure dan Ukuran Perusahaan*	Cybersecurity risk disclosure dan ukuran perusahaan (SIZE) secara bersama-sama (simultan)	Variabel independen hanya cybersecurity risk disclosure dan ukuran perusahaan,

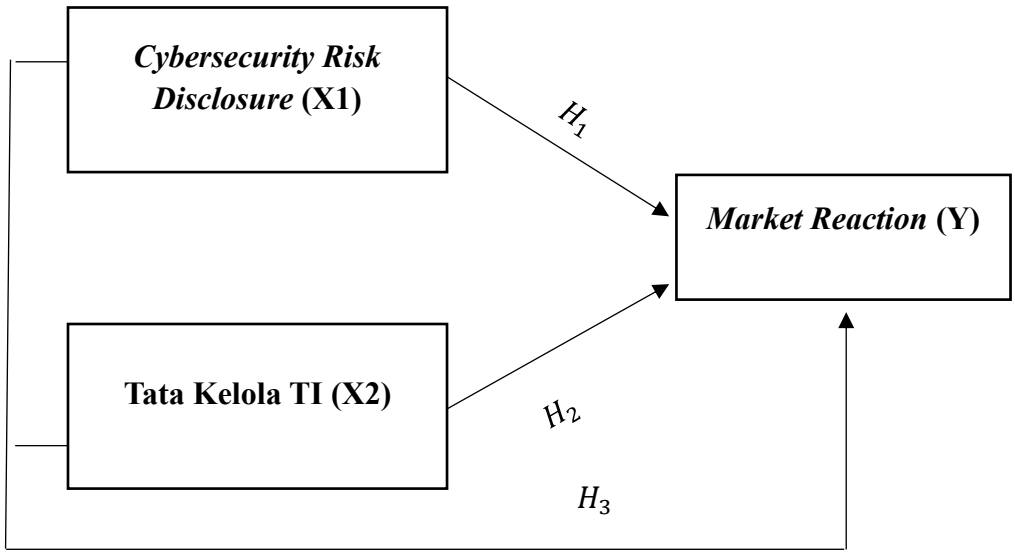
		Terhadap Harga Saham	berpengaruh signifikan terhadap harga saham. Secara parsial, hanya SIZE yang berpengaruh signifikan, sedangkan cybersecurity risk disclosure tidak berpengaruh signifikan terhadap harga saham.	sedangkan penelitian ini menambahkan Tata Kelola TI sebagai variabel independen kedua dan menggunakan indikator reaksi pasar yang lebih luas (CAR, volume, volatilitas).
6	Adams & Moore (2025)	*How informative are cybersecurity risk disclosures? Empirical analysis of firms targeted by ransomware*	Menganalisis 7.681 pernyataan terkait siber dari 61 perusahaan yang mengalami insiden ransomware (2018-2021). Menemukan bahwa perusahaan meningkatkan pengungkapan setelah insiden, tetapi kualitas pengungkapan bervariasi.	Berfokus pada perusahaan yang telah mengalami insiden ransomware di AS, sedangkan penelitian ini menguji pengungkapan risiko siber secara umum pada perusahaan sektor finansial dan teknologi di BEI, baik yang mengalami insiden maupun tidak.

C. Kerangka Pemikiran

Penelitian ini melibatkan tiga variabel, yaitu keterbukaan cybersecurity risk disclosure, tata kelola teknologi informasi, dan market reaction. Variabel bebas atau independen pada penelitian ini adalah keterbukaan *cybersecurity risk*

disclosure (X_1) dan tata kelola teknologi informasi (X_2), sementara variabel terikat atau dependennya adalah market reaction (Y). Kerangka berpikir dalam penelitian ini memaparkan secara sistematis hubungan kausal antarvariabel yang saling terkait. Dengan demikian, model kerangka berpikir digunakan untuk memudahkan peneliti dan pembaca dalam memahami konsep penelitian, yang disajikan sebagai berikut:

Gambar 2.1
Kerangka Pemikiran



D. Pengembangan Hipotesis

Pengembangan hipotesis merupakan proses merumuskan dugaan sementara yang masih perlu diuji kebenarannya melalui penelitian empiris, yang disusun secara sistematis berdasarkan kajian teori, hasil penelitian terdahulu, serta

kerangka pemikiran yang telah dibangun.[63] Proses ini menjadi tahapan krusial dalam penelitian kuantitatif karena berfungsi sebagai jembatan yang menghubungkan teori dengan realitas empiris, sekaligus memberikan arah yang jelas bagi peneliti dalam mengumpulkan dan menganalisis data.[64] Hipotesis yang dikembangkan dengan baik harus dirumuskan secara spesifik, dapat diuji secara empiris, didasarkan pada teori yang kuat, serta menyatakan hubungan logis antar variabel yang diteliti.[65]

1. Pengaruh Keterbukaan *Cybersecurity Risk Disclosure* terhadap *Market Reaction*

Perusahaan yang bergerak di sektor finansial dan teknologi memiliki karakteristik yang sangat bergantung pada sistem informasi digital dalam menjalankan operasional bisnisnya. Kedua sektor ini juga mengelola data sensitif nasabah dan pengguna dalam jumlah besar, sehingga kerentanan terhadap serangan *cyber* menjadi salah satu risiko utama yang perlu dikelola dengan baik. Di sisi lain, investor saat ini tidak hanya mempertimbangkan kinerja keuangan semata dalam mengambil keputusan investasi, tetapi juga menilai bagaimana perusahaan mengidentifikasi, mengelola, dan mengomunikasikan risiko-risiko non-keuangan yang berpotensi memengaruhi keberlanjutan usaha.[66]

---

[63] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, (Bandung: Alfabeta, 2019), hlm. 64

[64] Nur Indriantoro dan Bambang Supomo, *Metodologi Penelitian Bisnis untuk Akuntansi dan Manajemen*, (Yogyakarta: BPFE, 2018), hlm. 85

[65] Saifuddin Azwar, *Metode Penelitian*, (Yogyakarta: Pustaka Pelajar, 2018), hlm. 45

[66] Fera Rachmawati Sawity, dkk., "The Impact of Operational Risk Disclosure on Corporate Reputation and Financial Performance," *Jurnal Akuntansi dan Keuangan Indonesia*, Vol. 21, No. 1, 2024, hlm. 45-62

Berdasarkan teori sinyal *(signaling theory),* pengungkapan risiko *cyber* yang dilakukan perusahaan dapat dipandang sebagai sinyal positif bagi investor. Teori sinyal menjelaskan bahwa perusahaan cenderung akan mengumumkan informasi yang menunjukkan bahwa perusahaan dalam keadaan baik, sementara perusahaan akan menahan informasi yang cenderung menjadi sinyal buruk bagi investor.[67] Perusahaan yang secara sukarela mengungkapkan informasi terkait risiko *cyber* secara transparan menunjukkan bahwa manajemen memiliki kesadaran dan kemampuan dalam mengelola risiko tersebut. Sinyal ini mengurangi asimetri informasi antara manajemen dan investor, sehingga meningkatkan keyakinan investor terhadap kualitas manajemen risiko perusahaan. Peningkatan keyakinan tersebut akan tercermin pada reaksi pasar yang positif, yang diukur melalui *cumulative abnormal return* (CAR). Dalam kerangka teori keputusan individu *(single-person decision theory),* informasi didefinisikan sebagai bukti yang memiliki potensi untuk memengaruhi keputusan individu, sehingga ketersediaan informasi yang berkualitas akan sangat berpengaruh terhadap proses pembuatan keputusan oleh investor.[68]

Penelitian terdahulu secara konsisten mendukung bahwa pengungkapan risiko yang lebih luas dan berkualitas cenderung direspons positif oleh pasar. Arena, Petrides, dan Vourvachis menemukan bahwa pengungkapan risiko *cyber* yang komprehensif dan rinci berfungsi sebagai sinyal positif

[67] Ross, S. A., "The Economic Theory of Agency: The Principal's Problem," *American Economic Review*, Vol. 63, No. 2, 1973, hlm. 134-139

[68] Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R., "Signaling Theory: A Review and Assessment," *Journal of Management*, Vol. 37, No. 1, 2011, hlm. 39-67

yang signifikan kepada pasar, di mana perusahaan dengan tingkat pengungkapan yang tinggi mengalami abnormal return yang lebih positif dibandingkan dengan perusahaan dengan pengungkapan yang minimal.[69] Penelitian lain oleh Pratama dan Widjaja menguji efisiensi pasar bentuk setengah kuat di BEI dan menunjukkan bahwa pasar bereaksi terhadap informasi pengungkapan risiko *cyber*, meskipun kecepatan dan besaran reaksinya tidak sepenuhnya efisien dan dipengaruhi oleh karakteristik perusahaan seperti likuiditas saham.[70] Namun, terdapat temuan yang menunjukkan bahwa pengungkapan risiko *cyber* di Indonesia masih menghadapi kendala. Puspitasari dan Aryanty mengungkapkan bahwa tingkat pengungkapan risiko *cyber* di perusahaan-perusahaan terbuka Indonesia masih sangat rendah dan bersifat umum *(boilerplate),* disebabkan oleh kurangnya pemahaman manajemen, tidak adanya standar pengungkapan yang baku dari regulator, dan kekhawatiran akan reaksi negatif pasar jika mengungkapkan kerentanan.[71] Solikhawati dan Samsuri juga menemukan bahwa pengumuman insiden *cyber* menyebabkan penurunan harga saham yang signifikan, dengan penurunan yang lebih parah terjadi pada bank yang tidak memiliki pengungkapan risiko *cyber*

[69] Clara Arena, Yiannis Petrides, & Petros Vourvachis, "The Impact of *Cybersecurity Risk Disclosure* on Market Reaction: Evidence from Listed Companies," *Journal of Accounting and Public Policy*, Vol. 39, No. 4, 2020, hlm. 106-125

[70] Bima Cinintya Pratama & Indra Widjaja, "Market Response to Cybersecurity Disclosures in Indonesian Stock Exchange: A Semi-Strong Efficiency Perspective," *Indonesian Journal of Accounting Research*, Vol. 28, No. 1, 2025, hlm. 78-95

[71] Indah Ratna Puspitasari & Nila Aryanty, "*Cybersecurity Risk Disclosure* in Indonesian Listed Companies: A Qualitative Study," *Jurnal Riset Akuntansi dan Bisnis*, Vol. 23, No. 2, 2023, hlm. 112-130

yang memadai dalam laporan tahunannya sebelumnya.[72] Temuan ini justru memperkuat argumen bahwa keterbukaan risiko *cyber* sangat penting, karena perusahaan yang telah melakukan pengungkapan sebelumnya cenderung mengalami dampak negatif yang lebih kecil saat terjadi insiden. Dengan demikian, semakin tinggi tingkat keterbukaan *cybersecurity risk disclosure,* maka semakin besar pula respons positif yang diberikan oleh pasar, yang tercermin pada peningkatan *cumulative abnormal return* (CAR). Berdasarkan uraian tersebut, maka hipotesis yang diajukan adalah:

H_1 :Keterbukaan *cybersecurity riskdisclosure* berpengaruh terhadap *market reaction*.

2. Pengaruh Kualitas Tata Kelola Teknologi Informasi terhadap *Market Reaction*

Tata kelola teknologi informasi *(IT governance)* merupakan elemen penting yang mencerminkan sejauh mana perusahaan mengelola sumber daya TI secara akuntabel, aman, dan selaras dengan tujuan strategis bisnis. Dalam konteks perusahaan sektor finansial dan teknologi, keberadaan komite teknologi informasi atau *Chief Information Security Officer* (CISO) menjadi indikator kuat bahwa perusahaan memiliki komitmen terhadap tata kelola TI yang baik. Perusahaan yang memiliki struktur tata kelola TI yang

[72] Anis Solikhawati & Ahmad Samsuri, "The Effect of Cybersecurity Incidents on Stock Prices: Evidence from Indonesian Islamic Banks," *Journal of Islamic Finance*, Vol. 12, No. 3, 2023, hlm. 55-72

mapan dinilai lebih siap dalam menghadapi ancaman *cyber*, melindungi data nasabah, dan menjaga keberlanjutan operasional.[73]

Berdasarkan teori legitimasi *(legitimacy theory),* perusahaan berupaya untuk memperoleh legitimasi dari pemangku kepentingan dengan menunjukkan bahwa mereka beroperasi sesuai dengan ekspektasi dan norma yang berlaku di masyarakat. Penerapan tata kelola TI yang baik merupakan salah satu bentuk upaya legitimasi, karena menunjukkan bahwa perusahaan bertanggung jawab dalam melindungi aset informasi dan menjaga kepentingan nasabah.[74] Di sisi lain, teori agensi *(agency theory)* menjelaskan bahwa mekanisme tata kelola yang baik dapat mengurangi konflik kepentingan antara manajemen dan pemegang saham. Keberadaan komite TI atau CISO memperkuat fungsi pengawasan terhadap pemanfaatan TI, sehingga risiko penyalahgunaan atau kegagalan sistem dapat ditekan.[75]

Penelitian terdahulu mendukung bahwa tata kelola TI yang baik berdampak positif terhadap kinerja dan nilai perusahaan. Ikhssani, Mudra, dan Prasidya dalam penelitiannya pada sektor finansial dan teknologi di Indonesia menyimpulkan bahwa keberadaan struktur tata kelola TI yang formal (seperti komite TI atau CISO) secara signifikan meningkatkan

---

[73] Weill, P., & Ross, J. W., *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, (Boston: Harvard Business School Press, 2004), hlm. 45-78

[74] Suchman, M. C., "Managing Legitimacy: Strategic and Institutional Approaches," *Academy of Management Review*, Vol. 20, No. 3, 1995, hlm. 571-610

[75] Jensen, M. C., & Meckling, W. H., "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure," *Journal of Financial Economics*, Vol. 3, No. 4, 1976, hlm. 305-360

ketahanan *cyber* perusahaan, dan perusahaan dengan tata kelola TI yang kuat menunjukkan tingkat market confidence yang lebih tinggi, yang tercermin dari volatilitas harga saham yang lebih rendah pasca terjadinya insiden *cyber*.[76] Penelitian Sawity dkk. juga menemukan bahwa pengungkapan risiko operasional yang transparan (yang mencakup risiko *cyber*) memiliki dampak positif tidak langsung terhadap kinerja keuangan melalui peningkatan reputasi perusahaan, mendukung ide bahwa pengungkapan risiko merupakan investasi dalam reputational capital yang pada akhirnya dihargai oleh pasar. Dalam konteks pasar modal, investor cenderung memberikan respons positif terhadap perusahaan yang memiliki mekanisme tata kelola yang kuat, karena hal tersebut mengurangi risiko ketidakpastian dan meningkatkan keyakinan terhadap prospek jangka panjang perusahaan.

Dengan demikian, semakin baik kualitas tata kelola teknologi informasi yang diterapkan oleh perusahaan, yang diproksikan melalui keberadaan komite TI atau CISO, maka semakin besar pula respons positif yang diberikan pasar. Hal ini akan tercermin pada peningkatan *cumulative abnormal return* (CAR) perusahaan di bursa. Berdasarkan uraian tersebut, maka hipotesis yang diajukan adalah:

H_2 : Tata kelola teknologi informasi berpengaruh terhadap *market reaction*.

[76] Ahmad Ikhssani, Chandra Mudra, & Fandi Gunawan Prasidya, "The Role of IT Governance in Mitigating Cyber Risks: Evidence from Indonesian Financial and Technology Sectors," *Jurnal Sistem Informasi dan Teknologi*, Vol. 16, No. 1, 2024, hlm. 33-50

3. Pengaruh Keterbukaan *Cybersecurity Risk Disclosure* dan Tata Kelola Teknologi Informasi secara Simultan terhadap *Market Reaction*

Selain secara parsial, keterbukaan *cybersecurity risk disclosure* dan tata kelola teknologi informasi secara bersama-sama juga diduga memengaruhi market reaction. Kedua variabel ini saling melengkapi dalam membentuk persepsi investor terhadap kualitas manajemen risiko perusahaan. Perusahaan yang tidak hanya mengungkapkan risiko *cyber* secara transparan tetapi juga memiliki mekanisme tata kelola TI yang kuat menunjukkan kesungguhan dalam mengelola risiko digital secara menyeluruh.[77]

Investor cenderung lebih percaya pada perusahaan yang menunjukkan konsistensi antara apa yang diungkapkan *(disclosure)* dan apa yang diimplementasikan (tata kelola). Kombinasi keduanya memberikan sinyal yang lebih kuat dibandingkan hanya salah satunya saja. Penelitian tentang kerangka teori pelaporan terintegrasi menunjukkan bahwa perusahaan didorong untuk meningkatkan praktik pengungkapannya karena tiga alasan utama: untuk mengurangi asimetri informasi antara organisasi dan pemangku kepentingan; untuk memberikan sinyal kualitas, legitimasi, dan kesesuaian yang unggul kepada pemangku kepentingan serta untuk menjalankan akuntabilitas kepada pemangku kepentingan.[78] Temuan Solikhawati dan Samsuri memperkuat argumen ini, karena penelitian

---

[77] Nobanee, H., & Ellili, N., "Cybersecurity Disclosure and Firm Value," *Journal of Financial Reporting and Accounting*, Vol. 19, No. 3, 2021, hlm. 425-445

[78] De Haes, S., & Van Grembergen, W., *Enterprise Governance of Information Technology: Achieving Alignment and Value* (Switzerland: Springer, 2015), hlm. 112-135

mereka menunjukkan bahwa bank yang telah memiliki pengungkapan risiko *cyber* yang memadai dalam laporan tahunannya mengalami penurunan harga saham yang lebih kecil saat terjadi insiden *cyber*, dibandingkan dengan bank yang tidak memiliki pengungkapan sebelumnya. Hal ini mengindikasikan bahwa pengungkapan yang baik saja tidak cukup; diperlukan pula tata kelola yang kuat untuk memitigasi dampak negatif insiden di masa mendatang.

Dengan demikian, perusahaan yang memiliki tingkat keterbukaan risiko *cyber* yang tinggi sekaligus tata kelola TI yang baik akan mendapatkan respons pasar yang lebih positif dibandingkan perusahaan yang hanya unggul pada salah satu aspek saja. Berdasarkan uraian tersebut, maka hipotesis yang diajukan adalah:

H_3 : Keterbukaan *cybersecurity risk disclosure* dan tata kelola teknologi informasi secara simultan berpengaruh terhadap *market reaction*.

BAB III

METODE PENELITIAN

A. Jenis Penelitian

Penelitian ini merupakan penelitian kuantitatif dengan tingkat eksplanasi asosiatif yang bertujuan menganalisis hubungan sebab-akibat antara variabel independen (keterbukaan *cybersecurity risk disclosure* dan tata kelola TI) dengan variabel dependen (*market reaction*).[79] Penelitian ini termasuk kategori *ex post facto* dengan data sekunder yang dikumpulkan melalui studi dokumentasi terhadap laporan tahunan, laporan keberlanjutan, dan data pasar modal perusahaan sektor finansial dan teknologi di BEI periode 2020-2024.[80] Pengukuran variabel dilakukan melalui *content analysis*, *dummy variable*, dan penghitungan CAR, yang selanjutnya dianalisis menggunakan statistik inferensial untuk menguji hipotesis.[81]

B. Lokasi dan Waktu Penelitian

Penelitian ini dilaksanakan pada seluruh perusahaan sektor finansial dan teknologi yang tercatat di Bursa Efek Indonesia selama periode 2020-2024, dengan pengumpulan data berlangsung dari Desember 2025 sampai Juli 2026.

---

[79] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D,* (Bandung: Alfabeta, 2019), hlm. 64

[80] Nur Indriantoro dan Bambang Supomo, *Metodologi Penelitian Bisnis untuk Akuntansi dan Manajemen,* (Yogyakarta: BPFE, 2018), hlm. 85

[81] Imam Ghozali, *Aplikasi Analisis Multivariate dengan Program IBM SPSS 25*, Edisi 9, (Semarang: Badan Penerbit Universitas Diponegoro, 2018), hlm. 72

C. Jenis dan Sumber Data

Penelitian ini menggunakan data sekunder kuantitatif yang diperoleh dari sumber-sumber publik resmi. Jenis data yang digunakan adalah:

1. Data kuantitatif berupa skor pengungkapan risiko *cyber* yang diukur melalui *content analysis, variabel dummy* untuk tata kelola TI, nilai *cumulative abnormal return* (CAR).[82]
2. Data kualitatif berupa teks naratif tentang pengungkapan risiko *cyber* dalam laporan tahunan dan keberlanjutan perusahaan dikonversi menjadi data kuantitatif melalui teknik *scoring*.[83] Karena teks tidak dapat langsung diolah secara statistik, peneliti membuat daftar item pengungkapan, memberikan skor 0–2 pada setiap item, lalu menjumlahkannya menjadi indeks skor untuk setiap perusahaan per tahun.[84] Contohnya, perusahaan mungkin menulis: "Kami memiliki kebijakan keamanan data untuk mencegah serangan *cyber*", atau "Tahun ini kami mengalami insiden kecil yang telah ditangani", atau bahkan hanya menyebut risiko secara umum tanpa detail.

   Karena data ini berupa teks (bukan angka), sulit langsung digunakan untuk analisis statistik seperti regresi yang membutuhkan data numerik. Oleh karena itu, peneliti mengonversinya menjadi data kuantitatif melalui teknik scoring (juga disebut *content analysis* dengan pendekatan indeks atau

---

[82] Imam Ghozali, *Aplikasi Analisis Multivariate dengan Program IBM SPSS 25*, Edisi 9, (Semarang: Badan Penerbit Universitas Diponegoro, 2018), hlm. 72

[83] Krippendorff, K., *Content Analysis: An Introduction to Its Methodology*, 4th ed. (California: SAGE Publications, 2019), hlm. 45

[84] Sekaran, U., & Bougie, R., *Research Methods for Business: A Skill-Building Approach*, 7th ed. (United Kingdom: John Wiley & Sons, 2016), hlm. 156

skor).[85] Cara kerjanya yakni peneliti membuat daftar kriteria atau item pengungkapan yang relevan, berdasarkan standar seperti panduan OJK, SEC (untuk contoh internasional), GRI *(Global Reporting Initiative),* atau literatur sebelumnya.[86]

Untuk setiap item, peneliti membaca teks laporan dan memberikan skor. Contoh skala scoring yang umum 0 = Tidak diungkapkan sama sekali (tidak ada mention), 1 = Diungkapkan secara singkat/minimal (hanya disebut sekilas, tanpa detail), 2 = Diungkapkan secara rinci/lengkap (ada penjelasan jelas, contoh, atau data pendukung). Skala ini bisa disesuaikan, misalnya 0-3 atau 0-1 (hanya ada/tidak ada).

Nilai skor ini menjadi variabel kuantitatif (angka) yang bisa dianalisis secara statistik, misalnya diuji hubungannya dengan Cumulative Abnormal Return (CAR) menggunakan regresi.[87] Sumber data primer penelitian ini adalah dokumen-dokumen publik yang terdiri dari:

a. Laporan tahunan dan laporan keberlanjutan perusahaan sektor finansial dan teknologi yang terdaftar di Bursa Efek Indonesia (BEI) periode 2020-2024 yang diakses melalui website resmi perusahaan atau website BEI. (Di sini, teks naratif dari bagian risiko atau governance dibaca dan

[85] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*, (Bandung: Alfabeta, 2019), hlm. 147

[86] Krippendorff, K., *Content Analysis: An Introduction to Its Methodology*, 4th ed. (California: SAGE Publications, 2019), hlm. 45

[87] Sekaran, U., & Bougie, R., *Research Methods for Business: A Skill-Building Approach*, 7th ed. (United Kingdom: John Wiley & Sons, 2016), hlm. 156

diskor seperti dijelaskan di atas untuk mendapatkan variabel "tingkat keterbukaan cybersecurity risk disclosure".)[88]

b. Data harga saham harian untuk perhitungan abnormal return yang diperoleh dari Yahoo Finance, Refinitiv Eikon, atau sumber data pasar modal terpercaya lainnya. (Ini data kuantitatif langsung untuk menghitung CAR sebagai ukuran *market reaction*.)

c. Profil direksi dan komite perusahaan yang diambil dari annual report untuk mengidentifikasi keberadaan komite TI/CISO. (Ini bisa berupa *dummy variable*: 1 jika ada komite TI/CISO, 0 jika tidak – juga bentuk konversi sederhana dari teks profil menjadi angka.)[89]

Seluruh data tersebut dianalisis secara sistematis (misalnya dengan regresi) untuk menjawab rumusan masalah dan menguji hipotesis penelitian. Pendekatan ini memungkinkan penggabungan data teks (kualitatif) dengan data pasar (kuantitatif) secara akurat dan ilmiah.[90]

D. Populasi dan Sampel

1. Populasi

Populasi adalah wilayah generalisasi yang terdiri atas objek/subjek yang mempunyai kualitas dan karakteristik tertentu yang ditetapkan oleh peneliti

---

[88] Nur Indriantoro dan Bambang Supomo, *Metodologi Penelitian Bisnis untuk Akuntansi dan Manajemen*, (Yogyakarta: BPFE, 2018), hlm. 85

[89] De Haes, S., & Van Grembergen, W., *Enterprise Governance of Information Technology: Achieving Alignment and Value*, (Switzerland: Springer, 2015), hlm. 112

[90] Imam Ghozali, *Aplikasi Analisis Multivariate dengan Program IBM SPSS 25*, Edisi 9, (Semarang: Badan Penerbit Universitas Diponegoro, 2018), hlm. 82

untuk dipelajari dan kemudian ditarik kesimpulannya.[91] Populasi dalam penelitian ini adalah seluruh laporan tahunan dan laporan keberlanjutan perusahaan sektor finansial dan teknologi yang terdaftar di Bursa Efek Indonesia periode 2020-2024.

2. Sampel

Penelitian ini menggunakan teknik *purposive sampling* dalam pemilihan sampel, yang menurut Arikunto merupakan teknik pengambilan sampel dengan pertimbangan tertentu yang didasarkan pada tujuan penelitian.[92] Penerapan teknik ini dipandang tepat karena penelitian memerlukan sampel dengan karakteristik khusus yang relevan dengan variabel penelitian, khususnya dalam hal pengungkapan risiko *cyber* dan implementasi tata kelola TI.

Berdasarkan penerapan teknik purposive sampling dengan kriteria yang telah ditetapkan, terpilih 34 perusahaan sebagai sampel penelitian yang terdiri dari perwakilan kedua sektor dengan komposisi yang proporsional.

Tabel 3.1

Daftar Kriteria Pemilihan Sampel

No	Kriteria Penarikan Sampel	Jumlah
1	Perusahaan harus memiliki laporan tahunan yang terbit konsisten periode 2020-2024	113
2	Data harga saham harian tersedia tanpa jeda lebih dari 7 hari berturut-turut	(33)
3	Adanya bagian khusus mengenai risiko *cyber* dan tata kelola TI dalam laporan tahunan	(46)

[91] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D,* (Bandung: Alfabeta, 2019), hlm. 80

[92] Arikunto, S., *Prosedur Penelitian: Suatu Pendekatan Praktik* (Jakarta: Rineka Cipta, 2019), hlm. 178

Jumlah Sampel	34
Periode Penelitian	5
Jumlah Sampel Akhir	**150**

Pemilihan teknik *purposive sampling* dalam penelitian ini didasarkan pada beberapa pertimbangan mendasar. Pertama, penelitian memerlukan perusahaan dengan karakteristik khusus dalam pengungkapan risiko *cyber* dan tata kelola TI yang tidak dimiliki oleh semua perusahaan dalam populasi. Kedua, aspek ketersediaan data menjadi pertimbangan penting di mana hanya perusahaan dengan data lengkap dan konsisten selama periode penelitian yang dapat dianalisis secara komprehensif. Ketiga, teknik ini menjamin kualitas data yang tinggi untuk analisis yang akurat dan valid, mengingat hanya perusahaan dengan pengungkapan yang memadai yang dapat diikutsertakan. Keempat, relevansi penelitian mengharuskan sampel yang dipilih memiliki eksposur signifikan terhadap risiko *cyber* sesuai dengan fokus penelitian. Kelima, pertimbangan efisiensi memungkinkan penelitian dilakukan dengan sumber daya yang terbatas namun tetap menghasilkan temuan yang valid dan reliabel.[93]

Dengan menggunakan teknik purposive sampling, penelitian ini dapat memastikan bahwa sampel yang dianalisis memenuhi persyaratan metodologis dan mampu merepresentasikan fenomena yang diteliti secara komprehensif. Jumlah sampel sebanyak 34 perusahaan dianggap cukup untuk mewakili populasi dengan mempertimbangkan keterbatasan waktu

[93] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019), hlm. 85

dan sumber daya penelitian, sekaligus menjaga kualitas dan kedalaman analisis yang dilakukan. Pemilihan sampel melalui teknik ini juga memungkinkan peneliti untuk fokus pada perusahaan-perusahaan yang benar-benar memiliki praktik pengungkapan risiko *cyber* dan tata kelola TI yang dapat diobservasi dan diukur secara konsisten selama periode penelitian.[94]

E. Defenisi Operasional Variabel

1. Variabel Independen

Variabel independen adalah jenis variabel yang dipandang sebagai penyebab munculnya variabel dependen yang diduga sebagai akibatnya.[95] Dalam penelitian ini, variabel independennya adalah keterbukaan *cybersecurity risk disclosure* (X_1) dan tata kelola teknologi informasi (X_2).

Tabel 3.2
Variabel Operasional Independen dan Pengukurannya

Variabel	Defenisi Operasional	Alat Ukur	Skala Pengukuran
Cybersecurity Risk Disclosure (X_1)	Tingkat kelengkapan informasi tentang risiko *cyber* yang diungkapkan perusahaan dalam laporan tahunan dan laporan keberlanjutan	Item-item pengungkapan risiko *cyber* berdasarkan standar OJK, SEC, atau GRI	Teknik content analysis dengan skor 0-3: 0 = tidak diungkapkan, 1 = disebut secara umum, 2 = dijelaskan 1-2 cara mitigasi, 3 = dijelaskan

[94] Neuman, W. L., *Social Research Methods: Qualitative and Quantitative Approaches*, 7th ed. (Boston: Pearson, 2014), hlm. 248

[95] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019), hlm. 61

			secara rinci dan lengkap[2]
Tata Kelola TI (X_2)	Ada atau tidaknya struktur organisasi khusus yang menangani teknologi informasi dan keamanan *cyber* dalam perusahaan	Keberadaan komite teknologi informasi atau Chief Information Security Officer (CISO) dalam struktur organisasi	Variabel dummy: 1 = ada komite TI atau CISO, 0 = tidak ada

2. Variabel Dependen

Variabel dependen adalah variabel yang diduga sebagai akibat dari variabel independen.[96] Dalam penelitian ini, variabel dependennya adalah *market reaction* (Y).

Tabel 3.3
Variabel Operasional Dependen dan Pengukurannya

Variabel	Defenisi Operasional	Alat Ukur	Skala Pengukuran
Market Reaction (Y)	Respons pasar yang tercermin dari perubahan harga saham perusahaan dalam periode tertentu setelah laporan tahunan diterbitkan	Perubahan harga saham di sekitar tanggal publikasi laporan tahunan	*Cumulative Abnormal Return* (CAR) dihitung dengan mengakumulasi selisih antara *return* aktual dan *return* ekspektasi (*return* pasar) selama 3 hari setelah laporan tahunan diterbitkan

F. Teknik Pengumpulan Data

Teknik pengumpulan data adalah prosedur atau metode atau strategi yang digunakan untuk mengumpulkan data yang akan diteliti. Artinya, teknik ini memerlukan langkah yang strategis dan juga sistematis untuk mendapatkan data

[96] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019), hlm. 61

yang valid dan juga sesuai dengan kenyataannya.[97] Dalam penelitian ini, metode pengumpulan data yang digunakan adalah dokumentasi, di mana data sekunder berupa laporan tahunan, laporan keberlanjutan, dan data harga saham perusahaan sektor finansial dan teknologi yang terdaftar di Bursa Efek Indonesia (BEI) dikumpulkan, dicatat, dan dianalisis.[98] Data ini diperoleh dari website resmi perusahaan, website BEI, serta Yahoo Finance/Refinitiv Eikon, dengan periode waktu yang diteliti adalah tahun 2020 hingga 2024. Laporan tahunan dan laporan keberlanjutan tersebut mencakup informasi mengenai pengungkapan risiko *cyber* serta struktur tata kelola teknologi informasi yang tercatat di dalamnya.

G. Teknik Analisis Data

Analisis data merupakan rangkaian kegiatan yang dilakukan setelah seluruh informasi dari berbagai sumber data terkumpul. Kegiatan ini mencakup pengelompokan data berdasarkan variabel penelitian, penyusunan data dalam bentuk tabel, penyajian setiap variabel yang diteliti, serta perhitungan statistik untuk menjawab rumusan masalah dan menguji hipotesis. Dalam penelitian kuantitatif, teknik analisis data menggunakan metode statistik.[99]

---

[97] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019), hlm. 224

[98] Arikunto, S., *Prosedur Penelitian: Suatu Pendekatan Praktik* (Jakarta: Rineka Cipta, 2019), hlm. 274

[99] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019), hlm. 207

Penelitian ini menggunakan pendekatan kuantitatif untuk menguji pengaruh keterbukaan *cybersecurity risk disclosure* dan tata kelola teknologi informasi terhadap market reaction, dengan bantuan software SPSS versi 26.[100]

1. Statistik Deskriptif

   Statistik deskriptif berfungsi untuk menggambarkan data yang telah dikumpulkan tanpa menarik kesimpulan atau generalisasi.[101] Dalam penelitian ini, statistik deskriptif digunakan untuk menyajikan nilai minimum, maksimum, rata-rata, dan standar deviasi dari seluruh variabel, yaitu *cybersecurity risk disclosure*, tata kelola TI, *market reaction* (CAR).

2. Uji Asumsi Klasik

   Uji asumsi klasik merupakan serangkaian pengujian yang dilakukan untuk memastikan bahwa model regresi memenuhi persyaratan dasar, sehingga hasil analisis dapat diandalkan. Pengujian yang umum dilakukan meliputi uji normalitas, multikolinearitas, heteroskedastisitas, dan autokorelasi. Tujuan dari pengujian ini adalah untuk memastikan residual terdistribusi normal, tidak ada korelasi yang kuat antar variabel bebas, varians residual konstan, dan tidak ada pola tertentu pada residual antar observasi secara berurutan.[102]

---

[100] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 15

[101] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019), hlm. 147

[102] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 19

a. Uji Normalitas

Uji normalitas digunakan untuk mengetahui apakah residual dalam model regresi terdistribusi normal atau tidak. Salah satu metode yang dapat digunakan adalah uji Kolmogorov-Smirnov (K-S) yang tersedia dalam SPSS. Residual dikatakan normal jika nilai signifikansi uji tersebut > 0,05.[103]

b. Uji Multikolinieritas

Uji multikolinieritas bertujuan untuk mendeteksi adanya korelasi antar variabel independen dalam model. Model regresi yang baik seharusnya bebas dari multikolinieritas. Deteksi dapat dilakukan dengan melihat nilai VIF dan *Tolerance.* Model bebas multikolinieritas jika nilai VIF < 10 dan *Tolerance* > 0,10.[104]

c. Uji Heteroskedastisitas

Uji heteroskedastisitas digunakan untuk mengetahui apakah varians residual berbeda antar observasi. Jika varians berbeda, maka terjadi heteroskedastisitas. Deteksi dapat dilakukan melalui *grafik scatterplot* atau uji statistik seperti *Glejser.* Model regresi yang baik adalah ketika pola pada grafik scatterplot tidak menunjukkan bentuk tertentu, seperti pengelompokan di tengah, pola yang melebar, menyempit, atau semakin mengecil.[105]

---

[103] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 105

[104] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 110

[105] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 107

d. Uji Autokorelasi

Uji autokorelasi dengan metode Durbin-Watson digunakan untuk mendeteksi korelasi antar residual dalam model regresi. Autokorelasi dapat mengganggu efisiensi estimasi. Nilai DW berkisar antara 0 hingga 4. Nilai DW mendekati 2 menunjukkan tidak ada autokorelasi, sedangkan nilai mendekati 0 menunjukkan autokorelasi positif dan mendekati 4 menunjukkan autokorelasi negatif.[106]

3. Analisis Regresi Linier Berganda

Analisis regresi linier berganda adalah teknik statistik yang digunakan untuk menganalisis hubungan antara variabel terikat dengan dua atau lebih variabel bebas. Tujuannya adalah untuk menentukan garis regresi yang paling sesuai dan memprediksi nilai variabel dependen berdasarkan variabel independen.[107]

Penelitian ini menggunakan regresi linier berganda untuk menguji pengaruh *cybersecurity risk disclosure* (X_1) dan tata kelola TI (X_2) terhadap *market reaction* (Y). Model regresi yang digunakan adalah:

$$Y = \boldsymbol{\alpha}+\boldsymbol{\beta 1 X 1}+\boldsymbol{\beta 2 X 2}+\boldsymbol{e}$$

Keterangan:

Y = Market Reaction

α = Konstanta

[106] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 139

[107] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 111

$\boldsymbol{\beta}$ = Koefisien Regresi

X_1 = *Cybersecurity Risk Disclosure*

X_2 = Tata Kelola TI

$\boldsymbol{e}$ = Standar Error

4. Uji Hipotesis

   a. Uji Koefisien Determinasi (Adjusted R^2)

      Koefisien determinasi digunakan untuk mengukur seberapa besar kemampuan model dalam menjelaskan variasi variabel dependen. Nilai *Adjusted* R^2 berkisar antara 0 dan 1. Semakin tinggi nilainya, semakin baik model dalam menjelaskan variabel dependen. Untuk data *cross section*, nilai R^2 cenderung rendah karena variasi antar pengamatan besar, sedangkan untuk data *time series* nilainya cenderung tinggi.[108]

   b. Uji t (Parsial)

      Uji t digunakan untuk mengetahui pengaruh masing-masing variabel independen secara parsial terhadap variabel dependen. Pengujian dilakukan dengan membandingkan t hitung dengan t tabel atau melihat nilai signifikansi. Pengambilan keputusan dalam uji t dilakukan dengan membandingkan nilai t hitung dengan t tabel atau dengan melihat signifikansi yang ditetapka ($\alpha = 0{,}05$), maka hipotesis alternatif diterima yang berarti variabel independen tersebut berpengaruh signifikan

[108] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10, (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 97

terhadap variabel dependen. Sebaliknya apabila signifikansi lebih besar dari 0,05 maka hipotesis alternatif ditolak.[109]

c. Uji F (Simultan)

Uji F digunakan untuk menguji apakah semua variabel independen memiliki pengaruh simultan terhadap variabel dependen. Uji ini digunakan untuk mengetahui apakah semua variabel independen memiliki pengaruh yang signifikan terhadap variabel dependen. Nilai F yang signifikan menunjukkan bahwa semua variabel independen memiliki pengaruh simultan terhadap variabel dependen. Hasil uji ststistik F dapat dilihat pada output SPSS yaitu pada tabel ANOVA. Jika nilai Sig. > 0,05 maka dinyatakan tidak signifikan, dan jika nilai Sig. < 0,05 maka dinyatakan signifikan.47 Uji F juga dapat diuji menggunakan statistif F hitung yang dibandingkan dengan F tabel, yang dimana H0 ditolak jika F hitung > F tabel. Jika H0 diterima berarti tidak terdapat pengaruh yang signifikan antara variabel independen terhadap variabel dependen. Sebaliknya jika H0 ditolak, maka terdapat pengaruh yang signifikan antara variabel independen terhadap variabel dependen atau dengan kata lain persamaan regresi layak untuk digunakan. [110]

---

[109] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019), hlm. 255

[110] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 99

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

A. Gambaran Umum Objek Penelitian

Objek penelitian dalam skripsi ini adalah perusahaan sektor finansial dan teknologi yang terdaftar di Bursa Efek Indonesia (BEI) selama periode 2020-2024. Perusahaan-perusahaan tersebut dipilih karena sektor finansial dan teknologi merupakan sektor dengan ketergantungan tertinggi terhadap sistem teknologi informasi serta memiliki eksposur risiko *cyber* yang signifikan dibandingkan sektor lainnya. Aktivitas usaha di sektor finansial melibatkan pengelolaan data nasabah dalam skala besar, transaksi keuangan digital, serta kepatuhan terhadap regulasi perbankan dan pasar modal, sementara sektor teknologi mengelola platform digital dan data pengguna yang rentan terhadap serangan *cyber*. Kedua sektor ini menuntut adanya tata kelola teknologi informasi yang kuat serta transparansi dalam pengungkapan risiko *cyber* guna menjaga kepercayaan investor dan pemangku kepentingan lainnya.

Bursa Efek Indonesia sebagai bursa efek utama di Indonesia berperan penting dalam menyediakan akses data keuangan dan harga saham perusahaan publik. Hingga tahun 2024, jumlah perusahaan yang terdaftar di BEI mencapai lebih dari 900 emiten yang tersebar dalam berbagai sektor. Meskipun sektor finansial dan teknologi tidak mendominasi dari segi kuantitas, kontribusinya terhadap kapitalisasi pasar cukup signifikan dan menarik perhatian investor. Kedua sektor ini menjadi penggerak utama pertumbuhan ekonomi digital di Indonesia, seiring dengan meningkatnya penetrasi internet dan adopsi teknologi

digital pasca pandemi COVID-19. Perusahaan di sektor finansial, seperti perbankan, asuransi, dan perusahaan pembiayaan, telah bertransformasi secara digital dengan meluncurkan berbagai layanan perbankan elektronik yang memungkinkan nasabah melakukan transaksi secara instan dan aman. Sementara itu, sektor teknologi yang mencakup perusahaan jasa teknologi informasi dan perangkat lunak terus berkembang pesat seiring dengan meningkatnya kebutuhan akan solusi digital di berbagai aspek kehidupan.

Sektor finansial di BEI terdiri atas beberapa sub-sektor, antara lain perbankan, asuransi, perusahaan pembiayaan, dan lembaga keuangan lainnya. Sub-sektor perbankan merupakan yang paling dominan dengan jumlah emiten terbanyak. Sektor ini memiliki tingkat sensitivitas yang tinggi terhadap risiko *cyber* karena mengelola data nasabah dalam skala besar serta menjadi tulang punggung sistem pembayaran nasional. Regulasi dari Bank Indonesia dan Otoritas Jasa Keuangan (OJK) juga mewajibkan lembaga keuangan untuk melakukan pengungkapan risiko operasional secara transparan, termasuk risiko *cyber*, sehingga menjadikan sektor ini relevan dengan fokus penelitian. Perusahaan perbankan seperti Bank Central Asia, Bank Mandiri, Bank Rakyat Indonesia, dan Bank Negara Indonesia telah menjadi pelopor transformasi digital di sektor finansial dengan menghadirkan berbagai inovasi layanan digital yang memudahkan nasabah dalam mengakses produk perbankan. Namun, transformasi digital ini juga membawa tantangan baru berupa peningkatan risiko *cyber* yang harus dikelola dengan baik melalui pengungkapan yang transparan dan tata kelola TI yang kuat.

Sementara itu, sektor teknologi di BEI berkembang lebih lambat dibandingkan sektor finansial, namun menunjukkan tren pertumbuhan yang positif seiring dengan pesatnya adopsi digital di Indonesia. Emiten teknologi yang terdaftar umumnya bergerak di bidang jasa teknologi informasi dan pengembangan perangkat lunak. Meskipun jumlahnya tidak sebanyak sektor finansial, saham-saham teknologi mendapatkan perhatian yang besar dari investor karena potensi pertumbuhannya yang tinggi. Perusahaan di sektor ini juga memiliki eksposur risiko *cyber* yang tidak kalah besar, mengingat mereka mengelola data pengguna dalam jumlah besar dan sangat bergantung pada keamanan sistem informasi. Perusahaan seperti Telekomunikasi Indonesia, GoTo, dan Bukalapak menjadi contoh emiten teknologi yang terus berinovasi dan memperluas jangkauan layanan digital mereka, namun juga menghadapi tantangan keamanan *cyber* yang semakin kompleks.

Periode penelitian tahun 2020-2024 dipilih karena rentang waktu ini mencakup masa pandemi COVID-19 hingga masa pemulihan ekonomi, di mana aktivitas digital dan insiden *cyber* mengalami peningkatan yang pesat. Pandemi COVID-19 telah memaksa perusahaan untuk beradaptasi dengan cepat terhadap lingkungan digital, yang pada gilirannya meningkatkan kerentanan terhadap serangan *cyber*. Selama periode ini, berbagai insiden *cyber* besar terjadi di Indonesia, termasuk kebocoran data di beberapa institusi keuangan dan platform digital, yang menyoroti pentingnya pengungkapan risiko *cyber* dan tata kelola TI yang memadai. Dengan rentang waktu lima tahun, data yang terkumpul dinilai cukup representatif untuk melihat pola pengungkapan risiko

cyber dan implementasi tata kelola TI di perusahaan sektor finansial dan teknologi di Indonesia.

Data yang digunakan dalam penelitian ini berupa data sekunder, yaitu laporan tahunan, laporan keberlanjutan, dan data harga saham harian, yang diperoleh dari situs resmi Bursa Efek Indonesia, situs perusahaan terkait, serta Yahoo Finance atau Refinitiv Eikon. Laporan tahunan dan laporan keberlanjutan menjadi sumber utama untuk mengukur tingkat keterbukaan *cybersecurity risk disclosure* dan keberadaan struktur tata kelola TI, sementara data harga saham digunakan untuk menghitung cumulative abnormal return (CAR) sebagai proksi market reaction. Penggunaan data sekunder ini memungkinkan peneliti untuk menganalisis secara objektif praktik pengungkapan risiko *cyber* dan tata kelola TI yang dilakukan oleh perusahaan selama periode penelitian.

Berdasarkan kriteria pemilihan sampel yang telah ditetapkan melalui teknik purposive sampling, perusahaan yang menjadi objek penelitian adalah perusahaan sektor finansial dan teknologi yang secara konsisten menerbitkan laporan tahunan dan laporan keberlanjutan selama periode 2020-2024, serta memiliki data harga saham yang lengkap untuk menghitung cumulative abnormal return (CAR). Dari populasi awal sebanyak 78 perusahaan (58 perusahaan sektor finansial dan 20 perusahaan sektor teknologi), setelah melalui proses seleksi yang ketat, diperoleh 34 perusahaan yang memenuhi seluruh kriteria. Namun, setelah dilakukan pengujian outlier terhadap data CAR, ditemukan 3 perusahaan dengan nilai ekstrem sehingga dikeluarkan dari

sampel. Dengan demikian, sampel final dalam penelitian ini berjumlah 31 perusahaan yang terdiri dari perwakilan kedua sektor dengan komposisi yang proporsional.

Dengan karakteristik tersebut, perusahaan-perusahaan yang dijadikan objek penelitian dinilai mampu memberikan gambaran yang jelas mengenai pengaruh keterbukaan *cybersecurity risk disclosure* dan tata kelola teknologi informasi terhadap market reaction di pasar modal Indonesia. Penelitian ini diharapkan dapat memberikan kontribusi empiris bagi literatur mengenai pengaruh *cybersecurity risk disclosure* dan tata kelola TI terhadap market reaction di pasar modal Indonesia, mengingat topik ini masih jarang diteliti secara khusus di Indonesia. Selain itu, hasil penelitian ini diharapkan dapat menjadi masukan bagi regulator, khususnya Otoritas Jasa Keuangan (OJK), dalam menyusun kebijakan dan standar pengungkapan risiko *cyber* yang lebih komprehensif, serta menjadi panduan bagi perusahaan dan investor dalam memahami pentingnya transparansi risiko *cyber* dan tata kelola TI dalam menjaga stabilitas pasar modal.

B. Hasil Penelitian

1. Statistik Deskriptif

Statistik deskriptif merupakan teknik analisis data yang digunakan untuk memberikan gambaran umum mengenai karakteristik data penelitian. Analisis ini bertujuan untuk mendeskripsikan data sebagaimana adanya.[111]

[111] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019), hlm. 147

Dalam penelitian ini, statistik deskriptif digunakan untuk menggambarkan variabel *cybersecurity risk disclosure*, tata kelola teknologi informasi, dan *market reaction* pada perusahaan sektor finansial dan teknologi yang terdaftar di Bursa Efek Indonesia selama periode 2020-2024. Informasi yang disajikan dalam analisis ini yaitu nilai minimum, nilai maksimum, nilai rata-rata (*mean*), dan standar deviasi.[112]

Penelitian ini menggunakan data sekunder berupa laporan tahunan, laporan keberlanjutan, dan data harga saham perusahaan sektor finansial dan teknologi yang terdaftar di Bursa Efek Indonesia periode 2020-2024. Berdasarkan kriteria *purposive sampling* yang telah ditetapkan, diperoleh sampel awal sebanyak 34 perusahaan dengan total observasi 170 (34 perusahaan × 5 tahun). Namun, sebelum dilakukan analisis lebih lanjut, terlebih dahulu dilakukan prosedur pembersihan data (*data cleaning*) untuk memastikan kualitas data yang digunakan dalam penelitian. Langkah awal dalam prosedur pembersihan data adalah melakukan pengujian *outlier* terhadap variabel dependen yaitu *Market Reaction* yang diukur dengan *Cumulative Abnormal Return* (CAR). *Outlier* didefinisikan sebagai observasi yang memiliki karakteristik unik yang sangat berbeda dari observasi lainnya dan muncul dalam bentuk nilai ekstrem, baik untuk sebuah variabel tunggal maupun variabel kombinasi.[113] Keberadaan *outlier* dalam data dapat menyebabkan distorsi terhadap hasil

[112] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 19

[113] Santoso, S., *Statistik Multivariat: Konsep dan Aplikasi dengan SPSS* (Jakarta: Elex Media Komputindo, 2022), hlm. 45.

analisis regresi, seperti meningkatkan *standard error*, menurunkan kekuatan uji statistik, serta menghasilkan koefisien regresi yang bias atau tidak stabil.[114]

Tabel 4.1
Hasil Statistik Deskriptif Sebelum Outlier

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity Risk Disclosure	170	.00	3.00	2.0059	.76535
Tata Kelola	170	.00	1.00	.5765	.49558
Market reaction	170	-3443984332.00	506799557.00	-30499185.1471	303179254.03346
Valid N (listwise)	170				

Sumber: Data diolah SPSS, 2026

Berdasarkan Tabel 4.1 di atas dapat diketahui bahwa data yang dianalisis sebanyak 170 data, yang berasal dari laporan tahunan, laporan keberlanjutan, dan data harga saham perusahaan sektor finansial dan teknologi selama periode 2020-2024. Jumlah 170 ini didapat dari 34 sampel perusahaan dikali 5 tahun penelitian. Berdasarkan hasil analisis awal, diketahui bahwa persebaran data masih menunjukkan adanya nilai ekstrim pada variabel *market reaction*. Keberadaan data ekstrim tersebut berpotensi mempengaruhi hasil analisis statistik lanjutan, khususnya terkait pemenuhan asumsi normalitas, heteroskedastisitas, dan linearitas.[115]

Oleh karena itu, dilakukan analisis *outlier* sebagai langkah untuk mengidentifikasi dan mengeluarkan data yang tidak memenuhi kriteria. Hasil analisis menunjukkan bahwa terdapat 3 perusahaan (15 data

[114] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 36

[115] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 105

observasi) yang tergolong ekstrim dan menyebabkan distribusi data tidak normal, sehingga data tersebut dikeluarkan dari sampel penelitian. Dengan demikian, jumlah sampel yang digunakan dalam analisis selanjutnya adalah sebanyak 155 data (31 perusahaan × 5 tahun).

Tabel 4.2

Hasil Statistik Deskriptif Setelah Outlier

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity Riskdisclosure	155	1	3	2.03	.725
Tata Kelola TI	155	0	1	.60	.491
Market Reaction	155	-.406406643	.506799557	-.00017295993	.087822110663
Valid N (listwise)	155				

Sumber: Data diolah SPSS,2026

Berdasarkan Tabel 4.2 di atas, dapat diketahui gambaran statistik dari masing-masing variabel yang digunakan dalam penelitian. Variabel *cybersecurity risk disclosure* memiliki nilai minimum 1 dan nilai maksimum 3, dengan nilai rata-rata 2,03. Hasil tersebut menunjukkan bahwa setelah *outlier* dihilangkan, tingkat pengungkapan risiko *cyber* antar perusahaan cenderung lebih seragam, yang juga tercermin dari nilai standar deviasi yang menurun menjadi 0,725. Nilai rata-rata 2,03 menunjukkan bahwa rata-rata perusahaan sampel memiliki tingkat pengungkapan risiko *cyber* yang berada pada kategori sedang atau cukup baik.

Variabel tata kelola TI memiliki nilai minimum 0 dan maksimum 1, dengan nilai rata-rata sebesar 0,60. Nilai ini menunjukkan bahwa setelah

penghapusan *outlier*, proporsi perusahaan yang menerapkan tata kelola TI atau memiliki komite TI atau CISO adalah sebesar 60% dari total sampel. Standar deviasi sebesar 0,491 menunjukkan adanya variasi penerapan tata kelola TI yang cukup seimbang antar perusahaan.

Variabel *market reaction* memiliki nilai minimum -0,406406643 dan maksimum 0,506799557, dengan nilai rata-rata sebesar -0,000172960. Rentang nilai yang semakin sempit serta nilai standar deviasi sebesar 0,087822111 menunjukkan bahwa perbedaan reaksi pasar antar perusahaan setelah penghapusan *outlier* menjadi lebih kecil dan stabil. Nilai rata-rata yang mendekati nol mengindikasikan bahwa rata-rata reaksi pasar di sekitar periode pengumuman cenderung menunjukkan pergerakan atau *return* tidak normal yang sangat tipis di area negatif. Dengan demikian, data *market reaction* setelah penghapusan *outlier* dinilai lebih stabil dan representatif untuk digunakan dalam pengujian asumsi klasik dan analisis regresi.[116]

2. Uji Asumsi Klasik

Uji asumsi klasik digunakan agar data sampel yang diolah dapat mewakili populasi secara keseluruhan. Uji asumsi klasik terdiri dari uji normalitas, uji multikolinieritas, uji heteroskedastisitas, dan uji autokorelasi.[117]

---

[116] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 9

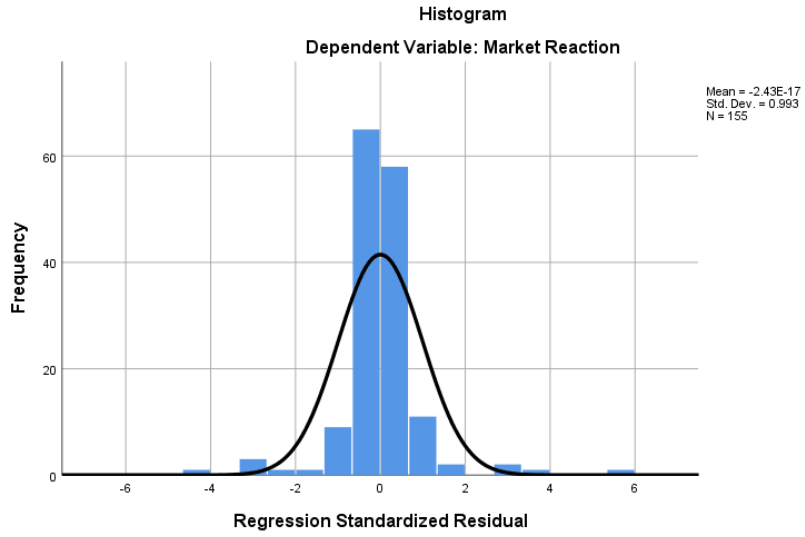
[117] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm.105

a. Uji Normalitas

Menurut Ghozali, uji normalitas bertujuan untuk mengetahui apakah residual dalam model regresi menyebar secara normal atau tidak. Uji normalitas juga melihat apakah model regresi yang digunakan memiliki distribusi normal atau mendekati normal. Data residual dinyatakan berdistribusi normal apabila signifikansi uji Kolmogorov-Smirnov > 0,05.

Pengujian normalitas dalam penelitian ini dilakukan secara visual melalui grafik Histogram dan Normal P-P Plot, serta secara statistik melalui uji One-Sample Kolmogorov-Smirnov (K-S).[118]

Gambar 4.1
Grafik Histogram



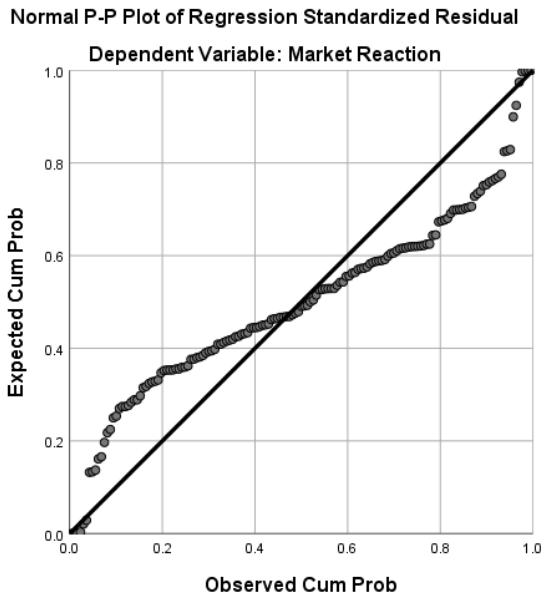
Sumber: data diolah SPSS, 2026

Berdasarkan grafik Histogram pada Gambar 4.1, terlihat bahwa garis melengkung hitam (*bell-shaped curve*) telah membentuk pola

[118] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 110

lonceng yang simetris dan seimbang, berpusat di sekitar angka 0. Batang-batang diagram bervariasi secara bertahap dan mayoritas tiang frekuensi berada di dalam alur garis lengkung kurva normal tersebut, tanpa adanya data pencilan ekstrem yang memisahkan diri di ujung kiri maupun kanan secara radikal.[119] Secara visual, sebaran data residual pada model regresi ini menunjukkan pola yang mengikuti kurva normal (*bell-shaped*), sehingga berdasarkan pendekatan grafik Histogram, dapat disimpulkan bahwa data residual dalam penelitian ini telah memenuhi asumsi normalitas.

Gambar 4.2
Grafik *Normal P-P Plot Of Regression Standardized Residual*.



Sumber: Data diolah SPSS, 2026

Untuk memperkuat hasil grafik histogram, pengujian visual selanjutnya menggunakan grafik *Normal P-P Plot of Regression*

[119] Santoso, S., *Statistik Multivariat: Konsep dan Aplikasi dengan SPSS* (Jakarta: Elex Media Komputindo, 2022), hlm. 78

Standardized Residual. Dasar pengambilan keputusan pada grafik *Normal P-P Plot* adalah jika titik-titik menyebar di sekitar garis diagonal dan mengikuti arah garis diagonal tersebut, maka model regresi memenuhi asumsi normalitas. Berdasarkan Gambar 4.2, terlihat bahwa titik-titik data menyebar di sekitar garis diagonal serta mengikuti arah garis diagonal tersebut secara konsisten dari ujung kiri bawah hingga kanan atas. Melalui pendekatan kedua grafik di atas, secara visual dapat disimpulkan bahwa data residual dalam penelitian ini telah memenuhi asumsi normalitas.

Tabel 4.3
Hasil Uji Normalitas
One-Sample Kolmogorov-Smirnov Test

		Unstandardized Residual
N		155
Normal Parameters[a,b]	Mean	.0000000
	Std. Deviation	.08608958
Most Extreme Differences	Absolute	.165
	Positive	.164
	Negative	-.165
Test Statistic		.165
Asymp. Sig. (2-tailed)		.000[c]
a. Test distribution is Normal.		
b. Calculated from data.		
c. Lilliefors Significance Correction.		

Sumber: Data diolah SPSS, 2026

Untuk mendukung hasil analisis grafik agar lebih objektif dan akurat secara statistik, dilakukan uji statistik *One-Sample Kolmogorov-Smirnov* dengan dasar keputusan jika nilai *Asymp. Sig. (2-tailed)* > 0,05, maka data berdistribusi normal. Berdasarkan Tabel 4.3 di atas, diperoleh nilai *Asymp. Sig. (2-tailed)* sebesar 0,000. Nilai tersebut lebih kecil dari taraf signifikansi 0,05 (0,000 < 0,05). Secara pengujian statistik murni,

hasil ini menunjukkan nilai residual belum berdistribusi normal. Adanya perbedaan kesimpulan antara hasil visual grafik (Histogram dan *Normal P-P Plot* yang menunjukkan normal) dan uji statistik Kolmogorov-Smirnov (yang menunjukkan 0,000) disebabkan oleh karakteristik variabel dependen dalam penelitian ini, yaitu *Market Reaction* yang diukur menggunakan *Cumulative Abnormal Return* (CAR). Data pasar modal memiliki fluktuasi harian dan tingkat volatilitas yang sangat tinggi, sehingga uji statistik berbasis parameter ketat seperti Kolmogorov-Smirnov menjadi sangat sensitif terhadap deviasi sekecil apa pun dan cenderung menghasilkan nilai signifikansi yang rendah pada sampel besar.

Oleh karena itu, ketidaknormalan secara statistik pada jumlah sampel sebanyak 155 data ini diatasi dengan bersandar pada Teorema Limit Pusat (*Central Limit Theorem*). Berdasarkan Teorema Limit Pusat, apabila jumlah sampel atau pengamatan yang digunakan berukuran besar atau lebih dari 30 (N > 30), maka asumsi normalitas dapat diabaikan karena distribusi sampling residual akan mendekati normal dengan sendirinya seiring bertambahnya jumlah sampel.[120] Mengingat hasil grafik Histogram dan *Normal P-P Plot* secara visual sudah menunjukkan sebaran data yang ideal dan mengikuti arah normal, serta jumlah sampel penelitian yang digunakan berukuran besar (155 >

[120] Imam Ghozali, *Aplikasi Analisis Multivariate dengan Program IBM SPSS 25*, Edisi 9, (Semarang: Badan Penerbit Universitas Diponegoro, 2018), hlm. 105

30), maka model regresi ini dinyatakan tetap aman, valid, dan layak digunakan untuk analisis regresi linear berganda serta pengujian hipotesis selanjutnya.

b. Uji Multikolinieritas

Uji multikolinieritas bertujuan untuk mengidentifikasi ada atau tidaknya korelasi yang tinggi antar variabel independen dalam model regresi. Pengujian ini dilakukan untuk memastikan bahwa setiap variabel independen mampu menjelaskan variabel dependen secara mandiri tanpa dipengaruhi secara signifikan oleh variabel independen lainnya.[121] Model regresi dinyatakan tidak mengalami multikolinieritas apabila nilai *tolerance* > 0,10 dan nilai VIF < 10. Nilai *tolerance* yang tinggi menunjukkan rendahnya tingkat korelasi antar variabel independen, sedangkan VIF yang kecil mengidentifikasikan bahwa variabel bebas tidak saling mempengaruhi secara berlebihan.

Tabel 4.4
Hasil Uji Multikolinieritas

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.049	.021		-2.333	.021		
	Cybersecurity Riskdisclosure	.026	.011	.218	2.358	.020	.739	1.353
	Tata Kelola TI	-.009	.017	-.049	-.526	.600	.739	1.353

a. Dependent Variable: Market Reaction

Sumber: data diolah SPSS, 2026

[121] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 110

Berdasarkan Tabel 4.4 di atas diketahui bahwa variabel *cybersecurity risk disclosure* dan tata kelola TI masing-masing memiliki nilai *tolerance* sebesar 0,739 dan nilai VIF sebesar 1,353. Dari hasil tabel tersebut menunjukkan bahwa nilai *tolerance* > 0,10 dan nilai VIF < 10, maka dapat disimpulkan bahwa data dalam penelitian ini tidak terjadi multikolinieritas dalam model regresinya.[122]

c. Uji Heteroskedastisitas

Uji heteroskedastisitas bertujuan untuk menguji apakah dalam model regresi terjadi ketidaksamaan varians dari residual satu pengamatan ke pengamatan yang lain. Jika varians dari residual satu pengamatan ke pengamatan lain tetap, maka disebut homoskedastisitas dan jika berbeda disebut heteroskedastisitas. Model regresi yang baik adalah model regresi yang memenuhi asumsi homoskedastisitas atau dengan kata lain tidak terjadi gejala heteroskedastisitas di dalam modelnya.[123]

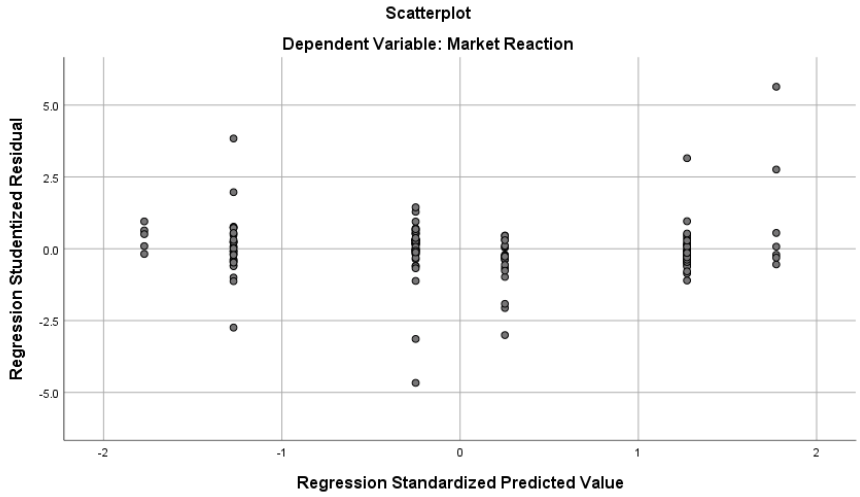
Dalam penelitian ini, metode yang digunakan untuk mendeteksi ada atau tidaknya gejala heteroskedastisitas adalah melalui analisis grafik *Scatterplot* dengan melihat pola persebaran titik-titik antara nilai prediksi variabel dependen (*ZPRED*) dengan nilai residualnya (*SRESID*). Kriteria pengujian menyatakan bahwa jika tidak ada pola tertentu yang jelas pada grafik, seperti titik-titik yang membentuk pola

[122] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 107

[123] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 139

tertentu yang teratur (bergelombang, melebar kemudian menyempit), serta titik-titik data menyebar secara acak baik di atas maupun di bawah angka 0 pada sumbu Y, maka disimpulkan tidak terjadi heteroskedastisitas.[124]

Gambar 4.3
Grafik *Scatterplot*



Sumber: data diolah SPSS, 2026

Berdasarkan hasil visualisasi grafik *Scatterplot* pada model final dengan jumlah sampel sebanyak 155 perusahaan yang disajikan pada Gambar 4.3, terlihat bahwa titik-titik data telah menyebar secara acak dan bervariasi di atas maupun di bawah angka 0 pada sumbu Y. Pola persebaran data tidak mengumpul hanya di satu tempat, tidak membentuk gelombang, tidak membentuk pola garis lurus horizontal, dan tidak membentuk pola runcing melebar ataupun menyempit. Seluruh titik pengamatan menyebar secara merata dan natural di dalam

[124] Santoso, S., *Statistik Multivariat: Konsep dan Aplikasi dengan SPSS* (Jakarta: Elex Media Komputindo, 2022), hlm. 85

ruang grafik tanpa didominasi oleh titik pencilan ekstrem setelah dilakukannya prosedur pembersihan data *outlier*.

Dengan demikian, hasil analisis visual ini memberikan kesimpulan empiris yang kuat bahwa model regresi linear berganda dalam penelitian ini telah sepenuhnya terbebas dari masalah asumsi klasik heteroskedastisitas, sehingga estimasi hubungan antar variabel dinyatakan valid dan objektif.[125]

d. Uji Autokorelasi

Uji autokorelasi bertujuan untuk menguji apakah terdapat hubungan atau korelasi antara residual pada satu pengamatan dengan residual pada pengamatan lainnya dalam model regresi. Pengujian ini dilakukan untuk memastikan bahwa residual bersifat independen dan tidak saling mempengaruhi antar periode pengamatan. Gejala autokorelasi dapat dideteksi dengan menggunakan uji Durbin-Watson (DW). Dasar pengambilan keputusan dapat dilihat jika Durbin-Watson terletak di antara dU dan 4 - dU artinya tidak terjadi autokorelasi. Model regresi yang baik adalah tidak terjadi autokorelasi. Menurut Ghozali, interpretasi uji Durbin-Watson dapat dilihat melalui rentang nilai statistik DW sebagai berikut: DW < 1,5 berarti terjadi autokorelasi positif, 1,5 ≤ DW ≤ 2,5 berarti tidak terjadi autokorelasi, dan DW > 2,5 berarti terjadi autokorelasi negatif.[126]

---

[125] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 139

[126] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 111

Tabel 4.5
Hasil Uji Autokorelasi
Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.198[a]	.039	.026	.086654102972	1.736
a. Predictors: (Constant), Tata Kelola TI, Cybersecurity Riskdisclosure					
b. Dependent Variable: Market Reaction					

Sumber:data diolah SPSS, 2026

Berdasarkan Tabel 4.5 di atas diperoleh nilai Durbin-Watson (DW) sebesar 1,736. Nilai ini kemudian dibandingkan dengan nilai tabel menggunakan derajat kepercayaan 5% dengan jumlah sampel 155 dan 2 variabel independen. Maka dari tabel DW didapatkan nilai dU sebesar 1,772 dan nilai 4 - dU sebesar 2,228. Kriteria untuk penilaian terjadinya autokorelasi yaitu DW > dU dan DW < 4 - dU. Berdasarkan perhitungan tersebut, nilai DW sebesar 1,736 berada di antara $1,5 \leq DW \leq 2,5$, maka dapat disimpulkan bahwa DW-test tidak terjadi autokorelasi.[127]

3. Analisis Regresi Linier Berganda

Analisis regresi linear berganda digunakan untuk mengetahui arah dan besarnya pengaruh variabel independen yang terdiri dari *Cybersecurity Risk Disclosure* (X_1) dan Tata Kelola TI (X_2) terhadap variabel dependen yaitu *Market Reaction* (Y). Pengujian ini dilakukan menggunakan nilai *Unstandardized Coefficients* (B) pada tabel *Coefficients*.

[127] Santoso, S., *Statistik Multivariat: Konsep dan Aplikasi dengan SPSS* (Jakarta: Elex Media Komputindo, 2022), hlm. 95

Tabel 4.6
Hasil Uji Regresi Linier Berganda

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.049	.021		-2.333	.021		
	Cybersecurity Riskdisclosure	.026	.011	.218	2.358	.020	.739	1.353
	Tata Kelola TI	-.009	.017	-.049	-.526	.600	.739	1.353
a. Dependent Variable: Market Reaction								

Sumber: Data diolah SPSS, 2026

Berdasarkan hasil data pada Tabel 4.6 di atas, maka rumus persamaan regresi linear berganda dalam penelitian ini adalah sebagai berikut:

$Y = -0{,}049 + 0{,}026X_1 - 0{,}009X_2 + e$

Keterangan:

Y = *Market Reaction* (Cumulative Abnormal Return/CAR)

-0,049 (α) = Konstanta, menunjukkan nilai *Market Reaction* ketika variabel independen (X_1 dan X_2) bernilai nol atau konstan

0,026 (β_1) = Koefisien regresi variabel *Cybersecurity Risk Disclosure*; menunjukkan besarnya pengaruh X_1 terhadap Y

-0,009 (β_2) = Koefisien regresi variabel Tata Kelola TI; menunjukkan besarnya pengaruh X_2 terhadap Y

X_1 = *Cybersecurity Risk Disclosure* (skor pengungkapan risiko *cyber*)

X_2 = Tata Kelola TI (variabel dummy: 1=ada komite TI/CISO, 0=tidak ada)

e = *Standar error* (faktor pengganggu di luar model)

Persamaan regresi di atas dapat diinterpretasikan sebagai berikut:

a. Nilai Konstanta (α) sebesar -0,049 menunjukkan bahwa jika variabel *Cybersecurity Risk Disclosure* (X_1) dan Tata Kelola TI (X_2) nilainya adalah konstan atau 0, maka nilai variabel *Market Reaction* (Y) adalah sebesar -0,049. Artinya, tanpa adanya pengungkapan risiko *cyber* dan tata kelola TI, reaksi pasar cenderung negatif meskipun dalam jumlah yang sangat kecil.
b. Koefisien Regresi *Cybersecurity Risk Disclosure* (β_1) sebesar 0,026 menunjukkan bahwa variabel *Cybersecurity Risk Disclosure* memiliki hubungan yang searah (positif) dengan *Market Reaction*. Jika tingkat pengungkapan risiko *cyber* meningkat sebesar 1 satuan (sedangkan variabel lainnya konstan), maka nilai *Market Reaction* akan mengalami peningkatan sebesar 0,026.[29] Hal ini mengindikasikan bahwa semakin tinggi skor pengungkapan risiko *cyber* yang dilakukan perusahaan, semakin besar pula respons positif yang diberikan oleh pasar.
c. Koefisien Regresi Tata Kelola TI (β_2) sebesar -0,009 menunjukkan bahwa variabel Tata Kelola TI memiliki hubungan yang berlawanan arah (negatif) dengan *Market Reaction*. Jika penerapan tata kelola TI meningkat sebesar 1 satuan (dari tidak memiliki komite TI/CISO menjadi memilikinya), maka nilai *Market Reaction* diprediksi akan mengalami penurunan tipis sebesar 0,009.[128] Namun, karena nilai koefisien ini sangat kecil dan tidak signifikan secara statistik (p-value

[128] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 97

0,600 > 0,05), pengaruh negatif ini tidak dapat dianggap sebagai temuan yang valid secara statistik. Dengan kata lain, meskipun secara matematis koefisiennya negatif, secara statistik variabel ini tidak terbukti berpengaruh terhadap *Market Reaction*.

Model persamaan regresi ini menunjukkan bahwa dari kedua variabel independen yang diuji, hanya *Cybersecurity Risk Disclosure* yang memiliki pengaruh signifikan terhadap *Market Reaction*, sementara Tata Kelola TI tidak memberikan pengaruh yang signifikan secara statistik. Hal ini mengindikasikan bahwa investor di pasar modal Indonesia, khususnya pada sektor finansial dan teknologi, lebih merespons informasi mengenai pengungkapan risiko *cyber* yang dilakukan perusahaan dibandingkan dengan keberadaan struktur tata kelola TI formal seperti komite TI atau CISO.[129]

4. Uji Hipotesis

Uji hipotesis dalam penelitian ini bertujuan untuk menguji pengaruh variabel independen terhadap variabel dependen. Pengujian dilakukan dengan menggunakan koefisien determinasi (R^2), uji F, dan uji t. Berikut disajikan hasil dari pengujian hipotesis tersebut.[130]

[129] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (Bandung: Alfabeta, 2019), hlm. 255

[130] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 98-106

a. Uji Koefisien Determinasi R^2

Uji koefisien determinasi (R^2) digunakan untuk mengukur seberapa jauh kemampuan model regresi dalam menjelaskan variasi variabel dependen. Nilai koefisien determinasi terletak antara nol dan satu ($0 \leq R^2 \leq 1$).[131] Hasil pengujian dapat dilihat pada tabel berikut ini.

Tabel 4.7
Hasil Uji Koefisien Determinasi R^2
Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.198[a]	.039	.026	.086654102972
a. Predictors: (Constant), Tata Kelola TI, Cybersecurity Riskdisclosure				

Sumber: Data diolah SPSS, 2026

Berdasarkan Tabel 4.7 di atas, diperoleh nilai *R Square* (Koefisien Determinasi) sebesar 0,039. Hal ini menunjukkan bahwa kontribusi atau kemampuan variabel independen yang terdiri dari *Cybersecurity Risk Disclosure* (X_1) dan Tata Kelola TI (X_2) dalam menjelaskan variasi variabel dependen yaitu *Market Reaction* (Y) adalah sebesar 3,9% (0,039 × 100%).[132] Sementara itu, sisanya sebesar 96,1% (100% - 3,9%) dijelaskan oleh variabel-variabel lain atau faktor-faktor lain di luar model penelitian yang tidak dimasukkan dalam penelitian ini (seperti faktor makroekonomi, kebijakan politik, kinerja keuangan lainnya, atau sentimen pasar global).

[131] Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R., "Signaling Theory: A Review and Assessment," *Journal of Management*, Vol. 37, No. 1, 2011, hlm. 39-67

[132] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 106

b. Uji t (Uji Parsial)

Uji t digunakan untuk menguji apakah secara parsial (individu) masing-masing variabel independen berpengaruh nyata atau tidak terhadap variabel dependen. Kriteria pengujian didasarkan pada nilai signifikansi (Sig.) < 0,05.[133] Berikut ini hasil uji t yang disajikan dalam tabel dibawah ini.

Tabel 4.8
Hasil Uji t
Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.049	.021		-2.333	.021		
	Cybersecurity Riskdisclosure	.026	.011	.218	2.358	.020	.739	1.353
	Tata Kelola TI	-.009	.017	-.049	-.526	.600	.739	1.353

a. Dependent Variable: *Market Reaction*

Sumber: Data diolah SPSS

Berdasarkan Tabel 4.8 (Tabel *Coefficients*), diperoleh hasil sebagai berikut:

1) Berdasarkan hasil uji statistik, diperoleh nilai Sig. sebesar 0,020 yang lebih kecil dari taraf signifikansi 0,05 (0,020 < 0,05) dan nilai t-hitung bernilai positif sebesar 2,358. Hal ini menunjukkan bahwa *Cybersecurity Risk Disclosure* berpengaruh positif dan signifikan terhadap *market reaction*. Dengan demikian, Hipotesis Pertama (H_1) diterima. Artinya, semakin luas dan transparan perusahaan mengungkapkan risiko *cyber* nya, pasar

[133] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 99

akan merespons secara positif dengan *return* tidak normal yang meningkat.

2) Berdasarkan hasil uji statistik, diperoleh nilai Sig. sebesar 0,600 yang jauh lebih besar dari taraf signifikansi 0,05 (0,600 > 0,05). Hal ini menunjukkan bahwa tata kelola TI tidak berpengaruh terhadap *market reaction*. Dengan demikian, Hipotesis Kedua (H_2) ditolak. Artinya, adanya komite atau penerapan tata kelola TI di dalam internal perusahaan belum menjadi pertimbangan utama bagi investor di pasar modal dalam berinvestasi, sehingga tidak memicu reaksi pasar.

c. Uji F (Uji Simultan)

Uji F digunakan untuk melihat apakah seluruh variabel independen yang terdiri dari *Cybersecurity Risk Disclosure* (X_1) dan Tata Kelola TI (X_2) secara bersama-sama (serentak) memiliki pengaruh terhadap variabel dependen yaitu *Market Reaction* (Y). Kriteria pengambilan keputusan adalah jika nilai signifikansi (Sig.) < 0,05, maka model regresi dinyatakan signifikan atau *fit*.[134]

Tabel 4.9
Hasil Uji F (Simultan)
ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.046	2	.023	3.090	.048[b]
	Residual	1.141	152	.008		
	Total	1.188	154			

[134] Ghozali, I., *Aplikasi Analisis Multivariate dengan Program IBM SPSS 26*, Edisi 10 (Semarang: Badan Penerbit Universitas Diponegoro, 2021), hlm. 106

a. Dependent Variable: *Market Reaction*
b. Predictors: (Constant), Tata Kelola TI, Cybersecurity Riskdisclosure

Sumber: data diolah SPSS, 2026

Berdasarkan Tabel 4.9 di atas, diperoleh nilai statistik F-hitung sebesar 3,090 dengan nilai signifikansi (Sig.) sebesar 0,048. Karena nilai signifikansi tersebut lebih kecil dari taraf signifikansi 0,05 (0,048 < 0,05), maka dapat disimpulkan bahwa secara simultan (serentak) variabel *Cybersecurity Risk Disclosure* (X_1) dan Tata Kelola TI (X_2) berpengaruh signifikan terhadap *Market Reaction* (Y). Hasil ini juga menunjukkan bahwa model regresi linear berganda yang digunakan dalam penelitian ini telah memenuhi kriteria kelayakan model (*goodness of fit*), sehingga model tersebut layak dan tepat digunakan untuk memprediksi reaksi pasar modal.

C. Pembahasan

1. Pengaruh *Cybersecurity Risk Disclosure* terhadap *Market Reaction*

Hasil pengujian hipotesis pertama (H_1) menunjukkan bahwa cybersecurity risk disclosure berpengaruh positif dan signifikan terhadap market reaction yang diukur dengan *cumulative abnormal return* (CAR). Nilai signifikansi sebesar 0,020 (< 0,05) dan koefisien regresi positif sebesar 0,026 mengindikasikan bahwa semakin tinggi tingkat keterbukaan pengungkapan risiko *cyber* perusahaan, maka semakin positif pula respons pasar yang tercermin dari peningkatan CAR.

Temuan ini sejalan dengan *Signaling Theory* yang dikemukakan oleh Spence, yang menyatakan bahwa perusahaan yang secara sukarela

mengungkapkan informasi secara transparan mengirimkan sinyal positif kepada investor tentang kualitas manajemen dan kesiapan perusahaan dalam menghadapi risiko[135]. Dalam konteks penelitian ini, pengungkapan risiko cyber yang komprehensif dan rinci berfungsi sebagai sinyal bahwa perusahaan memiliki kesadaran dan kemampuan dalam mengelola ancaman cyber, sehingga mengurangi asimetri informasi antara manajemen dan investor. Hal ini juga sesuai dengan teori efisiensi pasar bentuk setengah kuat, di mana harga saham menyesuaikan diri secara cepat terhadap informasi publik yang tersedia, termasuk pengungkapan risiko cyber dalam laporan tahunan.

Hasil penelitian ini mendukung temuan Damayanti yang menunjukkan bahwa *cybersecurity risk disclosure* dan ukuran perusahaan (SIZE) secara bersama-sama (simultan) berpengaruh signifikan terhadap harga saham. Meskipun secara parsial hanya SIZE yang berpengaruh signifikan, temuan simultan ini mengindikasikan bahwa pengungkapan risiko *cyber* tetap menjadi faktor yang dipertimbangkan investor ketika dikombinasikan dengan karakteristik perusahaan lainnya. Penelitian ini memperkuat argumen bahwa pengungkapan risiko *cyber* memiliki peran dalam membentuk persepsi investor, terutama di pasar modal Indonesia[136].

Temuan ini juga konsisten dengan Stiawan yang menemukan bahwa pengungkapan *Governance, Risk,* dan *Compliance* (GRC) secara simultan

---

[135] M. Spence,"Job Market Signaling," *The Quarterly Journal of Economics*, vol. 87, no. 3, 1973, hlm. 355-374

[136] Sari Damayanti, "Pengaruh Cybersecurity Risk Disclosure dan Ukuran Perusahaan Terhadap Harga Saham", (Skripsi, Universitas Pendidikan Indonesia, 2022), hlm. 36-72

berpengaruh positif signifikan terhadap reaksi pasar, dan secara spesifik, pengungkapan risiko *(risk disclosure)* berpengaruh positif signifikan terhadap nilai perusahaan[137]. Meskipun penelitian Stiawan menggunakan variabel GRC secara agregat, temuan tentang pengaruh positif pengungkapan risiko terhadap nilai perusahaan sejalan dengan hasil penelitian ini yang menunjukkan bahwa pengungkapan risiko cyber secara spesifik juga direspons positif oleh pasar.

Penelitian oleh Adams & Moore juga memberikan perspektif yang relevan, di mana mereka menganalisis 7.681 pernyataan terkait siber dari 61 perusahaan yang mengalami insiden ransomware (2018-2021) dan menemukan bahwa perusahaan meningkatkan pengungkapan setelah insiden, tetapi kualitas pengungkapan bervariasi[138]. Temuan ini mengindikasikan bahwa pasar menghargai pengungkapan yang informatif dan konsisten, yang sejalan dengan hasil penelitian ini bahwa pengungkapan risiko cyber yang lebih baik menghasilkan respons pasar yang positif.

Namun, temuan ini berbeda dengan hasil penelitian Karyani yang menemukan bahwa Voluntary Cyber Risk Disclosure (VCRD) justru dapat menurunkan ketahanan finansial bank, kecuali pengungkapan tentang

---

[137] Kadek Jonh Stiawan, "Market Reaction and Firm Value: A Governance, Risk and Compliance Disclosure Perspective," *International Journal of Economics, Management and Accounting*, vol. 3, no. 1, 2026, hlm. 163-170

[138] Matthew Adams dan Tyler Moore, "How Informative are Cybersecurity Risk Disclosures? Empirical Analysis of Firms Targeted by Ransomware," *Computers & Security*, vol. 159, no. 104626, 2025, hlm. 1-13

penyebab risiko yang tidak berpengaruh[139]. Penelitian Karyani et al. berfokus pada dampak pengungkapan terhadap ketahanan finansial dan mencakup 4 negara ASEAN (Indonesia, Malaysia, Thailand, Filipina), sedangkan penelitian ini berfokus pada reaksi pasar di BEI. Perbedaan fokus dan konteks ini dapat menjelaskan mengapa temuan berbeda, di mana pengungkapan risiko cyber mungkin berdampak negatif pada ketahanan finansial jika tidak dikelola dengan baik, tetapi tetap direspons positif oleh pasar dalam jangka pendek sebagai sinyal transparansi.

Penelitian oleh Jubaedah juga memberikan konteks tambahan, di mana mereka menemukan bahwa kepemilikan asing dan kepemilikan blok berpengaruh positif signifikan terhadap pengungkapan manajemen risiko siber, sedangkan kepemilikan manajemen dan kepemilikan tersebar tidak berpengaruh signifikan[140]. Temuan ini mengindikasikan bahwa investor asing dan pemilik saham mayoritas mendorong perusahaan untuk lebih transparan dalam mengungkapkan risiko cyber, yang pada gilirannya dapat memengaruhi respons pasar. Hal ini memperkuat argumen bahwa pengungkapan risiko cyber merupakan praktik yang didorong oleh tekanan dari pemangku kepentingan tertentu.

Dengan demikian, hasil penelitian ini mengkonfirmasi bahwa pengungkapan risiko cyber merupakan salah satu faktor penting yang

---

[139] Etikah Karyani, Taufik Faturohman, Ana Noveria, dan Raden Aswin Rahadi, "Financial Resilience in ASEAN-4 Banking Sector: Impact of Cyber Risk Disclosure," *Kasetsart Journal of Social Sciences*, vol. 45, no. 3, 2024, hlm. 901-914

[140] Siti Jubaedah, Agung Musta'in, Izza Nurlisti, dan Bayu Adam Maulana, "Cyber Risk Management Disclosure: A Stakeholder Theory Perspective," *Diponegoro International Journal of Busines,*vol. 7, no. 2, 2024, hlm. 133-146

memengaruhi persepsi investor di pasar modal Indonesia, khususnya pada sektor finansial dan teknologi yang sangat rentan terhadap ancaman cyber. Temuan ini mendukung penerapan regulasi seperti POJK No. 11/POJK.03/2022 yang mewajibkan perusahaan untuk mengungkapkan risiko cyber secara transparan dan tepat waktu.

2. Pengaruh Tata Kelola TI terhadap *Market Reaction*

Hasil pengujian hipotesis kedua (H_2) menunjukkan bahwa tata kelola teknologi informasi (IT governance) yang diproksikan melalui keberadaan komite TI atau CISO tidak berpengaruh signifikan terhadap market reaction. Nilai signifikansi sebesar 0,600 (> 0,05) dan koefisien regresi negatif sebesar -0,009 mengindikasikan bahwa keberadaan struktur tata kelola TI formal belum direspons secara signifikan oleh pasar.

Temuan ini tidak sejalan dengan *Agency Theory* yang dikemukakan oleh Jensen dan Meckling, yang menyatakan bahwa mekanisme tata kelola yang baik dapat mengurangi konflik kepentingan antara manajemen dan pemegang saham. Keberadaan komite TI atau CISO seharusnya memperkuat fungsi pengawasan terhadap pemanfaatan TI, sehingga risiko penyalahgunaan atau kegagalan sistem dapat ditekan dan direspons positif oleh pasar. Hasil ini juga bertentangan dengan *Legitimacy Theory* yang dikemukakan oleh Suchman, yang menyatakan bahwa perusahaan berupaya untuk memperoleh legitimasi dari pemangku kepentingan dengan menunjukkan bahwa mereka beroperasi sesuai dengan ekspektasi dan norma yang berlaku di masyarakat.

Hasil penelitian ini berbeda dengan temuan Stiawan yang menemukan bahwa pengungkapan *Governance* (sebagai bagian dari GRC) berpengaruh positif signifikan terhadap nilai perusahaan dan reaksi pasar[2]. Perbedaan ini dapat dijelaskan oleh fakta bahwa penelitian Stiawan mengukur pengungkapan tata kelola secara umum *(governance disclosure),* sementara penelitian ini secara spesifik mengukur keberadaan struktur tata kelola TI formal seperti komite TI atau CISO. Hal ini mengindikasikan bahwa investor mungkin lebih merespons pengungkapan tata kelola secara luas dibandingkan aspek teknis tata kelola TI yang spesifik.

Penelitian oleh Sofiani juga memberikan wawasan penting, di mana mereka menemukan bahwa ukuran perusahaan dan profitabilitas berpengaruh positif signifikan terhadap pengungkapan manajemen risiko siber, sedangkan aset tidak berwujud tidak berpengaruh signifikan[141]. Temuan ini mengindikasikan bahwa perusahaan besar dan profitable cenderung lebih banyak mengungkapkan risiko siber, tetapi investor mungkin lebih memperhatikan hasil akhir (pengungkapan) daripada struktur tata kelola yang mendasarinya. Hal ini sejalan dengan hasil penelitian ini, di mana keberadaan komite TI atau CISO tidak serta-merta direspons oleh pasar karena investor mungkin lebih fokus pada output pengungkapan daripada input struktur tata kelola.

[141] Mira Sofiani, Diani Putri Ramadhanty, dan Siti Jubaedah, "Cyber Risk Management Disclosure: The Impact of Firm Size, Profitability, and Intangible Asset," *International Journal of Entrepreneurship and Business Development,* vol. 7, no. 5, 2024, hlm. 929

Beberapa faktor dapat menjelaskan mengapa tata kelola TI tidak berpengaruh signifikan terhadap market reaction di Indonesia. Pertama, rendahnya literasi dan kesadaran investor ritel di Indonesia tentang pentingnya tata kelola TI. Data BEI menunjukkan bahwa pasar modal Indonesia didominasi oleh investor ritel (sekitar 80%), yang cenderung lebih fokus pada kinerja keuangan jangka pendek dan sentimen pasar dibandingkan aspek tata kelola perusahaan yang bersifat teknis seperti keberadaan komite TI atau CISO. Hal ini berbeda dengan penelitian Jubaedah et al. (2024) yang menemukan bahwa kepemilikan asing dan kepemilikan blok berpengaruh positif signifikan terhadap pengungkapan manajemen risiko siber, yang mengindikasikan bahwa investor besar dan asing lebih memperhatikan aspek tata kelola dibandingkan investor ritel.[142]

Kedua, pengungkapan tentang tata kelola TI di laporan tahunan perusahaan Indonesia masih bersifat terbatas dan tidak terstandarisasi. Berdasarkan observasi awal terhadap laporan tahunan perusahaan sampel, hanya sebagian kecil perusahaan yang memiliki komite khusus untuk mengawasi risiko cyber. Bahkan ketika perusahaan memiliki struktur tata kelola TI, informasi tersebut seringkali hanya disebutkan secara singkat tanpa penjelasan yang memadai tentang peran, tanggung jawab, dan efektivitas komite tersebut. Penelitian Damayanti juga menunjukkan bahwa hanya ukuran perusahaan yang berpengaruh signifikan terhadap harga

[142] Siti Jubaedah, Agung Musta'in, Izza Nurlisti, dan Bayu Adam Maulana, "Cyber Risk Management Disclosure: A Stakeholder Theory Perspective," *Diponegoro International Journal of Business* vol. 7, no. 2, 2024, hlm.133-146

saham secara parsial[1], yang mengindikasikan bahwa karakteristik perusahaan seperti ukuran lebih diperhatikan oleh investor dibandingkan struktur tata kelola.

Ketiga, keberadaan komite TI atau CISO belum tentu mencerminkan efektivitas tata kelola TI secara keseluruhan. Investor mungkin menganggap bahwa memiliki struktur formal saja tidak cukup, yang lebih penting adalah bagaimana struktur tersebut diimplementasikan dan terbukti efektif dalam mencegah atau menangani insiden cyber. Penelitian Adams & Moore menemukan bahwa kualitas pengungkapan risiko siber bervariasi secara signifikan antar perusahaan, yang mengindikasikan bahwa investor mungkin lebih merespons kualitas pengungkapan daripada keberadaan struktur formal[143].

Keempat, faktor budaya dan konteks pasar berkembang juga berperan. Penelitian Karyani menunjukkan bahwa di ASEAN-4, pengungkapan risiko siber justru dapat menurunkan ketahanan finansial bank jika tidak dikelola dengan baik. Hal ini mungkin membuat investor lebih berhati-hati dalam merespons aspek tata kelola TI, karena mereka mungkin belum melihat hubungan langsung antara struktur tata kelola dan kinerja keuangan perusahaan.

Dengan demikian, hasil penelitian ini menunjukkan bahwa meskipun tata kelola TI secara teoritis penting dalam kerangka Agency

[143] Matthew Adams dan Tyler Moore, "How Informative are Cybersecurity Risk Disclosures? Empirical Analysis of Firms Targeted by Ransomware," *Computers & Security*, vol. 159, no. 104626, 2025, hlm. 1-13

Theory dan Legitimacy Theory, dalam praktiknya investor di pasar modal Indonesia, khususnya di sektor finansial dan teknologi, belum sepenuhnya menghargai keberadaan struktur tata kelola TI formal sebagai sinyal positif. Hal ini mengindikasikan perlunya upaya peningkatan literasi investor dan standarisasi pengungkapan tata kelola TI di Indonesia.

3. Pengaruh *Cybersecurity Risk Disclosure* dan Tata Kelola TI secara simultan terhadap *Market Reaction*

Hasil pengujian hipotesis ketiga (H_3) menunjukkan bahwa secara simultan, variabel cybersecurity risk disclosure dan tata kelola TI berpengaruh signifikan terhadap market reaction. Nilai signifikansi sebesar 0,048 (< 0,05) dan nilai F-hitung sebesar 3,090 mengindikasikan bahwa kedua variabel independen secara bersama-sama memiliki pengaruh terhadap market reaction.

Temuan ini sejalan dengan kerangka pemikiran yang telah dibangun sebelumnya, di mana keterbukaan cybersecurity risk disclosure dan tata kelola TI secara bersama-sama membentuk persepsi investor terhadap kualitas manajemen risiko perusahaan. Perusahaan yang tidak hanya mengungkapkan risiko cyber secara transparan tetapi juga memiliki mekanisme tata kelola TI yang kuat menunjukkan kesungguhan dalam mengelola risiko digital secara menyeluruh. Investor cenderung lebih percaya pada perusahaan yang menunjukkan konsistensi antara apa yang diungkapkan (disclosure) dan apa yang diimplementasikan (tata kelola).

Kombinasi keduanya memberikan sinyal yang lebih kuat dibandingkan hanya salah satunya saja.

Hasil penelitian ini secara kuat mendukung temuan Stiawan (2026) yang menemukan bahwa pengungkapan Governance, Risk, dan Compliance (GRC) secara simultan berpengaruh positif signifikan terhadap reaksi pasar[2]. Meskipun penelitian Stiawan menggunakan variabel GRC secara agregat, temuan simultan ini sejalan dengan hasil penelitian ini, di mana pengungkapan risiko dan tata kelola secara bersama-sama memberikan sinyal yang lebih kuat kepada pasar. Hal ini mengindikasikan bahwa investor tidak hanya melihat satu aspek saja, tetapi mempertimbangkan keseluruhan kerangka tata kelola dan pengungkapan risiko dalam menilai perusahaan.

Penelitian Damayanti (2022) juga mendukung temuan ini, di mana cybersecurity risk disclosure dan ukuran perusahaan secara simultan berpengaruh signifikan terhadap harga saham[1]. Meskipun secara parsial hanya ukuran perusahaan yang berpengaruh signifikan, temuan simultan ini mengkonfirmasi bahwa pengungkapan risiko cyber tetap menjadi faktor yang dipertimbangkan investor ketika dikombinasikan dengan variabel lain. Penelitian ini memperluas temuan Damayanti dengan mengganti variabel ukuran perusahaan dengan tata kelola TI sebagai variabel independen kedua, dan tetap menemukan pengaruh simultan yang signifikan.

Namun, temuan ini berbeda dengan Jubaedah et al. (2024) yang berfokus pada faktor-faktor yang memengaruhi pengungkapan (struktur

kepemilikan)[5], sedangkan penelitian ini berfokus pada konsekuensi pasar dari pengungkapan tersebut. Meskipun berbeda fokus, kedua penelitian saling melengkapi, di mana Jubaedah et al. menunjukkan bahwa kepemilikan asing dan blok mendorong pengungkapan, sementara penelitian ini menunjukkan bahwa pengungkapan tersebut kemudian direspons oleh pasar ketika dikombinasikan dengan tata kelola TI.

Penelitian Sofiani et al. (2024) juga memberikan konteks tambahan, di mana mereka menemukan bahwa ukuran perusahaan dan profitabilitas berpengaruh positif signifikan terhadap pengungkapan manajemen risiko siber[6]. Temuan ini mengindikasikan bahwa perusahaan besar dan profitable cenderung lebih banyak mengungkapkan risiko siber, yang kemudian dikombinasikan dengan tata kelola TI untuk memberikan sinyal yang lebih kuat kepada pasar. Penelitian ini melengkapi temuan Sofiani et al. dengan menunjukkan bahwa pengungkapan tersebut memiliki konsekuensi pasar yang nyata.

Meskipun secara parsial tata kelola TI tidak berpengaruh signifikan, namun ketika dikombinasikan dengan cybersecurity risk disclosure, keduanya memberikan pengaruh yang signifikan secara simultan. Hal ini menunjukkan bahwa investor mungkin mempertimbangkan kedua faktor tersebut secara bersama-sama dalam menilai risiko perusahaan. Perusahaan dengan pengungkapan risiko cyber yang baik dan tata kelola TI yang kuat akan mendapatkan respons pasar yang lebih positif dibandingkan perusahaan yang hanya unggul pada salah satu aspek saja.

Nilai koefisien determinasi (R^2) yang rendah (3,9%) menunjukkan bahwa masih banyak faktor lain yang memengaruhi market reaction di luar kedua variabel ini. Faktor-faktor seperti kondisi makroekonomi, kebijakan moneter, stabilitas politik, sentimen investor global, serta kinerja keuangan fundamental perusahaan seperti profitabilitas, likuiditas, dan solvabilitas, kemungkinan besar memiliki pengaruh yang lebih dominan terhadap pergerakan harga saham. Penelitian Karyani et al. (2024) juga menunjukkan bahwa pengungkapan risiko siber dapat menurunkan ketahanan finansial jika tidak dikelola dengan baik[4], yang mengindikasikan bahwa konteks makroekonomi dan sektor juga memainkan peran penting. Penelitian Adams & Moore juga menemukan bahwa kualitas pengungkapan risiko siber bervariasi[3], yang menunjukkan bahwa faktor-faktor seperti ukuran perusahaan dan sumber daya juga memengaruhi efektivitas pengungkapan dan tata kelola.

Dengan demikian, hasil penelitian ini mengkonfirmasi bahwa meskipun pengaruhnya relatif kecil, keterbukaan cybersecurity risk disclosure dan tata kelola TI secara bersama-sama tetap memiliki pengaruh yang signifikan terhadap market reaction di pasar modal Indonesia. Temuan ini memberikan implikasi bahwa perusahaan sektor finansial dan teknologi perlu memperhatikan kedua aspek ini secara terintegrasi dalam strategi komunikasi dan tata kelola mereka untuk memaksimalkan kepercayaan investor dan respons pasar yang positif. Regulator seperti OJK juga perlu terus mendorong standarisasi pengungkapan risiko cyber dan tata kelola TI,

serta meningkatkan literasi investor tentang pentingnya aspek-aspek non-keuangan dalam menilai kinerja dan risiko perusahaan.

BAB V

KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan pada bab sebelumnya mengenai pengaruh keterbukaan *cybersecurity risk disclosure* dan tata kelola teknologi informasi terhadap *market reaction* pada perusahaan sektor finansial dan teknologi yang terdaftar di Bursa Efek Indonesia periode 2020-2024, maka dapat ditarik kesimpulan sebagai berikut:

1. Keterbukaan *cybersecurity risk disclosure* berpengaruh positif dan signifikan terhadap *market reaction* yang diukur dengan *cumulative abnormal return* (CAR). Hal ini dibuktikan dengan nilai signifikansi sebesar 0,020 (< 0,05) dan koefisien regresi positif sebesar 0,026. Temuan ini menunjukkan bahwa semakin tinggi tingkat keterbukaan pengungkapan risiko *cyber* yang dilakukan perusahaan, maka semakin positif pula respons pasar yang tercermin dari peningkatan CAR. Hasil ini mengkonfirmasi teori sinyal (*signaling theory*) bahwa pengungkapan risiko *cyber* yang transparan dan komprehensif berfungsi sebagai sinyal positif bagi investor dalam mengurangi asimetri informasi dan meningkatkan kepercayaan terhadap kualitas manajemen risiko perusahaan.
2. Tata kelola teknologi informasi yang diproksikan melalui keberadaan komite TI atau *Chief Information Security Officer* (CISO) tidak berpengaruh signifikan terhadap *market reaction*. Hal ini dibuktikan dengan nilai signifikansi sebesar 0,600 (> 0,05) dan koefisien regresi negatif sebesar

-0,009. Temuan ini mengindikasikan bahwa keberadaan struktur tata kelola TI formal belum menjadi pertimbangan utama investor di pasar modal Indonesia. Rendahnya literasi investor ritel yang mendominasi pasar modal Indonesia (sekitar 80%), keterbatasan pengungkapan tentang tata kelola TI dalam laporan tahunan, serta kurangnya standarisasi pelaporan menjadi faktor penyebab mengapa investor belum sepenuhnya menghargai keberadaan komite TI atau CISO sebagai sinyal positif.

3. Secara simultan, *cybersecurity risk disclosure* dan tata kelola teknologi informasi berpengaruh signifikan terhadap *market reaction*. Hal ini dibuktikan dengan nilai signifikansi sebesar 0,048 (< 0,05) dan nilai F-hitung sebesar 3,090. Temuan ini menunjukkan bahwa meskipun secara parsial tata kelola TI tidak berpengaruh signifikan, ketika dikombinasikan dengan *cybersecurity risk disclosure*, kedua variabel secara bersama-sama memberikan pengaruh yang signifikan terhadap respons pasar. Hal ini mengindikasikan bahwa investor mempertimbangkan kedua faktor tersebut secara terintegrasi dalam menilai risiko perusahaan. Namun, nilai koefisien determinasi (R^2) sebesar 0,039 (3,9%) menunjukkan bahwa kontribusi kedua variabel dalam menjelaskan variasi *market reaction* masih sangat kecil, sementara sisanya sebesar 96,1% dijelaskan oleh faktor-faktor lain di luar model seperti kondisi makroekonomi, kebijakan moneter, stabilitas politik, sentimen investor global, serta kinerja keuangan fundamental perusahaan.

B. Saran

Berdasarkan kesimpulan yang telah diuraikan, penelitian ini memberikan beberapa saran yang ditujukan kepada berbagai pihak terkait, serta saran bagi penelitian selanjutnya, sebagai berikut:

1. Perusahaan sektor finansial dan teknologi disarankan meningkatkan kualitas pengungkapan risiko *cyber* dalam laporan tahunan, tidak hanya bersifat generik (*boilerplate*) tetapi mencakup jenis ancaman spesifik, estimasi dampak finansial, strategi mitigasi, serta kerangka keamanan yang digunakan (ISO 27001 atau NIST). Perusahaan juga perlu lebih transparan mengungkapkan struktur tata kelola TI, termasuk keberadaan komite TI atau CISO, peran dan tanggung jawabnya, serta bukti efektivitas implementasinya. Selain itu, perusahaan perlu membangun strategi komunikasi risiko *cyber* yang proaktif dengan merespons cepat insiden *cyber* dan memanfaatkan media sosial untuk menyampaikan informasi transparan guna meminimalkan dampak negatif terhadap harga saham.
2. OJK disarankan menyusun pedoman teknis yang lebih rinci dan terstandarisasi mengenai pengungkapan risiko *cyber* dan tata kelola TI, termasuk format pelaporan, metrik wajib (frekuensi insiden, estimasi kerugian, tingkat keparahan), serta sanksi tegas bagi pelanggar. OJK dan BEI perlu mendorong perusahaan membentuk komite TI atau menunjuk CISO dan mewajibkan pengungkapan peran serta efektivitasnya. Regulator juga perlu melakukan sosialisasi dan edukasi berkelanjutan kepada

perusahaan dan investor tentang pentingnya pengungkapan risiko *cyber* dan tata kelola TI serta dampaknya terhadap stabilitas pasar modal.

3. Investor disarankan meningkatkan literasi dan pemahaman mengenai risiko *cyber* dan tata kelola TI sebagai faktor penting dalam menilai manajemen risiko perusahaan, tidak hanya terfokus pada kinerja keuangan jangka pendek. Investor perlu memperhatikan kualitas pengungkapan risiko *cyber* dalam laporan tahunan sebelum mengambil keputusan investasi, karena perusahaan dengan pengungkapan komprehensif cenderung lebih siap menghadapi ancaman *cyber.* Investor institusional disarankan mendorong perusahaan investasi untuk mempertimbangkan aspek keamanan cyber dan tata kelola TI dalam proses analisis dan pengambilan keputusan investasi.
4. Peneliti selanjutnya disarankan mengembangkan model pengukuran *cybersecurity risk disclosure* yang lebih komprehensif menggunakan analisis teks berbasis AI atau *machine learning*. Penelitian dapat memperluas periode dan menambahkan sektor lain dengan eksposur risiko *cyber* tinggi (infrastruktur, energi, kesehatan). Disarankan menambahkan variabel lain seperti ukuran perusahaan, profitabilitas, likuiditas saham, kepemilikan institusional, dan faktor makroekonomi. Pendekatan kualitatif seperti wawancara mendalam dengan manajemen, auditor, dan investor dapat digunakan untuk memahami alasan rendahnya pengungkapan risiko *cyber* di Indonesia. Studi komparatif antar negara ASEAN juga disarankan untuk melihat perbedaan praktik pengungkapan dan respons pasar di masing-masing negara.

DAFTAR PUSTAKA

Abdullah, Yusuf, Al-Qaradawi. (2001). *Fiqh al-Mu'amalat al-Maliyah fi al-Islam.* Beirut: Dar al-Qalam.

Al-Utaibi, Masoud. (2022). "The determinants of *cybersecurity risk disclosure* in firms' financial reporting: Empirical evidence". *Research in Economics,* Vol. 76. No. 2, 131-140.

Al-Ghazali, ibn Muhammad, Abu Hamid Muhammad. (2010). *Ihya' Ulum al-Din*. Beirut: Dar al-Kotob al-Ilmiyah.

Ahmad Ikhssani, Chandra Mudra, & Fandi Gunawan Prasidya. (2024). "The Role of IT Governance in Mitigating Cyber Risks: Evidence from Indonesian Financial and Technology Sectors". *Jurnal Sistem Informasi dan Teknologi*. Vol. 16. No. 1, 33-50

Anis Solikhawati & Ahmad Samsuri. (2023). "The Effect of Cybersecurity Incidents on Stock Prices: Evidence from Indonesian Islamic Banks". *Journal of Islamic Finance*. Vol. 12. No. 3, 55-72

Arena, C., Petrides, Y., & Vourvachis, P. (2020). "The Impact of *Cybersecurity Risk Disclosure* on Market Reaction: Evidence from Listed Companies." *Journal of Accounting and Public Policy*. Vol. 39. No. 4, 106-125.

Arikunto, S. (2019). *Prosedur Penelitian: Suatu Pendekatan Praktik*. Jakarta: Rineka Cipta.

Aryanty, N. Puspitasari, I. R. (2023). "*Cybersecurity Risk Disclosure* in Indonesian Listed Companies: A Qualitative Study." *Jurnal Riset Akuntansi dan Bisnis*. Vol. 23, No. 2, 208.

A. Samsuri, Solikhawati, A. (2023). "The Effect of Cybersecurity Incidents on Stock Prices: Evidence from Indonesian Islamic Banks". *Journal of Islamic Finance*. Vol. 12. No. 3, 65.

Babar, Muhammad Ali Chelsea Liu. (2024). "Corporate cybersecurity risk and data breaches: A systematic review of empirical research". *Australian Journal of Management.* Vol. 2, No. 1, 400-425.

BCA. (2024). *"BCA Annual Report 2024".* Jakarta: PT Bank Central Asia Tbk.

Bima Cinintya Pratama & Indra Widjaja. (2025). "Market Response to Cybersecurity Disclosures in Indonesian Stock Exchange: A Semi-Strong Efficiency Perspective." *Indonesian Journal of Accounting Research*. Vol. 28. No. 1, 78-95.

Clara Arena, Yiannis Petrides, & Petros Vourvachis. (2020). "The Impact of *Cybersecurity Risk Disclosure* on Market Reaction: Evidence from Listed

Companies." *Journal of Accounting and Public Policy*. Vol. 39. No. 4, 106-125

Cleary Gottlieb. (2025). *"Cybersecurity Disclosure and Enforcement Developments and Predictions".* New York: Cleary Publications.

Craig, A, MacKinlay. (1997). "Event Studies in Economics and Finance", *Journal of Economic Literature,* Vol. 35. No. 1, 1339.

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R., "Signaling Theory: A Review and Assessment." *Journal of Management*. Vol. 37. No. 1, 39-67.

De Haes, S., & Van Grembergen, W. (2019). *Enterprise Governance of Information Technology: Achieving Alignment and Value*. Switzerland: Springer.

Deloitte. (2024). *Global Cybersecurity Outlook 2024.* London: Deloitte Touche Tohmatsu Limited.

Ehrhardt, Michael C. Eugene F. Brigham. (2017). *Financial Management: Theory & Practice*. Boston: Cengage Learning.

ENISA. (2024). *"Threat Landscape: Finance Sector January 2023 to June 2024".* Luxembourg: ENISA Publications.

EY. (2024). *"Cybersecurity Oversight Disclosures: What Companies Shared in 2024".* London: EY Global.

Fama, Eugene F. (2017). "Market Efficiency: The Efficient Market Hypothesis (EMH)," *Handbook of the Economics of Finance*, Vol. 2. No.1, 382–417.

Faturohman, Taufik, Muhammad Ikhssani, Wahyu Ario Pratomo. (2024). "The Role of IT Governance in Mitigating Cybersecurity Risks and Enhancing Firm Value". *Jurnal Manajemen Teknologi*. Vol. 23. No. 1, 47.

Florackis et al. (2023). "Cybersecurity Risk", *The Review of Financial Studies*. Vol. 36. No. 1, 351–407.

Fortinet. (2024). *ASEAN Cybersecurity Outlook 2024*. Singapore: Fortinet.

Fera Rachmawati Sawity, dkk. (2024). "The Impact of Operational Risk Disclosure on Corporate Reputation and Financial Performance." *Jurnal Akuntansi dan Keuangan Indonesia*. Vol. 21. No. 1, 45-62.

Gottlieb, Cleary. (2025) *"Cybersecurity Disclosure and Enforcement Developments and Predictions".* New York: Cleary Publications.

Ghozali, Imam. (2018). *Aplikasi Analisis Multivariate dengan Program IBM SPSS 25*, Edisi 9. Semarang: Badan Penerbit Universitas Diponegoro.

Grembergen, Van, De Haes, S. (2015).W., *Enterprise Governance of Information Technology: Achieving Alignment and Value*. Switzerland: Springer.

HBT Law. (2025). *"Indonesia Personal Data And Sybersecurity Quartely Update July 2025 Edition".* Jakarta: HBT Publications.

IBM. (2024). *"Cost of a Data Breach Report 2024".* New York: IBM Security.Deloitte. *Global Cybersecurity Outlook 2024,* (London: Deloitte Touche Tohmatsu Limited, 2024), hlm. 15-35

International Monetary Fund. (2024). *Global Financial Stability Report: The Last Mile Financial Vulnerabilities and Risks.* Washington, DC: International Monetary Fund.

Indah Ratna Puspitasari & Nila Aryanty. (2023). "*Cybersecurity Risk Disclosure* in Indonesian Listed Companies: A Qualitative Study". *Jurnal Riset Akuntansi dan Bisnis*. Vol. 23, No. 2, 112-130.

Ikhssani, Muhammad et al. (2024). "Cybersecurity Technology Adoption, Investor Confidence, and Market Reaction: Evidence from Indonesian Listed Firms". *Journal of Financial Crime*. Vol. 31. No. 2, 50.

ISC2. (2024). *Indonesia Cybersecurity workforce Report 2024.* Alexandria: ISC2.Ikhssani, Muhammad et al. (2024). "Cybersecurity Technology Adoption, Investor Confidence, and Market Reaction: Evidence from Indonesian Listed Firms". *Journal of Financial Crime*. Vol. 31. No. 2, 48.

I. Widjaja, Pratama, B. C. (2025). "Market Response to Cybersecurity Disclosures in Indonesian Stock Exchange: A Semi-Strong Efficiency Perspective". *Indonesian Journal of Accounting Research*. Vol. 28. No. 1, 88.

Jensen, M. C., & Meckling, W. H. (1976). "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure." *Journal of Financial Economics*. Vol. 3. No. 4, 360.

Journal of Banking Regulation. (2025). *"Stock Market Effects of Major Cyber-Attacks: Evidence for Breached and Cybersecurity Listed Firms".* London: Palgrave Macmillan.

Krippendorff, K. (2019). *Content Analysis: An Introduction to Its Methodology*, 4th ed. California: SAGE Publications.

Marcus, Alan J. Zvi Bodie, Alex Kane. (2021). *Investments*. New York: McGraw-Hill Education.

Matters. (2024). *"Cybersecurity oversight disclosures: what companies shared in 2024".* US: firm of Ernst & Young Global Limited.

Mordor Intelligence. (2025). *"Indonesia Cybersecurity Market Size, Growth Trends & Forecast 2030".* Hyderabad: Mordor Intelligence.

Networks, Palo Alto. (2024). *Indonesia Cybersecurity Report 2024*. Jakarta: Palo Alto Networks.

Nur Indriantoro dan Bambang Supomo. (2018). *Metodologi Penelitian Bisnis untuk Akuntansi dan Manajemen.* Yogyakarta: BPFE.

Nobanee, H., & Ellili, N. (2021). "Cybersecurity Disclosure and Firm Value." *Journal of Financial Reporting and Accounting*. Vol. 19. No. 3, 425-445.

Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*, 7th ed. Boston: Pearson.

N. Ellili, Nobanee, H. (2021). "Cybersecurity Disclosure and Firm Value." *Journal of Financial Reporting and Accounting*. Vol. 19 No. 3, 425-445Grembergen, Van, De Haes, S. (2015).W., *Enterprise Governance of Information Technology: Achieving Alignment and Value*. Switzerland: Springer.

Pratama, B. C., & Widjaja, I. (2025). "Market Response to Cybersecurity Disclosures in Indonesian Stock Exchange: A Semi-Strong Efficiency Perspective." *Indonesian Journal of Accounting Research*. Vol. 28. No. 1. 78-95

Puspitasari, I. R., & Aryanty, N. (2023). "*Cybersecurity Risk Disclosure* in Indonesian Listed Companies: A Qualitative Study" *Jurnal Riset Akuntansi dan Bisnis*. Vol. 23. No. 2, 112-130

PwC. (2023). *ESG in Indonesia 2023.* Jakarta: PwC Indonesia.

Ross, S. A. (1973). "The Economic Theory of Agency: The Principal's Problem". *American Economic Review*. Vol. 63. No. 2, 134-139

SOCRadar. (2024). *"Indonesia Threat Landscape Report 2024".* Istanbul: SOCRadar Publications.

Sugiyono. (2019). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Bandung: Alfabeta.

Suchman, M. C. (1995). "Managing Legitimacy: Strategic and Institutional Approaches," *Academy of Management Review*. Vol. 20. No. 3, 571-610Nur Indriantoro dan Bambang Supomo. (2018). *Metodologi Penelitian Bisnis untuk Akuntansi dan Manajemen.* Yogyakarta: BPFESpence, Micael. (1973). "Job Market Signaling", *The Quarterly Journal of Economics,* Vol. 87. No. 3, 355-374.

Saifuddin Azwar. (2018). *Metode Penelitian*. Yogyakarta: Pustaka Pelajar.

Sawity, Fera Rachmawati, et al. (2024). "The Impact of Operational Risk Disclosure on Corporate Reputation and Financial Performance: Evidence from Indonesian Listed Companies". *Journal of Islamic Accounting and Business Research*. Vol. 15. No. 2, 241.

Supomo, Bambang, Nur Indriantoro. (2018). *Metodologi Penelitian Bisnis untuk Akuntansi dan Manajemen*. Yogyakarta: BPFE.

Sekaran, U., & Bougie, R. (2016). *Research Methods for Business: A Skill-Building Approach*, 7th ed. United Kingdom: John Wiley & Sons.Neuman, W. L. (2014). *Social Research Methods: Qualitative and Quantitative Approaches*, 7th ed. Boston: Pearson.

Santoso, S. (2022). *Statistik Multivariat: Konsep dan Aplikasi dengan SPSS*. Jakarta: Elex Media Komputindo.

Spence, M. (1973). "Job Market Signaling," *The Quarterly Journal of Economics*, Vol. 87. No. 3, 355-374.

Solikhawati, A., & Samsuri, A. (2023). "The Effect of Cybersecurity Incidents on Stock Prices: Evidence from Indonesian Islamic Banks." *Journal of Islamic Finance*. Vol. 12. No. 3, 55-72.

Vourvachis, Petros Claudia Arena, Yiannis Petrides. (2020). "Textual Analysis and Sentiment in Financial Disclosure: A Review of the Literature and Future Research Directions". *Journal of Accounting Literature*. Vol. 44. No. 1, 303–305.

Wu, J. (2024). "Impact of Cybersecurity Disclosure Frequency on Stock Price Crash Risk". *Journal of Corporate Accounting & Finance*. Vol. 35. No. 2, 45-62.

Weill, P., & Ross, J. W. (2004). *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston: Harvard Business School Press.

LAMPIRAN 1 : POPULASI PERUSAHAAN

No	Kode	Nama Perusahaan
1	AMAG	Asuransi Multi Artha Guna Tbk.
2	ASJT	Asuransi Jasa Tania Tbk.
3	BBCA	Bank Central Asia Tbk.
4	BBNI	Bank Negara Indonesia (Persero)
5	BBRI	Bank Rakyat Indonesia (Persero)
6	BBTN	Bank Tabungan Negara (Persero)
7	BDMN	Bank Danamon Indonesia Tbk.
8	BFIN	BFI Finance Indonesia Tbk.
9	BINA	Bank Ina Perdana Tbk.
10	BJTM	Bank Pembangunan Daerah Jawa T
11	BMRI	Bank Mandiri (Persero) Tbk.
12	BNGA	Bank CIMB Niaga Tbk.
13	BNII	Bank Maybank Indonesia Tbk.
14	BNLI	Bank Permata Tbk.
15	BSIM	Bank Sinarmas Tbk.
16	DNAR	Bank Oke Indonesia Tbk.
17	MCOR	Bank China Construction Bank
18	MEGA	Bank Mega Tbk.
19	NISP	Bank OCBC NISP Tbk.
20	PANS	Panin Sekuritas Tbk.
21	PNBN	Bank Pan Indonesia Tbk
22	PNBS	Bank Panin Dubai Syariah Tbk.
23	SRTG	Saratoga Investama Sedaya Tbk.
24	BRIS	Bank Syariah Indonesia (Persero)
25	AGRO	Bank Raya Indonesia Tbk.
26	ATIC	Anabatic Technologies Tbk.
27	EMTK	Elang Mahkota Teknologi Tbk.
28	MLPT	Multipolar Technology Tbk.
29	NFCX	NFC Indonesia Tbk.
30	DIVA	Distribusi Voucher Nusantara Tbk
31	HDIT	Hensel Davest Indonesia Tbk.
32	GLVA	Galva Technologies Tbk.
33	CASH	Cashlez Worldwide Indonesia Tbk
34	ZYRX	Zyrexindo Mandiri Buana Tbk.

LAMPIRAN 2 : SAMPEL PERUSAHAAN

No	Kode	Nama Perusahaan
1	AMAG	Asuransi Multi Artha Guna Tbk.
2	BBCA	Bank Central Asia Tbk.
3	BBNI	Bank Negara Indonesia (Persero)
4	BBRI	Bank Rakyat Indonesia (Persero)
5	BBTN	Bank Tabungan Negara (Persero)
6	BDMN	Bank Danamon Indonesia Tbk.
7	BFIN	BFI Finance Indonesia Tbk.
8	BINA	Bank Ina Perdana Tbk.
9	BJTM	Bank Pembangunan Daerah Jawa T
10	BMRI	Bank Mandiri (Persero) Tbk.
11	BNGA	Bank CIMB Niaga Tbk.
12	BNII	Bank Maybank Indonesia Tbk.
13	BNLI	Bank Permata Tbk.
14	BSIM	Bank Sinarmas Tbk.
15	DNAR	Bank Oke Indonesia Tbk.
16	MCOR	Bank China Construction Bank
17	MEGA	Bank Mega Tbk.
18	PANS	Panin Sekuritas Tbk.
19	PNBN	Bank Pan Indonesia Tbk
20	PNBS	Bank Panin Dubai Syariah Tbk.
21	SRTG	Saratoga Investama Sedaya Tbk.
22	BRIS	Bank Syariah Indonesia (Persero)
23	AGRO	Bank Raya Indonesia Tbk.
24	ATIC	Anabatic Technologies Tbk.
25	EMTK	Elang Mahkota Teknologi Tbk.
26	MLPT	Multipolar Technology Tbk.
27	NFCX	NFC Indonesia Tbk.
28	DIVA	Distribusi Voucher Nusantara Tbk
29	GLVA	Galva Technologies Tbk.
30	CASH	Cashlez Worldwide Indonesia Tbk
31	ZYRX	Zyrexindo Mandiri Buana Tbk.

LAMPIRAN 3 : DATA TABULASI SAMPEL PERUSAHAAN

No	Nama Perusahaan	Tahun	X1	X2	Y
1	Asuransi Multi Artha Guna Tbk.	2020	2	0	-0,023077843
		2021	2	0	-0,028480581
		2022	2	1	-0,035696713
		2023	2	1	0,021824594
		2024	2	1	0,106340147
2	Bank Central Asia Tbk.	2020	3	1	0,010290545
		2021	3	1	0,013617251
		2022	3	1	0,033867523
		2023	3	1	0,001883789
		2024	3	1	-0,001520284
3	Bank Negara Indonesia (Persero	2020	2	1	-0,006033148
		2021	2	1	0,010876987
		2022	2	1	0,054760314
		2023	2	1	0,02310461
		2024	2	1	0,041635525
4	Bank Rakyat Indonesia (Persero	2020	1	1	-0,046143852
		2021	1	1	0,049825546
		2022	1	1	0,023179201
		2023	1	1	-0,023159607
		2024	1	1	0,012275603
5	Bank Tabungan Negara (Persero)	2020	2	1	0,056384991
		2021	2	1	0,040491224
		2022	2	1	0,022392488
		2023	2	1	-0,055986173
		2024	2	1	0,018741695
6	Bank Danamon Indonesia Tbk.	2020	2	1	0,07684073
		2021	2	1	0,013460247
		2022	2	1	0,011956061
		2023	2	1	-0,016514905
		2024	2	1	-0,020928347
7	BFI Finance Indonesia Tbk.	2020	2	1	0,119720916
		2021	2	1	-0,009749722
		2022	2	1	0,050969349
		2023	3	1	0,053778522
		2024	3	1	0,01467671
8	Bank Ina Perdana Tbk.	2020	2	1	0,021641492

		2021	2	1	0,021263645
		2022	2	1	0,009371597
		2023	3	1	0,061738007
		2024	3	1	-0,011007379
9	Bank Pembangunan Daerah Jawa T	2020	3	1	-0,019881136
		2021	3	1	-0,026330856
		2022	3	1	-0,016867528
		2023	3	1	-0,031229863
		2024	3	1	0,067219645
10	Bank Mandiri (Persero) Tbk.	2020	3	1	0,10418487
		2021	3	1	0,020095991
		2022	3	1	0,014175888
		2023	3	1	-0,008688531
		2024	3	1	-0,072857291
11	Bank CIMB Niaga Tbk.	2020	3	1	-0,004573627
		2021	3	1	0,037838768
		2022	3	1	0,031361023
		2023	3	1	-0,052064095
		2024	3	1	0,009822525
12	Bank Maybank Indonesia Tbk.	2020	3	1	-0,010211835
		2021	3	1	-0,012144117
		2022	3	1	0,010997201
		2023	3	1	0,028120788
		2024	3	1	0,046234196
13	Bank Permata Tbk.	2020	3	1	-0,017663702
		2021	3	1	-0,010723579
		2022	3	1	0,002739702
		2023	3	1	-0,003508801
		2024	3	1	0,292464858
14	Bank Sinarmas Tbk.	2020	2	1	0,011257668
		2021	2	1	-0,014834792
		2022	2	1	-0,004414328
		2023	2	1	0,015102002
		2024	2	1	-0,009087527
15	Bank Oke Indonesia Tbk.	2020	2	1	-0,406406643
		2021	2	1	-0,018966656
		2022	2	1	0,040573877
		2023	2	1	0,020766555
		2024	2	1	0,048082515

16	Bank China Construction Bank I	2020	2	1	-0,031868386
		2021	2	1	0,007724269
		2022	2	1	-0,006568025
		2023	2	1	-0,01135993
		2024	2	1	0,009080629
17	Bank Mega Tbk.	2020	2	1	-0,274892922
		2021	2	1	0,021916951
		2022	2	1	0,014221234
		2023	2	1	0,022152877
		2024	2	1	0,018453298
18	Panin Sekuritas Tbk.	2020	1	0	-0,037188165
		2021	1	0	-0,000571153
		2022	1	0	-0,030116404
		2023	2	0	-0,019946872
		2024	2	0	0,031716162
19	Bank Pan Indonesia Tbk	2020	2	1	0,027628243
		2021	2	1	-0,056511678
		2022	2	1	-0,06304027
		2023	3	1	0,009594939
		2024	3	1	-0,045657752
20	Bank Panin Dubai Syariah Tbk.	2020	2	1	0,001251222
		2021	2	1	-0,010537239
		2022	2	1	-0,100806367
		2023	2	1	-0,015279296
		2024	2	1	0,054223525
21	Saratoga Investama Sedaya Tbk.	2020	1	0	-0,015917919
		2021	1	0	-0,071881803
		2022	1	0	-0,108062655
		2023	1	0	-0,054362994
		2024	1	0	-0,060006708
22	Bank Syariah Indonesia (Perser	2020	2	0	-0,253592711
		2021	3	0	-0,015505348
		2022	3	0	0,263548123
		2023	3	0	0,077067498
		2024	3	0	0,506799557
23	Bank Raya Indonesia Tbk.	2020	2	0	0,007349843
		2021	2	0	-0,079932207
		2022	3	0	0,036902011
		2023	3	0	0,013039627

		2024	3	0	0,004431438
24	Anabatic Technologies Tbk.	2020	2	0	-0,027142374
		2021	2	0	0,010524306
		2022	2	0	-0,0138405
		2023	2	0	-0,053312729
		2024	2	0	0,043491114
25	Elang Mahkota Teknologi Tbk.	2020	1	0	0,040735315
		2021	1	0	0,043367943
		2022	1	0	0,041705567
		2023	1	0	-0,038440132
		2024	1	0	0,039502728
26	Multipolar Technology Tbk.	2020	2	0	-0,018286412
		2021	2	0	-0,015794973
		2022	2	0	0,042999611
		2023	2	0	0,013436132
		2024	2	0	-0,04408131
27	NFC Indonesia Tbk.	2020	1	0	-0,016357618
		2021	1	0	0,146458957
		2022	1	0	-0,07423615
		2023	1	0	-0,257351323
		2024	1	0	-0,118952868
28	Distribusi Voucher Nusantara T	2020	1	0	-0,054955398
		2021	1	0	-0,003052134
		2022	1	0	-0,029378668
		2023	1	0	-0,029059888
		2024	1	0	-0,06063561
29	Galva Technologies Tbk.	2020	1	0	-0,00286171
		2021	1	0	0,018374807
		2022	1	0	0,023165138
		2023	1	0	-0,002135208
		2024	1	0	-0,021325932
30	Cashlez Worldwide Indonesia Tb	2020	2	0	-0,172806565
		2021	2	0	-0,160265557
		2022	2	0	0,029770797
		2023	2	0	-0,06137601
		2024	2	0	-0,018975224
31	Zyrexindo Mandiri Buana Tbk.	2020	1	0	0,306665229
		2021	1	0	0,004266394
		2022	1	0	0,024700815

		2023	1	0	-0,063315657
		2024	1	0	-0,040722254

LAMPIRAN 4 : HASIL PENGOLAHAN DATA MENGGUNAKAN SPSS 26

A. Analisis Statistik Deskriptif

1. Hasil Statistik deskriptif sebelum outlier

Descriptive Statistics

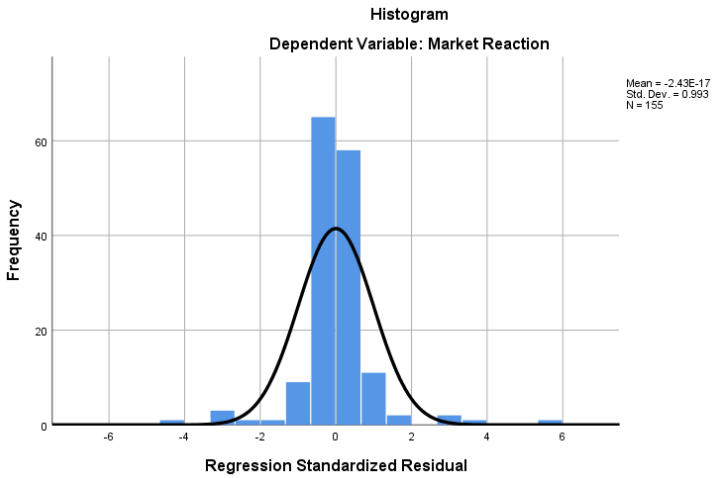
	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity Risk Disclosure	170	.00	3.00	2.0059	.76535
Tata Kelola	170	.00	1.00	.5765	.49558
Market reaction	170	-3443984332.00	506799557.00	-30499185.1471	303179254.03346
Valid N (listwise)	170				

2. Hasil Statistik deskriptif setelah outlier

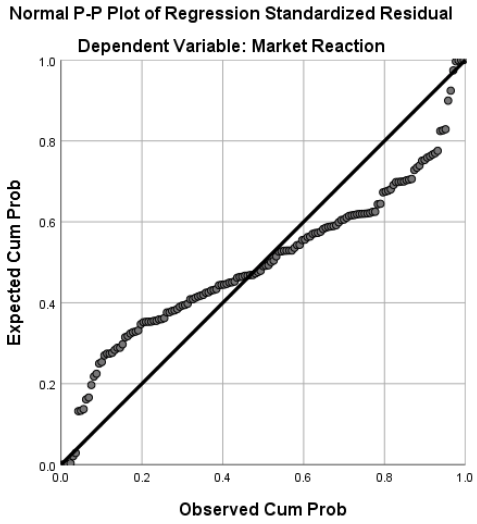
Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Cybersecurity Riskdisclosure	155	1	3	2.03	.725
Tata Kelola TI	155	0	1	.60	.491
Market Reaction	155	-.406406643	.506799557	-.00017295993	.087822110663
Valid N (listwise)	155				

B. Uji Normalitas



One-Sample Kolmogorov-Smirnov Test



		Unstandardized Residual
N		155
Normal Parameters[a,b]	Mean	.0000000
	Std. Deviation	.08608958
Most Extreme Differences	Absolute	.165
	Positive	.164
	Negative	-.165

Test Statistic	.165
Asymp. Sig. (2-tailed)	.000[c]
a. Test distribution is Normal.	
b. Calculated from data.	
c. Lilliefors Significance Correction.	

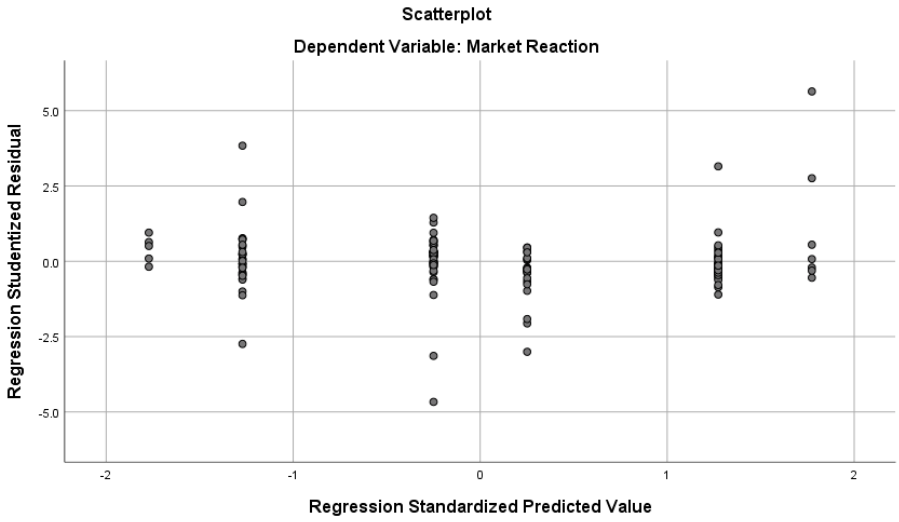
C. Uji Multikolinearitas

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.049	.021		-2.333	.021		
	Cybersecurity Riskdisclosure	.026	.011	.218	2.358	.020	.739	1.353
	Tata Kelola TI	-.009	.017	-.049	-.526	.600	.739	1.353

a. Dependent Variable: Market Reaction

D. Uji Heterokedastisitas



E. Uji Autokorelasi

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.198[a]	.039	.026	.086654102972	1.736
a. Predictors: (Constant), Tata Kelola TI, Cybersecurity Riskdisclosure					
b. Dependent Variable: Market Reaction					

F. Uji Analisis Regresi Linier Berganda

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.049	.021		-2.333	.021		
	Cybersecurity Riskdisclosure	.026	.011	.218	2.358	.020	.739	1.353
	Tata Kelola TI	-.009	.017	-.049	-.526	.600	.739	1.353
a. Dependent Variable: Market Reaction								

G. Uji Koefisien Determinasi R^2

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.198[a]	.039	.026	.086654102972
a. Predictors: (Constant), Tata Kelola TI, Cybersecurity Riskdisclosure				

H. Uji t

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	-.049	.021		-2.333	.021		
	Cybersecurity Riskdisclosure	.026	.011	.218	2.358	.020	.739	1.353
	Tata Kelola TI	-.009	.017	-.049	-.526	.600	.739	1.353

a. Dependent Variable: *Market Reaction*

I. Uji F (Simultan)

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.046	2	.023	3.090	.048[b]
	Residual	1.141	152	.008		
	Total	1.188	154			

a. Dependent Variable: *Market Reaction*

b. Predictors: (Constant), Tata Kelola TI, Cybersecurity Riskdisclosure

LAMPIRAN 5: SURAT KETERANGAN IZIN PENELITIAN

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI SJECH M. DJAMIL DJAMBEK BUKITTINGGI
FAKULTAS EKONOMI DAN BISNIS ISLAM
Kampus II : Jalan Gurun Aur Kubang Putih
Kabupaten Agam - Sumatera Barat - Telpon / Fax : (0752) 22875
Website : https://febi.uinbukittinggi.ac.id | Email : febi@uinbukittinggi.ac.id

Nomor : B-1547/Un.26.3/PP.07/07/2026 23 Juli 2026
Lamp. : -
Hal : ***Mohon Izin Penelitian***

Yth. Pimpinan Bursa Efek Indonesia
Jakarta

Assalamu'alaikum Wr. Wb

Dengan hormat, dalam rangka mengumpulkan data untuk penyusunan skripsi bagi mahasiswa Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri Sjech M. Djamil Djambek Bukittinggi, kami harapkan bapak/ibu untuk dapat kiranya memberi kesempatan melakukan penelitian kepada mahasiswa dibawah ini:

Nama	: **Rissa Giska**
NIM	: 3422014
Semester	: VIII (delapan)
Fakultas	: Ekonomi dan Bisnis Islam
Program Studi	: Akuntansi Syariah S1
Judul Skripsi	: ***"Pengaruh Keterbukaan Cybersecurity Riskdisclosure Dan Tata Kelola Teknologi Informasi Terhadap Market Reaction (Studi Pada Perusahaan Sektor Financial Dan Teknologi Di BEI Periode 2020-2024)"***
Lokasi Penelitian	: Bursa Efek Indonesia Jakarta
Waktu	: 3 April s.d. 3 Mei 2026

Demikian disampaikan, atas bantuannya diaturkan terima kasih.

Wassalam
Dekan

Dr. H. Aidil Alfin, M.Ag
NIP. 197205201999031007

LAMPIRAN 6: SURAT KETERANGAN SELESAI PENELITIAN

SURAT KETERANGAN SELESAI PENELITIAN

Yang bertanda tangan dibawah ini:

Nama	:	Rissa Giska
NIM	:	3422014
Program Studi	:	Akuntansi Syariah
Judul	:	Pengaruh Keterbukaan *Cybersecurity Riskdisclosure* Dan Tata Kelola Teknologi Informasi Terhadap *Market Reaction* (Studi Pada Perusahaan Sektor *Financial* Dan Teknologi Di BEI Periode 2020-2024)

Adalah benar telah melakukan penelitian sehubungan dengan judul tersebut menggunakan data sekunder, berupa laporan keuangan perusahaan yang terdaftar di Bursa Efek Indonesia yang di publikasikan dan diperoleh dari website www.idx.co.id dari perusahaan yang tercatat di BEI.

Dengan surat keterangan ini diberikan untuk dapat dipergunakan semestinya.

Bukittinggi, 3 Mei 2026
Saya yang menyatakan,



Rissa Giska
NIM. 3422014

LAMPIRAN 7: SK PEMBIMBING

SURAT KEPUTUSAN DEKAN FAKULTAS EKONOMI DAN BISNIS ISLAM
UNIVERSITAS ISLAM NEGERI SJECH M. DJAMIL DJAMBEK BUKITTINGGI
Nomor : 327/Un.26.3/HK.00.5/09/2025

Tentang

Penunjukan Dosen Pembimbing Skripsi Mahasiswa Program Studi S1 Akuntansi Syariah
Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri (UIN) Sjech M. Djamil Djambek Bukittinggi

DENGAN NAMA TUHAN YANG MAHA ESA

DEKAN FAKULTAS EKONOMI DAN BISNIS ISLAM

Membaca : Lembaran Pengajuan Judul Proposal Skripsi dan Penetapan Pembimbing oleh Ketua Program Studi S1 Akuntansi Syariah Fakultas Ekonomi dan Bisnis Islam Universitas Islam Negeri (UIN) Sjech M. Djamil Djambek Bukittinggi an **Rissa Giska** NIM. **3422014** tanggal 14 September 2025;

Menimbang :
a. bahwa untuk lebih terarah dan terkoordinirnya penulisan Skripsi mahasiswa UIN Sjech M. Djamil Djambek Bukittinggi, maka perlu ada Pembimbing.
b. bahwa nama yang tersebut dibawah ini, dipandang cakap dan mampu untuk diangkat sebagai Pembimbing.

Mengingat :
1 Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional, (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 47, Tambahan Lembaran Negara Republik Indonesia Nomr 4286);
2 Undang-Undang No. 12 Tahun 2012 tentang Pendidikan Tinggi, (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 158, Tambahan Lembaran Negara Republik Indonesia Nomr 5336);
3 Peraturan Pemerintah Nomor 4 Tahun 2014 tentang Penyelenggaraan Pendidikan Tinggi dan Pengelolaan Perguruan Tinggi, (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 16, Tambahan Lembaran Negara Republik Indonesia Nomr 5500);
4 Peraturan Pemerintah Nomor 46 Tahun 2019 tentang Pendidikan Tinggi Keagamaan, (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 120, Tambahan Lembaran Negara Republik Indonesia Nomr 6263);
5 Peraturan Presiden RI No. 85 Tahun 2022 tentang Perubahan Institut Agama Islam Negeri Bukittinggi menjadi Universitas Islam Negeri Sjech M.Djamil Djambek Bukittinggi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 135);.
6 Peraturan Menteri Agama Republik Indonesia Nomor 76 Tahun 2022 tentang Organisasi dan Tata Kerja Universitas Islam Negeri Sjech M. Djamil Djambek Bukittinggi (Berita Negara Republik IndonesiaTahun 2022 Nomor 1233);
7 Peraturan Menteri Agama Republik Indonesia Nomor 83 Tahun 2022 tentang Statuta Universitas Islam Negeri Sjech M. Djamil Djambek Bukittinggi (Berita Negara Republik Indonesia Tahun 2022 Nomor 1288);

MEMUTUSKAN

Menetapkan :

Pertama : Menyetujui Outlines, Daftar Kepustakaan bagi Skripsi mahasiswa yang bersangkutan dengan judul **"Pengaruh Keterbukaan Cybersecurity Riskdisclosure dan Tata Kelola TI Terhadap Market Reaction (Studi Pada Perusahaan Sektor Financial dan Teknologi Di BEI Periode 2020-2024)"**

Kedua : Menunjuk saudara :

Nama	:	**Tartila Devy, SE, M.Ak**
NIP	:	197808092023212009
Pangkat/Gol.Ruang	:	Penata Muda Tk. I/III/b/Asisten Ahli
Bidang Keahlian Pokok	:	Akuntansi
Memberi Mata Kuliah	:	Pengantar Akuntansi
Untuk Tugas	:	Pembimbing

Ketiga : Masa penulisan skripsi minimal selama 4 (empat) bulan sejak SK Pembimbing dikeluarkan.

Keempat : Apabila dikemudian hari ternyata terdapat kekeliruan dalam penetapan ini, akan diubah dan diperbaiki kembali sebagaimana mestinya.

Ditetapkan di : Bukittinggi
Pada Tanggal : 14 September 2025

AIDIL ADLIN

Tembusan :
1. Pembimbing;
2. Mahasiswa yang bersangkutan

LAMPIRAN 8: SURAT KETERANGAN BEBAS PLAGIAT

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI SJECH M. DJAMIL DJAMBEK BUKITTINGGI
FAKULTAS EKONOMI DAN BISNIS ISLAM
PROGRAM STUDI AKUNTANSI SYARIAH
Kampus II Jalan Gurun Aur Kubang Putih
Kabupaten Agam – Sumatera Barat – Telp/Fax: (0752) 22875
Website: http://febi.uinbukittinggi.ac.id | email: febi@uinbukittinggi.ac.id

SURAT KETERANGAN BEBAS PLAGIAT

Yang bertanda tangan di bawah ini, Ketua Prodi Akuntansi Syariah Fakultas Ekonomi dan Bisnis Islam UIN Sjech M.Djamil Djambek Bukittinggi, dengan ini menerangkan bahwa :

Nama	:	Rissa Giska
NIM	:	3422014
Program Studi	:	Akuntansi Syariah
Judul	:	Pengaruh Keterbukaan *Cybersecurity Riskdisclosure* dan Tata Kelola Teknologi Informasi Terhadap *Market Reaction* (Studi Pada Perusahaan Sektor *Financial* dan Teknologi Di BEI Periode 2020-2024)

Telah dilakukan pemeriksaan terhadap naskah karya ilmiah yang bersangkutan menggunakan turnitin dengan hasil similarity Index sebesar 25%. Berdasarkan hasil tersebut, karya ilmiah yang bersangkutan **dinyatakan bebas plagiarisme atau berada dalam batas wajar sesuai ketentuan akademik** yang berlaku di UIN Sjech M. Djamil Djambek Bukittinggi.

Demikianlah surat keterangan ini dibuat dengan sesungguhnya untuk dapat dipergunakan sebagaimana mestinya.

Bukittinggi, 28 Juli 2026
Ketua Prodi

Khadijah Nurani, SE., M.Si
NIP. 199112212019032014

BIODATA PENULIS



Penulis lahir di Kampung Pansur pada tanggal 21 Agustus 2004, sebagai anak ketiga dari 4 bersaudara. Putri dari Bapak Darmansyah dan Ibu Yuli Jasni. Penulis menempuh Pendidikan TK pada tahun 2009-2010 di TK Buah Manggis Jinang Kampung Pansur. Sekolah Dasar (SD) pada tahun 2010-2016 di SDN 06 Jinang Kampung Pansur. Sekolah Menengah Pertama Negeri (SMPN) 1 Koto XI Tarusan pada tahun 2016-2019 dilanjutkan pendidikan Sekolah Menengah Atas Negeri (SMAN) 1 Koto XI Tarusan tahun 2019-2022. Pada tahun 2022 penulis diterima sebagai mahasiswa Program Studi Akuntansi Syariah, Fakultas Ekonomi dan Bisnis Islam, Universitas Islam Negeri Sjech M.Djamil Djambek Bukittinggi. Penulis Melaksanakan penelitian di Bursa Efek Indonesia menggunakan data sekunder berupa laporan keuangan tahunan dan index saham, dengan judul Pengaruh Keterbukaan *Cybersecurity Riskdisclosure* Dan Tata Kelola Teknologi Informasi Terhadap *Market Reaction* (Studi Pada Perusahaan Sektor Financial Dan Teknologi Di Bei Periode 2020-2024).

Bukittinggi, 13 Juli 2026



RISSA GISKA