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

Rissa Giska[1], Tartila Devy[2]

[1,2]*Universitas Islam Negeri Sjech M. Djamil Djambek Bukittinggi*
E-mail : [1]rissagiska2@gmail.com, [2]tartiladevy@gmail.com

ABSTRACT

This study aims to examine the impact of cybersecurity risk disclosure and information technology governance on market reaction, as measured by cumulative abnormal return (CAR), in financial and technology sector companies listed on the Indonesia Stock Exchange from 2020 to 2024. This study was motivated by the significant increase in cyber threats in Indonesia, which increased by 154% during the period, with the financial and technology sectors as the primary targets. There is also a gap between regulatory expectations and current cyber risk disclosure practices in public companies. This study uses a quantitative approach with ex post facto methods and multiple linear regression. Data were collected from annual reports, sustainability reports, and daily stock price data. A sample of 31 companies, with a total of 155 observations over five years, was obtained through purposive sampling. Cybersecurity risk disclosure was assessed using content analysis with an ordinal scale, while IT governance was measured using a dummy variable based on the presence of an IT committee or CISO. The findings indicate that cybersecurity risk disclosure has a positive and significant effect on market reaction, suggesting that greater transparency in disclosing cyber risks leads to a more positive market reaction. Market response. However, IT governance did not significantly influence market reaction, as the presence of an IT committee or CISO has not yet become a key factor for investors in the Indonesian capital market. Simultaneously, both variables significantly influenced market reaction. These results suggest that companies should improve the quality of cybersecurity risk disclosures and enhance investor understanding of IT governance, while regulators should develop more standardized disclosure guidelines.

Keywords : *Cybersecurity Risk Disclosure, IT Governance, Market Reaction*

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah lanskap bisnis global secara mendalam, terutama di sektor keuangan dan teknologi, yang merupakan bagian kunci dari ekonomi digital. Transformasi digital telah mengadopsi teknologi canggih seperti kecerdasan buatan, *cloud computing*, *blockchain*, dan *platform fintech*, yang semuanya membantu membuat operasi lebih efisien, memperluas akses layanan, dan mendorong inovasi produk (Hetner, 2025). Di Indonesia, nilai ekonomi digital mencapai USD 82 miliar pada tahun 2023 dan diperkirakan mencapai USD 109 miliar pada tahun 2025, dengan *e-commerce* dan *fintech* sebagai kontributor utama. Namun, ledakan digital ini didorong oleh kerentanan siber yang besar. Indonesia berada di peringkat pertama ASEAN dengan 1,3 juta serangan siber paling terjadi pada tahun 2021 (Jubaedah et al., 2025). Sektor keuangan dan teknologi menjadi target utama, menyumbang 45% dari semua insiden. Serangan siber meningkat sebesar 154% selama periode 2020 hingga 2024, dan total kerugian ekonomi mencapai USD 6,85 miliar pada tahun 2024.

Peningkatan ancaman siber ini didorong oleh beberapa faktor utama. Pertama, adopsi teknologi baru seperti AI generatif telah memperluas permukaan serangan, memungkinkan penyerang menciptakan serangan *phishing* yang sangat personal dan sulit dideteksi (Hetner, 2025). Kedua, keterkaitan sistem global meningkatkan risiko rantai pasokan, karena masalah dengan dunia. Ketiga, Peningkatan penggunanan perangkat IoT menciptakan titik masuk baru bagi peneyerang. Biaya rata-rata pelanggaran data di sektor keuangan mencapai USD 6,08 juta per insiden pada tahun 2024, menjadikannya salah satu sektor dengan dampak finansial tertinggi.

Indonesia telah mengambil langkah-langkah dalam membuat aturan-aturan, terutama Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 yang membahas tentang penyelenggaraan informasi teknologi oleh bank umum, serta Peraturan Pemerintah Nomor 71 Tahun 2019 yang mengatur tentang sistem dan transaksi elektronik. Peraturan terhada perusahaan untuk menererapkan tata kelola TI yang kuat, mengungkapkan materiasi risiko siber, dan melaporkan secara tepat waktu. Secara global, aturan serupa seperti SEC Siber Disclosure Rule 2023 di Amerika Serikat menerapkan standar yang lebih ketat dengan memaksa pelaporan peristiwa siber yang signifikan dalam waktu empat hari kerja. (Haapamäki, Elina dan Sihvonen, 2026). Namun lemahnya penerapan di Indonesia menghadapi banyak tantangan, seperti pedoman teknis yang jelas, keterbatasan tenaga ahli kemanan siber yang mencapai defisit 25.000 orang, kesadaran yang rendah dari pihak-pihak yang bertanggung jawab, dan kekokmpleksan ekosistem digital yang melibatkan banyak pihak (Hetner, 2025). Akibatnya, muncul perbedaan antaran aturan yang diharapkan dan cara penerapannya di lapangan, di mana 70% dari penyebaran risiko siber di BEI masih menggunakan kalimat umum yang sama *(boilerplate)* dan 60% dari serangan siber yang berasa dari mitra atau vendor yang memiliki sistem keamanan yang tidak memadai (Jubaedah et al., 2025).

Penelitian terdahulu tentang pengungkapan risiko siber dan reaksi pasar menunjukkan hasil yang beragam. Chen, Henry, dan Jiang dalam *Journal of Business Ethics* menemukan bahwa perusahaan yang mengalami pelanggaran data meningkatkan pengungkapan risiko siber setelah insiden parah, dan pasar merespons negatif jika perusahaan justru mengurangi pengungkapan setelah insiden (Chen et al., 2023). Penelitian ini menggunakan lensa teori ekonomi dan etika pemangku kepentingan untuk menjelaskan keputusan manajemen dalam memperbarui pengungkapan risiko. Namun, Haapamäki dan Sihvonen dalam *International Journal of Accounting Information Systems* menemukan bahwa respons pasar terhadap pengungkapan risiko siber wajib di

AS justru minimal, dengan kualitas pengungkapan bervariasi dan lebih dipengaruhi oleh ukuran perusahaan, kinerja keuangan, dan kualitas auditor dibandingkan insiden siber masa lalu (Haapamäki, Elina dan Sihvonen, 2026). Penelitian ini menyoroti bahwa bahkan di bawah mandat regulasi, strategi diskresi perusahaan tetap berlanjut.

Di Indonesia, Jubaedah, Musta'in, Nurlisti, dan Maulana dalam *Diponegoro International Journal of Business* menemukan bahwa kepemilikan asing dan kepemilikan blok berpengaruh positif signifikan terhadap pengungkapan manajemen risiko siber, sedangkan kepemilikan manajemen dan kepemilikan tersebar tidak berpengaruh (Jubaedah et al., 2025). Penelitian ini menggunakan teori pemangku kepentingan dan berfokus pada faktor-faktor yang memengaruhi pengungkapan. Sementara itu, Kamillah, Damayanti, dan Fahrudi dalam *Profit* menemukan bahwa rapat dewan dan tata kelola TI berpengaruh positif signifikan terhadap pengungkapan siber di perbankan Indonesia, sedangkan keahlian TI dan keragaman gender tidak berpengaruh signifikan (Kamillah et al., 2026). Penelitian ini menggunakan *Upper Echelons Theory* dan menunjukkan bahwa koordinasi dan struktur manajemen merupakan faktor penting dalam meningkatkan transparansi siber.

Perbedaan utama antara penelitian sebelumnya dan studi ini terletak pada fokus analisisnya. Studi oleh Chen dan Sihvonen terutama berfokus pada pasar negara maju seperti Amerika Serikat, dengan konteks regulasi yang berbeda. Studi di Indonesia, seperti yang dilakukan oleh Jubaedah dan Kamillah, lebih berfokus pada faktor-faktor yang memengaruhi penyebaran (determinan) daripada konsekuensi pasar dari penyebaran tersebut. Meskipun beberapa studi global telah meneliti bagaimana pasar bereaksi terhadap peristiwa siber, sebagian besar studi tersebut belum secara khusus berfokus pada bagaimana pengungkapan risiko keamanan siber dan tata kelola TI memengaruhi reaksi pasar di negara berkembang seperti Indonesia. Hal ini terutama berlaku untuk sektor-sektor seperti keuangan dan teknologi, yang paling rentan terhadap ancaman siber. Selain itu, penelitian sebelumnya tentang tata kelola TI sebagai mekanisme yang dapat memperkuat kredibilitas kutipan belum diuji secara empiris dalam konteks risiko siber di Indonesia.

Berdasarkan penelitian tersebut, isu-isu yang dibahas dalam studi ini adalah : (1) tingkat dan kualitas penyebaran risiko keamanan siber di perusahaan keuangan dan teknologi yang terdaftar di BEI masih rendah dan tidak konsisten; (2) Implementasi struktur tata kelola TI yang ideal belum sepenuhnya diadopsi, terutama di perusahaan berkapitalisasi menengah; (3) Tidak ada kejelasan mengenai bagaimana pasar modal Indonesia menanggapi pengungkapan risiko keamanan siber; dan (4) Peran tata kelola TI sebagai mekanisme untuk memperkuat cakupannya belum diuji secara empiris di Indonesia.

Solusi yang diusulkan dalam penelitian ini adalah untuk menguji secara empiris dampak keterbukaan pengungkapan risiko keamanan siber dan tata kelola TI terhadap reaksi pasar, menggunakan pendekatan kuantitatif dengan metode *ex post facto* dan regresi linier berganda. Studi ini menggunakan analisis konten untuk menilai risiko siber pada skala ordinal (0-3) berdasarkan kelengkapan informasi dalam laporan tahunan, bersama dengan variabel dummy untuk mengukur keberadaan komite TI atau CISO sebagai proksi tata kelola TI . Reaksi pasar diukur menggunakan *Cumulative Abnormal Return* (CAR) melalui metode studi kejadian, dengan periode jendela tiga hari setelah laporan tahunan diterbitkan.

Tujuan penelitian ini adalah : (1) menganalisis pengaruh keterbukaan pengungkapan risiko keamanan siber terhadap reaksi pasar perusahaan keuangan dan teknologi yang terdaftar di BEI selama periode 2020-2024; (2) menganalisis pengaruh tata kelola TI terhadap reaksi pasar perusahaan keuangan dan teknologi yang terdaftar di BEI selama periode 2020-2024; dan (3) untuk

menganalisis efek gabungan dari keterbukaan pengungkapan risiko keamanan siber dan tata kelola TI terhadap reaksi pasar. Ini Studi ini diharapkan dapat memberikan wawasan konseptual dengan memperkaya literatur tentang peran pengungkapan risiko siber dan tata kelola TI sebagai sinyal dalam konteks pasar negara berkembang, serta menawarkan kontribusi praktis kepada perusahaan, investor, dan regulator dalam mengoptimalkan strategi komunikasi risiko dan keputusan investasi.

METODE

Penelitian ini merupakan penelitian kuantitatif dengan pendekatan *ex post facto* yang bertujuan menganalisis hubungan kausal antar variabel berdasarkan data yang telah terjadi tanpa melakukan manipulasi terhadap variabel independen. Pendekatan ini dipilih karena penelitian mengamati fenomena pengungkapan risiko siber dan tata kelola TI yang telah dipublikasikan perusahaan dalam laporan tahunan, serta reaksi pasar yang telah terjadi di Bursa Efek Indonesia (BEI) selama periode 2020-2024 . Lokasi penelitian mencakup seluruh perusahaan sektor finansial dan teknologi yang terdaftar di BEI, dengan periode pengumpulan data berlangsung dari Desember 2025 hingga Juli 2026.

Populasi penelitian adalah seluruh laporan tahunan dan laporan keberlanjutan perusahaan sektor finansial dan teknologi yang terdaftar di BEI periode 2020-2024. Teknik pengambilan sampel menggunakan *purposive sampling*, yaitu metode pemilihan sampel berdasarkan kriteria tertentu yang relevan dengan tujuan penelitian . Kriteria pemilihan sampel meliputi: (1) perusahaan memiliki laporan tahunan yang terbit konsisten selama 2020-2024; (2) data harga saham harian tersedia tanpa jeda lebih dari 7 hari berturut-turut; dan (3) terdapat bagian khusus mengenai risiko siber dan tata kelola TI dalam laporan tahunan . Dari 78 perusahaan awal yang memenuhi kriteria, diperoleh 31 perusahaan dengan total 155 observasi (31 perusahaan × 5 tahun) setelah proses pembersihan data outlier.

Variabel yang diukur dalam penelitian terdiri dari variabel independen dan dependen. Variabel independen pertama adalah siber *security risk disclosure* (X_1) yang diukur melalui *content analysis* terhadap laporan tahunan menggunakan skala ordinal 0-3 . Skor 0 diberikan jika perusahaan tidak mengungkapkan risiko siber; skor 1 jika hanya menyebut secara umum; skor 2 jika menjelaskan 1-2 strategi mitigasi; dan skor 3 jika mengungkapkan secara rinci dan lengkap mencakup jenis ancaman, dampak finansial, strategi mitigasi, dan kerangka keamanan yang digunakan . Variabel independen kedua adalah tata kelola TI (X_2) yang diukur menggunakan variabel *dummy* berdasarkan keberadaan komite TI atau *Chief Information Security Officer* (CISO) dalam struktur organisasi perusahaan, dengan nilai 1 jika ada dan 0 jika tidak ada . Variabel dependen adalah *market reaction* (Y) yang diukur menggunakan *Cumulative Abnormal Return* (CAR) dengan metode *event study* dalam periode tiga hari setelah publikasi laporan tahunan.

Instrumen penelitian terdiri dari *checklist content analysis* untuk mengukur pengungkapan risiko siber berdasarkan standar OJK dan SEC, serta data harga saham harian yang diperoleh dari Yahoo Finance dan Refinitiv Eikon untuk menghitung CAR. Perhitungan CAR dilakukan melalui beberapa tahap: pertama, menghitung *actual return* harian dengan rumus:

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

di mana $R_{i,t}$ adalah *return* aktual saham perusahaan *i* pada hari *t*, $P_{i,t}$ adalah harga saham perusahaan *i* pada hari *t*, dan $P_{i,t-1}$ adalah harga saham perusahaan *i* pada hari sebelumnya. Kedua,

menghitung *expected return* menggunakan model pasar (*Capital Asset Pricing Model*/CAPM) dengan persamaan:

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

Di mana $E(R_{i,t})$ adalah *expected return* saham perusahaan *i* pada hari *t*, α_i adalah intersep (konstanta) untuk saham *i*, β_i adalah koefisien beta yang mengukur sensitivitas *return* saham *i* terhadap *return* pasar, dan $R_{m,t}$ adalah *actual return* indeks pasar (IHSG) pada hari *t*. Parameter α_i dan β_i diestimasi menggunakan data selama *estimation window* 120 hari sebelum *event window*. Ketiga, menghitung *abnormal return* (AR) sebagai selisih antara *actual return* dan *expected return*:

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

Cumulative abnormal return (CAR) dihitung dengan menjumlahkan seluruh *abnormal return* selama *event window* 3 hari setelah publikasi laporan tahunan (t+1 sampai t+3):

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

Di mana $CAR_i(t_1,t_2)$ adalah *cumulative abnormal return* (CAR) saham perusahaan *i* dari hari t_1 sampai t_2, dengan t_1 = hari pertama *event window* (t+1) dan t_2 = hari terakhir *event window* (t+3). Publikasi laporan tahunan ditetapkan sebagai hari ke-0 (*event date*) berdasarkan tanggal yang tercantum dalam laporan tahunan yang diunggah di website BEI.

Teknik pengumpulan data dilakukan melalui metode dokumentasi dengan mengunduh laporan tahunan dari situs resmi BEI dan perusahaan, serta data harga saham dari Yahoo Finance dan Refinitiv Eikon. Data kemudian ditabulasi dan dianalisis menggunakan *software* SPSS versi 26. Teknik analisis data terdiri dari empat tahap utama. Pertama, analisis statistik deskriptif digunakan untuk menggambarkan nilai minimum, maksimum, rata-rata, dan standar deviasi seluruh variabel. Kedua, uji asumsi klasik dilakukan untuk memastikan model regresi memenuhi persyaratan dasar, meliputi uji normalitas Kolmogorov-Smirnov, uji multikolinieritas (VIF dan Tolerance), uji heteroskedastisitas (Grafik Scatterplot dan uji Glejser), dan uji autokorelasi Durbin-Watson.

Ketiga, analisis regresi linier berganda digunakan untuk menguji pengaruh variabel independen terhadap variabel dependen dengan persamaan:

$$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + e$$

Di mana *Y* adalah *market reaction* (CAR), α adalah konstanta, β_1 adalah koefisien regresi variabel *cybersecurity risk disclosure* (X_1), β_2 adalah koefisien regresi variabel tata kelola TI (X_2), dan *e* adalah *standard error* (faktor pengganggu di luar model). Keempat, uji hipotesis dilakukan melalui uji t (parsial) untuk menguji pengaruh masing-masing variabel independen secara individu terhadap variabel dependen, dan uji F (simultan) untuk menguji pengaruh seluruh variabel independen secara bersama-sama terhadap variabel dependen. Uji koefisien determinasi (R^2) digunakan untuk mengukur seberapa besar kemampuan model dalam menjelaskan variasi variabel dependen. Seluruh analisis statistik dilakukan dengan bantuan software SPSS versi 26 pada tingkat signifikansi 5% ($\alpha = 0,05$).

HASIL PENELITIAN DAN PEMBAHASAN

Penelitian ini menganalisis 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. Berdasarkan kriteria *purposive sampling*, diperoleh 31 perusahaan dengan total 155 observasi setelah proses pembersihan data *outlier*.

Tabel 1. 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: Hasil data yang diolah, 2026

Berdasarkan Tabel 1, variabel *cybersecurity risk disclosure* memiliki nilai rata-rata 2,03 dengan standar deviasi 0,725, yang mengindikasikan tingkat pengungkapan risiko siber berada pada kategori sedang hingga baik. Variabel tata kelola TI menunjukkan rata-rata 0,60, yang berarti 60% perusahaan sampel telah memiliki struktur tata kelola TI formal seperti komite TI atau CISO. Variabel *market reaction* memiliki rata-rata -0,000173 dengan standar deviasi 0,0878, menunjukkan reaksi pasar cenderung netral di sekitar periode pengumuman laporan tahunan.

Sebelum dilakukan analisis regresi, terlebih dahulu dilakukan uji asumsi klasik. Hasil uji normalitas dengan Kolmogorov-Smirnov menunjukkan nilai signifikansi 0,000, yang secara statistik mengindikasikan residual belum berdistribusi normal. Namun, berdasarkan Teorema Limit Pusat (*Central Limit Theorem*), dengan jumlah sampel 155 (>30), asumsi normalitas dapat diabaikan karena distribusi sampling residual akan mendekati normal seiring bertambahnya sampel (Ghozali, 2018). Hal ini diperkuat dengan grafik Histogram dan Normal P-P Plot yang secara visual menunjukkan sebaran data mengikuti kurva normal.

Hasil uji multikolinieritas menunjukkan nilai *Tolerance* sebesar 0,739 dan VIF sebesar 1,353 untuk kedua variabel independen. Nilai *Tolerance* > 0,10 dan VIF < 10 mengindikasikan tidak terjadi multikolinieritas antar variabel independen. Uji heteroskedastisitas melalui grafik *Scatterplot* menunjukkan titik-titik menyebar secara acak di atas dan di bawah angka 0, yang berarti tidak terjadi heteroskedastisitas. Uji autokorelasi Durbin-Watson menghasilkan nilai 1,736, yang berada pada rentang $1,5 \leq DW \leq 2,5$, sehingga disimpulkan tidak terjadi autokorelasi.

Analisis regresi linier berganda digunakan untuk menguji pengaruh variabel independen terhadap variabel dependen dengan persamaan:

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

Tabel 2. Regresi Linear Berganda

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	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: Hasil data yang diolah, 2026

Hasil uji koefisien determinasi (R^2) menunjukkan nilai *Adjusted R Square* sebesar 0,026, yang berarti variabel independen hanya mampu menjelaskan 2,6% variasi variabel dependen, sementara sisanya 97,4% dijelaskan oleh faktor-faktor lain di luar model.

Hasil uji t menunjukkan bahwa *cybersecurity risk disclosure* berpengaruh positif dan signifikan terhadap *market reaction* dengan nilai signifikansi 0,020 (< 0,05) dan koefisien regresi positif 0,026. Sementara itu, tata kelola TI tidak berpengaruh signifikan terhadap *market reaction* dengan nilai signifikansi 0,600 (> 0,05). Hasil uji F menunjukkan nilai signifikansi 0,048 (< 0,05), yang berarti secara simultan kedua variabel independen berpengaruh signifikan terhadap *market reaction*.

Pengaruh *Cybersecurity Risk Disclosure* terhadap *Market Reaction*

Hasil penelitian menunjukkan bahwa *cybersecurity risk disclosure* berpengaruh positif dan signifikan terhadap *market reaction*, yang mengindikasikan bahwa semakin tinggi tingkat keterbukaan pengungkapan risiko siber perusahaan, semakin positif pula respons pasar yang tercermin dari peningkatan *cumulative abnormal return* (CAR). Temuan ini sejalan dengan teori sinyal (*signaling theory*) yang dikemukakan oleh Spence (Spence, 1973), yang menjelaskan bahwa informasi yang disampaikan oleh pihak internal perusahaan kepada pihak eksternal berfungsi sebagai sinyal untuk mengurangi asimetri informasi antara manajemen dan investor. Perusahaan yang secara sukarela mengungkapkan informasi risiko siber secara transparan mengirimkan sinyal positif kepada investor mengenai kualitas manajemen dan kesiapan perusahaan dalam menghadapi ancaman siber (Brian et al., 2011).

Hasil ini konsisten dengan temuan Jameel (Jameel et al., 2025) yang menemukan bahwa pengungkapan risiko siber berhubungan positif dengan nilai perusahaan karena meningkatkan tata kelola, ketahanan operasional, dan kepercayaan investor di 12 negara Asia. Penelitian ini menggunakan teori sinyal dan teori legitimasi dengan sampel perusahaan multi-sektor dari 12 negara Asia pada periode 2020-2024, dan menyimpulkan bahwa pengungkapan risiko siber secara positif terkait dengan nilai perusahaan karena meningkatkan tata kelola, ketahanan operasional, dan kepercayaan investor (Jameel et al., 2025). Penelitian di Nigeria juga menunjukkan bahwa pengungkapan risiko siber memiliki efek positif dan signifikan terhadap valuasi pasar dengan koefisien 0,631 dan tingkat signifikansi p<0,01, yang mengindikasikan bahwa pelaporan risiko siber yang transparan meningkatkan kepercayaan investor dan mengurangi asimetri informasi (Augustine et al., 2023).

Namun, temuan ini berbeda dengan Haapamäki dan Sihvonen (Haapamäki et al., 2026) yang menemukan bahwa respons pasar terhadap pengungkapan risiko siber wajib di AS justru minimal, dengan kualitas pengungkapan lebih dipengaruhi oleh ukuran perusahaan dan kinerja keuangan. Penelitian ini menganalisis 3.440 pengungkapan Item 1C dalam laporan 10-K tahun 2024 dan menemukan bahwa investor dan analis memberikan respons minimal terhadap pengungkapan wajib tersebut, yang mengindikasikan bahwa strategi diskresi perusahaan tetap berlanjut bahkan di bawah mandat regulasi. Perbedaan ini dapat dijelaskan oleh konteks pasar yang berbeda, di mana pasar Indonesia yang didominasi investor ritel mungkin lebih responsif terhadap sinyal transparansi dibandingkan pasar maju yang telah memiliki regulasi ketat.

Pengaruh Tata Kelola TI terhadap *Market Reaction*

Hasil penelitian menunjukkan bahwa tata kelola TI tidak berpengaruh signifikan terhadap *market reaction*, dengan nilai signifikansi 0,600 (> 0,05). Temuan ini tidak sejalan dengan teori agensi (*agency theory*) yang dikemukakan oleh Jensen dan Meckling (1976), 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 (Michael et al., 1976).

Hasil ini berbeda dengan temuan Ikhssani yang menyimpulkan bahwa keberadaan struktur tata kelola TI formal secara signifikan meningkatkan ketahanan siber perusahaan dan menunjukkan tingkat kepercayaan pasar yang lebih tinggi, yang tercermin dari volatilitas harga saham yang lebih rendah pasca terjadinya insiden siber (Ikhssani et al., 2024). Penelitian ini juga sejalan dengan temuan Stiawan (2026) yang menemukan bahwa pengungkapan *Governance, Risk,* dan *Compliance* (GRC) secara simultan berpengaruh positif signifikan terhadap reaksi pasar, dan secara parsial pengungkapan governance dan risiko berpengaruh positif signifikan terhadap nilai perusahaan .

Perbedaan ini dapat dijelaskan oleh beberapa faktor. Pertama, rendahnya literasi investor ritel di Indonesia (sekitar 80%) yang cenderung lebih fokus pada kinerja keuangan jangka pendek dibandingkan aspek tata kelola perusahaan yang bersifat teknis. Kedua, pengungkapan tentang tata kelola TI di laporan tahunan perusahaan Indonesia masih bersifat terbatas dan tidak terstandarisasi, sehingga investor kesulitan menilai efektivitasnya. Tingkat pengungkapan risiko siber 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. Ketiga, keberadaan komite TI atau CISO belum tentu mencerminkan efektivitas tata kelola TI secara keseluruhan, karena yang lebih penting adalah bagaimana struktur tersebut diimplementasikan dan terbukti efektif dalam mencegah insiden siber (Jubaedah et al., 2025).

Pengaruh Simultan *Cybersecurity Risk Disclosure* dan Tata Kelola TI terhadap *Market Reaction*

Hasil penelitian menunjukkan bahwa secara simultan, *cybersecurity risk disclosure* dan tata kelola TI berpengaruh signifikan terhadap *market reaction* dengan nilai signifikansi 0,048 (< 0,05). Temuan ini sejalan dengan kerangka pemikiran bahwa kedua variabel secara bersama-sama membentuk persepsi investor terhadap kualitas manajemen risiko perusahaan. Perusahaan yang tidak hanya mengungkapkan risiko siber secara transparan tetapi juga memiliki mekanisme tata kelola TI yang kuat menunjukkan kesungguhan dalam mengelola risiko digital secara menyeluruh.

Hasil ini mendukung temuan Stiawan (Stiawan, 2025) yang menemukan bahwa pengungkapan *Governance, Risk*, dan *Compliance* (GRC) secara simultan berpengaruh positif signifikan terhadap reaksi pasar. Meskipun secara parsial tata kelola TI tidak berpengaruh signifikan, ketika dikombinasikan dengan *cybersecurity risk disclosure*, keduanya memberikan pengaruh yang signifikan secara simultan. Hal ini menunjukkan bahwa investor mempertimbangkan kedua faktor tersebut secara bersama-sama dalam menilai risiko perusahaan.

KESIMPULAN

Studi ini menemukan bahwa pengungkapan risiko keamanan siber memiliki efek positif dan signifikan terhadap reaksi pasar, yang diukur dengan *Cumulative Abnormal Return* (CAR) (sig. 0,020; koefisien 0,026). Semakin transparan pengungkapan tentang risiko siber, semakin positif respons pasar. Temuan ini mendukung teori signal, yang menunjukkan bahwa penyebaran informasi yang baik mengurangi asimetri informasi dan meningkatkan kepercayaan investor. Di sisi lain, manajemen teknologi informasi (seperti keberadaan komite TI atau CISO) tidak memiliki dampak signifikan terhadap CAR (sig. 0,600; koefisien -0,009). Ini menunjukkan bahwa investor di BEI belum mempertimbangkan struktur tata kelola TI sebagai faktor utama, mungkin karena rendahnya literasi investor ritel, pengungkapan yang terbatas, dan kurangnya pelaporan yang terstandarisasi. Pada saat yang sama, kedua variabel tersebut memiliki efek signifikan terhadap reaksi pasar (sig . 0,048 ; F- hitung 3,090). Namun, nilai R^2 hanya 0,039, artinya kedua variabel ini hanya menjelaskan 3,9% dari variasi CAR, dengan 96,1% dipengaruhi oleh faktor lain.

Untuk perusahaan Di sektor keuangan dan teknologi, tingkatkan kualitas pengungkapan risiko keamanan siber spesifik (seperti ransomware, pelanggaran data , dll.), termasuk perkiraan dampak, strategi mitigasi, dan kerangka kerja seperti ISO 27001 atau NIST. Lebih terbuka tentang keberadaan dan efektivitas komite TI/CISO dan berkomunikasi secara proaktif ketika terjadi insiden. Bagi regulator (OJK dan BEI), buat pedoman yang lebih rinci dan terstandarisasi untuk memperluas risiko keamanan siber dan tata kelola TI, termasuk metrik dan sanksi yang diperlukan. Tingkatkan kesadaran dan pendidikan bagi perusahaan dan investor. Bagi investor, tingkatkan pemahaman tentang risiko siber dan tata kelola TI, dan perhatikan kualitas informasi yang diungkapkan dalam laporan tahunan sebelum melakukan investasi. Bagi peneliti masa depan, gunakan analisis teks berbasis AI atau pembelajaran mesin untuk mengukur cakupan, waktu yang dibutuhkan, dan sektor yang terlibat , tambahkan kontrol variabel yang lebih komprehensif, dan lakukan studi kualitatif dan komparatif di seluruh negara ASEAN.

DAFTAR PUSTAKA

Augustine, A., Researcher, I., & Gbetuha, E. (2023). *Cybersecurity Breaches and Their Impact on Financial Reporting and Market Valuation : Evidence from Nigeria ' s Banking Sector*.

Brian L. Connelly , S. Trevis Certo, Christopher R. Reutzel, R. D. I. (2011). Signaling Theory: A Review and Assessment. *Journal of Management*, *37*(1), 39–67. https://doi.org/10.1177/0149206310388419

Chen, J., Henry, E., & Jiang, X. (2023). Is Cybersecurity Risk Factor Disclosure Informative ? Evidence from Disclosures Following a Data Breach. *Journal of Business Ethics*, *187*(1), 199–224. https://doi.org/10.1007/s10551-022-05107-z

Haapamäki, Elina dan Sihvonen, J. (2026). Mandatory cybersecurity disclosure: Early evidence

from 10-K reports. *International journal of accounting information systems*, *57*. https://osuva.uwasa.fi/handle/11111/20128

Hetner, A. Y.-S. and C. (2025). *The Wrong Crisis: How CrowdStrike Exposed the Cyber-Enterprise Risk Gap*. Global Association of Risk Professionals (GARP). https://www.garp.org/risk-intelligence/culture-governance/wrong-crisis-crowdstrike-250912

Jameel, A. H., Khalaf, A. J., Saleh, A. F., Sadaa, A. M., Hindi, W. K., Abdulateef, D. A., & Mahdi, A. S. (2025). *International Journal of Sustainable Development and Planning Corporate Value at Risk : Why We Should Care About Climate (IFRS S2) and Cybersecurity Risks ? 20*(7), 3073–3083.

Jubaedah, S., Musta, A., Nurlisti, I., & Maulana, B. A. (2025). *Cyber risk management disclosure : a stakeholder theory perspective*. *7*(2), 133–146. https://doi.org/10.14710/dijb.7.2.2024.133-146

Kamillah, N., Damayanti, C. R., Nugroho, A., & Imam, L. (2026). Board Characteristics and Information Technology Governance on Cybersecurity Disclosure in Indonesian Banking. *Jurnal Administrasi Bisnis*, *20*(2), 308–327.

M. F. Ikhssani, S. Rahayu, A. W. (2024). Information Technology Governance Infrastructure and Stock Price Volatility: Evidence from Emerging Markets. *Journal of Digital Banking & Finance*, *12*.

Michael C. Jensen, W. H. M. (1976). THEORY OF THE FIRM : MANAGERIAL BEHAVIOR , AGENCY COSTS AND OWNERSHIP STRUCTURE. *Journal of Financial Economics*, *3*(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Spence, M. (1973). Job Market Signaling. *Journal of Economics*, *87*(3), 355–374.

Stiawan, I. K. J. (2025). *Market Reaction and Firm Value : A Governance , Risk and Compliance Disclosure Perspective*. 1–8.