Journal of Social and Economics Research
Volume 7, Issue 2, Desember 2025
P-ISSN: 2715-6117 E-ISSN: 2715-6966
Open Access at: https://idm.or.id/JSER/index.php/JSER

TECHNOLOGY COMMITTEE SIZE AND LEVEL OF CYBERSECURITY DISCLUSURE IN BANKING IN INDONESIA

UKURAN KOMITE TEKNOLOGI DAN TINGKAT PENGUNGKAPAN KEAMANAN SIBER PADA PERBANKAN DI INDONESIA

Lia Sari
Universitas Tridinanti
E-mail: liasari1505@yahoo.co.id

ARTICLE INFO

Correspondent

Lia Sari
liasari1505@yahoo.co.id

Key words:
Cyber security disclosure, bangking, risk management, cyber risk

Website:
https://idm.or.id/JSER/index.php/JSER

Page: 1293 - 1306

ABSTRACT

Cybersecurity is a crucial part of banking risk management. Banks need to communicate to stakeholders about the cybersecurity risk management they have implemented and will continue to implement. This is where banking cybersecurity disclosure plays a crucial role for stakeholders. The formation of an information technology steering committee is a banking obligation based on POJK No. 11 of 2022 concerning the Implementation of Information Technology by Commercial Banks. This study examines the effect of the size of the technology committee on the level of cybersecurity disclosure in Indonesian banks. The observation period was from 2018 to 2023, for banks listed on the Indonesia Stock Exchange. The study findings indicate that the technology committee has a positive and statistically significant correlation with the level of cybersecurity disclosure among Indonesian banks. The size of the technology committee does have a beneficial and noteworthy impact on the level of cybersecurity information disclosed.

INFO ARTIKEL

Koresponden

Lia Sari
liasari1505@yahoo.co.id

Kata kunci:
Pengungkapan keamanan siber, cyber security disclosure, bank, manajemen resiko, resiko siber

Website:
https://idm.or.id/JSER/index.php/JSER

Hal: 1293 - 1306

ABSTRAK

Keamanan siber adalah bagian penting dari manajemen risiko perbankan. Bank perlu mengkomunikasikan kepada stakeholder mengenai manajemen risiko keamanan siber yang telah dan akan terus dilakukan bank. Disinilah peran penting pengungkapan keamanan siber perbankan bagi para stakeholder. Pembentukan komite pengarah teknologi informasi yang merupakan kewajiban perbankan berdasarkan POJK Nomor 11 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum. Studi ini mencoba melihat pengaruh ukuran komite teknologi terhadap tingkat pengungkapan keamanan siber pada perbankan Indonesia. Periode pengamatan sejak tahun 2018 s.d 2023, pada perbankan yang terdaftar di bursa efek Indonesia. Tenuan penelitian menunjukkan bahwa komite teknologi berkorelasi positif dan signifikan secara statistik dengan tingkat pengungkapan keamanan siber di antara bank-bank di Indonesia. Besarnya komite teknologi memang memberikan dampak yang menguntungkan dan patut diperhatikan pada tingkat informasi keamanan siber yang diungkapkan.

PENDAHULUAN

Keamanan siber telah muncul sebagai dimensi kritis dalam ranah manajemen risiko (Azzahrah et al., 2024; Li et al., 2018). Keamanan siber dapat diartikan sebagai pengamanan informasi dan perlindungan sistem elektronik, jaringan, perangkat keras, perangkat lunak, atau data dari akses atau bahaya yang tidak sah (Schatz & Wall, 2017). Kesadaran pentingnya keamanan siber telah meningkat dalam masyarakat kontemporer (Budiyanto & Mabruri, 2025; Cloramidine & Badaruddin, 2023). Akibatnya, ada kebutuhan mendesak untuk meningkatkan kesadaran perusahaan di bidang manajemen ancaman siber. Pengakuan perlindungan aset digital merupakan perhatian penting bagi organisasi, karena serangan siber dapat berdampak buruk pada kinerja perusahaan dan bahkan memengaruhi kesehatan mental (Fatihah et al., 2025).

Kemajuan teknologi informasi yang cepat, ditambah dengan meningkatnya frekuensi serangan siber (Aldasoro et al., 2022; Budiyanto & Mabruri, 2025) memaksa para pemangku kepentingan untuk mencari jaminan mengenai implementasi efektif manajemen keamanan siber oleh perusahaan. Pengungkapan keamanan siber merupakan agenda yang relatif baru dalam transparansi perusahaan. Meningkatnya insiden serangan siber memperkuat permintaan pemangku kepentingan untuk informasi yang cukup berkaitan dengan langkah-langkah keamanan siber. Para pemangku kepentingan mengadvokasi transparansi dari perusahaan publik mengenai manajemen risiko keamanan siber mereka. Menanggapi kekhawatiran yang meningkat ini, sangat penting bagi setiap perusahaan publik untuk membangun tata kelola keamanan siber yang kuat dan untuk memberikan pengungkapan komprehensif mengenai prioritas dan pengelolaan inisiatif keamanan siber.

Entitas yang terlibat dalam manajemen risiko harus memiliki kemampuan untuk mengidentifikasi dan mengurangi risiko secara efektif (Kamaruzaman et al., 2019).

Penyebaran informasi manajemen risiko menawarkan manfaat yang signifikan bagi organisasi dan para pemangku kepentingannya. Berbagai strategi yang bertujuan untuk meningkatkan keamanan siber mencakup peningkatan kapasitas, pembentukan kerangka kerja perlindungan dan keamanan yang terkonsentrasi pada pertahanan dunia maya, serta kemajuan komunikasi, sinergi kolaboratif, koordinasi, jaringan, dan kemitraan teknis untuk menumbuhkan komunitas keamanan siber (Agustin & Firdos, 2024).

Entitas publik harus mengakui pentingnya keamanan siber dan membuat pengungkapan yang sesuai mengenai masalah ini (Sofiani et al., 2024). Pengungkapan semacam itu memungkinkan entitas untuk menunjukkan akuntabilitas dan keterlibatan mereka dengan isu-isu ini, sehingga menumbuhkan kepercayaan di antara para pemangku kepentingan. Entitas publik seharusnya tidak hanya menerapkan program manajemen risiko cyber yang kuat tetapi juga mengkomunikasikan informasi yang tepat waktu dan relevan mengenai inisiatif tersebut kepada para pemangku kepentingan melalui pengungkapan keamanan siber.

Penulis akan membatasi ukuran pengungkapan keamanan siber ke satu bab atau sub bab dari laporan tahunan perbankan. Penulis menetapkan batasan ini karena teknologi informasi terkait erat dengan siber dan keamanan siber. Selain itu, diharapkan batasan ini akan meningkatkan konsentrasi penelitian ini, yang menggunakan konten analisis.

Penelitian ini bermaksud untuk menyelidiki pengaruh ukuran komite teknologi terhadap pengungkapan keamanan siber. Peneliti akan menggunakan *the new institutionalism theory*. Adapun rumusan masalah dalam penelitian ini adalah bagaimana pengaruh ukuran komite teknologi terhadap tingkat pengungkapan keamanan siber? Berdasarkan hal tersebut, tujuan dari penelitian ini adalah untuk menguji secara empiris pengaruh ukuran komite teknologi terhadap tingkat pengungkapan keamanan siber perbankan di Indonesia.

METODE PENELITIAN

Pengungkapan Keamanan Siber

Pengungkapan keamanan siber dapat didefinisikan sebagai pengungkapan yang ditujukan kepada pihak terkait mengenai keamanan informasi dan perlindungan sistem elektronik, jaringan, perangkat, program, atau data dari pencurian atau kerusakan. Di Indonesia, bahkan di Amerika Serikat dan Kanada, pengungkapan ini masih bersifat sukarela. Pengungkapan sukarela tersebut memberikan informasi yang lebih luas daripada pengungkapan wajib (Al Amosh & Khatib, 2022).

Belakangan ini, otoritas pengatur di Amerika Serikat dan Kanada telah menggarisbawahi pentingnya pengungkapan keamanan siber dan telah mengeluarkan panduan komprehensif (Gao et al., 2020; Héroux & Fortin, 2020). Pengungkapan keamanan siber telah menjadi perhatian para akademisi akuntansi dalam beberapa tahun terakhir. Meskipun demikian, sebagian besar penelitian sebelumnya dilakukan dalam konteks Amerika Serikat dan kanada. Investigasi sebelumnya menunjukkan kurangnya penelitian pengungkapan keamanan siber dalam kerangka negara berkembang (Sari et al., 2024), yang berisiko lebih tinggi menjadi sasaran serangan siber. Oleh karena itu, penelitian ini dilakukan dalam konteks Indonesia, yag merupakan negara berkembang, di mana pengungkapan keamanan siber dianggap sebagai opsi pelaporan sukarela bagi perusahaan.

Meningkatnya prevalensi pemanfaatan teknologi digital di Indonesia bersamaan dengan meningkatnya kerentanan keamanan siber (Budiyanto & Mabruri, 2025;

Cloramidine & Badaruddin, 2023). Menurut data *X-Force Threat Intelligence Index* 2022, 22,4% serangan cyber dalam 10 sektor terkemuka pada tahun 2021 diarahkan ke domain keuangan dan asuransi, dengan 70% dari serangan ini ditujukan khusus pada lembaga perbankan, 16% di entitas asuransi, dan 14% di berbagai sektor keuangan lainnya (https://www.ojk.go.id, 2022). Laporan dari BSSN menunjukkan bahwa hampir 1 miliar serangan cyber tercatat di Indonesia pada tahun 2022, dengan malware mewakili bentuk serangan dominan sebesar 56,84%, digantikan oleh pelanggaran data sebesar 14,75%, aktivitas Trojan sebesar 10,9%, dan bentuk lainnya sebesar 17,51% (https://www.antaranews.com). Laporan BSSN dari tahun 2023 menggambarkan bahwa Indonesia berada di antara 10 negara sumber anomali teratas serta di antara 10 negara tujuan anomali teratas(BSSN, 2024; Taufik, 2024). Indonesia memimpin peringkat untuk sumber dan tujuan anomali, diikuti oleh Amerika Serikat, Singapura, Jerman, Belanda, Prancis, Rusia, China, Republik Moldova, dan Republik Ceko.

Meskipun tidak ada sektor yang dikecualikan dari ancaman serangan cyber, penelitian ini berkonsentrasi pada sektor perbankan karena tiga alasan utama. Pertama, kerentanan perusahaan perbankan dan keuangan terhadap serangan cyber jauh lebih tinggi daripada bisnis di industri alternatif (Almansi, 2018). Direktur Penelitian dari Departemen Riset dan Regulasi Perbankan Otoritas Jasa Keuangan (OJK) menegaskan bahwa industri keuangan atau perbankan menempati posisi terdepan sebagai sektor yang paling terpengaruh oleh serangan cyber (Kontan.co.id, 2022).

Kedua, literatur yang ada telah menunjukkan bahwa pengungkapan keamanan siber dalam sektor perbankan menunjukkan karakteristik yang berbeda jika dibandingkan dengan entitas perusahaan lainnya. Perusahaan yang beroperasi di sektor keuangan telah melaporkan indeks pengungkapan keamanan siber tertinggi, yang juga menunjukkan pertumbuhan yang signifikan dari waktu ke waktu (Ramirez et al., 2022). Mengingat bahwa bank mewakili industri yang ditandai dengan tingkat pemanfaatan teknologi informasi yang tinggi, pengungkapan keamanan siber mereka sering berbeda dari sektor lain (Gao et al., 2020). Selain itu, perusahaan dalam domain keuangan, khususnya bank, tunduk pada kerangka peraturan yang ketat, menghasilkan kewajiban pengungkapan unik yang berbeda dari yang dikenakan pada entitas di industri lain (Haislip et al., 2020).

Ketiga, lanskap peraturan yang berkaitan dengan keamanan siber di Indonesia menempatkan penekanan yang signifikan pada sektor keuangan, dengan perbankan menjadi fokus utama pengawasan pemerintah, karena sektor ini dianggap berada pada risiko tertinggi serangan cyber. Pemerintah melalui OJK memberlakukan Peraturan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank (https://www.aseanbriefing.com, 2023). OJK menguraikan lebih lanjut peraturan ini dalam Surat Edaran Nomor 29/SEOJK.03/2022 (SEOJK 29) tanggal 27 Desember 2022. Peraturan ini dirancang khusus untuk sektor perbankan di Indonesia, tanpa peraturan serupa yang ditujukan untuk industri lain. Di sektor perbankan, kerangka peraturan yang mengatur manajemen risiko teknologi informasi ditentukan dalam POJK Nomor 38/POJK.03/2016, sebagaimana kemudian diubah menjadi POJK Nomor 13/POJK.03/2020.

Pada tahun 2022, OJK mengeluarkan Peraturan OJK Nomor 11/POJK.03/2022 tentang penyelenggaraan teknologi informasi oleh bank umum atau PTIB. Peraturan ini menggantikan POJK Nomor 13/POJK.03/2020. PTIB mencakup dimensi data, teknologi, manajemen risiko, kolaborasi, dan kerangka kelembagaan bank umum, semuanya bertujuan untuk memperkuat ketahanan dan kematangan operasional dalam entitas keuangan ini. Peraturan baru, yang dirumuskan oleh Otoritas Jasa Keuangan

(OJK), merupakan kerangka kerja keamanan siber perdana di Indonesia yang dirancang khusus untuk sektor keuangan, khususnya perbankan. OJK menjelaskan ketentuan tersebut dalam Surat Edaran Nomor 29/SEOJK.03/2022 (SEOJK 29), tanggal 27 Desember 2022. Surat edaran ini berisi rincian lengkap mengenai pelaksanaan Peraturan Nomor 11/POJK.03/2022 tentang Organisasi Teknologi Informasi oleh Bank (https://www.aseanbriefing.com, 2023). Hingga saat ini, peraturan yang ada tidak memberlakukan kewajiban bagi perusahaan untuk mengungkapkan informasi keamanan siber.

Entitas publik diharuskan memberikan informasi yang optimal sebagai indikator metrik kinerja mereka. Investor akan memanfaatkan informasi ini untuk mengevaluasi, memperkirakan, dan membuat keputusan berdasarkan informasi mengenai penilaian saham perusahaan. Informasi penting yang mencerminkan kinerja perusahaan dirangkum dalam laporan tahunan. Di luar data keuangan, investor memerlukan informasi non-keuangan untuk memfasilitasi proses pengambilan keputusan investasi mereka. Informasi yang disebarluaskan dalam bentuk pengungkapan sukarela dianggap meningkatkan nilai perusahaan, karena perusahaan yang menunjukkan transparansi tersebut dianggap lebih baik. Chaidir dkk. (2024) mengidentifikasi bahwa transparansi dalam pengungkapan risiko cyber dapat menumbuhkan kepercayaan, meningkatkan stabilitas relasional, dan meningkatkan efisiensi operasional dalam rantai pasokan.

Pengungkapan yang jelas dan dapat dipahami dapat secara signifikan meningkatkan transparansi dan akuntabilitas laporan keuangan (Sukma et al., 2025). Pengungkapan keamanan siber dalam laporan tahunan memungkinkan entitas publik untuk mengkomunikasikan kepada pasar keterlibatan proaktif mereka dalam mencegah, mendeteksi, dan mengurangi konsekuensi serangan siber. Sari dkk. (2025) memberikan bukti empiris yang menunjukkan bahwa pengungkapan keamanan siber cenderung meningkat setelah terjadinya insiden keamanan siber. Pengungkapan keamanan siber berfungsi untuk mengurangi biaya litigasi potensial yang dikaitkan dengan berkurangnya tanggung jawab terkait dengan peningkatan transparansi terkait dengan pengungkapan tersebut. Berkman et al., (2018) menetapkan korelasi positif antara kesadaran keamanan siber dan penilaian pasar.

Penulis melihat beberapa hal berikut terkait pengungkapan keamanan siber pada perbankan Indonesia: 1. Belum ada peraturan tertulis dari pihak berwenang, seperti Otoritas Jasa Keuangan (OJK) atau BAPEPAM, yang mengatur pengungkapan keamanan siber secara sukarela atau wajib. 2. Tingkat serangan siber yang tinggi, terutama yang melibatkan perbankan Indonesia, membuat stakeholder membutuhkan informasi yang cukup tentang keamanan siber. Tetapi pengungkapan tentang keamanan siber perbankan Indonesia tidak seragam, bahkan mungkin rendah.

Dalam penelitian ini, penulis menggunakan indeks pengungkapan keamanan siber yang dikembangkan oleh Sari (2025). Indeks pengungkapan keamanan siber milik Sari (2025) dikembangkan dari literatur terdahulu terkait pengembangan indeks pengungkapan keamanan siber milik (Firoozi & Mohsni, 2023); (Ramirez et al., 2022); (EY, 2022); (Ernst & Young LLP, 2021); (Héroux & Fortin, 2020). Indeks tersebut juga mengakomodir POJK No. 11 tahun 2022; SEOJK No. 29 tahun 2022; dan SEC *Cybersecurity Risk Management, Strategy, Governance, dan Incident Disclosure* 2023. Penelitian ini menggunakan tingkat pengungkapan keamanan siber sebagai jumlah total pengungkapan keamanan siber yang dilakukan bank dalam bab teknologi informasi laporan tahunan bank. Total item pengungkapan sebanyak 73 item, dengan nilai 1 untuk setiap item yang diungkapkan, dan nilai 0 jika tidak diungkapkan.

Komite Teknologi

Pembentukan komite teknologi yang terpisah dari komite lainnya, seperti komite risiko dan komite audit, dapat membantu tata kelola teknologi informasi dengan meningkatkan kemungkinan pengungkapan keamanan siber dan menunjukkan kredibilitas terkait keamanan siber, termasuk tindakan pencegahan dan identifikasi serangan siber (Higgs et al., 2016). Dari perspektif teori institusional baru, pembentukan komite teknologi menunjukkan bahwa perusahaan berkomitmen untuk memenuhi persyaratan keamanan siber lingkungan institusional. Komite teknologi menunjukkan kepada pihak berwenang bahwa perusahaan berkomitmen untuk menjaga keamanan siber (Higgs et al., 2016). Peng & Krivacek (2020) menyarankan agar direksi membentuk komite keamanan siber untuk menilai risiko keamanan siber perusahaan. Higgs et al. (2016) melaporkan bahwa perusahaan yang memiliki komite teknologi melaporkan lebih banyak pelanggaran keamanan.

Regulator dan investor membutuhkan informasi mengenai tata kelola dalam hal keamanan siber. Pembentukan komite teknologi mencerminkan penerapan tata kelola perusahaan yang baik. Dari perspektif teori institusi baru, pembentukan komite teknologi menunjukkan komitmen perusahaan untuk memenuhi tuntutan lingkungan institusional terkait keamanan siber. Adanya komite teknologi memberikan sinyal kepada para pemangku kepentingan bahwa perusahaan memiliki komitmen untuk menjaga keamanan siber (Higgs et al., 2016). Penelitian ini akan menggunakan ukuran komite teknologi sebagai faktor penentu dalam pengungkapan keamanan siber. Semakin besar ukuran komite teknologi, semakin banyak anggota yang terlibat dalam mengawasi dan mengarahkan perusahaan dalam hal keamanan siber. Ukuran komite teknologi yang besar menunjukkan tingkat komitmen perusahaan yang tinggi terkait tata kelola keamanan siber. Hal ini akan berdampak positif terhadap tingkat pengungkapan keamanan siber perusahaan.

Higgs et al. (2016) menemukan adanya korelasi positif yang signifikan antara keberadaan komite teknologi dengan laporan mengenai breach keamanan siber. Buckby et al. (2015) menemukan bahwa keberadaan komite teknologi berkaitan dengan peningkatan pengungkapan risiko. Berdasarkan tinjauan literatur, belum banyak penelitian empiris yang menyelidiki pengaruh ukuran komite teknologi terhadap tingkat pengungkapan keamanan siber. Dalam penelitian sebelumnya, komite teknologi yang dianalisis selalu menggunakan variabel dummy (Haislip et al., 2020; Higgs et al., 2016). Di Indonesia, Otoritas Jasa Keuangan mewajibkan bank untuk membentuk Komite Pengarah Teknologi Informasi. Karena itu, penelitian ini akan menggunakan ukuran komite, seperti yang sering digunakan dalam penelitian mengenai komite audit atau komite risiko.

Pengawasan merupakan aktivitas penting dalam *good corporate governance*. Teori keagenan menyatakan bahwa kualitas pengawasan dapat mengurangi tingkah laku oportunistik agen yang berpotensi merugikan kepentingan prinsipal. Komite audit yang berukuran besar dapat melindungi dan mengontrol proses akuntansi dan keuangan karena meningkatnya nasihat dari para anggota yang ahli. Secara empiris terbukti bahwa ukuran komite audit berpengaruh signifikan terhadap kinerja perusahaan (Kipkoech & Rono, 2016). Ukuran komite audit yang lebih besar dapat meningkatkan fungsi pengawasan, dan hasil empiris menunjukkan bahwa ukuran komite audit berpengaruh dalam meningkatkan kualitas pelaporan terintegrasi (Raimo et al., 2021).

Alur Pikir

Semakin besar ukuran komite teknologi dan jumlah anggotanya, semakin banyak orang yang akan mengawasi dan mengarahkan perusahaan dalam hal keamanan siber. Ukuran komite teknologi yang lebih besar menunjukkan bahwa perusahaan sangat berkomitmen pada keamanan siber, yang akan berdampak positif pada tingkat pengungkapan keamanan siber perusahaan. Ukuran komite teknologi berpengaruh terhadap pengungkapan keamanan siber.

Sumber: diolah penulis (2025)

Gambar 2. Kerangka Fikir

Jenis Penelitian

Variabel penelitian adalah karakteristik yang melekat pada orang, benda, atau subjek lain yang nilai-nilainya berbeda dari satu subjek ke subjek lainnya. Dalam penelitian ini, terdapat variabel independen dan variabel dependen. Variabel dependen adalah pengungkapan keamanan siber. Pengungkapan keamanan siber dapat diperoleh dari laporan tahunan perusahaan dalam bentuk kalimat yang menjelaskan tentang risiko keamanan siber serta upaya mengurangi risiko tersebut. Analisis konten dalam laporan tahunan perbankan akan dibatasi pada bagian atau sub-bagian "Teknologi Informasi". Indeks pengungkapan keamanan siber menggunakan indeks yang telah dikembangkan dalam penelitian terdahulu oleh Sari (2025). Variabel pengungkapan keamanan siber diukur dengan menghitung jumlah item pengungkapan keamanan siber dalam laporan tahunan dibagi dengan total item pengungkapan keamanan siber (73 item). Variabel independen yang digunakan adalah ukuran komite teknologi, yang diukur dengan jumlah anggota komite pengarah teknologi informasi dalam suatu bank.

Tabel 1. Definisi Operasional

Konsep	Nama Variabel (Proksi)	Definisi Operasional	Indikator	Skala
Variabel Independen				
Komite Teknologi	Ukuran Komite teknologi	jumlah anggota komite pengarah teknologi informasi suatu bank	jumlah anggota komite pengarah teknologi informasi	Rasio
Variabel Dependen				
Pengungkapan Keamanan Siber	Pengungkapan Keamanan Siber	Pengungkapan terkait keamanan siber dalam laporan tahunan suatu bank khususnya Bab/sub Bab Teknologi Informasi	Jumlah item yang diungkapkan n maximal 73	Rasio

Sumber: Penulis (2025)

Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh bank yang terdaftar di bursa efek Indonesia periode 2018 s.d 2023. Sampel ditentukan dengan metode *purposive sampling*, yaitu bank yang memiliki informasi mengenai ukuran komite teknologi yang

dimilikinya dan disebutkan dalam laporan tahunan bank. Dengan metode ini, didapat 222 sampel bank.

Jenis dan Sumber Data

Penelitian ini menggunakan data sekunder, yaitu data yang sudah diproses oleh pihak lain untuk tujuan tertentu dan kemudian dikumpulkan oleh peneliti sebagai bahan penelitian (Fauzi et al., 2019). Data sekunder yang digunakan meliputi pengungkapan keamanan siber dan ukuran komite teknologi. Data tersebut diperoleh dari Laporan Tahunan bank-bank yang terdaftar di Bursa Efek Indonesia.

Peneliti mengumpulkan laporan tahunan perusahaan dari website resmi perusahaan. Data yang dikumpulkan mencakup laporan tahunan perusahaan untuk periode pengamatan, yaitu sejak tahun 2018 hingga tahun 2023. Data yang akan dianalisis berupa data panel, yaitu data yang merupakan kombinasi dari data *time-series* dan data *cross-section* (Fauzi et al., 2019).

Teknik Analisis Data

Hipotesis

Peng & Krivacek (2020) merekomendasikan pembentukan komite keamanan siber di dalam dewan direksi untuk mengevaluasi risiko perusahaan terkait keamanan siber. Komite teknologi dibentuk untuk menangani masalah terkait teknologi informasi. Regulator dan investor membutuhkan informasi terkait tata kelola keamanan siber. Pembentukan komite teknologi menunjukkan praktik tata kelola perusahaan yang baik. Hal ini juga menunjukkan kepada pasar bahwa perusahaan mampu dan bersedia melakukan manajemen risiko terkait teknologi informasi melalui pembentukan komite teknologi yang selevel dewan direksi.

Penelitian Higgs et al. (2016) menemukan bahwa perusahaan dengan komite teknologi melaporkan lebih banyak breach keamanan siber dibandingkan perusahaan tanpa komite teknologi (2,5% vs 0,5%). Ini mencerminkan adanya korelasi positif antara pelaporan dan keberadaan komite teknologi. Keberadaan komite teknologi menunjukkan komitmen perusahaan terhadap keamanan siber. Dalam penelitian tentang komite manajemen risiko, hasil empiris menunjukkan bahwa kualitas pengungkapan manajemen risiko dipengaruhi secara positif dan signifikan oleh ukuran komite manajemen risiko. Perusahaan dengan komite manajemen risiko yang lebih besar cenderung menyediakan pengungkapan manajemen risiko dengan kualitas yang lebih tinggi (Jia et al., 2019).

Peneliti menduga bahwa ukuran komite teknologi berpengaruh positif terhadap tingkat pengungkapan keamanan siber. Dengan demikian, hipotesis yang diajukan adalah:
Ha : Ukuran komite teknologi berpengaruh positif signifikan terhadap tingkat pengungkapan keamanan siber.

HASIL DAN PEMBAHASAN

Tabel 2. Statistik Deskriptif

Variabel	N	Minimum	Maximum	Mean	Std. Deviation	Variance
UKT	222	4,00	38,00	11,7703	5,37014	28,838
PKS	222	2,00	30,00	12,2252	6,20565	38,510

Sumber: Diolah (2025)

Komite Teknologi

Ukuran komite teknologi dalam sampel penelitian menunjukkan perbedaan yang cukup besar. Nilai terendah adalah 4 anggota, menunjukkan bahwa ada bank dengan komite

teknologi yang cukup kecil, sedangkan nilai tertinggi mencapai 38 anggota, menunjukkan adanya bank dengan komite teknologi yang jauh lebih besar dan mungkin memiliki kepentingan serta fungsi yang lebih kompleks. Secara rata-rata, jumlah anggota komite teknologi adalah 11,77, yang dapat dianggap sebagai ukuran yang umum dan dominan pada sebagian besar bank dalam sampel penelitian.

Distribusi data menunjukkan bahwa sekitar 43,24% bank memiliki komite teknologi dengan anggota kurang dari 10, sedangkan sebagian besar, yaitu 52,25%, memiliki komite teknologi dengan jumlah anggota 10 sampai 20. Bank dengan komite teknologi lebih dari 20 anggota tidak banyak, hanya sekitar 3,6%. Perbedaan ini menunjukkan adanya perbedaan dalam kebijakan pengelolaan serta kebutuhan masing-masing bank terhadap aspek teknologi, yang mungkin mencerminkan perbedaan dalam strategi organisasi dalam menghadapi tantangan digitalisasi dan risiko teknologi.

Dari analisis rata-rata selama periode pengamatan 2018 hingga 2023, ukuran komite teknologi di bank-bank sampel secara umum relatif stabil meskipun ada sedikit perubahan dari tahun ke tahun. Pada tahun 2018, rata-rata jumlah anggota sebesar 11,32, relatif tidak berubah pada tahun 2019 sebesar 11,30. Pada tahun 2020, rata-rata meningkat sedikit menjadi 11,41 dan berlanjut pada tahun 2021 sebesar 11,68. Peningkatan lebih signifikan terjadi pada tahun 2022 dengan rata-rata mencapai 12,49, tetapi pada tahun 2023, rata-rata menurun sedikit menjadi 12,43. Secara keseluruhan, pola ini menunjukkan bahwa struktur komite teknologi di sektor perbankan Indonesia relatif konsisten, dengan adanya peningkatan moderat yang mencerminkan kebutuhan yang semakin tinggi terhadap pengawasan dan pengelolaan aspek teknologi di tengah dinamika digitalisasi perbankan.

Pengungkapan Keamanan Siber

Statistik deskriptif mengenai pengungkapan keamanan siber menunjukkan bahwa nilai minimum adalah 2, menunjukkan adanya bank dengan tingkat pengungkapan yang sangat rendah, sedangkan nilai maksimum mencapai 30, menunjukkan adanya bank yang memiliki tingkat transparansi yang tinggi. Rata-rata pengungkapan mencapai 12,2252, yang menunjukkan bahwa secara umum, tingkat pengungkapan keamanan siber di bank-bank sampel masih relatif moderat.

Analisis distribusi menunjukkan bahwa terdapat variasi dalam tingkat kepatuhan dan transparansi pengungkapan keamanan siber antar bank. Dari total sampel, sekitar 2,70% bank hanya mengungkapkan 2 item, sedangkan 2,25% mengungkapkan 3 item. Selanjutnya, 9,01% mengungkapkan 4 item, 2,70% mengungkapkan 5 item, serta 4,95% mengungkapkan 6 item. Kategori dengan 7 hingga 10 item terdiri dari 6,31% (7 item), 2,70% (8 item), 4,05% (9 item), dan 7,21% (10 item).

Di tingkat yang lebih tinggi, terdapat 4,50% bank yang mengungkapkan 11 item, 5,86% dengan 12 item, 6,31% dengan 13 item, 5,86% dengan 14 item, dan 6,31% dengan 15 item. Bank dengan kategori 16 hingga 19 item masing-masing tercatat sebesar 5,41% (16 item), 2,70% (17 item), 5,41% (18 item), dan 2,52% (19 item). Menariknya, terdapat proporsi terbesar yaitu 12,61% bank yang mengungkapkan 20 item atau lebih, menunjukkan bahwa sebagian kecil bank telah mencapai tingkat pengungkapan keamanan siber yang relatif komprehensif. Distribusi ini secara keseluruhan menunjukkan bahwa meskipun ada variasi dalam tingkat pengungkapan keamanan siber, mayoritas bank tetap berada dalam kategori menengah, dengan sebagian kecil yang menunjukkan praktik pengungkapan yang lebih luas dan mendalam.

Analisis rata-rata tahunan menunjukkan adanya peningkatan konsisten dalam tingkat pengungkapan keamanan siber di bank-bank sampel selama periode 2018 hingga 2023. Pada tahun 2018, rata-rata jumlah pengungkapan keamanan siber sebesar 9,92 item, meningkat menjadi 10,97 item pada tahun 2019 dan 11,89 pada tahun 2020. Kenaikan terus berlanjut dengan 12,16 item pada tahun 2021 serta 13,27 item pada tahun 2022. Peningkatan paling signifikan terjadi pada tahun 2023, dengan rata-rata mencapai 15,14 item. Pola ini menunjukkan adanya pergeseran positif menuju praktik pengungkapan keamanan siber yang lebih komprehensif, yang mungkin disebabkan oleh tingkat kesadaran yang meningkat mengenai risiko siber, tuntutan regulasi, serta harapan stakeholder terhadap transparansi dan akuntabilitas dalam sektor perbankan.

Pengaruh Ukuran Komite Teknologi pada Pengungkapan Keamanan Siber

Temuan yang diperoleh dari analisis regresi mengungkapkan bahwa variabel yang berkaitan dengan ukuran komite teknologi memberikan dampak positif dan signifikan secara statistik pada tingkat pengungkapan keamanan siber, dengan taraf signifikansi 1%; sehingga, hipotesis diterima. Hasil ini menunjukkan bahwa peningkatan ukuran komite teknologi dalam lembaga perbankan berkorelasi dengan peningkatan level pengungkapan keamanan siber.

Dari perspektif teori agensi, kehadiran komite teknologi yang lebih substansif meningkatkan kemanjuran pengawasan yang berkaitan dengan manajemen risiko *cyber*. Komposisi komite yang diperluas memfasilitasi diversifikasi keahlian dan fortifikasi mekanisme kontrol, sehingga mengurangi asimetri informasi yang ada antara manajemen dan pemegang saham. Selain itu, komite yang lebih besar cenderung memiliki sumber daya yang ditingkatkan yang mempromosikan kepatuhan terhadap peraturan yang lebih ketat dan standar keamanan informasi, sehingga meningkatkan transparansi dalam pengungkapan risiko cyber.

Dalam konteks teori kelembagaan baru, dampak nyata dari ukuran komite teknologi pada pengungkapan keamanan siber dapat dianggap berasal dari tekanan normatif dan mimetik yang lazim dalam industri. Lembaga perbankan yang dicirikan oleh struktur komite teknologi yang lebih besar cenderung menghadapi harapan kelembagaan yang tinggi untuk mengadopsi praktik transparansi yang selaras dengan norma industri dan persyaratan peraturan. Selain itu, keberadaan komite teknologi yang lebih luas memungkinkan bank untuk meniru praktik terbaik yang telah diadopsi oleh lembaga peer, sehingga mengamankan legitimasi dalam lingkungan bisnis yang semakin mengamanatkan pengungkapan informasi yang berkaitan dengan keamanan siber.

Studi ini memberikan bukti empiris bahwa komite teknologi memainkan peran penting dalam mendorong transparansi dan akuntabilitas di antara bank mengenai hal-hal terkait keamanan siber. Temuan ini menguatkan penelitian yang dilakukan oleh Higgs et al. (2016), yang mengidentifikasi korelasi positif dan signifikan antara kehadiran komite teknologi dan frekuensi insiden keamanan siber yang dilaporkan, menunjukkan peningkatan kesadaran organisasi dan akuntabilitas mengenai risiko cyber. Selain itu, Buckby et al. (2015) mengungkapkan bahwa kehadiran komite teknologi berkorelasi positif dengan peningkatan tingkat pengungkapan risiko, yang mencakup risiko teknologi informasi. Ini menggarisbawahi bahwa struktur tata kelola yang secara khusus mengakomodasi fungsi teknologi dapat memperkuat pengawasan dan pengungkapan dalam kaitannya dengan masalah teknologi yang semakin kritis.

Sesuai dengan ini, (Raimo et al., 2021) menunjukkan bahwa ukuran komite audit berkontribusi pada peningkatan kualitas pelaporan terintegrasi, secara fundamental menggarisbawahi pentingnya peran komite dalam dewan untuk memastikan

transparansi informasi perusahaan. Oleh karena itu, temuan ini menegaskan bahwa keberadaan dan kemampuan komite teknologi merupakan elemen penting dalam tata kelola bank yang efektif, terutama mengingat kompleksitas dan urgensi yang dihadirkan oleh ancaman cyber dalam sektor perbankan.

Hasil ini semakin memperkuat pernyataan bahwa komite teknologi sangat penting dalam bidang tata kelola perusahaan. Kehadiran dan besarnya komite teknologi berfungsi sebagai mekanisme kelembagaan yang memfasilitasi peningkatan transparansi dalam pengungkapan risiko keamanan siber kepada pemangku kepentingan. Pembentukan komite teknologi yang lebih besar dan mahir dapat menjadi keharusan strategis bagi bank yang bertujuan untuk meningkatkan akuntabilitas dan mengurangi risiko sistemik yang terkait dengan ancaman cyber. Akibatnya, peningkatan kapasitas dan peran strategis komite teknologi diantisipasi menjadi prioritas bagi bank yang berusaha untuk meningkatkan kebijakan pengungkapan keamanan siber.

SIMPULAN

Berdasarkan temuan yang diperoleh dari penelitian ini, dapat dipastikan bahwa transparansi terkait keamanan siber dalam sektor perbankan di Indonesia secara signifikan dipengaruhi oleh mekanisme tata kelola internal. Dimensi komite teknologi telah menunjukkan korelasi positif dan signifikan secara statistik dengan tingkat pengungkapan keamanan siber di antara bank-bank di Indonesia. Besarnya komite teknologi memang memberikan dampak yang menguntungkan dan patut diperhatikan pada tingkat informasi keamanan siber yang diungkapkan. Komposisi komite teknologi yang lebih besar dalam entitas berkorelasi dengan peningkatan kemungkinan organisasi mengungkapkan informasi keamanan siber yang relevan. Ini menggarisbawahi peran penting yang dimainkan kapasitas pengawasan teknologi dalam mendorong transparansi keamanan *cyber*.

Implikasi Teoritis dan Praktis

Temuan bahwa ukuran komite teknologi secara positif dan signifikan mempengaruhi pengungkapan keamanan siber berkontribusi wawasan empiris yang berharga yang menambah wacana tentang tata kelola teknologi informasi dalam konteks teori lembaga, berfungsi sebagai mekanisme kontrol internal yang bertujuan untuk mengurangi asimetri informasi antara manajemen dan pemangku kepentingan.

Sangat penting bagi manajemen perusahaan untuk meningkatkan integritas struktural komite teknologi, karena kemanjurannya dalam mempengaruhi pengungkapan keamanan siber secara positif telah dibuktikan. Ini menyoroti pentingnya membentuk komite khusus yang secara strategis menangani pertimbangan teknologi dan keamanan informasi.

DAFTAR PUSTAKA

Agustin, N. aulia, & Firdos, R. M. (2024). Studi Literatur: Ancaman Cybercrime di Indonesia dan Pentingnya Pemahaman akan Fenomena Kejahatan Digital. Jurnal Mahasiswa Teknik Informatika, 3(1), 126–131. https://doi.org/10.35473/jamastika.v3i1.2841

Al Amosh, H., & Khatib, S. F. A. (2022). *Theories of corporate disclosure: A literature review. Corporate Governance and Sustainability Review*, 6(1), 46–59. https://doi.org/10.22495/cgsrv6i1p5

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). *The drivers of cyber risk.*

Journal of Financial Stability, 60(Maret 2022), 100989. https://doi.org/10.1016/j.jfs.2022.100989

Almansi, A. A. (2018). Financial Sector ' s Cybersecurity: *Regulations and Supervision*. https://documents.worldbank.org/

Azzahrah, B. T., Naufal, M., Hamdi, R., Raynee, R., & Layla, Z. (2024). Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital : Studi Kasus dan Implementasi. Jurnal Pendidikan Tambusai, 8(2), 23934–23943.

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). *Cybersecurity awareness and market valuations. Journal of Accounting and Public Policy, xxx*(xxxx), 1–19. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

BSSN. (2024). Lanskap Keamanan Siber Indonesia 2023 (Nomor 70).

Buckby, S., Gallery, G., & Ma, J. (2015). *An analysis of risk management disclosures: Australian evidence*. Managerial Auditing Journal, 30(8/9), 812–869.

Budiyanto, D., & Mabruri, M. (2025). Pentingnya Keamanan Siber dalam Era Digital: Tinjauan Global dan Kondisi di Indonesia. Prosiding Seminar Nasional Sains dan Teknologi Seri III Fakultas Sains dan Teknologi, Universitas Terbuka, 2(1), 981–994.

Chaidir, M., Permana, N., & Yulianti, G. (2024). Pengungkapan Risiko Keamanan Siber: Dampaknya Terhadap Hubungan Pelanggan-Pemasok Dalam Rantai Pasok Perusahaan. Jurnal Visi Manajemen, 10(3), 283–296. https://stiepari.org/index.php/jvm/article/view/586%0Ahttps://stiepari.org/index.php/jvm/article/download/586/628

Cloramidine, F., & Badaruddin, M. (2023). Mengukur Keamanan Siber Indonesia Melalui Indikator Pilar Kerjasama Dalam Global Cybersecurity Index (GCI). Populis : Jurnal Sosial dan Humaniora, 8(1), 57–73. https://doi.org/10.47313/pjsh.v8i1.1957

Ernst & Young LLP. (2021). *How cybersecurity risk disclosures and oversight are evolving in 2021*. ey.com/us/boardmatters.

EY. (2022*). How cyber governance and disclosures are closing the gaps in 2022* (Nomor August 2022).

Fatihah, W. A., Putri, M. E., Dhyah, A., Putri, E., Ratnaduhita, I., Dayyan, M., Bhayangkara, U., Raya, J., History, A., Mental, K., & Digital, E. (2025). Penerapan Protokol Perlindungan Data, Serta Dukungan Dari 4.0. Jurnal Psikologi dan Bimbingan Konseling, 10(2).

Fauzi, F., Dencik, A. B., & Asiati, D. I. (2019). Metodologi Penelitian untuk Manajemen dan Akuntansi (1 ed.). Salemba Empat.

Firoozi, M., & Mohsni, S. (2023). *Cybersecurity disclosure in the banking industry: a comparative study*. International Journal of Disclosure and Governance, 20(July 2023), 451–477. https://doi.org/10.1057/s41310-023-00190-8

Gao, L., Calderon, T. G., & Tang, F. (2020). *Public companies' cybersecurity risk disclosures. International Journal of Accounting Information Systems*, 38(100468), 1–22. https://doi.org/10.1016/j.accinf.2020.100468

Haislip, J., Karim, K. E., Lin, K. J., & Pinsker, R. E. (2020). *The influences of CEO IT expertise and board-level technology committees on form 8-K disclosure timeliness.* Journal of Information Systems, 34(2), 167–185. https://doi.org/10.2308/isys-52530

Héroux, S., & Fortin, A. (2020). *Cybersecurity Disclosure by the Companies on the S & P / TSX 60 Index*. Accounting Perspectives, 19(2), 73–100. https://doi.org/10.1111/1911-3838.12220

Higgs, J. L., Pinsker, R., Smith, T., & Young, G. R. (2016). *The Relationship Between Board-Level Technology Committees and Reported Security Breaches*. Journal of Information Systems, 30(3), 1–44. https://doi.org/10.2308/isys-51402

Jia, J., Li, Z., & Munro, L. (2019). *Risk management committee and risk management disclosure: evidence from Australia*. Pacific Accounting Review, 31(3), 438–461. https://doi.org/10.1108/PAR-11-2018-0097

Kamaruzaman, S. A., Ali, M. M., Ghani, E. K., & Gunardi, A. (2019). *Ownership structure, corporate risk disclosure and firm value: A Malaysian perspective*. International Journal of Managerial and Financial Accounting, 11(2), 113–131. https://doi.org/10.1504/IJMFA.2019.099766

Kipkoech, S. R., & Rono, L. (2016). *Audit committee size, experience and firm financial performance. Evidence Nairobi Securities Exchange, Kenya*. Research Journal of Finance and Accounting, 7(15), 87–95. www.iiste.org

Li, H., No, W. G., & Wang, T. (2018). *SEC' S Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors.* International Journal of Accounting Information Systems, xxx(xxxx), 1–16. https://doi.org/10.1016/j.accinf.2018.06.003

Peng, J., & Krivacek, G. (2020). *The Growing Role of Cybersecurity Disclosures*. ISACA Journal, 1, 1–7. www.isaca.org

Raimo, N., Vitolla, F., Marrone, A., & Rubino, M. (2021). *Do Audit Committee Attributes Influence Integrated Reporting Quality? An Agency Theory Viewpoint*. Business Strategy and the Environment, 30(1), 522–534. https://doi.org/10.1002/bse.2635

Ramirez, M., Ariza, L. R., Miranda, M. E. G. M., & Vartika. (2022). *The Disclosures of Information on Cybersecurity in Listed Companies in Latin America – Proposal for a Cybersecurity Disclosure Index.* Sustainability, 14(1390), 1–23. https://www.mdpi.com

Sari, L. (2025). Determinan Pengungkapan Keamanan Siber Perbankan di Indonesia. Disertasi. Universitas Sriwijaya.

Sari, L., Adam, M., Fuadah, L. L., & Yusnaini. (2025). *Cyber Security Disclosure of Bank Syariah Indonesia: a Comparative Study.* TPM - Testing, Psychometrics, Methodology in Applied Psychology, 32(S4), 221–240.

Sari, L., Adam, M., Fuadah, L. L., & Yusnaini. (2024). *Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review.* KnE Social Sciences, 2024, 387–398. https://doi.org/10.18502/kss.v9i14.16113

Schatz, D., & Wall, J. (2017). *Towards a More Representative Definition of Cyber Security*. Journal of Digital Forensics, Security and Law, 12(2), 53–74. https://doi.org/10.15394/jdfsl.2017.1476

Sofiani, M., Ramadhanty, D. P., & Jubaedah, S. (2024). *Cyber Risk Management Disclosure: The Impact of Firm Size, Profitability, and Intangible Asset Cyber Risk Management Disclosure: The Impact of Firm Size, Profitability, and Intangible Asset.* International Journal of Entrepreneurship and Business Development, 07(05), 929–937.

Sukma, P. S., Lubis, F. K., Wulandari, K. F., Azhari, N., Islam, U., Utara, S., Islam, U.,

Utara, S., Islam, U., Utara, S., Islam, U., & Utara, S. (2025). Peran Keamanan Siber Dalam Meningkatkan Transparansi dan Akuntabilitas terhadap Laporan Keuangan di Bank Sayariah Indonesia. Jurnal Bisnis Net, 8(1), 496–505.

Taufik, N. (2024). Kajian Ketahanan Siber : Manajemen Kerentanan. In Politeknik Siber dan Sandi Negara. https://poltekssn.ac.id/wp-content/uploads/