DETERMINAN PENGUNGKAPAN KEAMANAN SIBER PERBANKAN DI INDONESIA

Disertasi Oleh :
LIA SARI
01013681924003

Diajukan sebagai salah satu syarat untuk meraih gelar Doktor
Pada
Program Studi Doktor Ilmu Ekonomi
Kekhususan Akuntansi Keuangan

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS SRIWIJAYA
FAKULTAS EKONOMI
2025

HALAMAN PENGESAHAN

Judul Disertasi	: Determinan Pengungkapan Keamanan Siber Perbankan di Indonesia
Nama	: Lia Sari
NIM	: 01013681924003
Program Studi	: Doktor Ilmu Ekonomi
Kekhususan	: Akuntansi Keuangan

Menyetujui,
Promotor,

Prof. Dr. H. Mohamad Adam, S.E., M.E.
NIP. 196706241994021002

Co Promotor 1,

Prof. Dr. Luk Luk Fuadah, S.E., MBA., Ak
NIP. 197405111999032001

Co Promotor 2,

Dr. E. Yusnaini, S.E., M.Si., Ak
NIP. 197704172010122001

Ketua Program Studi
Doktor Ilmu Ekonomi,

Prof. Dr. H. Didik Susetyo, M.Si
NIP. 196007101987031003

Dekan Fakultas Ekonomi
Universitas Sriwijaya,

Prof. Dr. Azwardi, S.E., M.Si
NIP. 196805181993031003

Tanggal Lulus : 30 Juli 2025

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas rahmat dan karunia-Nya, sehingga disertasi berjudul *"Determinan Pengungkapan Keamanan Siber pada Perbankan di Indonesia"* ini dapat diselesaikan. Penelitian ini menganalisis pengaruh keragaman dewan, ukuran komite teknologi, ukuran perusahaan, profitabilitas perusahaan, pertumbuhan perusahaan, dan kepemilikan asing terhadap pengungkapan keamanan siber, serta menguji peran moderasi kepemilikan asing pada hubungan ukuran perusahaan dan profitabilitas dengan pengungkapan keamanan siber.

Kebaruan penelitian ini terletak pada pembangunan indeks pengungkapan keamanan siber khusus perbankan Indonesia, yang disusun berdasarkan regulasi nasional dan standar internasional. Indeks ini diharapkan dapat memberikan kontribusi akademik sekaligus praktis dalam penguatan transparansi dan tata kelola risiko siber di sektor perbankan.

Penulis menyampaikan terima kasih kepada pimpinan Universitas Sriwijaya, para promotor dan pembimbing, serta seluruh pihak yang telah memberikan dukungan. Ucapan teristimewa penulis haturkan kepada keluarga tercinta atas doa dan semangat yang tiada henti. Semoga disertasi ini bermanfaat bagi pengembangan ilmu pengetahuan dan praktik pengelolaan keamanan siber di Indonesia.

Palembang, September 2025

Penulis

Lia Sari

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET & TEKNOLOGI
UNIVERSITAS SRIWIJAYA
PROGRAM STUDI DOKTOR ILMU EKONOMI
FAKULTAS EKONOMI
Jalan Raya Palembang-Prabumulih Km. 32 Inderalaya (Ogan Ilir) Kode Pos 30662
Tel: (0711) 580964, 580646 Fax:(0711) 580964
Jl. Srijaya Negara Bukit Besar Palembang 30139
Laman:http://fe.unsri.ac.id – email : dekanfe@unsri.ac.id

MATRIK PERBAIKAN DISERTASI

Nama : Lia Sari
NIM : 01013681924003
Program Studi : Doktor Ilmu Ekonomi
Kekhususan : Akuntansi Keuangan
Promotor : Prof. Dr. H. Mohamad Adam, SE., ME (.....)

Co Promotor : 1. Prof. Dr. Luk Luk Fuadah, SE., MBA., Ak (.....)*

2. Dr. E. Yusnaini, S.E., M.Si., Ak. (.....)*

No.	Dosen Penguji	Saran dan Masukan	Ket.	Tanda Tangan
1.	Prof. Dr. H. Mohamad Adam, SE., ME	-Perbaiki sesuai saran		
2.	Prof. Dr. Luk Luk Fuadah, SE., MBA., Ak	-Perbaiki sesuai saran	Acc	
3.	Dr. E. Yusnaini, S.E., M.Si., Ak.	-Perbaiki sesuai saran	Acc	
4.	Prof. Dr. Lindrianasari	-Jika tujuan penelitian sudah terjawab, sebutkan di kesimpulan dan implikasi penelitian (konfirmasi kembali IPKS di bab 5) -Tambahkan lagi referensi penelitian terdahulu, terutama untuk kepemilikan asing -Perjelas teori -Diskusikan lagi Hipotesis ke 7		
5.	Prof. Dr. Deris Setiawan	-Tambahkan referensi (tambahkan diskusi mengenai pra dan pasca insiden, laporan BSSN, framework keamanan siber, SOP, ISO 27000, dll) -Perjelas ontologi -Di bab 2 tambahkan sub section tentang telah		

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET & TEKNOLOGI
UNIVERSITAS SRIWIJAYA
PROGRAM STUDI DOKTOR ILMU EKONOMI
FAKULTAS EKONOMI
Jalan Raya Palembang-Prabumulih Km. 32 Inderalaya (Ogan Ilir) Kode Pos 30662
Tel: (0711) 580964, 580646 Fax:(0711) 580964
Jl. Srijaya Negara Bukit Besar Palembang 30139
Laman:http://fe.unsri.ac.id – email : dekanfe@unsri.ac.id

		menjawab & diskusi		
6.	Dr. Yulia Saftiana, M.Si., Ak	- Tambahkan lagi justifikasi hasil memperlemah - Perdalam Kepemilikan asing - Ukuran komite teknologi, H2 tambahkan justifikasi		Yulia

Palembang, September 2025
Ketua Program Studi
Doktor Ilmu Ekonomi,

Prof. Dr. H. Didik Susetyo, M.Si.
NIP 196007101987031003

*) paraf

SURAT PERNYATAAN BEBAS PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama	: Lia Sari
NIM	: 01013681924003
Program Studi	: Program Studi Doktor Ilmu Ekonomi
Kekhususan	: Akuntansi Keuangan

Dengan ini menyatakan bahwa disertasi dengan judul:
"Determinan Pengungkapan Keamanan Siber Perbankan di Indonesia"
adalah **benar-benar hasil karya ilmiah saya sendiri dan bukan merupakan plagiat dari karya orang lain.** Apabila di kemudian hari terbukti terdapat unsur plagiat dalam disertasi tersebut, saya bersedia menerima sanksi sesuai ketentuan yang berlaku di Universitas Sriwijaya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya untuk dipergunakan sebagaimana mestinya.

Palembang, 24 September 2025
Yang membuat pernyataan,

Lia Sari
NIM 01013681924003

UCAPAN TERIMA KASIH

Puji syukur ke hadirat Allah SWT atas segala rahmat, karunia, dan pertolongan-Nya, sehingga penulis dapat menyelesaikan disertasi dengan judul *"Determinan Pengungkapan Keamanan Siber pada Perbankan di Indonesia"*. Dalam kesempatan ini, penulis menyampaikan penghargaan dan terima kasih yang tulus kepada pihak-pihak yang telah memberikan bimbingan, dukungan, serta doa selama proses penyusunan disertasi ini.

Ucapan terima kasih penulis sampaikan kepada:

1. Rektor Universitas Sriwijaya, Bapak Prof. Dr. Taufik Marwa, S.E., M.Si
2. Dekan Fakultas Ekonomi Universitas Sriwijaya, Bapak Prof. Dr. Azwardi, S.E., M.Si.
3. Koordinator Program Studi Doktor Ilmu Ekonomi, Bapak Prof. Dr. H. Didik Susetyo, S.E., M.Si.
4. Ketua Jurusan Ekonomi Pembangunan Fakultas Ekonomi Universitas Sriwijaya, Bapak Dr. Mukhlis, S.E., M.Si.
5. Komisi Penguji Internal, Ibu Dr. Yulia Saftiana, S.E., M.Si., Ak. dan Komisi Penguji Eksternal, Prof. Dr. Deris Setiawan, M.T., Ph.D., dan Prof. Dr. Lindrianasari, S.E., M.Si., Ak., CA., Cert. DA.
6. Tim Promotor, Bapak Prof. Dr. H. Mohammad Adam, S.E., M.E., Ibu Prof. Dr. Luk Luk Fuadah, S.E., M.B.A., Ak. dan Ibu Dr. E. Yusnaini, S.E., M.Si., Ak., yang telah memberikan bimbingan, masukan dan arahan dalam penyusunan disertasi ini.
7. Seluruh Bapak Ibu Dosen Program Pascasarjana Fakultas Ekonomi Universitas Sriwijaya, untuk ilmu yang telah diberikan dengan tulus.

8. Seluruh pengelola dan staf administrasi Program Pascasarjana Fakultas Ekonomi Universitas Sriwijaya, terkhusus Ibu Komta Irawati, S.Pd atas dedikasi dan pelayanan yang telah diberikan dengan tulus.

9. Rektor Universitas Sjakhyakirti, Bapak Dr. Drs. Hermansyah, M.Si., dan para Wakil Rektor Universitas Sjakhyakirti

10. Dekan Fakultas Ekonomi Universitas sjakhyakirti, Bapak Zein Ghazali, S.E., MM., M.Si dan para wakil Dekan yang telah memberikan izin, dukungan kelembagaan, serta semangat kepada saya dalam menjalani studi doktoral ini.

11. Ketua Program Studi Akuntansi Universitas Sjakhyakirti, Ibu Masnoni, S.E., M.Si. Juga rekan-rekan kerja saya di Universitas Sjakhyakirti, yang dengan penuh pengertian memberikan dukungan selama proses studi ini berlangsung.

12. Kedua orang tua saya tercinta, Ibu Ratna Nurdjani, S.Pd dan Ayah Drs. Amir Syarif, atas doa yang tak pernah terputus, kasih sayang, dan pengorbanan yang menjadi pondasi setiap langkah saya.

13. Suami saya yang sangat saya cintai, Setia Budi, S.Kep.,Ns, atas kesabaran, dukungan, dan cinta yang menjadi energi utama dalam menghadapi segala dinamika studi ini.

14. Anak-anak saya yang saya banggakan, Achmad Zaki Hilmi, Farhan Muzhaffar Hafizzuddin, Halwa Nur Amalina, Alina Nur'aini dan Rizka Arsyila yang senantiasa menjadi sumber semangat dan pengingat akan tujuan besar dalam hidup saya.

15. Keluarga besar saya kakak, adik, ipar, mamang, bibik, dan seluruh saudara, atas dukungan moral, spiritual, dan materiil yang tidak ternilai harganya.

16. Sahabat seperjuangan di Program Studi Doktor Ilmu Ekonomi Universitas Sriwijaya, Dr. Septiani Fransisca, Dr. Yuni Ekawarti, Dr. Mahdi Hendrich, Dr. Lisa Hermawati, Dr. Siti Khairani, Dr. Maulan Irwadi, (Cand) Dr. Indah Sari

dan (Cand) Dr. Idham Chalid, atas kebersamaan, diskusi ilmiah, serta motivasi yang saling menguatkan.

17. Semua pihak, yang tidak bisa saya sebutkan satu persatu, yang telah berperan dalam penyelesaian disertasi ini.

Akhirnya, penulis menyadari bahwa disertasi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan demi penyempurnaan karya ilmiah ini. Semoga disertasi ini bermanfaat bagi pengembangan ilmu pengetahuan dan praktik di bidang ekonomi, khususnya terkait pengungkapan keamanan siber pada perbankan di Indonesia.

Palembang, September 2025

Lia Sari

BAB I

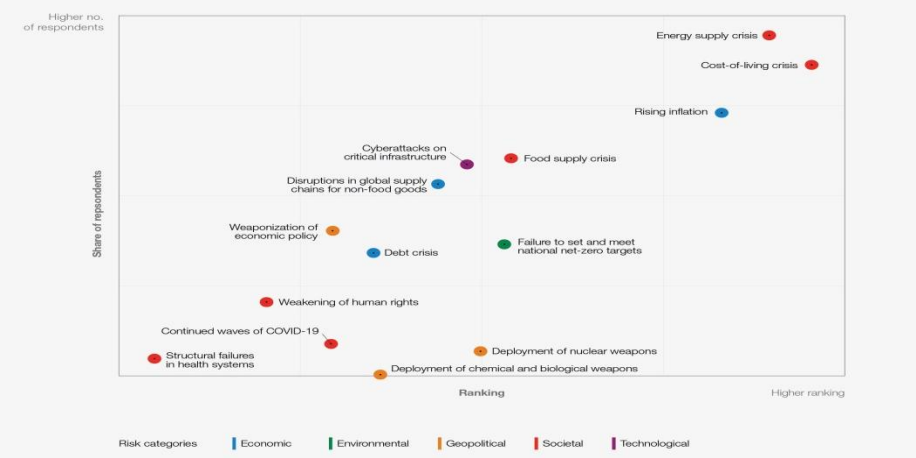
PENDAHULUAN

1.1 Latar Belakang Penelitian

Selama satu dekade terakhir, digitalisasi terjadi di segala bidang, termasuk perbankan. Perkembangan digitalisasi berlangsung dengan sangat cepat yang menawarkan kemudahan dan kepraktisan dalam aktivitas keuangan. Digitalisasi perbankan melibatkan penggunaan teknologi digital dalam kegiatan perbankan.

Digitalisasi dan teknologi digital juga menimbulkan ancaman berupa ancaman siber. Risiko siber menjadi salah satu risiko terbesar perusahaan yang menggunakan sistem teknologi informasi dalam kegiatan operasionalnya (Georg-Schaffner & Prinz, 2021). *Global Risks Perception Survey* (GRPS) 2022-2023 yang dilakukan oleh *World Economic Forum* menunjukkan bahwa "Serangan siber terhadap infrastruktur penting" sebagai salah satu risiko dari 5 besar teratas tahun 2023 dengan risiko terbesar potensi dampaknya pada skala global, terlihat pada Gambar 1.1 (World Economic Forum, 2023).

Sistem keuangan global sedang mengalami transformasi digital yang belum pernah terjadi sebelumnya, dan hal ini dipercepat oleh pandemi COVID-19 (https://www.imf.org, 2021). Bank semakin intensif menggunakan teknologi informasi dalam operasionalnya. Saat ini sedang marak transformasi ke mata uang digital dan modernisasi sistem pembayaran, dimana keamanan siber menjadi semakin penting.



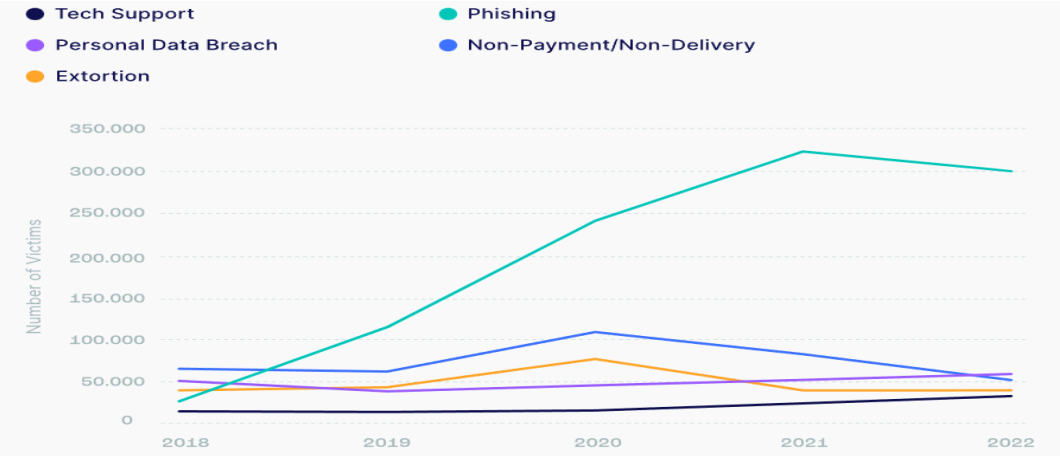
Sumber : *World Economic Forum Global Risks Perception Survei* 2022-2023

Gambar 1.1
Top Risiko Global

Pelaku kejahatan mengambil keuntungan dari transformasi digital ini dan menimbulkan ancaman yang semakin besar terhadap sistem keuangan global, stabilitas keuangan, dan kepercayaan terhadap integritas sistem. Pandemi ini bahkan telah memberikan target baru bagi para peretas. Sektor keuangan mengalami serangan siber terkait COVID-19 terbesar kedua, setelah sektor kesehatan (https://www.imf.org, 2021).

Ancaman terhadap keamanan siber adalah masalah global. Meskipun serangan siber di negara maju cenderung merugikan dengan nilai kerugian yang besar, namun peningkatan jumlah serangan di negara berkembang juga perlu mendapat perhatian. Karena di negara-negara berkembang dorongan menuju inklusi keuangan lebih besar terjadi, sehingga banyak orang beralih ke layanan keuangan digital seperti sistem pembayaran seluler. Layanan keuangan digital juga menawarkan lingkungan yang kaya akan target bagi para peretas (https://www.imf.org).

Gambar 1.2 berikut menunjukkan 5 besar jenis kejahatan siber yang terjadi dalam 5 tahun terakhir (2018-2022) berdasarkan *global cybercrime report*, yaitu *Phising, Non-Payment/Non-Delivery, Personal data Breach, Extortion,* dan *Tech Support*.



Sumber : https://seon.io/resources/global-cybercrime-report/

Gambar 1.2
Top 5 Kejahatan Siber secara Global

Keamanan siber telah menjadi dimensi baru dalam pengelolaan manajemen risiko (Azzahrah et al., 2024; Li et al., 2018). Keamanan siber dapat didefinisikan sebagai pengamanan informasi dan perlindungan terhadap sistem elektronik, jaringan, peralatan, program ataupun data dari pencurian ataupun kerusakan (Schatz & Wall, 2017). Keamanan siber telah menjadi salah satu isu yang penting saat ini (Budiyanto & Mabruri, 2025; Cloramidine & Badaruddin, 2023). Sejalan dengan itu, pentingnya kesadaran perusahaan dalam mengelola ancaman siber perlu ditingkatkan. Kesadaran melindungi aset digital merupakan perhatian penting dari

perusahaan karena serangan siber dapat berpengaruh terhadap kinerja perusahaan, bahkan kesejahteraan mental (Fatihah et al., 2025).

Pesatnya perkembangan teknologi informasi, diikuti dengan tingginya serangan siber (Aldasoro et al., 2022; Budiyanto & Mabruri, 2025), mendorong *stakeholder* untuk memperoleh kepastian bahwa perusahaan telah melaksanakan manajemen terkait keamanan siber dengan baik . Pengungkapan keamanan siber (*cyber security disclosure*) adalah agenda pengungkapan perusahaan yang relatif baru. Tingginya serangan siber memunculkan kebutuhan *stakeholder* akan informasi yang memadai terkait keamanan siber. *Stakeholder* menuntut transparansi dari perusahaan publik mengenai manajemen risiko keamanan siber. Untuk mengatasi kekhawatiran yang meningkat ini, setiap perusahaan publik harus memastikan tata kelola keamanan siber yang kuat dan memberikan pengungkapan yang memadai tentang bagaimana keamanan siber diprioritaskan dan dikelola.

Perusahaan dengan manajemen risiko yang aktif seharusnya mampu mengidentifikasi dan menangani risiko secara efektif (Kamaruzaman et al., 2019). Pengungkapan manajemen risiko memberikan keuntungan bagi perusahaan dan para *stakeholder*. Berbagai metode untuk memperkuat keamanan siber meliputi peningkatan kapasitas, pengembangan sistem perlindungan dan keamanan yang berfokus pada pertahanan siber, serta peningkatan komunikasi dan sinergi, koordinasi, jaringan, serta kolaborasi teknis untuk menciptakan komunitas keamanan siber (Agustin & Firdos, 2024).

Perusahaan publik harus memahami pentingnya keamanan siber dan melakukan pengungkapan yang memadai untuk masalah ini (Sofiani et al., 2024).

Pengungkapan tersebut akan memungkinkan perusahaan untuk menunjukkan akuntabilitas dan keterlibatan mereka dalam masalah ini dan membangun kepercayaan *stakeholder*. Perusahaan publik seharusnya tidak hanya melaksanakan program manajemen risiko siber yang efektif tetapi juga memberikan informasi yang tepat waktu dan berguna tentang inisiatif tersebut kepada *stakeholder* melalui pengungkapan keamanan siber.

Dalam beberapa tahun terakhir, badan regulator di Amerika Serikat dan Kanada telah menyoroti pentingnya pengungkapan keamanan siber dan menerbitkan panduan terperinci (Gao et al., 2020; Héroux & Fortin, 2020). Pengungkapan keamanan siber telah menjadi perhatian para peneliti akuntansi akhir-akhir ini. Namun, sebagian besar dari penelitian terdahulu dilakukan dalam konteks amerika serikat, di mana pengungkapan keamanan siber merupakan *quasi-compulsory* (Mazumder & Hossain, 2022). Penelitian terdahulu menunjukkan langkanya penelitian pengungkapan keamanan siber dalam konteks negara berkembang (Sari et al., 2024), yang berisiko lebih tinggi menjadi sasaran serangan siber. Oleh karena itu, penelitian ini dilakukan dalam konteks Indonesia yang merupakan negara berkembang, dimana pengungkapan keamanan siber merupakan pilihan pengungkapan sukarela bagi perusahaan.

Fenomena meningkatnya penggunaan teknologi digital di Indonesia juga diikuti dengan meningkatnya ancaman keamanan siber (Budiyanto & Mabruri, 2025; Cloramidine & Badaruddin, 2023). Berdasarkan data *X-Force Threat Intelligence Index* 2022, IBM *Security*, serangan siber yang terjadi pada 10 besar industri di 2021 sebanyak 22,4% terjadi pada industri keuangan dan asuransi

dengan rincian 70% serangan yang ditujukan kepada perbankan, 16% perusahaan asuransi, dan 14% sektor keuangan lainnya (https://www.ojk.go.id, 2022). Laporan BSSN menunjukkan bahwa terdapat hampir 1 miliar serangan siber di Indonesia pada tahun 2022. Paling banyak terjadi berupa *malware* sebanyak 56,84%, diikuti dengan kebocoran data sebanyak 14,75%, *Trojan activity* sebanyak 10,9% dan lain-lain 17,51% (https://www.antaranews.com).

Laporan BSSN tahun 2023 menunjukkan bahwa Indonesia merupakan negara teratas yang menjadi top 10 sumber anomali dan juga negara teratas yang menjadi top 10 tujuan anomali (BSSN, 2024; Taufik, 2024). Indonesia menempati urutan teratas sumber dan tujuan anomali, diikuti oleh Amerika serikat, Singapura, Jerman, Belanda, Prancis, Rusia, Tiongkok, Republik Moldova, dan Republik Ceko.

Kasus serangan siber Bank Syariah Indonesia (BSI) pada awal Mei 2023 menunjukkan bahwa risiko siber nyata adanya. Pada Sabtu, 13 Mei 2023, geng *ransomware LockBit* mengaku bertanggung jawab atas gangguan semua layanan di BSI, dan menyatakan insiden *down* di bank tersebut adalah perbuatan mereka. Pada serangan itu, 15 juta catatan pelanggan, informasi karyawan, dan sekitar 1,5 *terabyte* data internal telah dicuri. Pada akhirnya, data tersebut ditemukan telah dirilis di internet karena negosiasi gagal (kompas.com).

Serangan siber yang menargetkan Pusat Data Nasional (PDN) Indonesia tahun 2024 adalah salah satu bukti nyata betapa tidak siapnya infrastruktur keamanan siber kita dalam menghadapi ancaman siber yang semakin kompleks (Ramadhani et al., 2025). Dampak finansial serangan siber bisa berupa uang

tebusan, biaya respons dan pemulihan, biaya hukum, pemantauan, dan biaya tambahan tak terduga lainnya. Selain itu, korban juga harus menanggung potensi kerugian kehilangan reputasi.

Meskipun tidak ada sektor yang kebal dari serangan siber, penelitian ini difokuskan pada sektor perbankan karena tiga alasan. Pertama, risiko serangan siber pada bisnis perbankan dan keuangan lebih besar daripada bisnis di industri lain (Almansi, 2018). Direktur Penelitian, Departemen Penelitian dan Pengaturan Perbankan Otoritas Jasa Keuangan (OJK) menyatakan, industri keuangan atau perbankan merupakan sektor yang menjadi peringkat pertama atau paling banyak mendapatkan serangan siber (Kontan.co.id, 2022).

Kedua, penelitian terdahulu menunjukkan bahwa pengungkapan keamanan siber di perbankan berbeda dengan perusahaan lainnya. Perusahaan di sektor keuangan melaporkan indeks pengungkapan keamanan siber tertinggi dan terus tumbuh secara signifikan (Ramirez et al., 2022). Bank sebagai industri dengan intensitas penggunaan teknologi informasi yang tinggi, pengungkapan keamanan sibernya cenderung berbeda dibanding perusahaan lain (Gao et al., 2020). Perusahaan-perusahaan di sektor keuangan, terutama bank, bersifat *highly regulated* dan persyaratan pengungkapan mereka berbeda dari perusahaan di sektor lain (Haislip et al., 2020).

Ketiga, regulasi dan peraturan terkait keamanan siber di Indonesia, sektor keuangan khususnya perbankan merupakan fokus utama pemerintah, karena sektor ini paling berisiko untuk mengalami serangan siber. Pemerintah melalui OJK menerbitkan Peraturan Nomor 11/POJK.03/2022 tentang Penyelenggaraan

Teknologi Informasi oleh Bank (https://www.aseanbriefing.com, 2023). OJK menjabarkan aturan tersebut dalam surat edaran nomor 29/SEOJK.03/2022 (SEOJK 29) tanggal 27 Desember 2022. Peraturan ini dikhususkan untuk perbankan di Indonesia, dan belum ada peraturan serupa yang ditujukan untuk sektor lain.

Tabel 1.1
5 Emiten dengan Nilai Kapitalisasi Pasar Terbesar di BEI

No.	Kode	Emiten	Jumlah Saham Beredar	Kapitalisasi Pasar
1.	BBCA	Bank Central Asia Tbk.	122.042.299.500	1.067.870.121
2.	BBRI	PT Bank Rakyat Indonesia (Persero) Tbk	150.043.411.587	709.705.337
3.	BYAN	Bayan Resources Tbk	33.333.335.000	692.500.035
4.	BMRI	Bank Mandiri (Persero) Tbk.	46.199.999.998	477.015.000
5.	TLKM	Telkom Indonesia (Persero) Tbk.	99.062.216.600	402.192.599

Sumber : idx.co.id, 2022

Perbankan di Indonesia mendominasi pasar saham dengan *market capitalization* yang besar (lihat Tabel 1.1). Pada akhir penutupan perdagangan tahun 2022, kapitalisasi pasar atau *market capitalization* Bursa Efek Indonesia (BEI) tercatat sebesar Rp 9.499,14 triliun (DataIndonesia.id). Dua emiten perbankan menempati posisi teratas sebagai saham berkapitalisasi pasar terbesar yakni PT Bank Central Asia Tbk. (BBCA) dan PT Bank Rakyat Indonesia (persero) Tbk. (BBRI). Dari 825 emiten yang sahamnya telah tercatat di BEI, PT Bank Central Asia Tbk. (BBCA) berada di posisi puncak saham dengan kapitalisasi pasar terbesar mencapai Rp1.067,87 triliun. Proporsi nilai tersebut setara dengan 10,98%

dari total *market capitalization*. Saham dengan kapitalisasi pasar terbesar kedua ditempati oleh PT Bank Rakyat Indonesia (persero) Tbk. (BBRI) dengan nilai mencapai Rp709,71 triliun. 709.705. Nilai tersebut setara dengan 7,80% dari total *market capitalization*. Posisi ke empat adalah PT Bank Mandiri (Persero) Tbk. (BMRI) dengan nilai kapitalisasi pasar mencapai Rp477,02 triliun atau 4,83% dari total *market capitalization*.

Saat ini, perbankan menggunakan berbagai teknologi keuangan, seperti *mobile banking, internet banking*, prosedur pinjaman tanpa kertas, mata uang digital, *blockchain*, dll. Deputi Direktur Basel & Perbankan Internasional, Departemen Penelitian dan Pengaturan Perbankan OJK mengatakan, serangan siber yang sering dialami perbankan menyangkut lima hal, diantaranya *unencrypted data, malware, unsecured third party services, manipulated data*, dan *website* atau *application spoofing*. Diprediksi, probabilitas serangan siber di sektor keuangan di masa depan bisa semakin meningkat jika bank-bank tidak siap melakukan mitigasi keamanan siber (https://ekonomi.republika.co.id, 2022). Serangan siber menyerang data pribadi dan organisasi (Adriansyah & Anugrah, 2024). Serangan siber berpotensi menyebabkan kerugian data dan finansial serta gangguan bisnis (Azzahrah et al., 2024), juga merusak reputasi dan kepercayaan publik terhadap institusi (Sukma et al., 2025).

Regulasi mengenai pengungkapan risiko dalam laporan tahunan mengacu kepada Surat Edaran Otoritas Jasa Keuangan Nomor 16/SEOJK.04/2021 tentang Bentuk dan Isi Laporan Tahunan Emiten Atau Perusahaan Publik. Perusahaan diwajibkan untuk mengungkapkan jenis dan tingkat risiko. Bagi perbankan,

regulasi mengenai manajemen risiko teknologi informasi diatur dalam POJK Nomor 38/POJK.03/2016 sebagaimana telah diubah menjadi POJK Nomor 13/POJK.03/2020.

Pada 2022, OJK telah menerbitkan Peraturan OJK No.11/POJK.03/2022 mengenai penyelenggaraan teknologi informasi oleh bank umum atau PTIB. Aturan ini menggantikan POJK Nomor 13/POJK.03/2020. Saat ini, PTIB baru mencakup aspek data, teknologi, manajemen risiko, kolaborasi dan tatanan institusi bank umum dalam rangka meningkatkan ketahanan dan kematangan operasional bagi bank umum. Aturan baru yang dikembangkan Otoritas Jasa Keuangan (OJK) ini merupakan aturan keamanan siber pertama di Indonesia yang dikhususkan untuk sektor keuangan, khususnya perbankan. OJK menjabarkan aturan tersebut dalam surat edaran Nomor 29/SEOJK.03/2022 (SEOJK 29) tanggal 27 Desember 2022. Surat edaran tersebut berisi rincian pelaksanaan Peraturan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank (https://www.aseanbriefing.com, 2023). Dari aturan-aturan yang ada, pengungkapan keamanan siber belum menjadi kewajiban bagi perusahaan.

Perusahaan publik harus mampu memberikan informasi terbaik sebagai proksi atas kinerjanya. Investor akan menggunakan informasi tersebut dalam menilai, memprediksi, serta mengambil keputusan terhadap suatu saham perusahaan. Informasi-informasi penting mengenai kinerja perusahaan tercermin dalam laporan tahunan. Selain informasi keuangan, investor juga memerlukan informasi non keuangan untuk membuat keputusan investasi. Informasi berupa pengungkapan sukarela dianggap dapat meningkatkan nilai perusahaan karena

perusahaan dinilai lebih transparan. Chaidir et al. (2024) menemukan bahwa transparansi dalam pengungkapan risiko siber dapat meningkatkan kepercayaan, stabilitas hubungan, dan efisiensi operasional dalam rantai pasok.

Pengungkapan yang jelas dan mudah dipahami dapat meningkatkan transparansi dan akuntabilitas laporan keuangan (Sukma et al., 2025). Pengungkapan keamanan siber dalam laporan tahunan memungkinkan perusahaan publik untuk mengungkapkan kepada pasar bahwa perusahaan secara aktif terlibat dalam mencegah, mendeteksi, dan memperbaiki dampak serangan siber. Sari et al. (2025) menemukan bukti bahwa pengungkapan keamanan siber menunjukkan peningkatan setelah terjadinya insiden keamanan siber. Pengungkapan keamanan siber berfungsi untuk mengurangi biaya litigasi potensial karena pengurangan kewajiban akibat peningkatan transparansi yang terkait dengan pengungkapan. Berkman et al., (2018) menemukan adanya hubungan positif antara kesadaran keamanan siber dan nilai pasar.

Fenomena terkait pengungkapan keamanan siber pada perbankan Indonesia yang penulis amati adalah sebagai berikut :

1. Belum ada aturan tertulis dari pihak berwenang, misalnya Otoritas jasa Keuangan (OJK) ataupun BAPEPAM , mengenai pengungkapan keamanan siber, baik yang wajib ataupun sukarela.
2. Tingginya tingkat serangan siber, terutama terhadap perbankan Indonesia membuat *stakeholder* membutuhkan informasi terkait keamanan siber yang memadai. Namun, pengungkapan keamanan siber oleh perbankan Indonesia bervariasi, bahkan cenderung rendah.

Dalam penelitian ini, penulis akan membatasi pengukuran item pengungkapan keamanan siber pada bab ataupun sub bab dengan judul Teknologi Informasi yang ada dalam laporan tahunan perbankan. Batasan ini penulis lakukan karena teknologi informasi berkaitan erat dengan siber dan keamanan siber. Selain itu, batasan itu diharapkan akan meningkatkan fokus penelitian ini yang menggunakan konten analisis.

Penulis mengamati fenomena terkait pengungkapan keamanan siber pada perbankan di Indonesia. Dari laporan tahunan perbankan yang terdaftar di Bursa Efek Indonesia pada tahun 2018-2022 (224 bank yang penulis amati), 80,8% memiliki bab ataupun sub bab dengan judul Teknologi Informasi, dalam laporan tahunannya. 19,2% tidak memiliki bab ataupun sub bab dengan judul Teknologi Informasi, dalam laporan tahunannya. Namun, panjangnya pengungkapan dalam bab ataupun sub bab dengan judul Teknologi Informasi bervariasi antar bank. Jika dilihat berdasarkan jumlah halaman bab ataupun sub bab dengan judul Teknologi Informasi, maka didapatkan informasi sebagai berikut :

Tabel 1.2
Jumlah Halaman Teknologi Informasi
dalam Laporan Tahunan Bank tahun 2018-2022

No.	Jumlah halaman	Jumlah Laporan Tahunan Bank	Persentase
1	0	43	19,19
2	1-5	103	45,98
3	6-10	45	20,09
4	11-15	19	8,48
5	16-20	12	5,36
6	>20	2	0,9
Total		**224**	**100**

Sumber : Diolah Penulis, 2025

Dari Tabel 1.2 diatas terlihat bahwa 19,19% bank tidak memiliki bab/ sub bab teknologi informasi. Sebagian besar Bank (45,98%) hanya mengungkapkan 1 hingga 5 halaman, 20,09% hanya mengungkapkan 6-10 halaman, 8,48% mengungkapkan 11-15 halaman, 5,36% yang mengungkapkan hingga 20 halaman. dan hanya 0,9% yang mengungkapkan lebih dari 20 halaman. Panjang pengungkapan keamanan siber yang bervariasi antar bank, menarik untuk diteliti lebih jauh, faktor apa saja yang mempengaruhi variasi tersebut.

Telaah literatur terhadap penelitian-penelitian terdahulu terkait determinan pengungkapan keamanan siber dan hasil analisis *vos viewer* yang memperlihatkan peta penelitian terkait pengungkapan keamanan siber (tabel 3 di halaman 35-38 dan gambar 3 di halaman 39) menunjukkan bahwa tema penelitian terkait keamanan siber dalam bidang akuntansi berkaitan erat dengan tata kelola perusahaan, tata kelola teknologi informasi, kewaspadaan keamanan siber, pengungkapan risiko, dan pengungkapan keamanan siber. Topik mengenai determinan pengungkapan keamanan siber masih jarang diteliti. Lebih jauh lagi, penelitian mengenai determinan pengungkapan keamanan siber di Indonesia merupakan topik penelitian baru, dan masih jarang dilakukan.

Penelitian ini merujuk penelitian-penelitian terdahulu dengan beberapa pengembangan. Berdasarkan *new institutional theory, agency theory* dan *upper echelon theory,* penelitian ini menyelidiki determinan pengungkapan keamanan siber pada perbankan di Indonesia. Penelitian ini bertujuan untuk menguji secara empiris faktor-faktor yang diduga sebagai determinan pengungkapan keamanan siber perbankan di indonesia. Penelitian ini akan mengkaji pengaruh keragaman

dewan, ukuran komite teknologi, faktor karakteristik perusahaan (ukuran perusahaan, profitabilitas, *growth opportunity*), dan kepemilikan asing terhadap pengungkapan keamanan siber. Penelitian ini juga akan menyelidiki pengaruh moderasi kepemilikan asing dalam memperkuat pengaruh ukuran perusahaan dan profitabilitas perusahaan terhadap pengungkapan keamanan siber. Penelitian ini juga akan mengembangkan indeks pengungkapan keamanan siber untuk sektor perbankan. Penelitian ini menarik untuk diteliti karena penelitian terkait pengungkapan keamanan siber masih relatif jarang dilakukan (Gao et al., 2020). Penelitian terdahulu juga menunjukkan *research gap* yang membuat topik determinan pengungkapan keamanan siber semakin menarik untuk diteliti.

Dalam kerangka *Upper Echelon Theory*, Hambrick & Mason (1984) mengemukakan bahwa karakteristik demografis anggota dewan direksi, seperti gender, pengalaman, dan pendidikan, mencerminkan nilai dan pola pikir mereka, yang pada akhirnya membentuk kebijakan organisasi termasuk pendekatan terhadap risiko non-keuangan. Dari sudut pandang *the agency theory,* kehadiran anggota dewan perempuan yang lebih banyak dapat meminimalkan asimetri informasi dan meningkatkan transparansi perusahaan dan lingkungan informasi (Radu & Smaili, 2022). Fokus pada keragaman gender (*gender diversity*) penting karena sejumlah riset menunjukkan bahwa perempuan cenderung memiliki orientasi kehati-hatian dan kepedulian terhadap pemangku kepentingan yang lebih tinggi, yang dapat mendorong pengungkapan informasi CSR maupun kebijakan risiko termasuk keamanan siber (AlJanadi, 2025).

Dari ranah empiris, Héroux & Fortin (2024) dalam studi terhadap 250 perusahaan pada *S&P/TSX Composite* menemukan bahwa atribut dewan, termasuk jumlah perempuan, berkorelasi positif dengan tingkat pengungkapan risiko keamanan siber, khususnya aspek mitigasi risiko dan *governance cybersecurity*. Penelitian lain menemukan hasil serupa, bahwa keragaman gender dalam dewan berpengaruh positif signifikan terhadap pengungkapan keamanan siber (Mazumder & Hossain, 2022; Radu & Smaili, 2022). Sementara itu, penelitian di India terhadap 30 perusahaan keuangan yang terdaftar di S&P BSE 150 (2013–2022) menunjukkan bahwa keragaman gender tidak berpengaruh signifikan terhadap pengungkapan keamanan siber (Shukla & Pandey, 2023). Dengan dasar *upper echelon theory* dan *agency theory* temuan empiris tersebut, penelitian ini akan menelaah bagaimana keragaman dewan mempengaruhi level pengungkapan keamanan siber.

Regulator dan investor membutuhkan informasi tentang tata kelola terkait keamanan siber. Pembentukan komite teknologi yang terpisah dari komite lainnya (seperti komite risiko, komite audit), dapat meningkatkan tata kelola teknologi informasi dengan meningkatkan kemungkinan pengungkapan keamanan siber dan membantu menunjukkan kredibilitas terkait keamanan siber termasuk tindakan pencegahan dan identifikasi serangan siber (Higgs et al., 2016). Pembentukan komite teknologi menunjukkan praktek tata kelola perusahaan yang baik. Hal ini menunjukkan pada pasar bahwa perusahaan mau dan mampu untuk melaksanakan manajemen risiko terkait teknologi informasi melalui pembentukan komite teknologi.

Dari sudut pandang *the new institutional theory,* pembentukan komite teknologi menunjukkan komitmen perusahaan untuk memenuhi tuntutan lingkungan institusional terkait keamanan siber. Keberadaan komite teknologi memberikan petunjuk kepada *stakeholder* bahwa perusahaan memiliki komitmen untuk memastikan keamanan siber (Higgs et al., 2016). Peng & Krivacek (2020) merekomendasikan pembentukan komite keamanan siber di dalam direksi untuk menilai risiko perusahaan terkait keamanan siber. Higgs et al. (2016) menggunakan istilah komite teknologi dalam penelitiannya dan menemukan bahwa perusahaan yang memiliki komite teknologi melaporkan lebih banyak *breaches* daripada perusahaan tanpa komite teknologi.

Penelitian-penelitian terdahulu yang menyelidiki peran komite teknologi dalam deteksi dan pelaporan insiden siber menggunakan *dummy* untuk komite teknologi (Berkman et al., 2018; Haislip et al., 2020; Higgs et al., 2016). Penelitian ini akan menggunakan ukuran komite teknologi sebagai faktor determinan. Semakin besar ukuran komite teknologi dimana semakin besar jumlah anggota komite teknologi, maka akan semakin banyak yang mengawasi dan mengarahkan perusahaan dalam hal keamanan siber. Ukuran komite teknologi yang besar menunjukkan komitmen perusahaan yang tinggi terkait keamanan siber. Hal ini akan berpengaruh positif terhadap level pengungkapan keamanan siber perusahaan. Ukuran komite teknologi diduga dapat meningkatkan level pengungkapan keamanan siber oleh perusahaan. Literatur terkait komite audit menunjukkan bahwa ukuran komite audit yang lebih besar dapat meningkatkan fungsi pengawasan, dan

hasil empiris menunjukkan bahwa ukuran komite audit mempunyai pengaruh positif terhadap kualitas pelaporan terintegrasi (Raimo et al., 2021).

Karakteristik perusahaan yang akan diteliti dalam penelitian ini ada tiga, yaitu ukuran perusahaan, profitabilitas, dan *growth opportunity*. *The new institutional theory* memandang bahwa, perusahaan besar cenderung menerima lebih banyak tekanan *stakeholders* untuk melakukan pengungkapan keamanan siber. *The agency theory* memandang bahwa semakin besar ukuran perusahaan, semakin besar kemampuan perusahaan untuk membiayai pengungkapan keamanan siber yang lebih banyak dan lengkap dalam rangka meminimalkan asimetri informasi (Radu & Smaili, 2022). Besarnya asset yang dimilikinya membuat perusahaan mampu membayar biaya tambahan untuk pengungkapan tersebut (Mazumder & Hossain, 2022; Radu & Smaili, 2022). Disaat usaha kecil dan menengah sering kali kesulitan membangun infrastruktur keamanan teknologi informasi, perusahaan besar dan multinasional dituntut untuk memiliki sumber daya keuangan dan struktur tata kelola untuk merespons dan beradaptasi terhadap tantangan ancaman siber (Georg-Schaffner & Prinz, 2021)

Perusahaan besar dan terdaftar lebih besar kemungkinannya untuk menarik minat investor, sehingga perusahaan-perusahaan tersebut harus lebih bersedia untuk mematuhi praktik pengungkapan (Ibrahim & Karajeh, 2020). Selain itu, laporan tahunan perusahaan-perusahaan terkemuka menjadi tolok ukur praktik terbaik pengungkapan. Dalam penelitian ini, ukuran perusahaan akan menggunakan ukuran total aset, karena total aset yang dimiliki perusahaan menunjukkan kemampuan perusahaan untuk membayar biaya tambahan terkait pengungkapan keamanan

siber. Total aset tepat digunakan sebagai proksi ukuran perusahaan untuk sektor perbankan yang merupakan perusahaan jasa, selain itu, ukuran ini sudah banyak digunakan pada penelitian-penelitian sebelumnya (Mazumder & Hossain, 2022; Radu & Smaili, 2022). Penelitian mengenai ukuran perusahaan menunjukkan hasil yang berbeda-beda, penelitian Gao et al. (2020) menemukan hasil positif signifikan dan negatif signifikan. Hasil positif dan signifikan juga ditemukan oleh Radu & Smaili (2022). Mazumder & Hossain (2022) menemukan hasil yang tidak signifikan.

Dari sudut pandang *the new institutional theory,* perusahaan dengan tingkat profitabilitas yang tinggi lebih mampu untuk melakukan pengungkapan keamanan siber yang lebih luas, dalam rangka menghadapi tekanan dari lingkungan institusional terkait manajemen keamanan siber. Kinerja keuangan dan ekonomi perusahaan mempunyai hubungan positif dengan pengungkapan informasinya. Perusahaan yang memiliki pendapatan tinggi lebih mampu memberikan pengungkapan sukarela seperti informasi strategis, keuangan dan tanggung jawab sosial perusahaan (Ibrahim & Karajeh, 2020). Meskipun memberikan informasi ini kepada *stakeholder* umumnya meningkatkan biaya, hal ini mungkin dianggap sebagai kontribusi sosial berharga yang diberikan oleh perusahaan. Penelitian terdahulu tentang pengaruh profitabilitas terhadap pengungkapan keamanan siber menunjukkan hasil yang positif signifikan (Radu & Smaili, 2022) dan positif tidak signifikan (Gao et al., 2020; Mazumder & Hossain, 2022). Penelitian ini akan menggunakan ROA sebagai ukuran profitabilitas, karena ROA menggambarkan seberapa efektif perusahaan menghasilkan laba bersih dari total aset yang

dimilikinya. Proksi ini dipilih karena penulis menilai bahwa ROA tepat untuk menggambarkan profitabilitas pada perusahaan jasa seperti bank. Selain itu, ROA telah banyak digunakan pada penelitian-penelitian terdahulu sebagai proksi profitabilitas.

Faktor *growth opportunity* juga diduga merupakan determinan pengungkapan keamanan siber. Dari sudut pandang *the new institutional theory,* bank dengan potensi pertumbuhan yang lebih tinggi cenderung mengurangi tekanan institusional dari pemangku kepentingan internal dan investor dengan menyediakan pengungkapan sukarela yang luas termasuk pengungkapan keamanan siber. Dari sudut pandang *agency theory,* perusahaan yang bertumbuh cenderung mengalami asimetri informasi dan biaya agensi yang lebih besar, sehingga bank-bank dengan tingkat pertumbuhan yang lebih tinggi berpotensi untuk mengurangi asimetri informasi dengan menyediakan pengungkapan keamanan siber yang lebih besar (Mazumder & Hossain, 2022).

Namun, berbeda dengan teori, bukti empiris dari penelitian terdahulu menunjukkan hasil berbeda. Radu & Smaili (2022) juga Mazumder & Hossain (2022) menemukan pengaruh negatif sigifikan *growth opportunity* terhadap pengungkapan keamanan siber. *Growth opportunity* dalam penelitian ini akan menggunakan ukuran MBVR. MBVR atau *market to book value rasio* menggambarkan pandangan investor terhadap nilai perusahaan, dan rasio ini mampu menggambarkan peluang pertumbuhan suatu perusahaan di masa depan. MBVR tepat digunakan sebagai proksi *growth opportunity* karena penelitian ini menyelidiki perbankan yang terdaftar di Bursa Efek Indonesia.

Penelitian terdahulu menunjukkan bahwa adanya *guidance* ataupun panduan dan aturan yang dikeluarkan oleh regulator memberikan pengaruh yang signifikan terhadap pengungkapan keamanan siber (Gao et al., 2020). Panduan SEC tentang pengungkapan keamanan siber tahun 2018 memperluas cakupan pengungkapan keamanan siber (Peng & Krivacek, 2020). Meskipun panduan tersebut dimaksudkan untuk perusahaan publik amerika serikat, dampak kepatuhannya bisa berdampak luas, karena panduan tersebut juga diaplikasikan untuk anak perusahaan asing mereka.

Kepemilikan asing akan membawa pengetahuan dan wawasan terkait praktek pengungkapan keamanan siber dari berbagai negara. Dari sudut pandang *the new institutional theory,* kepemilikan asing dapat mendorong proses isomorfisme terkait pengungkapan keamanan siber. Semakin besar persentase kepemilikan asing dalam suatu bank, maka akan semakin besar dorongan untuk melaksanakan praktek terbaik pengungkapan keamanan siber seperti halnya pada perusahaan-perusahaan di negara maju, yang sudah lebih mapan dalam hal pengungkapan keamanan siber. Kepemilikan asing berpengaruh terhadap pengungkapan keamanan siber.

Teori *Upper Echelon* yang dikembangkan oleh Hambrick & Mason (1984) menyatakan bahwa karakteristik individu dan latar belakang pengalaman para pengambil keputusan strategis dalam organisasi akan mempengaruhi bagaimana organisasi merespons isu eksternal dan mengambil keputusan strategis. Kehadiran pemegang saham asing dapat mempengaruhi komposisi dan cara berpikir manajemen puncak, karena mereka sering kali menuntut profesionalisme yang

lebih tinggi serta mendorong adopsi praktik pelaporan yang transparan dan berorientasi pada kepatuhan global.

Heroux & Fortin (2021) menunjukkan bahwa perusahaan dengan tingkat kepemilikan asing yang tinggi lebih cenderung mengungkapkan kebijakan dan risiko keamanan siber secara terbuka. Hal ini dapat terjadi karena pemilik asing, yang umumnya berasal dari yurisdiksi dengan regulasi yang lebih ketat, memiliki harapan terhadap standar pelaporan yang lebih tinggi dan penerapan praktik tata kelola yang lebih kuat. Dalam perspektif *upper echelon theory*, tekanan dan nilai-nilai yang dibawa oleh investor asing dapat mempengaruhi pemikiran dan keputusan strategis eksekutif perusahaan lokal, termasuk dalam hal bagaimana perusahaan merespons risiko siber dan bagaimana transparansi informasi dibentuk sebagai bagian dari legitimasi institusional. Oleh karena itu, penting untuk menelaah secara empiris bagaimana pengaruh kepemilikan asing sebagai bentuk tekanan struktural eksternal dapat membentuk kecenderungan manajemen dalam mengungkapkan informasi terkait keamanan siber.

Penulis tertarik untuk meneliti peranan kepemilikan asing sebagai pemoderasi karena kepemilikan asing dengan wawasan dan pengalaman terkait regulasi pengungkapan keamanan siber yang lebih baik dapat memperkuat pengaruh faktor ukuran perusahaan dan profitabilitas terhadap pengungkapan keamanan siber. Semakin besar ukuran perusahaan dan profitabilitas perusahaan, maka semakin lengkap pengungkapan keamanan siber yang dilakukan perusahaan, karena besarnya tekanan institusional yang diterima perusahaan. Semakin besar persentase kepemilikan asing dalam suatu perusahaan, maka semakin besar

kekuatan dan daya tawar yang mendorong perusahaan untuk melakukan pengungkapan keamanan siber yang lengkap. Kepemilikan asing berperan sebagai pemoderasi yang memperkuat pengaruh ukuran perusahaan dan profitabilitas perusahaan terhadap luas pengungkapan keamanan siber perusahaan.

Semakin besar persentase kepemilikan asing maka mampu untuk mengurangi *agency cost*. Mekanisme ini terjadi karena tingginya kepemilikan asing akan meningkatkan kemampuan monitoring terhadap perusahaan sehingga mempengaruhi secara positif praktik pengungkapan keamanan siber perusahaan. Pengaruh positif ukuran perusahaan dan profitabilitas perusahaan terhadap luas pengungkapan keamanan siber akan semakin kuat dengan semakin tingginya kepemilikan asing pada perusahaan tersebut.

Dalam kerangka *upper echelon theory* (Hambrick & Mason, 1984), keputusan strategis perusahaan tidak hanya ditentukan oleh struktur organisasi semata, tetapi juga dipengaruhi oleh latar belakang, nilai, dan tekanan yang dihadapi oleh para pengambil keputusan. Kepemilikan asing berpotensi mempengaruhi pola pikir manajemen puncak dengan membawa nilai-nilai tata kelola global, ekspektasi pelaporan yang lebih ketat, serta kepedulian terhadap risiko non-keuangan seperti keamanan siber. Oleh karena itu, kepemilikan asing tidak hanya berperan langsung terhadap kebijakan disclosure, tetapi juga dapat memoderasi sejauh mana perusahaan besar dan perusahaan yang menguntungkan terdorong untuk mengungkapkan informasi keamanan siber.

Oleh karena itu, penting untuk mengkaji secara empiris bagaimana kepemilikan asing dapat memoderasi pengaruh faktor internal perusahaan, dalam

hal ini, ukuran perusahaan dan profitabilitas perusahaan terhadap pengungkapan keamanan siber, khususnya dalam konteks negara berkembang seperti Indonesia. Pengaruh moderasi kepemilikan asing terhadap hubungan antara ukuran perusahaan dan profitabilitas terhadap pengungkapan keamanan siber semakin menarik untuk diteliti karena sepengetahuan penulis, hal ini belum pernah diteliti sebelumnya.

Untuk mengukur pengungkapan keamanan siber pada perbankan, penulis mengembangkan indeks pengungkapan keamanan siber berdasarkan indeks pengungkapan keamanan siber milik Firoozi & Mohsni (2023); Ramirez et al. (2022); EY (2022) ; Ernst & Young LLP (2021); Héroux & Fortin (2020) , POJK No. 11 tahun 2022, SEOJK No. 29 tahun 2022, dan SEC *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* 2023. Tingkat pengungkapan keamanan siber yang digunakan dalam penelitian ini adalah jumlah total pengungkapan keamanan siber yang dilakukan bank dalam bab teknologi informasi dalam laporan tahunan bank. Total item pengungkapan adalan 73 item, dengan nilai 1 untuk setiap item yang diungkapkan, dan nilai 0 jika tidak dungkapkan.

Berdasarkan latar belakang, penulis tertarik untuk meneliti dan menguji secara empiris pengaruh keragaman dewan, ukuran komite teknologi, karakteristik perusahaan (ukuran perusahaan, profitabilitas, dan *growth opportunity*) serta kepemilikan asing terhadap pengungkapan keamanan siber perbankan di Indonesia. Penelitian ini juga menyelidiki pengaruh moderasi kepemilikan asing terhadap pengaruh ukuran perusahaan dan profitabilitas terhadap pengungkapan keamanan

siber. Penelitian ini akan menggunakan sampel perbankan indonesia yang terdaftar di bursa efek indonesia tahun 2018 sampai dengan 2023. Penelitian ini berjudul Determinan Pengungkapan Keamanan Siber Perbankan di Indonesia.

1.2 Perumusan Masalah

Penelitian ini bermaksud untuk menyelidiki determinan pengungkapan keamanan siber. Peneliti akan menggunakan *upper echelon theory*, *the new institutionalism theory* dan *the agency theory*. Adapun rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana pengaruh keragaman dewan terhadap pengungkapan keamanan siber?
2. Bagaimana pengaruh ukuran komite teknologi terhadap pengungkapan keamanan siber?
3. Bagaimana pengaruh ukuran perusahaan terhadap pengungkapan keamanan siber?
4. Bagaimana pengaruh profitabilitas terhadap pengungkapan keamanan siber?
5. Bagaimana pengaruh *growth opportunity* terhadap pengungkapan keamanan siber?
6. Bagaimana pengaruh kepemilikan asing terhadap pengungkapan keamanan siber?
7. Apakah kepemilikan asing memoderasi pengaruh ukuran perusahaan terhadap pengungkapan keamanan siber?

8. Apakah kepemilikan asing memoderasi pengaruh profitabilitas terhadap pengungkapan keamanan siber?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menguji secara empiris berbagai faktor yang diduga sebagai determinan pengungkapan keamanan siber perbankan di Indonesia. Penelitian ini akan menguji pengaruh keragaman dewan, ukuran komite teknologi, ukuran perusahaan, profitabilitas, *growth opportunity,* dan kepemilikan asing terhadap pengungkapan keamanan siber. Selain itu, penelitian ini juga akan menyelidiki pengaruh kepemilikan asing dalam memperkuat pengaruh ukuran perusahaan, dan profitabilitas terhadap pengungkapan keamanan siber perusahaan perbankan di Indonesia. Penelitian ini juga akan mengembangkan indeks pengungkapan keamanan siber yang dapat dipergunakan sebagai panduan dalam menyusun pengungkapan keamanan siber dalam laporan tahunan perbankan indonesia.

1.4 Manfaat Penelitian

1.4.1 Manfaat Teoritis

Berikut adalah manfaat teoritis dari penelitian ini :

1. Penelitian ini akan mengembangkan indeks pengungkapan keamanan siber terbaru yang lebih cocok untuk perbankan Indonesia karena sudah merujuk kepada POJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi

Informasi oleh Bank, dan SEOJK nomor 29/SEOJK.03/2022 terkait keamanan siber pada bank umum.

2. Indeks pengungkapan keamanan siber yang penulis kembangkan dalam penelitian ini telah memasukkan panduan terbaru dari SEC terkait pengungkapan keamanan siber tahun 2023.
3. Penelitian ini diharapkan dapat menambah literatur dan mengembangkan pengetahuan mengenai determinan pengungkapan keamanan siber. Penelitian ini diharapkan dapat memperkaya bukti empiris mengenai determinan pengungkapan keamanan siber, khususnya pengaruh keragaman dewan, ukuran komite teknologi, ukuran perusahaan, profitabilitas, *growth opportunity*, dan kepemilikan asing terhadap pengungkapan keamanan siber. Penelitian ini diharapkan juga dapat memperkaya bukti empiris pengaruh moderasi kepemilikan asing dalam memperkuat pengaruh ukuran perusahaan dan profitabilitas perusahaan terhadap pengungkapan keamanan siber.

1.4.2 Manfaat Praktis

Berikut adalah manfaat praktis dari penelitian ini :

1. Penelitian ini diharapkan dapat menjadi panduan bagi perbankan dalam membuat pengungkapan keamanan siber yang lebih lengkap, berdasarkan indeks pengungkapan keamanan siber yang penulis kembangkan.
2. Penelitian ini diharapkan dapat memberikan gambaran yang jelas mengenai determinan pengungkapan keamanan siber dan keluasan pengungkapan keamanan siber pada perbankan di Indonesia pada pihak yang berwenang,

khususnya pada sektor perbankan di Indonesia misalnya Otoritas Jasa Keuangan, Bank Indonesia, dan Bursa Efek Indonesia,

3. Bagi Akademisi, penelitian ini dapat menjadi acuan bagi penelitian selanjutnya terkait pengungkapan keamanan siber dan determinannya.

1.5 Orisinalitas Penelitian

Penelitian ini merupakan studi pertama yang berupaya mengembangkan indeks pengungkapan keamanan siber yang secara khusus dirancang untuk sektor perbankan di Indonesia. Indeks ini dikonstruksi dengan mempertimbangkan berbagai regulasi yang relevan, termasuk ketentuan yang ditetapkan oleh Otoritas Jasa Keuangan (OJK) terkait keamanan siber, serta panduan terkini dari *Securities and Exchange Commission* (SEC) mengenai pengungkapan keamanan siber. Selain itu, penelitian ini juga mengacu pada berbagai indeks pengungkapan keamanan siber yang telah dikembangkan dalam studi-studi sebelumnya, sehingga dapat memperkaya perspektif dan memastikan relevansi akademis serta praktis dari indeks yang dihasilkan.

Selain itu, penggunaan variabel ukuran komite teknologi sebagai determinan pengungkapan keamanan siber, yang belum pernah dikaji dalam penelitian terdahulu, khususnya pada konteks perbankan di Indonesia. Penelitian ini juga memberikan kontribusi baru melalui pengujian peran moderasi kepemilikan asing terhadap hubungan antara ukuran perusahaan dan pengungkapan keamanan siber.

Tabel 1.3
Orisinalitas Penelitian

No.	Item	Orisinalitas
1.	Ukuran Pengungkapan Keamanan Siber	Penulis mengembangkan indeks pengungkapan keamanan siber berdasarkan indeks pengungkapan keamanan siber milik (Ernst & Young LLP, 2021; EY, 2022; Firoozi & Mohsni, 2023; Héroux & Fortin, 2020; Ramirez et al., 2022), POJK No. 11 tahun 2022, SEOJK No. 29 tahun 2022, dan SEC *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure* 2023. Indeks pengungkapan keamanan siber yang penulis kembangkan lebih sesuai untuk perbankan Indonesia, karena dikembangkan berdasarkan POJK dan SEOJK terbaru, yang belum pernah dirujuk dalam indeks pengungkapan keamanan siber terdahulu.
2.	Ukuran komite teknologi	Variabel komite teknologi pernah diteliti pengaruhnya terhadap frekuensi pelaporan *breach* (Higgs et al., 2016) . Pada penelitian ini, penulis meneliti komite teknologi sebagai faktor yang diduga mempengaruhi level pengungkapan keamanan siber, dengan menggunakan variabel ukuran komite teknologi, yang belum pernah digunakan dalam penelitian sebelumnya.

Sumber : Diolah Penulis, 2025

Daftar Pustaka

Adriansyah, R. A., & Anugrah, A. F. (2024). Analisis Bibliometrik Keamanan Perusahaan Penjualan Online Untuk Mencegah Terjadinya Kejahatan Siber. *Jurnal Sistem Informasi dan Informatika (Simika)*, *7*(2), 113–120. https://doi.org/10.47080/simika.v7i2.3185

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-Maghzom, A., Hussainey, K., & Aly, D. (2016). Corporate governance and risk disclosure: Evidence from Saudi Arabia. *ICorporate Ownwrship and Control Journal*, *13*(2), 145–166. https://doi.org/10.1504/IJAAPE.2019.096748

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

AlJanadi, Y. (2025). Gender diversity and disclosure: a meta-analysis. *International Journal of Disclosure and Governance*, *0123456789*. https://doi.org/10.1057/s41310-024-00285-w

Arcy, J. D., & Basoglu, A. (2022). The Influences of Public and Institutional Pressure on Firms ' Cybersecurity Disclosures. *Journal of the Association for Information Systems*, *23*(3), 779–805. https://doi.org/10.17705/1jais.00740

Ashraf, M., Jiang, J. X., & Wang, I. Y. (2022). Are there trade-offs with mandating timely disclosure of cybersecurity incidents ? Evidence from state-level data breach disclosure laws. *The Journal of Finance and Data Science*, *8*, 202–213. https://doi.org/10.1016/j.jfds.2022.08.001

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.

Calderon, T. G., & Gao, L. (2020). Cybersecurity risks disclosure and implied audit risks : Evidence from audit fees. *International Journal Audit*, *Special Is*(October), 1–16. https://doi.org/10.1111/ijau.12209

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

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*(September), 199–224. https://doi.org/10.1007/s10551-022-05107-z

Cheng, X., Hsu, C., & Wang, T. (2022). Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions. *Communications of the Association for Information Systems*, *50*(26), 481–500. https://doi.org/10.17705/1CAIS.05022

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

DiMaggio, P. J., & Powell, W. W. (1983). Introduction. In *New Institutional Theory* (hal. 1–38).

Eaton, T. V, & Grenier, J. H. (2019). Accounting and Cybersecurity Risk Management. *Current Issues in auditing*, *13*(2), 1–9. https://doi.org/10.2308/ciia-52419

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).

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

Georg-Schaffner, L., & Prinz, E. (2021). Corporate management boards ' information security orientation : an analysis of cybersecurity incidents in DAX 30 companies. In *Journal of Management and Governance*. Springer US. https://doi.org/10.1007/s10997-021-09588-4

Hambrick, D. C., & Mason, P. A. (1984). Upper Echelons : The Organization as a Reflection of Its Top Managers. *The Academy of Management Review*, *35*(9), 193–206. https://doi.org/https://doi.org/10.2307/258434

Havakhor, T., Rahman, M. S., & Zhang, T. (2021a). Cybersecurity Investments and the Cost of Capital. *S&P Global Market Intelligence*, 1–48. https://weis2020.econinfosec.org

Havakhor, T., Rahman, M. S., & Zhang, T. (2021b). Disclosure of Cybersecurity Investments and the Cost of Capital. *SSRN elsevier e-journals*, 1–22.

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

Héroux, S., & Fortin, A. (2024). Board of directors' attributes and aspects of cybersecurity disclosure. *Journal of Management and Governance*, *28*(2), 359–404. https://doi.org/10.1007/s10997-022-09660-7

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

Hilary, G., Segal, B., & Zhang, M. H. (2016). Cyber-Risk Disclosure : Who Cares ? *Georgetown McDonough School of Business Research Paper*, *Oct*(2852519), 1–59.

Ibrahim, A. E., Hussainey, K., Nawaz, T., Ntim, C., & Elamer, A. (2022). A systematic literature review on risk disclosure research: State-of-the-art and future research agenda. *International Review of Financial Analysis*, *82*, 102217. https://doi.org/10.1016/j.irfa.2022.102217

Jensen, M. C., & Meckling, W. H. (1976). Theory Of The Firm : Managerial Behavior, Agency Costs and Ownership Structure. *Journal of Financial Economic*, *3*, 305–360.

Jubaedah, S., Musta'in, A., Nurlisti, I., & Adam Maulana, B. (2024). Cyber risk management disclosure: A stakeholder theory perspective. *Diponegoro International Journal of Business*, *7*(2), 133–146. https://doi.org/10.14710/dijb.7.2.2024.133-146

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

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

Masoud, N., & Al-utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms ' financial reporting : Empirical evidence. *Research in Economics*, *76*(2), 131–140. https://doi.org/10.1016/j.rie.2022.07.001

Mazumder, M. M. M., & Hossain, D. M. (2022). Voluntary cybersecurity disclosure in the banking industry of Bangladesh : does board composition matter ? *Journal of Accounting in Emerging Economies*, *13*(2), 1–23. https://doi.org/10.1108/JAEE-07-2021-0237

Mbithi, E., Moloi, T., & Wangombe, D. (2023). An empirical examination of board-related and firm-specific drivers on risk disclosure by listed firms in Kenya : a mixed-methods approach. *Corporate Governance*, *23*(2), 298–322. https://doi.org/10.1108/CG-11-2021-0395

Nieuwesteeg, B. F. ., & Eijkelenboom, E. V. . (2022). An Analysis of Changing Transparency regarding Cybersecurity in Annual Reports. *SSRN elsevier e-journals*. https://papers.ssrn.com

Nolan, C., Lawyer, G., & Dodd, R. M. (2019). Cybersecurity : today ' s most pressing governance issue. *Journal of Cyber Policy*, *4*(3), 425–441. https://doi.org/10.1080/23738871.2019.1673458

Ogbanufe, O., Kim, D. J., & Jones, M. C. (2021). Informing cybersecurity strategic commitment through top management perceptions : The role of institutional pressures. *Information & Management*, *58*(7), 103507. https://doi.org/10.1016/j.im.2021.103507

Radu, C., & Smaili, N. (2022). Board Gender Diversity and Corporate Response to Cyber Risk : Evidence from Cybersecurity Related Disclosure. *Journal of Business Ethics*, *177*, 351–374. https://doi.org/10.1007/s10551-020-04717-9

Rahmawati, L. (2024). Faktor-faktor yang mempengaruhi Cybersecurity Disclosure (CSD) di Perusahaan Sektor Perbankan yang Terdaftar di Bursa Efek Indonesia Tahun 2019-2022. In *Universitas Islam Indonesia*.

Ramadhani, E. H., Enriko, I. K. A., & Sari, E. L. I. P. (2025). Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional. *Jurnal Indonesia : Manajemen Informatika dan Komunikasi*, *6*(1), 570–580. https://doi.org/10.35870/jimik.v6i1.1210

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., 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

Shukla, M., & Pandey, P. (2023). *Cybersecurity Oversight and Board Diversity: The Disclosure Paradigm* (hal. 151–173). https://doi.org/10.4018/978-1-6684-8893-5.ch010

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.

Swift, O., Colon, R., & Davis, K. (2020). The Impact of Cyber Breaches on the Content of Cybersecurity Disclosures. *Journal of Forensic and Investigative Accounting*, *12*(2), 197–212.

Tang, M., Alazab, M., Luo, Y., & Donlon, M. (2018). Disclosure of cyber security vulnerabilities : time series modelling. *International Journal Electronic*

Security and Digital Forensics, *10*(3), 255–275.

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

Wu, Q., Yoon, K., & No, W. G. (2023). The Effect of Remote Workforce on Firms' Cybersecurity Risk Disclosures and Incidents. *S&P Global Market Intelligence*, 1–23. https://papers.ssrn.com/

https://www.ojk.go.id/id/kanal/perbankan/data-dan-statistik/laporan-profil-industri-perbankan, diakses pada 20 Maret 2023

https://money.kompas.com/read/2023/05/15/113711826/bsi-bisnis-ransomware-dan-negosiasi-pemerasan?page=all., diakses pada 27 Mei 2023

https://ekonomi.republika.co.id/berita//rc0smt383/ojk-sektor-keuangan-paling-banyak-mendapat-serangan-siber-pada-2021?, diakses pada 20 Maret 2023

https://kbbi.lektur.id/komite, diakses pada 26 juni 2023

https://keuangan.kontan.co.id/news/serangan-siber-paling-banyak-menyerang-industri-perbankan, diakses pada 9 Juli 2023

https://www.ojk.go.id/ojk-institute/id/capacitybuilding/upcoming/1032/best-practices-penanganan-insiden-keamanan-siber-di-sektor-jasa-keuangan, diakses pada 14 Desember 2023

https://www.imf.org/en/Publications/fandd/issues/2021/03/global-cyber-threat-to-financial-systems-maurer, diakses pada 7 November 2023

https://seon.io/resources/global-cybercrime-report/, diakses pada 14 Desember 2023

https://idx.co.id/id/data-pasar/laporan-statistik/digital-statistic/monthly/biggest-market-capitalization-most-active-stocks, diakses pada Januari 2025