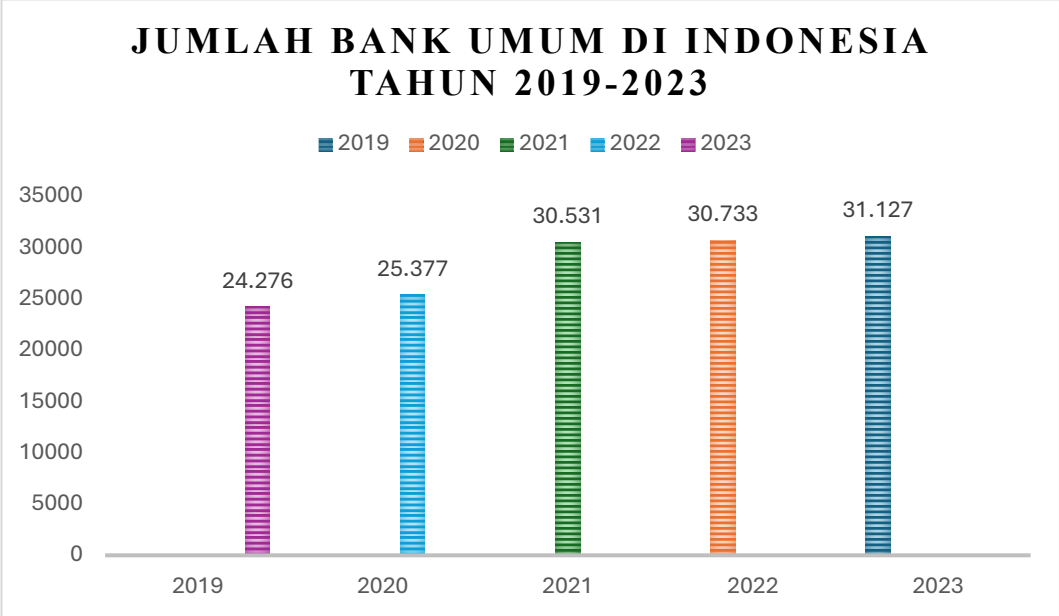
BAB I
PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Bursa Efek Indonesia (BEI) merupakan pihak yang menyelenggarakan dan menyediakan sistem serta sarana mencocokkan penawaran untuk membeli dan menjual efek kepada pihak lain yang bertujuan memperdagangkan efek. Berdasarkan BEI, industri yang terdaftar di BEI terbagi menjadi 12 sektor, 35 subsektor, 69 industri dan 130 subindustri (Sidik, 2021). Salah satu sektor yang terdapat di BEI adalah sektor keuangan di mana dalam sektor tersebut diklasifikasikan menjadi 5 subsektor salah satunya subsektor perbankan. Menurut UU Nomor 10 Tahun 1998 subsektor perbankan mencangkup segala hal yang berkaitan dengan badan usaha dalam bentuk bank, termasuk kelembagaan, kegiatan usaha, serta cara dan proses melaksanakan usahanya. Menurut UU Nomor 10 Tahun 1998 tentang perbankan, kegiatan usaha yang dilakukan perbankan, yaitu menghimpun dana, menyalurkan dana, dan memberikan jasa bank lainnya. Subsektor perbankan terbagi menjadi tiga jenis, yaitu bank umum, bank perkreditan rakyat, dan bank syariah.

Dalam penelitian ini, objek penelitian hanya berfokus pada perusahaan subsektor perbankan yang terdaftar di BEI tahun 2019–2023. Salah satu sektor keuangan yang terdapat dalam klasifikasi keuangan IDX *(Indonesia Stock Exchange)* merupakan subsektor perbankan yang memberikan variasi layanan dan produk keuangan kepada masyarakat, dari yang berbasis teknologi, berbasis syariah, hingga bank konvensional besar dengan layanan lengkap. Berdasarkan data dari Badan Pusat Statistik, jumlah kantor bank umum dari tahun 2019–2023 mengalami kenaikan. Hal tersebut dapat dilihat pada gambar 1. 1.



Gambar 1. 1 Jumlah Bank Umum di Indonesia Tahun 2019–2023

Sumber : bps.go.id (data yang telah diolah, 2024)

Gambar 1. 1 menunjukkan bahwa terdapat kenaikan jumlah bank selama 5 tahun terakhir, hal ini membuat persaingan bisnis antar bank meningkat. Selain itu, menurut Indeks Literasi dan Inklusi Keuangan menyebutkan bahwa salah satu lembaga keuangan yang memberikan dampak terbesar bagi perkembangan ekonomi adalah lembaga keuangan perbankan. Bank memberikan dampak besar karena perkembangan ekonomi yang semakin pesat dan dibutuhkannya lembaga keuangan yang dapat mengatur, menghimpun, serta menyalurkan dana yang dipercayakan oleh masyarakat dapat berbentuk simpanan (Alamsyah *et al.,* 2022). Selain itu, keterhubungan antara sektor perbankan dalam mengalokasikan dan mengembangkan keuangan di lingkungan bisnis membantu seluruh sektor bisnis untuk mengelola kegiatan bisnis menjadi lebih efektif dan efisien (Poh *et al.,* 2018), sehingga setiap bank harus memiliki kinerja yang lebih baik agar dapat bersaing dalam industri yang sama dan lebih dipercaya oleh masyarakat untuk menyimpan dana mereka.

Sektor perbankan merupakan sistem keuangan yang terdiri dari beberapa perusahaan yang bergerak di bidang jasa keuangan, khususnya dalam mengelola

dana dari masyarakat untuk kemudian digunakan dalam berbagai kegiatan ekonomi. Perbankan meliputi berbagai jenis bank, seperti bank umum, bank syariah, bank perkreditan rakyat, dan lainnya. Fungsi utama perbankan adalah mengumpulkan dana dari masyarakat, mengalokasikannya ke berbagai sektor ekonomi, hingga menyediakan jasa keuangan lainnya seperti asuransi, kartu kredit, dan lain-lain. Perbankan konvensional terbagi menjadi dua sektor yakni sektor Badan Usaha Milik Negara (BUMN) dan sektor bank umum. Berdasarkan regulasi yang tertuang dalam Undang-Undang No. 19 Tahun 2003 tentang BUMN, Bank Badan Usaha Milik Negara (BUMN) didefinisikan sebagai lembaga keuangan yang sebagian besar modalnya berasal dari negara. Sementara itu, bank umum menurut POJK Nomor 12/POJK.03/2021 ialah bank yang beroperasi secara konvensional dan menyajikan jasa dalam aktivitas pembayaran. Terdapat dua kategori pada bank umum, yakni Bank Umum Konvensional dan Bank Umum Syariah (Muhri *et al*., 2022). Namun, karena sebagian besar sahamnya dimiliki oleh negara, mayoritas masyarakat cenderung lebih memilih Bank Badan Usaha Milik Negara (BUMN) dibandingkan dengan bank konvensional lain yang belum terlihat jelas kredibilitasnya dalam mengamankan dana dan melakukan kegiatan investasi (Octaviani & Saraswati, 2018).

Berdasarkan penjelasan yang telah diuraikan, bank memiliki peran penting dalam menciptakan sumber pertumbuhan ekonomi yang dapat memengaruhi tercapainya target pertumbuhan kedepannya. Bank harus terus didorong untuk tumbuh berdaya saing dan memiliki ketangguhan untuk menghadapi berbagai tantangan saat ini. Oleh karena itu, peneliti tertarik untuk menjadikan perusahaan subsektor perbankan yang terdaftar di BEI tahun 2019–2023 sebagai objek pada penelitian ini.

1.2 Latar Belakang Penelitian

Di era saat ini, perkembangan teknologi berkembang dengan cepat, yang pasti akan menyebabkan perubahan besar dalam hal sosial, ekonomi, dan budaya. Namun, ada ancaman seperti penyebaran virus, pembajakan, dan serangan terhadap layanan perangkat lunak di balik kemajuan ini (Ginanjar, 2022). Serangan siber menurut Suherman *et al*. (2018) adalah jenis kejahatan baru yang muncul sebagai

akibat dari kemajuan teknologi informasi. *Cybersecurity disclosure* melibatkan penggunaan komputer dalam pelaksanaannya serta kejahatan yang berkaitan dengan kerahasiaan, integritas, dan keberadaan data (Zaid et al., 2020). Hal ini dikarenakan sistem komputer memiliki karakteristik yang berbeda dari kejahatan konvensional, sistem komputer harus diperhatikan dengan cermat (Bourdon, 2017).

Dalam industri perbankan, ancaman keamanan siber sering kali terjadi, terutama dalam bentuk *phishing*, *malware* dan kebocoran data. *Phishing* merupakan suatu bentuk kegiatan yang bersifat mengancam atau menjebak seseorang dengan konsep memancing orang tersebut (Suherman *et al*., 2018). Serangan *malware* perbankan semakin sering terjadi dalam beberapa tahun terakhir yang menimbulkan ancaman besar bagi lembaga keuangan dan pelanggan mereka. Serangan ini dapat mengakibatkan pencurian informasi sensitif, kerugian finansial, dan merusak reputasi (Fitria, 2023).

Sektor perbankan merupakan salah saktu sektor yang terdampak besar dari kejahatan siber. Tidak ada sektor manapun yang aman dari serangan siber, akan tetapi risiko serangan siber pada sektor perbankan dan keuangan 300 kali lipat lebih tinggi daripada sektor industri lain (Mirchandani, 2018). Berdasarkan data Badan Siber dan Sandi Negara (BSSN), serangan siber terbesar selama 2020 terjadi di sektor keuangan (23%), industri manufaktur (17,7%) dan sektor energi (10,2%) (Otoritas Jasa Keuangan, 2022). Sektor perbankan tersebut menjadi target dalam kejahatan siber karena saat ini kegiatan perekonomian dan keuangan sudah menggunakan teknologi digital. Ada beberapa alasan mengapa kejahatan siber di sektor perbankan lebih sering terjadi. Kemudahan akses data dan kelalaian pengguna menjadi alasan utama kejahatan siber.

Kejahatan siber yang terjadi di sektor perbankan salah satunya adalah kasus kebocoran data nasabah. Di Indonesia kasus ini terjadi pada tahun 2021 pada PT Bank Pembangunan Daerah Jawa Timur (Bank Jatim). Data yang bocor dari *database* bank jatim dijual di Raid Forums dan dijual dengan harga Rp3,5 miliar (Bestari, 2021). Dua tahun kemudian, Bank Syariah Indonesia juga mengalami serangan siber yang membuat kasus tersebut menjadi sorotan. Pada pertengahan tahun 2023, para nasabah bank syariah millik pemerintah tersebut tidak bisa

mengakses dan menggunakan layanan ATM maupun *m-banking*. Kejadian tersebut diduga karena adanya serangan dari hacker. Gangguan yang dialami Bank Syariah Indonesia (BSI) diyakini disebabkan oleh serangan siber berupa *ransomware* yang dilakukan oleh sekelompok peretas yang menyatakan diri mereka sebagai *LockBit Ransomware Group* (Dewan Perwakilan Rakyat, 2023). Kejadian tersebut menyita perhatian masyarakat dan pemerintah dikarenakan gangguan sistem BSI tersebut berlangsung selama beberapa hari dan membuat khawatir nasabah akan keamanan data maupun simpanan uang yang ada di dalam rekening nasabah.

Serangan siber yang semakin kompleks dan terorganisir sekarang dapat memasuki sistem keamanan perbankan dan mencuri informasi sensitif. Ini karena perbankan mengelola data sensitif, seperti informasi pribadi, rekening bank, dan transaksi keuangan, yang sangat berharga bagi penjahat siber untuk melakukan pencurian identitas. Peraturan Otoritas Jasa Keuangan (OJK) Nomor 12/POJK.03/2018 mengatur layanan perbankan digital yang ditawarkan oleh bank umum dalam upaya menjaga keamanan transaksi digital. Salah satu tujuan utama peraturan ini adalah untuk menjamin bahwa bank penyelenggara memiliki infrastruktur yang memadai serta menerapkan prinsip perlindungan nasabah.

Untuk meminimalisir terjadinya kejahatan di sektor perbankan maka penting bagi perusahaan untuk menyusun manajemen risiko keamanan siber dan strategi mengenai keamanan data pengguna. Penyusunan manajemen risiko mengenai keamanan siber akan membantu *stakeholder* dalam menilai keberlangsungan prospek bisnis di masa depan terutama dalam aspek ancaman dan risiko permasalahan keamanan siber. Kejahatan siber dilakukan oleh pelaku kejahatan dengan cara mencuri data rahasia untuk mendapatkan keuntungan finansial yang cepat dan melanggar hukum (Bourdon, 2017). Praktik penyusunan manajemen risiko keamanan siber merupakan mekanisme dan konsekuensi yang harus dilakukan dari implementasi tata kelola perusahaan yang baik. Salah satu prinsip tata kelola perusahan yang baik adalah *stakeholder* perlu mendapatkan perhatian yang serius, termasuk dalam mematuhi peraturan yang berlaku dan menjalin kerjasama yang aktif demi memastikan hubungan berkelanjutan jangka panjang antara *stakeholder* dan perusahaan (Aliniar & Wahyuni, 2017). Oleh

karena itu, terdapat peningkatan tuntutan pemangku kepentingan terhadap hal yang lebih besar dari transaparansi perusahaan publik dalam cara mereka mengidentifikasi, mengukur, dan mengelola risiko siber (SecurityScorecard, 2021). Akibatnya, perusahaan harus menunjukkan bahwa mereka perlu bertindak untuk memenuhi tanggung jawab dari *stakeholder* dengan mengungkapkan keamanan siber dalam pengungkapan sukarela perusahaan. Perusahaan dengan sukarela memberikan informasi kepada *stakeholder* mengenai strategi keamanan siber di dalam laporan tahunan. Dengan adanya komitmen perusahaan dalam mengungkapkan sistem manajemen risiko mengenai keamanan siber perusahaan, maka akan membuat *stakeholder* menjadi tenang dan mempercayai kinerja perusahaan dengan baik. Perusahaan dapat mengungkapkan manjemen risiko mengenai kemanan siber dan perusahaan melalui *cybersecurity disclosure*. Pengungkapan keamanan siber merupakan pengungkapan yang masih menjadi agenda baru dari perusahaan (Mazumder & Hossain, 2023). Di Indonesia pengungkapan ini belum menjadi kewajiban yang harus dilaporkan oleh perusahaan karena sifatnya yang masih sukarela. Pengungkapan mengenai kemanan siber di Indonesia ini sudah sejalan dengan peraturan Otoritas Jasa Keuangan. Dalam peraturan Nomor 11/PJOK.03/2022 tentang penyelenggaraan teknologi informasi oleh bank umum, maka perlu untuk mengatur ketentuan pelaksanaan mengenai ketahanan dan keamanan siber bagi bank umum (Otoritas Jasa Keuangan, 2022). Pengungkapan keamanan siber ini dapat ditemukan di dalam laporan tahunan perusahaan.

Pengungkapan keamanan siber oleh perusahaan menjadi salah satu upaya untuk meningkatkan transparansi kepada pemangku kepentingan dan investor. Namun, tingkat pengungkapan informasi terkait *cybersecurity disclosure* sangat bervariasi antar perusahaan (Zaid et al., 2020). Tindak kejahatan dalam perbankan berbeda dengan kejahatan konvensional, tetapi memiliki tujuan yang sama, yaitu untuk mendapatkan informasi rekening, kartu kredit, meretas sistem basis data bank, dan merampok bank (Faridi, 2019). Salah satu faktor yang memengaruhi tingkat pengungkapan ini adalah karakteristik dewan direksi dan komisaris. Menurut penelitian Li *et al. (*2020) mengidentifikasi hubungan positif antara ukuran

dewan direksi dan dewan komisaris dengan tingkat pengungkapan keamanan siber. Dewan yang lebih besar memberikan pengawasan yang lebih baik terhadap pengungkapan keamanan siber**.** Oleh karena itu, penting bagi perbankan untuk terus memperkuat sistem keamanan siber mereka untuk melindungi informasi pelanggan dan mempertahankan kepercayaan masyarakat. Penelitian ini bertujuan untuk menganalisis fenomena *cybersecurity disclosure* di sektor perbankan Indonesia, mengidentifikasi ancaman-ancaman utama yang dihadapi serta upaya yang dilakukan oleh perusahaan perbankan dalam menghadapi risiko tersebut. Keamanan siber mempunyai kedudukan berarti dalam melindungi keamanan data perihal yang krusial untuk melindungi informasi dalam media penyimpanan serta menjamin data yang dikirim dalam kondisi nyaman dan proteksi sistem data terhadap ancaman siber (Ginanjar, 2022).

Perusahaan-perusahaan perbankan yang terdaftar di BEI periode 2019–2023 menghadapi tantangan besar dalam menjaga keamanan informasi. Selain memenuhi peraturan dan ketentuan terkait pengungkapan informasi, perusahaan juga harus menghadapi tuntutan pasar yang semakin menekankan pada transparansi dan tata kelola perusahaan yang baik. Oleh karena itu, studi mengenai pengaruh karakteristik dewan terhadap *cybersecurity disclosure* dalam konteks perbankan di Indonesia menjadi relevan dan penting. Pengungkapan informasi terkait *cybersecurity disclosure* menjadi semakin penting bagi *stakeholder,* terutama investor dan regulator untuk menilai kesiapan dan ketahanan bank dalam menghadapi ancaman siber. Berdasarkan penelitian sebelumnya yang dilakukan oleh Alodat terdapat beberapa faktor yang memengaruhi pengungkapan *cybersecurity disclosure*, diantaranya *board size, board independent, board diversity,* dan *board meeting*. Perbedaan penelitian ini dengan penelitian terdahulu yang dilakukan oleh Alodat terletak pada objek penelitian dan periode yang digunakan. Penulis menggunakan perusahaan subsektor perbankan yang terdaftar di BEI sebagai objek penelitian dan periode 2019–2023 yang digunakan dalam penelitian ini.

Board size merupakan jumlah banyaknya anggota dewan komisaris dan dewan direksi dalam suatu perusahaan (Emanuel *et al*., 2022). Penelitian oleh

Alkurdi *et al*. (2019) menunjukkan bahwa terdapat hubungan positif dan signifikan antara ukuran dewan direksi dan pengungkapan keamanan siber. Artinya, perusahaan dengan ukuran dewan direksi yang lebih besar memberikan pengungkapan yang lebih banyak terhadap keamanan siber. Penelitian oleh Ma'wa & Setiawan (2024) menganalisis pengaruh berbagai faktor, termasuk ukuran dewan terhadap pengungkapan keamanan siber pada perusahaan-perusahaan yang terdaftar di BEI yang hasilnya menunjukkan bahwa komposisi ukuran dewan tidak memiliki pengaruh yang signifikan terhadap pengungkapan keamanan siber. Menurut teori agensi, *board size* yang lebih besar cenderung meningkatkan *cybersecurity disclosure* karena keberagaman keahlian dan pengalaman anggota dewan dapat meningkatkan fungsi pengawasan dan mendorong transparansi informasi yang lebih baik terkait risiko keamanan siber untuk mengurangi asimetri informasi antara agen (manajemen) dan prinsipal (pemegang saham) (Alodat *et al*., 2024).

Board independent adalah anggota komisaris yang tidak terafiliasi dengan direksi anggota dewan komisaris lainnya dan pemegang saham pengendali serta bebas dari hubungan bisnis atau hubungan lainnya (Adhitama & Imelda, 2020). Hasil menunjukkan bahwa hubungan antara independensi dewan dan pengungkapan keamanan siber bersifat positif dan signifikan. Artinya, perusahaan dengan persentase direktur independen yang lebih besar akan lebih meningkatkan tata kelola keamanan siber dengan memberikan pengungkapan yang berharga kepada pengguna dan berbagai pemangku kepentingan. Hasil ini konsisten dengan perspektif pemangku kepentingan bahwa dewan yang lebih independen cenderung mempertimbangkan tuntutan pemangku kepentingan. Lebih jauh lagi, dewan independen mendorong transparansi dan tata kelola yang baik, mengurangi asimetri informasi, menyediakan lebih banyak pengungkapan tentang risiko keamanan siber, dan mengurangi masalah keagenan (Adhitama & Imelda, 2020). Penelitian oleh Gibson (2020) posisi dewan komisaris independen tidak memiliki pengaruh signifikan terhadap pengungkapan keamanan siber. Hasil ini menunjukkan bahwa meskipun ada harapan bahwa dewan independen dapat meningkatkan transparansi, faktanya tidak ada bukti kuat yang mendukung pengaruh tersebut dalam konteks

keamanan siber. Menurut teori agensi, dewan komisaris independen yang lebih dominan dapat memperkuat pengawasan terhadap manajemen dan mengurangi konflik keagenan, sehingga mendorong transparansi yang lebih tinggi dalam pengungkapan informasi keamanan siber perusahaan (Jizi & Dixon, 2020).

Board diversity adalah keragaman dari anggota dewan yang menyangkut karakteristik mereka dalam menyampaikan pandangan mereka masing-masing (Yogiswari & Badera, 2019). Hubungan positif tetapi tidak signifikan antara keberagaman gender dewan dan pengungkapan keamanan siber (Alodat *et al*., 2024). Penelitian oleh Ma'wa & Setiawan (2024) menganalisis pengaruh menganalisis pengaruh keberagaman gender pada dewan terhadap pengungkapan keamanan siber di sektor perbankan Indonesia. Hasilnya menunjukkan bahwa keberadaan perempuan di dewan komisaris meningkatkan pengungkapan keamanan siber, tetapi keberadaan perempuan di dewan direksi memiliki dampak negatif yang signifikan terhadap pengungkapan tersebut. Temuan Ma'wa & Setiawan (2024) ini menyoroti kompleksitas hubungan antara keberagaman dewan dan pengungkapan keamanan siber dengan hasil yang tidak konsisten tergantung pada posisi dalam struktur dewan. Menurut teori agensi, keberagaman dewan *(board diversity)* dapat meningkatkan pengungkapan informasi keamanan siber *(cybersecurity disclosure)* karena dewan yang beragam cenderung memiliki kapasitas pengawasan yang lebih kuat dan dapat mengurangi konflik keagenan antara manajemen dan pemegang saham melalui transparansi informasi yang lebih baik (Zaid et al., 2020).

Board meeting sebagai jumlah rapat dewan direksi yang diadakan setiap tahun (Christian & Bangun, 2021). Hasil penelitian menunjukkan hubungan antara rapat dewan direksi dan pengungkapan keamanan siber hasilnya signifikan positif. Temuan ini berarti bahwa perusahaan dengan frekuensi rapat dewan direksi memberikan tingkat pengungkapan keamanan siber yang lebih tinggi. Frekuensi rapat dewan direksi menunjukkan ketekunannya dalam mempertimbangkan pembahasan masalah pengungkapan keamanan siber yang mengurangi asimetri informasi dan memastikan transparansi yang lebih besar (Alodat *et al*., 2024). Menurut teori agensi, frekuensi rapat dewan *(board meeting)* yang lebih tinggi

dapat memperkuat fungsi pengawasan dewan terhadap manajemen, sehingga mendorong pengungkapan informasi keamanan siber yang lebih komprehensif untuk mengurangi asimetri informasi dan konflik kepentingan antara prinsipal dan agen (Lakshan & Wijekoon, 2019).

Penelitian oleh Rudiatno & Cheryta (2022) mengeksplorasi bagaimana struktur dan frekuensi pertemuan dewan memengaruhi pengelolaan risiko keamanan siber. Hasilnya menunjukkan bahwa tidak memiliki pengaruh signifikan antara jumlah pertemuan dewan dan efektivitas pengelolaan pengungkapan keamanan siber. Meskipun pertemuan sering dianggap sebagai platform untuk meningkatkan kesadaran risiko, hasil penelitian ini menunjukkan bahwa keberadaan prosedur dan kebijakan yang jelas lebih menentukan daripada frekuensi pertemuan.

Berdasarkan uraian dalam latar belakang masih terdapat fenomena serta hasil penelitian yang dilakukan oleh peneliti sebelumnya terkait *cybersecurity disclosure*. Selain itu, juga masih terdapat beberapa inkonsistensi hasil penelitian dari penelitian-penelitian terdahulu sehingga masih relevan untuk melakukan kembali penelitian terkait. Oleh karena itu, penulis tertarik untuk melakukan pengujian kembali terkait dengan variabel-variabel yang memengaruhi *cybersecurity disclosure* dengan judul: **Pengaruh Karakteristik Dewan terhadap *Cybersecurity Disclosure* (Studi pada Perusahaan Perbankan yang Terdaftar di Bursa Efek Indonesia Periode 2019–2023).**

1.3 Rumusan Masalah

Berdasarkan latar belakang dan rumusan masalah penelitian diatas, maka penelitian ini menghasilkan pertanyaan penelitian sebagai berikut:

1. Bagaimana karakteristik dewan, seperti *board size, board independent, board diversity*, dan *board meeting* terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023?
2. Apakah karakteristik dewan, seperti *board size, board independent , board diversity*, dan *board meeting* berpengaruh secara simultan terhadap

cybersecurity disclosure pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023?

3. Apakah *board size* berpengaruh secara parsial terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023?
4. Apakah *board independent* berpengaruh secara parsial terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023?
5. Apakah *board diversity* dewan berpengaruh secara parsial terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023?
6. Apakah *board meeting* berpengaruh secara parsial terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023?

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah yang telah dibuat, maka tujuan dalam penelitian ini sebagai berikut:

1. Untuk mengetahui karakteristik dewan, seperti *board size, board independent, board diversity,* dan *board meeting* terhadap *cybersecurity disclsoure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023.
2. Untuk mengetahui apakah karakteristik dewan, *board size, board independent, board diversity,* dan *board meeting* berpengaruh secara simultan terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023.
3. Untuk mengetahui apakah *board size* berpengaruh secara parsial terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023.

4. Untuk mengetahui apakah *board independent* berpengaruh secara parsial terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023.
5. Untuk mengetahui apakah *board diversity* berpengaruh secara parsial terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023.
6. Untuk mengetahui apakah *board meeting* berpengaruh secara parsial terhadap *cybersecurity disclosure* pada perusahaan perbankan yang terdaftar di BEI periode 2019–2023.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat secara teoritis maupun praktis bagi berbagai pihak yang berkaitan, yaitu sebagai berikut:

1.5.1 Aspek Teoritis

Penelitian ini diharapkan dapat menambah literatur mengenai pengaruh karakteristik dewan terhadap pengungkapan informasi perusahaan, khususnya dalam konteks keamanan siber di sektor perbankan. Memberikan kontribusi pada literatur tata kelola perusahaan dan pengungkapan informasi, khususnya dalam konteks *cybersecurity disclosure* di sektor perbankan. Memperluas pemahaman tentang peran karakteristik dewan dalam memengaruhi praktik pengungkapan informasi perusahaan.

1.5.2 Aspek Praktis

Bagi perusahaan perbankan, penelitian ini dapat memberikan wawasan mengenai pentingnya komposisi dewan yang memiliki keahlian dan pengalaman dalam mengelola *cybersecurity disclosure* serta bagaimana hal tersebut dapat memengaruhi transparansi perusahaan dalam hal pengungkapan informasi.

1. Bagi perusahaan perbankan: Memberikan wawasan tentang pentingnya komposisi dewan yang tepat dalam meningkatkan kualitas *cybersecurity disclosure*.

2. Bagi regulator: Menyediakan informasi yang dapat digunakan sebagai pertimbangan dalam pengembangan kebijakan terkait tata kelola perusahaan dan pengungkapan keamanan siber.
3. Bagi investor: Membantu dalam memahami faktor-faktor yang memengaruhi kualitas *cybersecurity disclosure* yang dapat digunakan dalam pengambilan keputusan investasi.

1.6 Sistematika Penulisan Tugas Akhir

Penelitian ini dibagi menjadi lima bab yang terdiri dari beberapa subbab. Sistematika penyusunan skripsi ini adalah sebagai berikut:

a. **BAB I PENDAHULUAN**

   Bab ini membahas mengenai gambaran umum objek penelitian yang digunakan dalam penelitian, yaitu perusahaan perbankan yang terdaftar di BEI tahun 2019–2023. Latar belakang penelitian menggambarkan fenomena yang layak untuk diteliti, perumusan masalah yang mengidentifikasi masalah yang didasarkan pada latar belakang penelitian, tujuan penelitian, manfaat penelitian secara teoritis maupun praktis, dan sistematika penullisan tugas akhir.

b. **BAB II TINJAUAN PUSTAKA**

   Bab ini menjelaskan landasan teori yang berkaitan dengan variabel yang diteliti. Selain itu, pada bab ini juga membahas mengenai penelitian-penelitian terdahulu yang digunakan sebagai referensi dalam penelitian ini, kerangka pemikiran, dan hipotesis penelitian yang digunakan sebagai jawaban sementara dari penelitian ini.

c. **BAB III METODE PENELITIAN**

   Bab ini berisi tentang jenis penelitian, operasional variabel, tahapan penelitian, populasi dan sampel yang digunakan, pengumpulan data dan sumber data, serta teknik analisis data yang digunakan.

d. **BAB IV HASIL PENELITIAN DAN PEMBAHASAN**

   Bab ini menyajikan karakterisitik data penelitian, analisis data beserta interpretasinya, hasil penelitian, dan pembahasan dari hasil penelitian tersebut.

e. **BAB V KESIMPULAN DAN SARAN**

Bab ini berisi kesimpulan dari hasil analisis yang telah dilakukan. Selain itu, pada bab ini berisi mengenai saran yang dapat digunakan untuk para peneliti berikutnya.