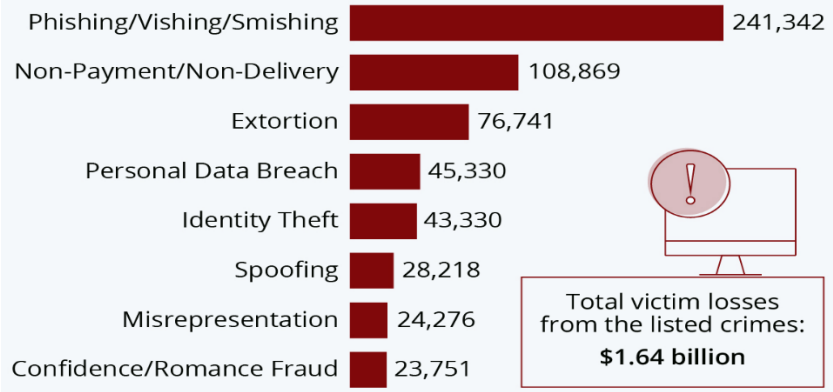
BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

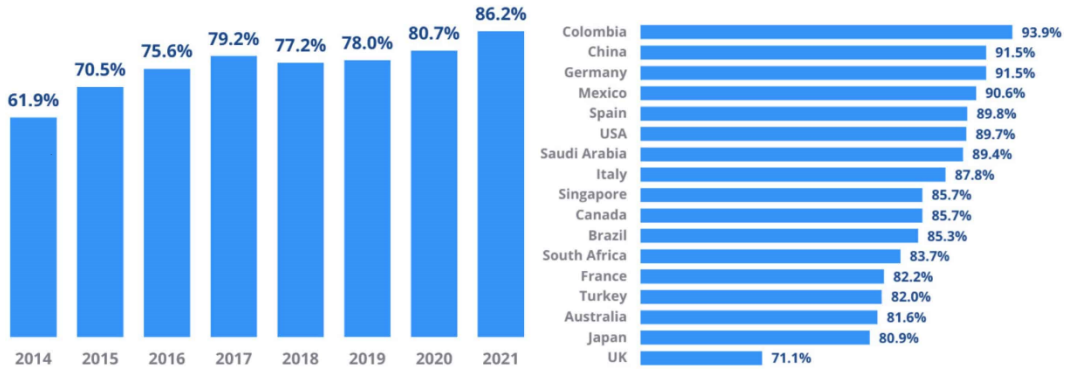
Kemajuan dan literasi teknologi informasi dalam dua dekade terakhir (2000-2020) mendorong perusahaan-perusahaan dari berbagai negara seluruh dunia untuk memanfaatkan teknologi informasi dengan berbagai aspek turunannya dalam upaya mendukung keunggulan bersaing dan keuntungan bisnisnya. Teknologi informasi potensial memberikan banyak kemudahan kepada banyak perusahaan agar menjadi lebih sukses dan menjadi pemenang di lingkungan bisnis yang selalu berubah cepat. Namun, penggunaan teknologi informasi bukannya tanpa risiko. Seiring besarnya manfaat, dalam praktik perusahaan yang menggunakan teknologi informasi sebagai salah satu dasar keunggulan bersaing bisnisnya juga cenderung mengalami banyak masalah akibat kejahataan siber (*cybercrime*) atau serangan siber (*cyberattacks*). Selama dekade terakhir, kejahataan atau serangan semakin meningkat, khususnya menyerang berbagai perusahaan, atau bahkan lembaga-lembaga pemerintahan yang sering menyebabkan kekacauan di ruang publik (NGFW, 2021). Dalam kasus ini, perusahaan harus dilindungi dan banyak pengusaha perlu berinvestasi sekaligus mendidik karyawannya dalam menyediakan berbagai proses layanan online serta perlindungan online. Perlindungan ini dapat menolak akses yang tidak wajar dalam sistem teknologi informasi perusahaan, melindungi perusahaan dari virus dan spam, serta mengamankan konektivitas VPN dan memblokir website yang tidak disetujui.

Di Amerika Serikat, kasus kejahatan atau serangan siber juga sering terjadi. Richter (2021) menjelaskan dalam *The Most Common Types of Cyber Crime* bahwa jenis paling umum kejahatan siber di Amerika Serikat adalah *phishing*/*vishing* atau *smishing* (241.342 kasus), yang disusul *non-payment* atau *non-delivery* (108.869 kasus), pemerasan (*extortion*) (76.741 kasus), pelanggaran data pribadi (*personal data breach*) (45.330 kasus), dan pencurian identitas (*identity theft*) (43.330 kasus). Jumlah kerugian akibat kejahatan siber di Amerika Serikat pada 2020 sebagaimana dilaporkan oleh FBI mencapai $1,64 milyar (Gambar 1). Banyaknya kejahatan siber ini terjadi secara merata, baik level individu, perusahaan maupun organisasi publik.



Gambar 1.1
Jenis-Jenis Paling Umum Kejahatan Siber di Amerika Serikat
(Sumber: Zaharia, 2022)

Dalam kejahatan siber global, kerugian diprediksi mencapai $10,5 trilyun setahun pada 2025. Zaharia (2022) menunjukkan banyaknya kejahatan siber, taktik serangan yang paling sering digunakan oleh pelaku kejahatan, dan apa yang perlu dilakukan dalam memerangi kejahatan siber dan serangan siber. Pada Maret 2021-Februari 2022, terdapat 153 juta sampel *malware* baru dan terjadi 5% peningkatan daripada sebelumnya (145,8 juta). Hampir 50% PC bisnis dan 53% PC konsumen yang pernah terinfeksi terinfensi kembali pada tahun yang sama pada 2021. Sekitar 86,2% dari organisasi yang disurvei dipengaruhi oleh serangan siber yang sukses (Gambar 2a) dan Colombia ditemukan menjadi negara yang paling keras terkena serangan siber pada 2019 dan 93,9% dari semua perusahaan yang disurvei terancam serangan siber setidaknya sekali dalam tahun terakhir (Gambar 2b).



(a) (b)

Gambar 1.2
(a) Serangan Siber dari Tahun ke Tahun (2014-2021); (b) Serangan Siber Terbanyak ke Berbagai Negara Seluruh dunia (Sumber: Zaharia, 2022)

Dalam konteks perusahaan, masalah kejahatan atau serangan siber tersebut pada umumnya terjadi dalam perusahaan-perusahaan yang menggunakan teknologi informasi sebagai salah satu unsur keunggulan bersaing dari bisnisnya. Beriringan dengan meningkatnya kasus kejahatan atau serangan siber ini, berbagai perusahaan berusaha mencari solusi teknologi dalam mencegah berbagai resiko adanya celah keamanan siber yang disebabkan oleh karyawan seperti pencurian data, kerusakan atau hilangnya data, menyimpan pada sistem perangkat lunak berbahaya (misalnya, terinfeksi virus) atau kelemahan keahlian karyawan teknologi informasi di bidang keamanan digital bagi bisnis mereka. Tantangan utama yang dihadapi perusahaan selain organisasi publik pemerintahan adalah bagaimana menyiapkan pencegahan keamanan siber terhadap semua sistem informasinya (Minnaar, 2014). Selama ini, salah satu cara paling efektif perusahaan untuk melakukan perlindungan data adalah dengan meningkatkan pengetahuan keamanan siber (*cybersecurity knowledge*) dan menaikkan kesadaran keamanan (*security awareness*) semua karyawan perusahaan dalam memperkuat budaya keamanan siber (*cybersecurity culture*) yang diikuti bersama di perusahaan (Corriss, 2010). Dengan pesatnya perkembangan teknologi informasi, banyak kasus serangan keamanan semakin meningkat pesat, menjadikan perlindungan pada informasi privasi semakin kompleks penanganannya dan penuh tantangan untuk mengatasinya.

Negara yang semakin banyak menerapkan teknologi informasi dan semakin terhubung dengan internet cenderung mengalami peningkatan risiko serangan siber. Di Indonesia perubahan pola hidup masyarakat yang banyak mengandalkan internet pada masa pandemi Covid-19 (2020-2022) ternyata berimbas pada kenaikan jumlah upaya serangan siber. Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa sepanjang Januari-Agustus 2020, terdapat hampir 190 juta upaya serangan siber di Indonesia, naik lebih dari empat kali lipat dibandingkan periode yang sama pada 2019 sekitar 39 juta (Salsabila, 2020). Pemakaian internet dan transaksi digital ini semakin banyak sehingga pelaku kejahatan siber semakin gencar melancarkan aksi. Peningkatan itu disebabkan oleh kebijakan menjaga jarak (*social distancing*) yang membuat warga bekerja, belajar, dan melakukan berbagai aktivitas lain dari rumah melalui internet yang memusat di wilayah pemukiman. Salah satu parameter utama

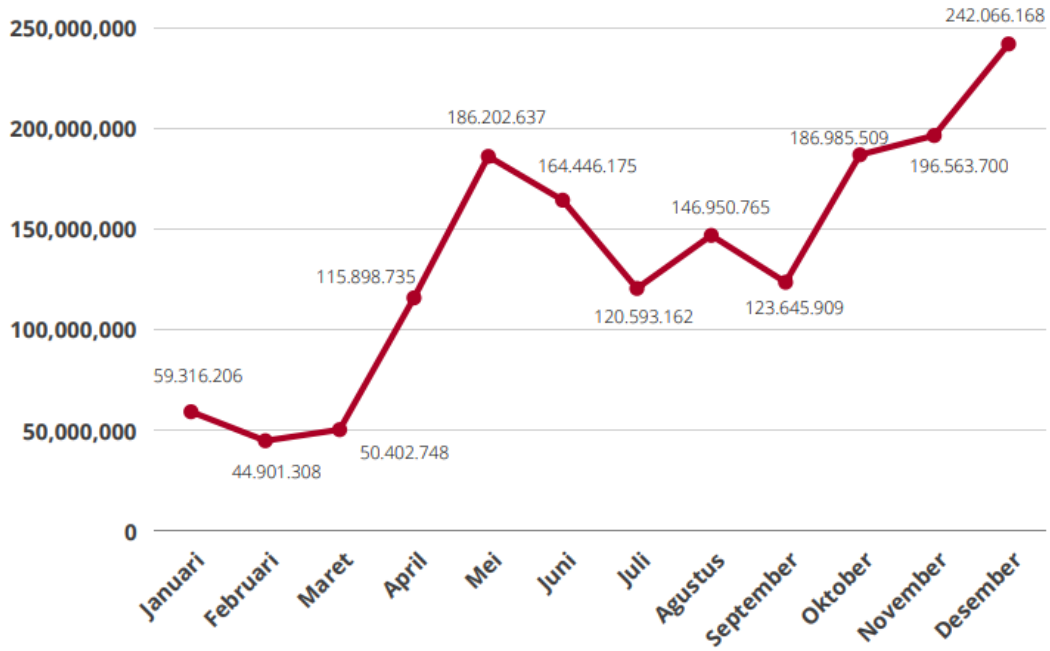
serangan siber adalah kegiatan peretas yang melakukan *scanning* di port situs yang terbuka dengan mengirimkan paket *SYN scan*. Di era pandemi Covid-19 ini, kasus kejahatan siber meningkat dengan modus semakin beragam seperti oknum meminta sumbangan atas nama korban pandemi, pencurian data dan pembobolan rekening.

Pada dasarnya kejahatan siber adalah segala aktivitas ilegal yang digunakan pelaku kejahatan menggunakan teknologi informasi dan sistem jaringan komputer yang secara langsung menyerang teknologi sistem informasi korban. Target pelaku kejahatan siber adalah peralatan (*device*) atau perangkat keras (*hardware*) maupun perangkat lunak (*software*) atau data pribadi korban. Pelaku dan korban kejahatan siber ini sama-sama tidak terlihat, sehingga sifatnya kompleks. Menurut data dari POLRI, sejak April 2020, setidaknya ada 937 kasus dilaporkan, dan tiga kasus yang tertinggi adalah provokasi, konten kebencian, dan ujaran kebencian sebanyak 473 kasus, disusul penipuan online (259 kasus) dan konten porno (82 kasus) (Salsabila, 2020). Hal ini terkait residu politik Indonesia setelah pemilihan daerah dan pemilu nasional yang membelah masyarakat. Kondisi ini diperparah kejahatan baru di masa pandemi yaitu pemanfaatan barang dan alat kesehatan dengan menaikan harga di atas normal atau bahkan menimbun yang menjadikan kelangkaan di masyarakat.

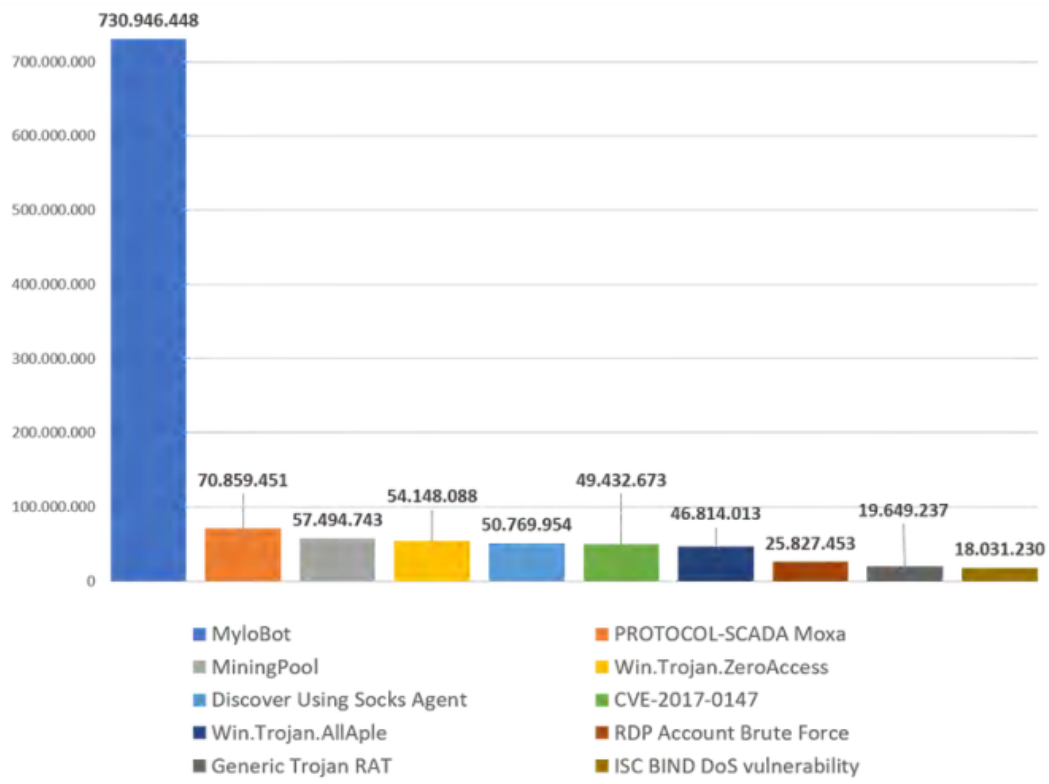
Dalam konteks perusahaan, cepatnya perkembangan digital juga memicu peningkatan kejahatan siber sektor perbankan, yang ditandai dengan 5.000 laporan pengaduan tindakan penipuan (*fraud*) setiap minggu atau sekitar 200.000 laporan penipuan (*fraud*) sejak Maret 2020 dengan media paling banyak digunakan adalah *Whatsapp* serta *Instagram* (Walfajri, 2021). Perkembangan kejahatan siber tersebut membawa ancaman bagi dunia perbankan. Dalam konteks tersebut, perilaku dan kesadaran nasabah serta pegawai bank menjadi hal yang penting untuk mengurangi risiko kejahatan siber di sektor perbankan. Namun, terdapat masalah utama yang dihadapi oleh perbankan (Walfajri, 2021), yaitu: *pertama*, aplikasi pihak ketiga di *smartphone* memungkinkan ada kelemahan keamanan jika dibuat oleh pengembang yang tidak berpengalaman; *kedua*, jaringan Wifi Publik merupakan salah satu cara mudah bagi peretas untuk memperoleh akses dan data ke berbagai informasi akun yang tersimpan di *smartphone*; dan *ketiga*, *mobile malware* seperti virus, trojan, *rootkit* dan lainnya, yang biasa berkembang seiring dengan berkembangnya industri

perbankan. Terkait dengan masalah tersebut, setidaknya ada lima kategori ancaman kejahatan siber utama di dalam industri perbankan, yaitu: (a) *Mobile Devices* yang saat ini banyak digunakan untuk sistem pembayaran; (b) *Digital Connectivity*, yang telah meningkatkan keterpaparan data penting melalui adopsi sistem digital dan interkonektivitas; (c) *Malware*, yang semakin berkembang seiring dengan semakin canggihnya teknologi informasi yang mudah diakses dan otomatis; (d) *Partnership*, yang memungkinkan terjadinya konvergensi siber komersial dan pemerintah; dan *API*, yaitu penggunaan vendor pihak ketiga menimbulkan risiko di luar kendali langsung pihak perusahaan (Walfajri, 2021). Dalam konteks itu, perbankan serta nasabahnya harus memahami dan mengenali apa saja bentuk penipuan digital yang marak terjadi untuk meminimalisir risiko kerugian, bahkan bisa menghindarinya.

Menurut BSSN (2021), Kelompok Operasi Deteksi, Penanggulangan dan Pemulihan, Penanganan Insiden dan Krisis Siber Nasional melakukan pemantauan dan menemukan jumlah sebesar 1.637.973.022 kasus anomali trafik serangan siber sepanjang tahun 2021 dengan anomali tertinggi pada Desember 2021 (Gambar 1.3).



Gambar 1.3
Jumlah Anomali Kasus Ancaman dan Serangan Siber di Indonesia Sepanjang 2021 (Sumber: BSSN, 2021)



Gambar 1.4
10 Anomali Tertinggi Kasus Ancaman dan Serangan Siber di Indonesia Sepanjang 2021 (Sumber: BSSN, 2021)

Gambar 1.4 menunjukkan bahwa sepanjang 2021 telah terjadi banyak kasus anomali ancaman dan serangan siber di Indonesia. Setidaknya sebanyak 44,62% anomali trafik ancaman serangan siber didominasi oleh MyloBot Botnet. Kasus ini diikuti beberapa kasus lain yang memiliki keterhubungan dengan botnet lain dalam serangannya, *seperti MiningPool*, *Discover Using Socks Agent*, *Win.Trojan.All Aple*, *Generic Trojan RAT*, *PROTOCOL-SCADA Moxa*, *Win.Trojan.Zero Access*, *CVE-2017-0147*, *RDP Account Brute Force*, dan *ISC BIND DoS vulnerability*.

Dalam konteks itu, Botnet paling banyak dan berbahaya bagi keamanan siber karena Botnet adalah jaringan computer yang terinfeksi oleh *malware* yang berada di bawah kendali satu pihak penyerang. Botnet dirancang untuk pengiriman *spam*, pencurian data, *ransomware*, *click fraud*, *Denial-of-Service* (Dos), dan lain-lain. MyloBot Botnet banyak menargetkan sistem operasi Microsoft Windows yang menyebar melalui spam *e-mail* dan unduhan *file* yang terinfeksi. Ancaman besarnya

adalah bahwa setelah terinstal, botnet mematikan *Windows Defender* dan *Windows Update* sambil memblokir *port* tambahan di *Firewall*. Selain itu, *botnet* mematikan dan menghapus file .exe yang berjalan dari folder %APPDATA% yang potensial menyebabkan hilangnya data. MyloBot Botnet dapat berkembang menjadi ancaman keamanan siber besar di Indonesia karena jenis botnet ini mempunyai kemampuan mengunduh dan mengeksekusi semua jenis muatan setelah berhasil menginfeksi dan memungkinkan para penyerangnya untuk mengambil kendali penuh atas sistem pengguna. BSSN (2021) menunjukkan ada beberapa langkah mitigasi yang dapat dilakukan untuk mencegah dampak yang diakibatkan oleh MyloBot Botnet, yaitu: selalu melakukan *update* dan *patch* perangkat computer dan antivirus yang dipakai, selalu melakukan pencadangan data yang ada di komputer secara berkala, selalu menggunakan *password* yang kuat, menghindari akses terhadap situs web atau domain yang tidak terpercaya, dan menghindari untuk mengunduh dan membuka *e-mail* dari alamat pengirim yang tidak dikenal.

Selain *MyloBot Botnet*, *Protocol-Scada Moxa* juga menjadi ancaman bagi keamanan siber besar di Indonesia. Kerentanan perangkat *Moxa* memungkinkan penyerang untuk menyisipkan *malware*, salah satunya Triton, yang menargetkan beberapa modul komunikasi yang berbeda dan jaringan di berbagai protocol, salah satunya protocol Modbus. Triton dapat menyebabkan terjadinya *Denial-of-Service* (DOS) dan *Man-in-the-Middle attack* pada sistem, dan serangan ini mempengaruhi operasi dan stabilitas sistem. Selain itu, ada juga aktivitas *MiningPool*, yang dapat mengakibatkan terjadi penggunaan perangkat CPU untuk melakukan proses *mining* tanpa ada otorisasi dari pemilik perangkat, yang menyebabkan perangkat korban mengalami penurunan daya, memori, dan kegunaan operasional perangkat korban. Banyak ancaman keamanan siber juga muncul dari menyebarnya *Win.Trojan.Zero Access*, yang mampu mengunduh *malware* jenis lain ke komputer yang disusupinya dan menampilkan informasi palsu tentang ancaman siber pada komputer. *Discover Using Socks Agent* juga sangat berbahaya bagi keamanan siber di Indonesia karena sering disalahgunakan penyerang untuk melakukan berbagai aktivitas kejahatan, seperti eksploitasi koneksi SSH serta distribusi *botnet* dan *malware*. Ancaman siber ini juga berasal dari berbagai program virus yang berkembang dari waktu ke waktu.

Peningkatan risiko keamanan siber diakibatkan beberapa faktor seperti tidak memadainya pengembangan teknologi keamanan siber dan meningkatnya serangan yang kompleks dan rumit (Reegard, Blackett, and Katta, 2019). Masalah utama dari perusahaan yang mengalami serangan siber adalah lemahnya keamanan siber pada departemen atau divisi teknologi informasi (Lin, Zhu, & Son, 2015). Dalam hal ini diperlukan apa yang disebut keamanan siber (*cybersecurity*) sebagai upaya dalam pencegahan dari bahaya, pemakaian oleh pihak yang tidak berhak, dari exploitasi, dan kemampuan untuk melakukan restorasi terhadap informasi digital dan sistem komunikasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan (Axelrod, 2006). Untuk itu, diperlukan keterampilan keamanan siber, yaitu suatu kemampuan berbasis pengetahuan teknis, kemampuan, dan pengalaman yang berkaitan dengan perangkat keras dan perangkat lunak yang diperlukan untuk menjalankan keamanan sistem informasi untuk melakukan mitigasi serangan siber (Choi *et al*., 2015). Pada perusahaan menengah ke atas, keterampilan keamanan siber ini dapat ditingkatkan dengan menerapkan pelatihan pada karyawan teknologi informasi dengan berbagai pelatihan tentang kesadaran keamanan (*security awareness*), rekayasa sosial (*social engineering*), pengetahuan keamanan informasi (*information security knowledge*), sampai kebijakan dan risiko keamanan (*security policy and risk*). Perusahaan perlu menyediakan pelatihan untuk mengatasi masalah rendahnya kecakapan karyawan terkait keamanan siber, sehingga diharapkan dapat mengetahui cara mencegah dan bertahan terhadap serangan siber (Kim & Lowry, 2020).

Dalam praktik, ancaman kejahatan atau serangan siber bukan hanya terjadi pada perusahaan, melainkan juga organisasi sektor publik, baik pada pemerintahan pusat maupun daerah. Bahkan perusahaan-perusahaan milik negara dan daerah juga sering menjadi sasaran kejahatan atau serangan siber. Artinya, organisasi publik, termasuk perusahaan sektor publik, pada dasarnya perlu mengembangkan budaya keamanan siber, yang mendukung perilaku perlindungan keamanan siber pegawai organisasi publik sendiri. Dalam konteks itu, pengetahuan dan kesadaran keamanan siber pegawai perlu ditingkatkan untuk memperkuat budaya keamanan siber, yang pada gilirannya diharapkan mampu mendukung pembiasaan perilaku perlindungan keamanan siber di kalangan pegawai organisasi publik.

Pada tingkat operasional, keamanan siber organisasi bukan hanya menjadi urusan bagian Teknologi Informasi, melainkan juga harus diatasi melalui langkah-langkah organisasi, dan bukan sekedar langkah teknis belaka. Mengabaikan faktor manusia dapat menjadi salah satu penyebab utama tingginya risiko keamanan siber (Metalidou *et al*., 2014). Artinya, orang-orang organisasi publik harus mengambil tanggung jawab terhadap pemeliharaan budaya siber yang aman di tempat kerja. Tanpa budaya tanggung jawab ini, SDM yang awalnya diandalkan menjadi unsur keunggulan bersaing cenderung menjadi penyebab utama kejahatan atau serangan siber. Di sini pentingnya manajemen organisasi publik selalu mengembangkan dan memelihara budaya keamanan siber agar dapat mendukung perilaku perlindungan keamanan siber dalam lingkungan bisnis yang kompetitif dan berubah cepat. Oleh karena itu, peneliti tertarik menguji pengaruh dari budaya keamanan siber terhadap perilaku perlindungan keamanan siber, yang didasari oleh pengetahuan maupun kesadaran keamanan siber, dalam organisasi publik di Indonesia.

1.2. Rumusan Masalah

Berdasarkan latarbelakang masalah penelitian tersebut, masalah penelitian ini dapat dirumuskan sebagai berikut:

1. Apakah pengetahuan keamanan siber berpengaruh terhadap kesadaran keamanan siber pada pegawai organisasi publik di Indonesia?
2. Apakah pengetahuan keamanan siber berpengaruh terhadap budaya keamanan siber pada pegawai organisasi publik di Indonesia?
3. Apakah pengetahuan keamanan siber berpengaruh terhadap perilaku perlindungan keamanan siber pada pegawai organisasi publik di Indonesia?
4. Apakah kesadaran keamanan siber berpengaruh terhadap budaya keamanan siber pada pegawai organisasi publik Indonesia?
5. Apakah kesadaran keamanan siber berpengaruh terhadap perilaku perlindungan keamanan siber pada pegawai organisasi publik di Indonesia?
6. Apakah budaya keamanan siber berpengaruh terhadap perilaku perlindungan keamanan siber pada pegawai organisasi publik di Indonesia?

1.3. Tujuan Penelitian

Dengan perumusan masalah tersebut, beberapa tujuan penelitian ini dapat ditetapkan sebagai berikut.

1. Menguji pengaruh pengetahuan keamanan siber terhadap kesadaran keamanan siber pada pegawai organisasi publik di Indonesia.
2. Menguji pengaruh pengetahuan keamanan siber terhadap budaya keamanan siber pada pegawai organisasi publik di Indonesia.
3. Menguji pengaruh pengetahuan keamanan siber terhadap perilaku perlindungan keamanan siber pada pegawai organisasi publik di Indonesia.
4. Menguji pengaruh kesadaran keamanan siber terhadap budaya keamanan siber pada pegawai organisasi publik Indonesia.
5. Menguji pengaruh kesadaran keamanan siber terhadap perilaku perlindungan keamanan siber pada pegawai organisasi publik di Indonesia.
6. Menguji pengaruh budaya keamanan siber terhadap perilaku perlindungan keamanan siber pada pegawai organisasi publik di Indonesia.

1.4. Manfaat Penelitian

Seiring dengan meningkatnya risiko kejahatan dan serangan siber pada dua dekade terakhir (2000-2020), hasil penelitian ini diharapkan memberikan kontribusi dalam meningkatkan perlindungan keamanaan siber di Indonesia sebagai berikut.

1. Manfaat teoretis

   Hasil penelitian ini dapat menjadi bahan pertimbangan dalam upaya mengembangkan teori dan konsep perilaku perlindungan keamanan siber, terutama dengan melibatkan faktor-faktor yang diasumsikan mempengaruhi seperti pengetahuan, kesadaran dan budaya keamanan siber, baik di sektor publik maupun swasta.
2. Manfaat praktis.

   Diharapkan hasil penelitian ini dapat memberikan masukan tentang pentingnya organisasi publik di Indonesia, baik sudah atau akan melakukan transformasi digital, memberikan prioritas pelatihan untuk meningkatkan pengetahuan, kesadaran maupun budaya keamanan siber kepada pegawai

secara rutin dan berkelanjutan agar perilaku pegawai dalam perlindungan keamanan siber organisasi menjadi lebih baik dan dapat mengurangi resiko terjadinya kejahatan dan serangan siber.

Hasil penelitian ini diharapkan dapat menjadi bahan pertimbangan bagi pemerintah dalam memberikan perlindungan keamanan siber agar bisa terhindar dari risiko kejahatan dan serangan siber akibat lemahnya sistem keamanan siber, serta dapat segera menangani kasus kejahatan dan serangan siber yang terjadi secara hukum, khususnya di kalangan organisasi publik yang baru melakukan transformasi digital.

Hasil penelitian ini juga diharapkan dapat menjadi masukan peneliti selanjutnya untuk mengkaji topik keamanan siber secara lebih mendalam, baik secara kuantitatif maupun kualitatif, baik dalam sektor publik maupun swasta, agar hasilnya dapat memberikan temuan yang komprehensif dalam meningkatkan standar minimal keamanan siber menuju transformasi digital, baik dari aspek pengetahuan, kesadaran maupun perilaku pegawai dalam memberikan perlindungan keamanan siber organisasi maupun perusahaan.