BAB II
TINJAUAN PUSTAKA DAN KERANGKA PIKIR

2.1. Tinjauan Pustaka

2.1.1. Teori Utama, Teori Menengah, dan Teori Terapan

Penelitian mengenai perilaku perlindungan keamanan siber (c*ybersecurity protection behavior*) dapat dijelaskan dengan berbagai teori yang bersumber dari teori utama (*grand theory*), yaitu Teori Tindakan Beralasan (*Theory of Reasoned Action*—TRA) (Ajzen & Fishbein, 1980). Perilaku ini menjelaskan tentang cara masyarakat berperilaku seperti apa yang mereka inginkan dan apa saja alasan yang melandasi perilaku tersebut dalam berbagai konteks. Teori ini memberi penjelasan mengenai pengaruh intensi terhadap perilaku, khususnya dalam konteks teknologi informasi dan kepatuhan terhadap kebijakan keamanan siber (*cybersecurity policy compliance*) (Pahnila *et al*., 2007).

Intensi untuk mematuhi aturan-aturan keamanan siber ini berkaitan dengan sikap-sikap utama berdasarkan motivasi tertentu yang berorientasi pada kepatuhan terhadap kebijakan keamanan siber. Oleh karena itu, penelitian ini menggunakan Teori Motivasi Perlindungan (*Protection Motivation Theory*—PMT) (Maddux & Rogers, 1983) sebagai teori menengah (*middle-range theory*). Asumsinya adalah bahwa kebijakan keamanan siber dapat mendorong perilaku untuk melindungi aset-aset informasi dari serangan atau ancaman yang ditujukan kepada mereka di tengah ketakutan yang muncul yang menghasilkan sikap dan perilaku perlindungan.

Akhirnya, dalam upaya menjelaskan perilaku perlindungan keamanan siber, peneliti menggunakan Teori Perilaku Berencana (*Theory of Planned Behavior*—TPB) (Ajzen, 1991) sebagai teori terapan. Teori ini menjelaskan bahwa motivasi perlindungan keamanan siber itu menghasilkan tindakan beralasan dengan rencana yang disadari untuk menghasilkan dampak yang dikehendaki dalam menghindari kejahatan, serangan atau ancaman terhadap keamanan siber. Asumsinya, jika suatu organisasi terkena kejahatan, serangan atau ancaman keamanan siber, pegawainya tentu merasakan dampaknya, merasakan adanya ketakutan dan mendorong perilaku untuk mencegah kejahatan, serangan atau ancaman keamanan siber tersebut dalam

konteks kepatuhan pada kebijakan keamanan siber (Pahnila *et al*., 2007). Namun, kepekaan dari pegawai untuk terlibat dalam perilaku perlindungan keamanan siber organisasi juga dipengaruhi oleh kuat-lemahnya nilai-nilai budaya organisasi yang terinternalisasi pada diri pegawai. Artinya, semakin kuat pengetahuan keamanan siber (*cybersecurity knowledge*) maupun kesadaran keamanan siber (*cybersecurity awareness*) pegawai, tentunya semakin kuat pula nilai-nilai budaya keamanan siber (*cybersecurity culture*) di kalangan mereka, dan pada gilirannya dapat memperkuat perilaku perlindungan keamanan siber di kalangan pegawai organisasi.

2.1.2. Perilaku Perlindungan Keamanan Siber

Keamanan siber (*cybersecurity*) mengacu pada aktifitas, proses, kapabilitas atau kemampuan, atau kedudukan di mana sistem informasi dan komunikasi serta informasi yang tersimpan di dalamnya telah terlindungi dari kerusakan, pemakaian, modifikasi, atau eksploitasi dari pihak yang tidak berhak (NICCS, 2014). Pengguna yang menggunakan informasi tanpa kemampuan memakai alat-alat keamanan siber (*cybersecurity tool*) dianggap telah melanggar keamanan informasi (Nurse, Creese, Goldsmith, & Lamberts, 2011). Dalam sistem keamanan siber, upaya perlindungan informasi dilakukan pada lokasi yang paling banyak memiliki potensi celah terbesar mengalami kejahatan atau serangan siber (Mitnick & Simon, 2002).

Dalam perlindungan keamanan siber, keterampilan keamanan siber semakin diperlukan seiring dengan semakin kuatnya tren kejahatan atau serangan siber di berbagai organisasi. Perlindungan keamanan siber ini diarahkan pada perlindungan perangkat teknologi informasi yang mereka miliki agar perangkat ini terhindar dari serangan *malware* dan pencurian data (*data breach*). Malware adalah *malicious software* yang dirancang untuk membahayakan, menyusup, atau merusak sistem komputer dengan kode-kode tertentu di mana korbannya tidak langsung menyadari serangan terhadap sistem komputer mereka (NIST, 2013). Sementara itu, pencurian data umumnya terjadi pada perusahaan dan kejahatan atau serangan keamanan siber ini menunjukkan risiko keamanan siber terbesar terhadap reputasi organisasi, bukan hanya bagi kerugian keuangan perusahaan (Syed & Dhillion, 2015). Privacy Rights Clearinghouse (2014) melaporkan bahwa lebih dari 607 juta data telah hilang atau

dicuri dari sekitar 3.500 kasus kebocoran data. Risiko keamanan siber ini terjadi di berbagai perusahaan akibat para ahli atau insinyur bidang keamanan sibernya tidak dapat menangani isu-isu pencurian data tesebut dengan baik.

Berdasarkan penjelasan tersebut, dapat disimpulkan bahwa dalam penelitian ini, perilaku perlindungan keamanan siber dapat dipahami sebagai perilaku pegawai dalam melakukan perlindungan terhadap keamanan data pada teknologi informasi yang digunakan organisasi publik. Perilaku perlindungan keamanan siber ini dapat dilihat dari beberapa indikator utama sebagai berikut: penggunaan anti virus pada komputer berkala (*up-to-date*) (Z_a), merespons perilaku tidak wajar yang terjadi pada komputer (Z_b), menyikapi peringatan *malware* yang diterima (Z_c), berperan aktif mengikuti pelatihan keamanan yang disediakan oleh organisasi publik (Z_d), dan peduli pada keamanan informasi organisasi publik (Z_e).

2.1.3. Budaya Keamanan Siber

Dengan meningkatnya pemanfaatan teknologi informasi dalam kehidupan sehari-hari, organisasi publik perlu berusaha mencari solusi teknis terkini agar para pegawainya dapat menjaga sistem perlindungan keamanan siber. Dalam praktiknya pengetahuan dan kesadaran keamanan siber saja sering tidak cukup dalam rangka melindungi keamanan siber organisasi publik karena adanya kemajuan teknologi keamanan siber yang lebih canggih dari waktu ke waktu. Dalam konteks itu, faktor manusia tetap menjadi unsur terlemah dalam matarantai keamanan siber organisasi publik, sehingga mengembangkan budaya keamanan siber dalam organisasi dapat mengurangi risiko faktor manusia (Enisa, 2017). Dalam hal ini, budaya keamanan siber organisasi mengacu pada pengetahuan, keyakinan, persepsi, sikap, asumsi, norma, dan nilai orang-orang mengenai keamanan siber dan bagaimana semua itu terwujud dalam perilaku orang-orang itu dalam menggunakan informasi. Budaya keamanan siber berkaitan dengan budaya yang berlaku dalam organisasi, sehingga semua orang di dalamnya menjadikan pertimbangan keamanan informasi sebagai bagian integral dari pekerjaan dan kebiasaan kerja sehari-hari pegawai. Budaya ini membentuk sikap dan perilaku pegawai yang tepat dalam melindungi aset informasi organisasi serta menjadi bagian dari budaya organisasi yang lebih luas.

Huang dan Pearlson (2019) menjelaskan budaya keamanan siber sebagai bagian dari budaya organisasi berkaitan dengan sikap, asumsi, keyakinan, nilai, dan pengetahuan yang digunakan oleh pegawai untuk berinteraksi dengan sistem dan prosedur organisasi. Interaksi ini menghasilkan perilaku yang dapat diterima yang menjadi bagian dari cara organisasi melindungi aset informasinya. Sikap, asumsi, keyakinan, nilai, dan pengetahuan dalam budaya keamanan siber ini mendorong perilaku pegawai sesuai dengan sistem teknologi informasi dalam organisasi. Jadi, budaya keamanan siber menekankan perilaku pegawai yang mematuhi kebijakan keamanan informasi serta keterlibatan pribadi dalam keamanan siber, khususnya untuk melindungi dan menjaga organisasi dari kejahatan atau serangan siber.

Secara umum, budaya keamanan siber mengacu pada budaya dari organisasi yang memungkinkan pegawai memiliki komitmen yang kuat pada keamanan siber serta kepatuhan kebijakan keamanan siber dalam mengantisipasi risiko keamanan siber. Budaya keamanan siber ini semakin banyak dibutuhkan oleh organisasi yang mengandalkan cadangan data pada teknologi komunikasi dan informasi skala besar. Saat ini semakin banyak organisasi menghadapi situasi yang penuh resiko dalam pengelolaan organisasi yang berbasis teknologi informasi akibat masih lemahnya program manajemen risiko keamanan informasi, kurang terfokusnya penilaian atas resiko keamanan siber, dan rendahnya kemampuan mengatur program keamanan informasi, baik dalam penciptaan maupun pemeliharaan, melalui penjagaan ketat oleh tim audit teknologi informasi.

Organisasi yang memiliki kemampuan untuk menjalankan semua penilaian resiko yang terfokus, komprehensif, dan akurat dapat menghasilkan fondasi yang diperlukan untuk membangun sistem keamanan informasi. Sistem seperti ini harus didukung dengan budaya keamanan siber yang mendasari efektivitas pelaksanaan program keamanan informasi dengan kepatuhan tinggi pada kebijakan keamanan siber. Selain itu, budaya keamanan siber juga mendorong dokumentasi yang baik berupa dokumentasi fisik, administratif maupun teknis, sehingga semua informasi yang dibutuhkan di perusahaan diperoleh dari hasil penilaian resiko yang terfokus, komprehensif, dan akurat sesuai prinsip kepatuhan kebijakan keamanan siber.

Budaya keamanan siber dapat terbentuk di kalangan pegawai organisasi jika mereka mempunyai komitmen organisasi yang kuat. Dengan komitmen organisasi yang kuat, pegawai memiliki identifikasi keterlibatan pribadi dalam organisasi di tengah relasi antara mereka dengan organisasi tempat mereka bekerja (Mowday, 1998). Diharapkan bahwa semakin tinggi komitmen organisasi pegawai terhadap organisasi, semakin tinggi pula kinerja mereka dalam menyelesaikan tugas, dalam konteks ini sesuai dengan prinsip kepatuhan kebijakan keamanan siber.

Berdasarkan penjelasan tersebut, dapat disimpulkan bahwa bagi organisasi publik yang banyak mengandalkan teknologi informasi dan keamanan siber untuk melindungi data, budaya keamanan siber dipandang penting dan harus diikuti oleh semua pegawai pada berbagai tingkat. Kuatnya budaya keamanan siber ini ditandai dengan tiga indikator utama, yaitu: kuatnya komitmen pegawai terhadap keamanan siber (Y_a), kesediaan mempelajari situasi dan kondisi keamanan data dan informasi organisasi (Y_b), dan kepatuhan pada kebijakan keamanan siber untuk menghindari terjadinya kejahatan dan serangan siber (Y_c).

2.1.4. Pengetahuan Keamanan Siber

Perusahaan berbasis teknologi informasi selalu berusaha melawan adanya serangan siber yang dapat menyebabkan terjadinya kebocoran akibat pencurian data (*data breach*). Ancaman pencurian data ini nyata dan selalu meningkat dari waktu ke waktu (Sudareswaran, 2018). Di perusahaan, semua pihak yang terkait idealnya selalu terlibat dalam melindungi keamanan informasi perusahaan. Oleh karena itu, setiap pegawai memerlukan pelatihan keamanan informasi (*information security training*) agar mereka mengetahui cara menghindari terjadinya masalah kejahatan atau serangan siber. Asumsinya, semakin tinggi pengetahuan keamanan siber yang dimiliki oleh pegawai, maka semakin tinggi pula kesadaran dan budaya keamanan siber pegawai organisasi dalam melindungi keamanan siber perusahaan. Karena itu, para manajer senior perlu membangun budaya keamanan siber yang baik dengan memberikan pelatihan keamanan siber kepada pegawainya. Hal ini karena pelaku kejahatan siber memiliki kemampuan lebih di bidang teknologi informasi dan selalu selangkah lebih maju dari sasaran walaupun organisasi yang menjadi calon korban

kejahatan atau serangan siber sudah memiliki sistem keamanan siber yang membaik (Chronopoulos, Panousis, & Grossklags, 2017).

Tanpa memiliki pengetahuan keamanan siber yang memadai, pegawai akan menyebabkan terjadinya kejahatan atau serangan siber terhadap organisasi. Apabila organisasi tidak memberikan pelatihan yang baik kepada para pegawainya, mereka cenderung tidak dapat menjalankan kepatuhan kebijakan keamanan siber. Terkait hal ini, Calder dan Watkins (2015) menjelaskan bahwa masih banyak kejadian di organisasi di mana pegawai membuka lampiran berkas di email yang diterimanya dan tanpa disadari kasus ini mengakibatkan komputernya terinfeksi virus. Menurut Barrett *et al*. (2016), selama puluhan tahun, informasi yang tersimpan di komputer harus selalu diperhatikan. Jika organisasi mengalami serangan siber, reputasinya terancam hilang, pelanggan mengalami krisis kepercayaan, dan organisasi itu akan mengalami kerugian atau penurunan citra di ruang publik.

Dalam konteks tersebut, pelatihan keamanan informasi menjadikan pegawai lebih banyak memiliki pengetahuan keamanan siber dalam pekerjaan sehari-hari, khususnya di perusahaan yang bergantung pada teknologi informasi. Penggunaan teknologi internet dapat memfasilitasi pegawai dalam segala aktifitas berbasis siber skala besar. Namun, pengetahuan tentang alat bantu yang dimiliki diperlukan untuk memberikan perlindungan antisipatif terhadap ancaman siber agar resiko kejahatan siber berkurang (Abawajy, 2014). Salah satu pelatihan teknologi informasi adalah *Phishing Simulator* sebagai pelatihan yang efektif untuk peningkatan pengetahuan keamanan siber terkait email berbahaya yang dikirim oleh penjahat (*hacker*).

Penjelasan tersebut menunjukkan bahwa pengetahuan keamanan siber bagi pegawai perusahaan sangat penting untuk mengantisipasi terjadinya kejahatan atau serangan siber. Dengan pelatihan keamanan informasi, pegawai dapat mendukung perusahaan dengan mengatasi kelemahan dan celah yang ada pada sistem teknologi informasi di perusahaan, sehingga pegawai tidak akan dengan mudah memberikan informasi rahasia perusahan baik karena kesengajaan maupun karena insiden yang tidak dikehendaki, khususnya pada saat mereka sedang menjalankan suatu tombol fungsi pada aplikasinya (Sackie-Mensah, 2016). Robert (2018) mengatakan bahwa kelemahan utama dalam jaringan suatu perusahaan adalah pada orang, bukan pada

teknologinya. Oleh karena itu, perusahaan harus serius mengadakan pelatihan yang memadai untuk pegawai di perusahaan agar mereka bekerja dengan benar sehari-hari di kantor sesuai dengan kepatuhan kebijakan keamanan siber.

Berdasarkan penjelasan tersebut, dapat disimpulkan bahwa dalam sebuah organisasi publik, pegawai perlu memiliki pengetahuan memadai tentang keamanan siber di tempat mereka bekerja. Pengetahuan keamaaan siber ini berkaitan dengan alat bantu atau perangkat yang ada dan diperlukan organisasi untuk memberikan perlindungan dalam melawan ancaman kejahatan atau serangan siber, khususnya untuk memperlambat kejadian yang merusak sistem keamanan siber. Pengetahuan keamanan siber berkaitan dengan tiga indikator, yaitu pengetahuan mengenai risiko keamanan (X_{1a}), pengetahuan perlindungan keamanan (X_{1b}), dan pengetahuan komputer (X_{1c}). Dalam praktik, tiga indikator pengetahuan keamanan siber tersebut dapat ditingkatkan melalui program pelatihan keamanan siber.

2.1.5. Kesadaran Keamanan Siber

Kesadaran keamanan siber (*cybersecurity awareness*) adalah kesadaran tentang praktek-praktek dan peraturan-peraturan yang berkaitan dengan keamanan siber yang dipelajari melalui pelatihan dan berdasarkan peraturan keamanan siber yang ada. Menurut Qualdri (2013), peraturan keamanan siber ini mencakup semua level, meliputi semua domain, dan harus dilaksanakan berkesinambungan. Melalui pelatihan, bagian teknologi informasi organisasi dapat memperkenalkan topik-topik keamanan siber yang berkembang saat ini beserta celah kejahatan maupun serangan siber, dan berusaha membuat organisasi menjadi lebih aman. Banyak kelemahan keamanan siber terjadi dalam organisasi akibat kurangnya kesadaran pegawai.

Shaw *et al* (2009) menjelaskan bahwa kesadaran keamanan siber mengacu pada derajat pemahaman pegawai mengenai pentingnya keamanan informasi dan tanggung jawab mereka serta bertindak melaksanakan kontrol keamanan informasi secara memadai untuk melindungi data dan jejaring organisasi. Dalam organisasi yang mengandalkan penggunaan teknologi informasi, hal paling penting yang perlu diwaspadai adalah kejahatan *hacker*, yang selalu berusaha untuk mencari celah atau kelemahan keamanan siber organisasi, termasuk kelemahan di kalangan pegawai.

Jika pegawai kurang memiliki kesadaran keamanan siber, faktor manusia ini dapat menjadi penyebab utama kebocoran siber. Menyadari celah atau kelemahan ini, manajemen organisasi perlu mengadakan pelatihan tentang pentingnya kesadaran keamanan siber dalam meningkatkan kesadaran kejahatan siber maupun kesadaran kebijakan keamanan siber di kalangan pegawai mereka (Dodge, 2007). Jadi, dapat disimpulkan bahwa semakin tinggi kesadaran keamanan siber maupun kesadaran kebijakan keamanan siber, maka semakin tinggi pula kesadaran keamanan siber di dalam organisasi yang bersangkutan.

Berdasarkan penjelasan tersebut, maka dapat disimpulkan bahwa kesadaran keamanan siber adalah derajat pemahaman pegawai tentang pentingnya keamanan informasi dan tanggung jawab mereka serta bertindak untuk melaksanakan kontrol keamanan informasi ini hingga tingkat yang memadai untuk melindungi data dan jejaring organisasi. Kesadaran keamanan siber ini dapat dilihat dari tiga indikator, yaitu kesadaran untuk patuh pada kebijakan keamanan siber di dalam organisasi, yang dapat menghindari resiko kebocoran data (X_{2a}), kesadaran untuk mengikuti pelatihan secara rutin (X_{2b}) dan kesadaran melakukan perlindungan secara rutin seperti pencadangan (*backup*), pemakaian kata kunci yang kuat (*strong password*) dan penggantian kata kunci secara berkala (X_{2c}).

2.1.6. Penelitian Terdahulu

Sebenarnya penelitian tentang keamanan siber sudah pernah dilakukan oleh beberapa peneliti sebelumnya. Namun, topik yang mereka kaji berbeda dari topik penelitian sekarang, demikian pula tujuan, metode, dan hasil penelitiannya.

1. Li, He, Xu, Ash, Anwar, dan Yuan (2019) melakukan penelitian mengenai dampak kesadaran kebijakan keamanan siber terhadap perilaku keamanan siber pegawai. Penelitian ini dilakukan karena seiring dengan meningkatnya volume dan kompleksitas teknologi internet dan aplikasi bergerak (*mobile application*), ternyata meningkat pula serangan siber yang berbahaya, dan akibatnya masyarakat menghadapi risiko keamanan siber yang lebih besar di ruang siber dibandingkan sebelumnya. Penelitian ini dilakukan dengan metode kuantitatif menggunakan teknik analisis ANOVA. Hasil penelitian

ini menunjukkan bahwa ketika pegawai menyadari kebijakan dan prosedur keamanan informasi perusahaan, mereka lebih kompeten dalam mengelola tugas-tugas keamanan siber dibandingkan karyawan yang tidak menyadari kebijakan dan prosedur keamanan siber. Selain itu, lingkungan keamanan informasi organisasi itu secara positif mempengaruhi kemampuan penilaian ancaman dan kemampuan menghadapinya, yang pada gilirannya juga secara positif berkontribusi pada perilaku kepatuhan keamanan siber mereka.

2. Al-Alawi dan Al-Bassam (2019) melakukan penelitian tentang faktor-faktor yang diduga mempengaruhi kesadaran keamanan siber di sektor perbankan. Penelitian ini dilakukan dengan metode kuantitatif dan dianalisis dengan teknik deskriptif. Hasil penelitian ini menunjukkan bahwa faktor kepatuhan keamanan siber memiliki nilai mean tertinggi (4,28), dan budaya keamanan siber nilai mean terendah (4,24), tetapi kedua faktor ini memiliki pengaruh signifikan terhadap kesadaran keamanan siber. Responden umumnya sangat setuju tentang perlunya faktor-faktor ini di sektor perbankan. penelitian ini menunjukkan faktor penting yang dapat membantu memperbaiki kebijakan atau pedoman dalam meningkatkan kesadaran keamanan siber organisasi, untuk mengenali ancaman siber, dampak serangan siber dan bagaimana cara mengurangi risiko siber dan menghindari kejahatan siber yang memenetrasi ruang siber organisasi.
3. Zwilling, Klien, Lesjak, Wiechetek, Cetin dan Basim (2020) melakukan penelitian mengenai hubungan antara kesadaran, pengetahuan, dan perilaku keamanan siber dengan alat perlindungan keamanan siber di antara individu berbeda. Penelitian ini dilakukan dengan metode kualitatif dengan teknik analisis perbandingan. Hasil penelitian ini menunjukkan bahwa pengguna internet memiliki kesadaran ancaman siber yang memadai, tetapi umumnya hanya menerapkan langkah-langkah perlindungan keamanan siber minimal, umum dan sederhana. Penelitian ini juga menemukan bahwa pengetahuan siber yang lebih tinggi berhubungan dengan lebih tingginya kesadaran siber. Selain itu, kesadaran siber juga berhubungan dengan alat-alat perlindungan, tetapi tidak berkaitan dengan informasi yang akan mereka ungkap.

4. Pham, Ulhaq, Nguyen dan Nkhoma (2021) melakukan penelitian eksploratif mengenai pengaruh tiga metode berbagi pengetahuan (pelatihan keamanan, komunikasi media sosial, ahli keamanan lokal) terhadap praktik keamanan siber. Penelitian ini dilakukan mengingat dalam ekonomi global berjejaring, ancaman keamanan siber meningkat luar biasa dan infrastruktur keamanan siber pada tingkat organisasi maupun nasional sering tidak efektif melawan semua ancaman ini. Penelitian ini dilakukan dengan metode kualitatif dan teknik analisis fenomenologi. Hasil penelitian menunjukkan bahwa metode/ saluran berbagi informasi mempunyai pengaruh terhadap praktik keamanan siber pegawai. Pertama, metode pelatihan keamanan periodik dan siaran via email kurang efektif mendorong partisipan mengembangkan kemampuan keamanan dan seringkali diabaikan. Kedua, berbagi pengetahuan keamanan via media sosial dan ahli keamanan lokal berkontribusi pada pemeliharaan kesadaran keamanan pegawai. Media sosial dianggap sebagai saluran yang lebih disukai untuk menyebarkan info kewaspadaan keamanan siber yang sudah mendesak. Ahli keamanan lokal diakui mampu menyediakan nasihat tentang keamanan tepat waktu dan sesuai dengan konteks.

Berdasarkan penjelasan tersebut, maka dapat disimpulkan bahwa beberapa penelitian terdahulu tersebut memiliki topik dan tujuan penelitian yang berbeda dari penelitian sekarang. Penelitian ini tidak berfokus pada dampak kesadaran kebijakan keamanan siber terhadap perilaku keamanan siber para pegawai (Li, He, Xu, Ash, Anwar, & Yuan, 2019); faktor-faktor yang mempengaruhi kesadaran keamanan siber di sektor perbankan (Al-Alawi & Al-Bassam, 2019); hubungan kesadaran, pengetahuan, dan perilaku keamanan siber dengan alat perlindungan keamanan siber di antara individu (Zwilling, Klien, Lesjak, Wiechetek, Cetin & Basim, 2020); dan pengaruh tiga metode berbagi pengetahuan (pelatihan keamanan, komunikasi media sosial, ahli keamanan lokal) terhadap praktik keamanan siber (Pham, Ulhaq, Nguyen & Nkhoma, 2021). Penelitian ini berfokus pada pengaruh pengetahuan dan kesadaran keamanan siber terhadap budaya keamanan siber, yang mempengaruhi perilaku perlindungan keamanan siber dalam organisasi publik di Indonesia.

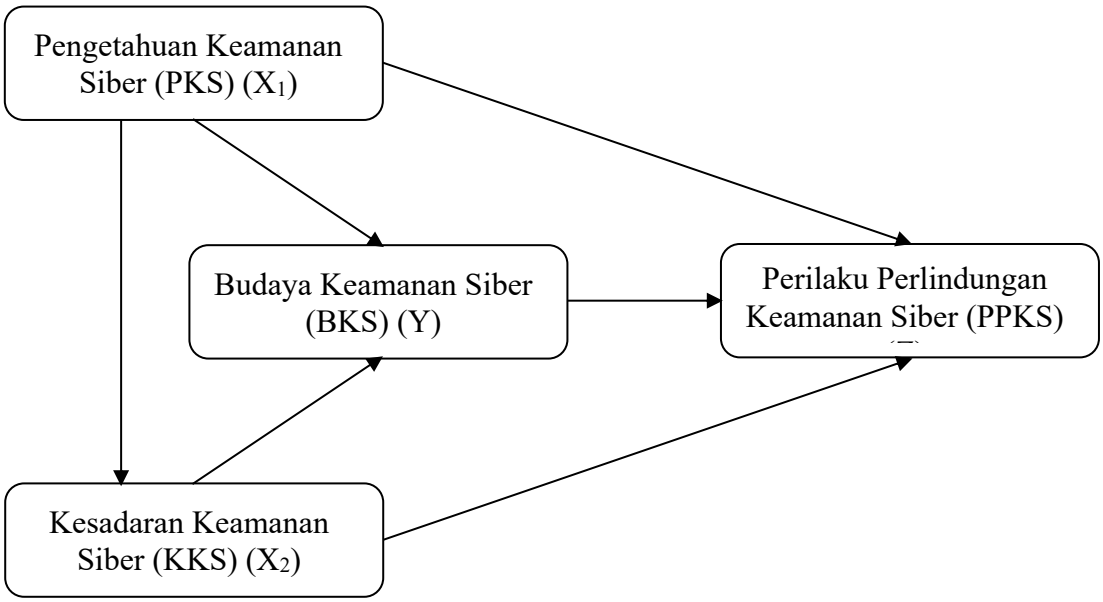
Tabel 2.1 Hasil Penelitian Terdahulu

No.	Penulis (Tahun)	Judul & Jurnal	Tujuan	Metode	Hasil
1.	Li, He, Xu, Ash, Anwar, dan Yuan (2019)	*Investigating the impact of cybersecurity policy awareness on employee's cybersecurity behavior (International Journal of International Management)*	Menyelidiki dampak kesadaran kebijakan siber terhadap perilaku keamanan siber	Kuantitatif (ANOVA)	Ketika karyawan menyadari kebijakan dan prosedur keamanan informasi perusahaan, mereka lebih kompeten untuk mengelola tugas-tugas keamanan siber daripada karyawan yang tidak menyadari kebijakan dan prosedur keamanan siber,
2.	Al-Alawi dan Al-Bassam (2019)	*Assesing the Factors of Cybersecurity Awareness in the Banking Sector (Arab Gulf Journal of Scientific Research—AGJSR)*	Mengidentifikasi faktor-faktor kesadaran keamanan siber di sektor perbankan.	Kuantitatif (Analisis deskriptif)	Kepatuhan keamanan siber memiliki nilai mean tertinggi (4,28), dan budaya keamanan siber nilai mean terendah (4,24), tetapi kedua faktor ini memiliki pengaruh signifikan terhadap kesadaran keamanan siber. Responden sangat setuju tentang perlunya faktor-faktor ini di sektor perbankan.
3.	Zwilling, Klien, Lesjak, Wiechetek, Cetin dan Basim (2020)	*Cyber Security Awareness, Knowledge and Behavior: A Comparative Study (Journal of Computer Information Systems)*	Menguji pengaruh kesadaran dan pengetahuan keamanan siber terhadap perilaku keamanan siber	Kuantitatif	Pengguna internet memiliki kesadaran siber yang memadai tetapi hanya menerapkan langkah perlindungan minimal, umum dan sederhana. Pengetahuan siber lebih tinggi berkaitan dengan kesadaran siber lebih tinggi. Kesadaran siber juga berkaitan dengan alat perlindungan, bukan dengan informasi yang siap mereka ungkap.
4.	Pham, Ulhaq, Nguyen dan Nkhoma (2021)	*An Exploratory Study of the Effects of Knowledge Sharing Methods on Cyber Security Practice (Australasian Journal of Information Systems)*	Menguji pengaruh metode tiga berbagi pengetahuan (pelatihan keamanan, komunikasi media sosial, dan ahli keamanan lokal) terhadap praktik keamanan pengguna	Kualitatif (Fenomenologi)	Metode atau saluran berbagi informasi memiliki pengaruh terhadap praktik keamanan siber pegawai. Metode training keamanan periodik dan siaran via email ditemukan kurang efektif dalam mendorong partisipan mengembangkan kemampuan keamanan dan sering diabaikan. Berbagi pengetahuan keamanan melalui media sosial dan ahli keamanan lokal berkontribusi pada pemeliharaan kesadaran keamanan pegawai. Media sosial dianggap sebagai saluran yang lebih disukai untuk menyebarkan info kewaspadaan keamanan siber yang urgen. Ahli keamanan lokal dipuji karena menyediakan nasihat keamanan tepat waktu dan sesuai dengan konteks.

Sumber: Tinjauan Pustaka (2022)

2.2. Kerangka Pikir

Penelitian ini menguji model perilaku perlindungan keamanan siber dengan asumsi bahwa Perilaku Perlindungan Keamanan Siber (PPKS) (Z) dipengaruhi oleh Budaya Keamanan Siber (BKS) (Y), yang bersama-sama dipengaruhi pula oleh Pengetahuan Kemanan Siber (PKS) (X_1) dan Kesadaran Keamanan Siber (KKS) (X_2) di kalangan pegawai organisasi publik, khususnya di Indonesia.



Gambar 2.1
Kerangka Pikir Penelitian

2.3. Pengembangan Hipotesis

Berdasarkan kerangka pikir penelitian tersebut, beberapa hipotesis dalam model perilaku perlindungan keamanan siber ini dapat diajukan sebagai berikut.

1. Pengetahuan Keamanan Siber dan Kesadaran Keamanan Siber

   Dalam organisasi publik, pengetahuan keamanan siber memainkan peran penting sebagai dasar tumbuhnya kesadaran keamanan siber pegawai. Pengetahuan keamanan siber pegawai memungkinkan mereka lebih sadar mengenai kemungkinan terjadinya serangan siber yang dapat menyebabkan terjadinya kebocoran akibat pencurian data (*data breach*) sebagai ancaman

yang nyata dan meningkat dari waktu ke waktu (Sudareswaran, 2018). Hal ini penting karena semua pihak dalam organisasi perlu mengetahui cara-cara menghindari terjadinya masalah kejahatan atau serangan siber. Kesadaran keamanan siber berkaitan dengan kesadaran mengenai praktek-praktek dan peraturan-peraturan yang berkaitan dengan keamanan siber yang dipelajari melalui pelatihan berdasarkan peraturan keamanan siber yang ada. Banyak kelemahan keamanan siber terjadi di dalam organisasi akibat kurangnya kesadaran pegawai, yang jelas menunjukkan rendahnya derajat pemahaman pegawai mengenai arti pentingnya keamanan informasi dan tanggung jawab mereka serta bertindak melaksanakan kontrol keamanan informasi secara memadai untuk melindungi data dan jejaring organisasi (Shaw *et al*., 2009). Jika pegawai kurang memiliki kesadaran keamanan siber, faktor ini menjadi penyebab utama kebocoran siber. Menyadari celah kelemahan ini, pimpinan organisasi perlu mengadakan suatu pelatihan tentang pentingnya kesadaran keamanan siber dalam peningkatan kesadaran kejahatan siber dan kebijakan keamanan siber di kalangan pegawai (Dodge, 2007). Tanpa pengetahuan dan kesadaran keamanan siber yang memadai, pegawai dapat menyebabkan terjadinya kejahatan atau serangan siber terhadap organisasi. Jika organisasi tidak memberikan pelatihan yang baik kepada pegawai, mereka tidak dapat menjalankan kepatuhan kebijakan keamanan siber. Tanpa pengetahuan dan kesadaran keamanan siber, masih banyak kejadian dalam organisasi di mana pegawainya membuka lampiran berkas email yang diterimanya dan tanpa disadari kasus ini mengakibatkan komputernya terinfeksi virus (Calder dan Watkins, 2015). Pelatihan keamanan informasi menjadikan pegawai lebih memiliki pengetahuan keamanan siber terkait pekerjaan sehari-hari dalam organisasi yang bergantung pada teknologi informasi. Pengetahuan tentang alat bantu yang dimilikinya diperlukan untuk memberikan perlindungan terhadap ancaman siber agar resiko kejahatan siber berkurang (Abawajy, 2014). Dengan pelatihan keamanan informasi, pegawai dapat mendukung organisasi dengan mengatasi kelemahan dan celah dalam sistem teknologi informasi sehingga pegawai tidak mudah memberikan informasi rahasianya

karena sengaja atau karena insiden yang tidak dikehendaki ketika mereka sedang menjalankan tombol fungsi dalam aplikasi (Sackie-Mensah, 2016). Pengetahuan keamanan siber dapat dilihat dari pengetahuan tentang risiko keamanan, pengetahuan tentang perlindungan keamanan, dan pengetahuan tentang komputer, sedangkan kesadaran keamanan siber berkaitan dengan kesadaran untuk patuh pada kebijakan keamanan siber di dalam organisasi yang dapat menghindari resiko kebocoran data, kesadaran untuk mengikuti pelatihan secara rutin, dan kesadaran melakukan perlindungan secara rutin seperti pencadangan, pemakaian kata kunci yang kuat, dan penggantian kata kunci secara berkala. Jadi, pengetahuan keamanan siber pegawai ini sangat penting agar mereka memiliki kesadaran keamanan siber dan lebih mampu mengantisipasi kejahatan atau serangan siber. Asumsinya, semakin tinggi pengetahuan keamanan siber yang dimiliki oleh pegawai, semakin tinggi pula kesadaran keamanan siber pegawai dalam melindungi keamanan siber perusahaan. Berdasarkan pemahaman tersebut, hipotesis penelitian ini dapat dirumuskan sebagai berikut.

Hipotesis 1 (H_1)

Pengetahuan keamanan siber memiliki pengaruh yang positif dan signifikan terhadap kesadaran keamanan siber dalam organisasi publik.

2. Pengetahuan Keamanan Siber dan Budaya Keamanan Siber

Dalam organisasi publik, pengetahuan keamanan siber berpengaruh pada terbentuknya budaya keamanan siber. Melawan serangan siber seperti kebocoran akibat pencurian data (*data breach*) perlu didasari dengan nilai-nilai budaya keamanan siber. Dalam praktiknya pengetahuan dan kesadaran keamanan siber saja sering tidak cukup dalam rangka melindungi keamanan siber organisasi publik karena adanya kemajuan teknologi keamanan siber yang lebih canggih dari waktu ke waktu. Dalam konteks itu, faktor manusia tetap menjadi unsur terlemah dalam matarantai keamanan siber organisasi publik, sehingga mengembangkan budaya keamanan siber dalam organisasi dapat mengurangi risiko faktor manusia (Enisa, 2017). Budaya keamanan siber mengacu pada pengetahuan, keyakinan, persepsi, sikap, asumsi, norma

dan nilai orang-orang mengenai keamanan siber dan bagaimana semua itu terwujud di dalam perilaku orang-orang itu dalam menggunakan informasi. Dengan budaya keamanan siber, semua orang dalam organisasi menjadikan pertimbangan keamanan informasi sebagai bagian integral dari pekerjaan dan kebiasaan kerja sehari-hari pegawai. Budaya ini membentuk sikap dan perilaku pegawai yang tepat dalam melindungi aset informasi serta menjadi bagian dari budaya organisasi yang lebih luas. Budaya keamanan siber pada dasarnya merupakan bagian dari budaya organisasi berkaitan dengan sikap, asumsi, keyakinan, nilai, dan pengetahuan yang digunakan pegawai untuk berinteraksi dengan sistem dan prosedur dari organisasi, yang menghasilkan perilaku yang diterima dan menjadi bagian dari cara organisasi melindungi aset informasinya (Huang & Pearlson, 2019). Sikap, asumsi, keyakinan, nilai, dan pengetahuan dalam budaya keamanan siber mendorong perilaku pegawai sesuai dengan sistem teknologi informasi dari organisasi. Budaya keamanan siber menekankan perilaku pegawai yang mematuhi kebijakan keamanan informasi serta keterlibatan pribadi dalam keamanan siber untuk melindungi dan menjaga organisasi dari kejahatan atau serangan siber. Nilai budaya keamanan siber mengacu pada budaya organisasi yang menjadikan pegawai mempunyai komitmen kuat pada keamanan siber serta kepatuhan kebijakan keamanan siber dalam mengantisipasi kejahatan keamanan siber. Budaya keamanan siber mendorong dokumentasi fisik, administratif, dan teknis, sehingga semua informasi yang dibutuhkan organisasi diperoleh dari hasil penilaian resiko yang terfokus, komprehensif, dan akurat sesuai prinsip kepatuhan kebijakan keamanan siber. Pengetahuan dan budaya keamanan siber pegawai sangat penting untuk mengantisipasi kejahatan atau serangan siber, sehingga mereka tidak dengan mudah memberikan informasi rahasia organisasi karena sengaja maupun karena insiden yang tidak dikehendaki ketika mereka sedang menjalankan tombol fungsi pada aplikasinya (Sackie-Mensah, 2016). Mereka perlu memiliki pengetahuan yang memadai tentang keamanan siber di tempat mereka bekerja agar terbentuk budaya keamanan siber yang bisa memperkuat perilaku perlindungan keamanan siber. Dengan

pengetahuan keamanan siber terkait dengan risiko keamanan, perlindungan keamanan, dan pengetahuan komputer, diasumsikan nilai budaya keamanan siber juga meningkat dilihat dari komitmen pegawai terhadap keamanan, kesediaan mempelajari situasi dan kondisi keamanan data dan informasi organisasi, dan kepatuhan terhadap kebijakan keamanan siber dalam rangka menghindari terjadinya kejahatan dan serangan siber. Dengan pemahaman tersebut, hipotesis penelitian ini dapat dirumuskan sebagai berikut.

Hipotesis 2 (H_2)

Pengetahuan keamanan siber memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan siber dalam organisasi publik.

3. Pengetahuan Keamanan Siber dan Perilaku Perlindungan Keamanan Siber

Dalam organisasi publik, pengetahuan keamanan siber memainkan peran penting dalam memperkuat perilaku perlindungan keamanan siber. Pengetahuan keamanan siber sangat penting bagi pegawai perusahaan untuk mengantisipasi terjadinya kejahatan atau serangan siber. Dengan pelatihan tentang keamanan informasi, pegawai dapat mendukung perusahaan dengan mengatasi kelemahan dan celah pada sistem teknologi informasi organisasi, sehingga pegawai tidak akan dengan mudah memberikan informasi rahasia perusahaan karena sengaja maupun karena insiden yang tidak dikehendaki ketika mereka sedang menjalankan tombol fungsi pada aplikasinya (Sackie-Mensah, 2016). Organisasi idealnya mengadakan pelatihan memadai untuk pegawainya agar mereka bekerja dengan benar sehari-hari di kantor sesuai kepatuhan kebijakan keamanan siber. Dengan pengetahuan keamaaan siber, pegawai diharapkan dapat menggunakan alat bantu atau perangkat yang ada dan diperlukan organisasi untuk memberikan perlindungan dalam melawan ancaman kejahatan atau serangan siber untuk memperlambat kejadian yang merusak sistem keamanan siber. Perilaku perlindungan keamanan siber ini diarahkan pada aktifitas, proses, kapabilitas, atau kedudukan di mana sistem informasi dan komunikasi serta informasi yang tersimpan di dalamnya dapat terlindungi dari kerusakan, pemakaian, modifikasi, atau eksploitasi dari para pihak yang tidak berhak (NICCS, 2014). Perlindungan informasi dilakukan

pada lokasi yang paling banyak memiliki potensi celah yang terbesar untuk mengalami kejahatan atau serangan siber (Mitnick & Simon, 2002). Hal ini diarahkan pada perlindungan perangkat teknologi informasi yang dimiliki agar perangkat ini terhindar dari serangan *malware* dan pencurian data (*data breach*). Dengan pengetahuan keamanan siber mengenai risiko keamanan, pengetahuan perlindungan keamanan, dan pengetahuan computer, perilaku perlindungan keamanan siber dapat dikembangkan melalui penggunaan anti virus pada komputer berkala (*up-to-date*), merespons perilaku tidak wajar yang terjadi pada komputer, menyikapi peringatan *malware* yang diterima, berperan aktif mengikuti pelatihan keamanan yang disediakan organisasi, dan peduli pada keamanan informasi organisasi. Asumsinaya, semakin kuat pengetahuan keamanan siber pegawai, semakin besar pula peningkatan perilaku perlindungan keamana siber. Berdasarkan pemahaman tersebut, hipotesis penelitian ini dapat dirumuskan sebagai berikut.

Hipotesis 3 (H_3)

Pengetahuan keamanan siber memiliki pengaruh yang positif dan signifikan terhadap perilaku perlindungan keamanan siber dalam organisasi publik.

4. Kesadaran Keamanan Siber dan Budaya Keamanan Siber

Dalam organisasi publik, kesadaran keamanan siber sangat penting dalam membentuk budaya keamanan siber. Kesadaran keamanan siber pada umumnya berkaitan dengan kesadaran tentang praktek dan peraturan terkait keamanan siber yang dipelajari melalui pelatihan dan berdasarkan peraturan keamanan siber yang ada. Kesadaran keamanan siber mengacu pada derajat pemahaman pegawai tentang pentingnya keamanan informasi dan tanggung jawab mereka serta bertindak melaksanakan kontrol keamanan informasi secara memadai untuk melindungi data dan jejaring organisasi (Shaw *et al*., 2009). Pelatihan mengenai arti pentingnya kesadaran keamanan siber perlu diadakan dalam meningkatkan kesadaran kejahatan siber maupun kesadaran kebijakan keamanan siber di kalangan pegawai mereka (Dodge, 2007). Hal ini penting untuk memperkuat budaya keamanan siber. Dalam konteks itu, faktor manusia menjadi unsur terlemah dalam matarantai keamanan siber,

sehingga mengembangkan budaya keamanan siber dalam organisasi dapat mengurangi risiko faktor manusia (Enisa, 2017). Budaya keamanan siber ini mengacu pada pengetahuan, keyakinan, persepsi, sikap, asumsi, norma, dan nilai dari orang-orang mengenai keamanan siber dan bagaimana semua itu terwujud dalam perilaku mereka dalam menggunakan informasi (Huang & Pearlson, 2019). Interaksi ini menghasilkan perilaku yang diterima sebagai bagian dari cara organisasi melindungi aset informasinya, yang mendorong perilaku pegawai sesuai dengan sistem teknologi informasi dari organisasi. Budaya keamanan siber menekankan perilaku dari pegawai yang mematuhi kebijakan keamanan informasi serta keterlibatan pribadi dalam keamanan siber untuk melindungi dan menjaga organisasi dari kejahatan atau serangan siber. Semakin tinggi kesadaran keamanan siber dan kebijakan keamanan siber, semakin tinggi pula kesadaran keamanan siber di dalam organisasi yang bersangkutan. Dengan kesadaran keamanan siber mengenai kepatuhan pada kebijakan keamanan siber yang dapat menghindari resiko kebocoran data, kesadaran mengikuti pelatihan secara rutin, dan kesadaran melakukan perlindungan rutin seperti pencadangan, pemakaian kata kunci yang kuat, dan penggantian kata kunci secara berkala, semakin kuat budaya perilaku keamanan siber. Budaya keamanan siber didasari oleh komitmen pegawai pada keamanan siber, kesediaan mempelajari situasi dan kondisi keamanan data dan informasi organisasi dan kepatuhan pada kebijakan keamanan siber untuk menghindari kejahatan dan serangan siber. Berdasarkan pemahaman tersebut, hipotesis penelitian ini dapat dirumuskan sebagai berikut.

Hipotesis 4 (H_4)

Kesadaran keamanan siber memiliki pengaruh yang positif dan signifikan terhadap budaya keamanan siber dalam organisasi publik.

5. Kesadaran Keamanan Siber dan Perilaku Perlindungan Keamanan Siber

Dalam organisasi publik, kesadaran keamanan siber sangat penting dalam mendorong perilaku perlindungan keamanan siber. Kesadaran terkait keamanan siber ini mengacu pada kesadaran tentang praktek dan peraturan yang berkaitan dengan keamanan siber yang dipelajari melalui pelatihan dan

berdasarkan peraturan keamanan siber yang ada. Kesadaran keamanan siber mengacu pada derajat pemahaman pegawai tentang pentingnya keamanan informasi dan tanggung jawab mereka serta bertindak melaksanakan kontrol keamanan informasi secara memadai untuk melindungi data dan jejaring organisasi (Shaw *et al*., 2009). Pelatihan pentingnya kesadaran keamanan siber perlu diadakan dalam peningkatan kesadaran kejahatan siber maupun kesadaran kebijakan keamanan siber di kalangan pegawai (Dodge, 2007). Semakin tinggi kesadaran keamanan siber dan kebijakan keamanan siber, semakin tinggi pula kesadaran keamanan siber di dalam organisasi. Dengan kesadaran untuk patuh pada kebijakan keamanan siber di dalam organisasi yang dapat menghindari resiko kebocoran data, kesadaran untuk mengikuti pelatihan secara rutin, dan kesadaran melakukan perlindungan secara rutin seperti pencadangan, pemakaian kata kunci yang kuat, dan penggantian kata kunci secara berkala, diharapkan semakin kuat pula perilaku perlindungan keamanan siber. Upaya perlindungan informasi dilakukan pada lokasi yang paling banyak memiliki potensi celah terbesar mengalami kejahatan atau serangan siber (Mitnick & Simon, 2002). Perlindungan keamanan siber ini diarahkan pada perlindungan perangkat teknologi informasi yang dimiliki agar perangkat ini terhindar dari serangan *malware* dan pencurian data (*data breach*). Perilaku perlindungan keamanan siber ini adalah perilaku pegawai dalam melakukan perlindungan terhadap keamanan data di dalam sistem teknologi informasi organisasi melalui penggunaan antivirus pada komputer berkala, respons perilaku tidak wajar pada komputer, sikap pada peringatan *malware* yang diterima, peran aktif mengikuti pelatihan keamanan yang disediakan oleh organisasi publik, dan kepedulian pada keamanan informasi organisasi publik. Semakin tinggi kesadaran keamanan siber, semakin kuat perilaku perlindungan keamanan siber. Berdasarkan pemahaman tersebut, hipotesis penelitian ini dapat dirumuskan sebagai berikut.

Hipotesis 5 (H_5)

Kesadaran keamanan siber memiliki pengaruh yang positif dan signifikan terhadap perilaku perlindungan keamanan siber dalam organisasi publik.

6. Budaya Keamanan Siber dan Perilaku Perlindungan Keamanana Siber

Dalam organisasi publik, budaya keamanan siber memainkan peran penting dalam memperkuat perilaku perlindungan keamanan siber. Faktor manusia menjadi unsur terlemah pada matarantai keamanan siber organisasi dan mengembangkan budaya keamanan siber organisasi dapat mengurangi risiko faktor manusia (Enisa, 2017). Budaya keamanan siber mengacu pada pengetahuan, keyakinan, persepsi, sikap, asumsi, norma, dan nilai orang-orang mengenai keamanan siber dan bagaimana semua itu terwujud dalam perilaku mereka dalam menggunakan informasi. Interaksi ini menghasilkan perilaku yang diterima sebagai bagian dari cara organisasi melindungi aset informasi. Sikap, asumsi, keyakinan, nilai, dan pengetahuan dalam budaya keamanan siber ini mendorong perilaku pegawai sesuai sistem teknologi informasi di dalam organisasi (Huang & Pearlson, 2019). Budaya keamanan siber menekankan perilaku pegawai yang mematuhi kebijakan keamanan informasi serta keterlibatan pribadi dalam keamanan siber untuk melindungi dan menjaga organisasi dari kejahatan atau serangan siber. Dengan budaya keamanan siber, pegawai organisasi dapat melindungi sistem informasi dan komunikasi serta informasi yang dimilikinya dari kerusakan, pemakaian, modifikasi, atau eksploitasi dari pihak yang tidak berhak (NICCS, 2014). Perlindungan keamanan siber diarahkan pada perangkat teknologi informasi agar perangkat ini terhindar dari *malware* dan pencurian data. Perlindungan keamanan siber dilakukan oleh pegawai melalui penggunaan antivirus pada komputer secara berkala, respons perilaku tidak wajar pada komputer, sikap terhadap peringatan *malware* yang diterima, peran aktif mengikuti pelatihan keamanan yang disediakan organisasi, dan peduli pada keamanan informasi organisasi. Asumsinya, semakin tinggi budaya keamanan siber, semakin kuat pula perilaku perlindungan keamanan siber. Berdasarkan pemahaman tersebut, hipotesis penelitian ini dapat dirumuskan sebagai berikut

Hipotesis 6 (H_6)

Budaya keamanan siber memiliki pengaruh yang positif dan signifikan terhadap perilaku perlindungan keamanan siber dalam organisasi publik.