E-ISSN: 3025-0994
Halaman 3224-3237
Volume 4 Nomor 4 Tahun 2026

Consistency Of Protection Motivation Theory Constructs in Cybersecurity Behaviour: A Systematic Literature Review (2020–2026)

Echa Helmanessa Ginting[1], Sambas Ade Kesuma[2], Efran Jonathan Simbolon[3]

[1,2,3] Program Studi S1 Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Sumatera Utara
e-mail: echahelmanessa@icloud.com, sambas@usu.ac.id, efranjonathan@students.usu.ac.id

Abstrak

Perilaku pengguna masih menjadi titik lemah keamanan siber, dan *Protection Motivation Theory* (PMT) menjadi teori yang paling sering dipakai untuk menjelaskannya, tetapi temuan tentang konstruknya tidak konsisten. Penelitian ini bertujuan memetakan penerapan PMT dalam studi perilaku keamanan siber terbitan 2020–2026, mengidentifikasi konstruk yang konsisten dan tidak konsisten beserta kondisi yang menyertainya, serta merumuskan implikasinya bagi pengendalian internal keamanan informasi. Tinjauan pustaka sistematis dilakukan mengikuti pedoman PRISMA 2020. Sebanyak 302 rekaman dihimpun dari ScienceDirect, IEEE Xplore, dan Taylor & Francis Online, kemudian disaring hingga diperoleh 50 studi yang dianalisis dengan tabel frekuensi, tabulasi silang, dan sintesis naratif. Hasil kajian menunjukkan bahwa *response efficacy* merupakan konstruk paling konsisten (signifikan pada 27 dari 36 studi), disusul *perceived severity* dan *self-efficacy*, sedangkan *perceived vulnerability* (23 dari 39) dan *response cost* (10 dari 26) paling tidak konsisten. *Vulnerability* selalu signifikan pada konteks *phishing*, tetapi jarang signifikan pada konteks kata sandi dan kepatuhan kebijakan keamanan, sedangkan *response cost* tidak pernah signifikan dalam studi kepatuhan kebijakan. Hanya lima studi mengukur perilaku teramati, dan hubungan konstruk PMT dengan perilaku tersebut lebih lemah daripada dengan niat. Model lengkap yang memuat *maladaptive rewards* hanya diuji oleh tiga studi. Delapan studi berasal dari Indonesia dan seluruhnya berupa makalah prosiding. Temuan ini mengarahkan pengendalian internal pada penguatan efikasi karyawan, komunikasi ancaman yang spesifik, dan pemantauan perilaku aktual.

Kata Kunci: Protection Motivation Theory; Perilaku Keamanan Siber; Keamanan Informasi; Pengendalian Internal; Tinjauan Pustaka Sistematis

Abstract

User behaviour remains a weak point in cybersecurity, and Protection Motivation Theory (PMT) is the theory most often used to explain it, yet findings on its constructs are inconsistent. This

study aimed to map how PMT was applied in cybersecurity behaviour studies published between 2020 and 2026, to identify which constructs were consistent or inconsistent and under which conditions, and to derive implications for internal control over information security. A systematic literature review was conducted following the PRISMA 2020 guideline. A total of 302 records were retrieved from ScienceDirect, IEEE Xplore, and Taylor & Francis Online and screened, which yielded 50 studies that were analysed through frequency tables, cross-tabulation, and narrative synthesis. Response efficacy is the most consistent construct (significant in 27 of 36 studies), followed by perceived severity and self-efficacy, whereas perceived vulnerability (23 of 39) and response cost (10 of 26) are the least consistent. Vulnerability is always significant in phishing contexts but rarely in password and policy compliance contexts, and response cost is never significant in policy compliance studies. Only five studies measure observed behaviour, and PMT constructs relate more weakly to such behaviour than to intention. The full model including maladaptive rewards is tested in only three studies. Eight studies come from Indonesia, all of them conference papers. These findings direct internal control towards strengthening employee efficacy, communicating specific threats, and monitoring actual behaviour.

Keywords: Protection Motivation Theory; Cybersecurity Behaviour; Information Security; Internal Control; Systematic Literature Review

LATAR BELAKANG

Serangan siber terhadap organisasi terus terjadi, dan sebagian besar pelanggaran data masih melibatkan tindakan manusia. Dari 12.195 pelanggaran data terkonfirmasi yang dianalisis Verizon (2025), unsur manusia terlibat pada sekitar 60% kasus. Di Indonesia, Badan Siber dan Sandi Negara mencatat 122,79 juta serangan siber atau anomali lalu lintas internet sepanjang Januari–Agustus 2024, dengan sektor perbankan serta minyak dan gas sebagai sasaran utama (Infobanknews, 2024). Serangan *ransomware* terhadap Pusat Data Nasional Sementara pada Juni 2024 juga berdampak pada 282 instansi (Antara, 2024).

Bagi organisasi, perilaku aman karyawan termasuk dalam cakupan pengendalian internal. Kerangka COSO menempatkan pengendalian umum atas teknologi, termasuk manajemen keamanan, sebagai salah satu prinsip aktivitas pengendalian (COSO, 2013). Di Indonesia, kewajiban pengamanan data dan teknologi informasi diatur antara lain dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Republik Indonesia, 2022) dan POJK Nomor 11/POJK.03/2022 (Otoritas Jasa Keuangan, 2022). Aturan dan perangkat tersebut hanya efektif apabila dipatuhi penggunanya.

Teori yang paling sering dipakai untuk menjelaskan perilaku tersebut adalah *Protection Motivation Theory* (PMT) (Alsharida et al., 2023). PMT dikembangkan oleh Rogers (1975) dan direvisi oleh Rogers (1983). Motivasi melindungi diri dibentuk oleh penilaian ancaman (*threat appraisal*), yang mencakup *perceived severity*, *perceived vulnerability*, dan *maladaptive rewards*, serta penilaian penanggulangan (*coping appraisal*), yang mencakup *response efficacy*, *self-efficacy*, dan *response cost*. Rasa takut (*fear*) diposisikan sebagai respons emosional dari penilaian ancaman.

Meskipun banyak dipakai, temuan tentang konstruk PMT tidak seragam. Meta-analisis atas 92 studi mendukung tiga dari lima prediktor niat, memberi dukungan campuran bagi *perceived vulnerability*, dan tidak mendukung *response cost*; hubungan antarkonstruk juga lebih kuat pada konteks pribadi daripada konteks kerja (Mou et al., 2022). PMT juga lebih kuat menjelaskan perilaku sukarela, ancaman yang spesifik, dan ancaman yang menyasar individu (Sommestad et al., 2015). Penerapan PMT dalam riset keamanan informasi dinilai belum sepenuhnya mengikuti rumusan dan praktik pengujiannya di bidang psikologi (Haag et al., 2021; Siponen et al., 2024), sedangkan definisi dan butir pengukuran konstruknya berbeda-beda antarstudi (Gerdin et al., 2025; Gerdin et al., 2026). Inkonsistensi temuan PMT dengan demikian diduga berkaitan dengan konteks ancaman, setting, cara pengukuran, dan kelengkapan model.

Tinjauan khusus PMT yang paling banyak dirujuk (Haag et al., 2021; Mou et al., 2022) terbit pada 2021–2022, sehingga belum mencakup studi sesudahnya. Tinjauan yang lebih baru memiliki fokus yang berbeda, yaitu perlindungan data pribadi dalam organisasi (Idayani et al., 2026), perluasan PMT dengan kebiasaan dan kesadaran keamanan pada perilaku keamanan organisasi (Susyanto et al., 2026), serta perilaku keamanan pegawai sektor publik yang ternyata terkonsentrasi di Indonesia dan Malaysia (Sengati et al., 2026). Belum ditemukan tinjauan yang memetakan konsistensi setiap konstruk PMT menurut konteks ancaman, setting, dan jenis luaran pada studi 2020–2026, lalu mengaitkannya dengan pengendalian internal. Oleh karena itu, artikel ini bertujuan menjawab tiga pertanyaan, yaitu (RQ1) bagaimana karakteristik studi dan penerapan PMT dalam studi perilaku keamanan siber 2020–2026; (RQ2) konstruk PMT mana yang konsisten dan tidak konsisten, serta pada kondisi apa inkonsistensi muncul; dan (RQ3) apa implikasinya bagi pengendalian internal keamanan informasi dan celah penelitian apa yang masih terbuka.

METODE

Penelitian ini merupakan tinjauan pustaka sistematis yang dilaporkan mengikuti pedoman PRISMA 2020 (Page et al., 2021). Dalam kerangka PICO, populasi berupa individu yang menghadapi ancaman siber, intervensi berupa penerapan PMT, pembanding berupa perbedaan konteks, setting, luaran, dan kelengkapan model, serta luaran berupa niat atau perilaku keamanan.

Rentang 2020–2026 dipilih karena tiga alasan. Pertama, tinjauan dan meta-analisis PMT yang paling banyak dirujuk terbit pada 2021–2022, sehingga studi sesudahnya belum tercakup. Kedua, konteks ancaman berubah sejak 2020, antara lain melalui penipuan bertema pandemi COVID-19 (Tang et al., 2021), pekerjaan di luar kantor (Ogbanufe et al., 2023), dan penipuan berbasis *deepfake* (Pramod et al., 2025). Ketiga, kritik konseptual dan metodologis terhadap penerapan PMT baru menguat belakangan (Siponen et al., 2024; Gerdin et al., 2025). Studi 2020–2021 tetap diikutkan agar seluruh periode sejak pandemi tercakup. Artikel dihimpun dari ScienceDirect, IEEE Xplore, dan Taylor & Francis Online pada 23 Oktober 2026. Kata kunci "protection motivation" dipasangkan dengan istilah *cybersecurity*, *information security*, nama ancaman (*phishing*, *ransomware*, *malware*), dan nama perilaku (*security behavior*, *security compliance*, *password*). Pada ScienceDirect, kueri dipecah menjadi dua karena batas delapan operator Boolean dan diterapkan pada judul, abstrak, serta kata kunci

dengan filter 2020–2026 dan artikel riset; kueri setara diterapkan pada metadata IEEE Xplore dan abstrak Taylor & Francis Online.

Penelusuran difokuskan pada terbitan Elsevier, IEEE, dan Taylor & Francis. Ketiganya merupakan penerbit ilmiah besar dengan proses telaah sejawat yang mapan dan menerbitkan jurnal inti bidang keamanan informasi dan sistem informasi, seperti *Computers & Security*, *Computers in Human Behavior*, *IEEE Access*, dan *Journal of Management Information Systems*. Fokus ini juga memastikan teks lengkap setiap artikel dapat diperoleh dan diperiksa langsung, sehingga seluruh hasil pengodean dapat ditelusuri ke sumbernya. Penerbit ditentukan dari prefiks DOI dan dicek melalui Crossref apabila data ekspor bertentangan. Artikel diikutsertakan apabila berupa studi empiris primer dengan data individu, menjadikan PMT kerangka utama atau bagian model terintegrasi dan menguji konstruknya, mengukur niat atau perilaku keamanan siber, serta berupa artikel jurnal atau prosiding berbahasa Inggris terbitan 2020–2026. Kode pengeluaran terdiri atas E1 (PMT bukan kerangka uji), E2 (bukan konteks keamanan siber), E3 (bukan studi empiris perilaku individu), E4 (di luar 2020–2026), dan E5 (penerbit di luar cakupan).

Alur pemilihan artikel disajikan pada Gambar 1. Dari 302 rekaman, 121 rekaman dikeluarkan sebelum penyaringan karena duplikat, terbit di luar 2020–2026 (ekspor IEEE Xplore belum terfilter tahun), atau berasal dari penerbit di luar cakupan. Ekspor Taylor & Francis tidak memuat abstrak, sehingga 14 abstrak diperiksa melalui OpenAlex dan sisanya dinilai dari judul. Teks lengkap seluruh 67 artikel yang lolos penyaringan berhasil diperoleh, dan 50 artikel memenuhi kriteria.

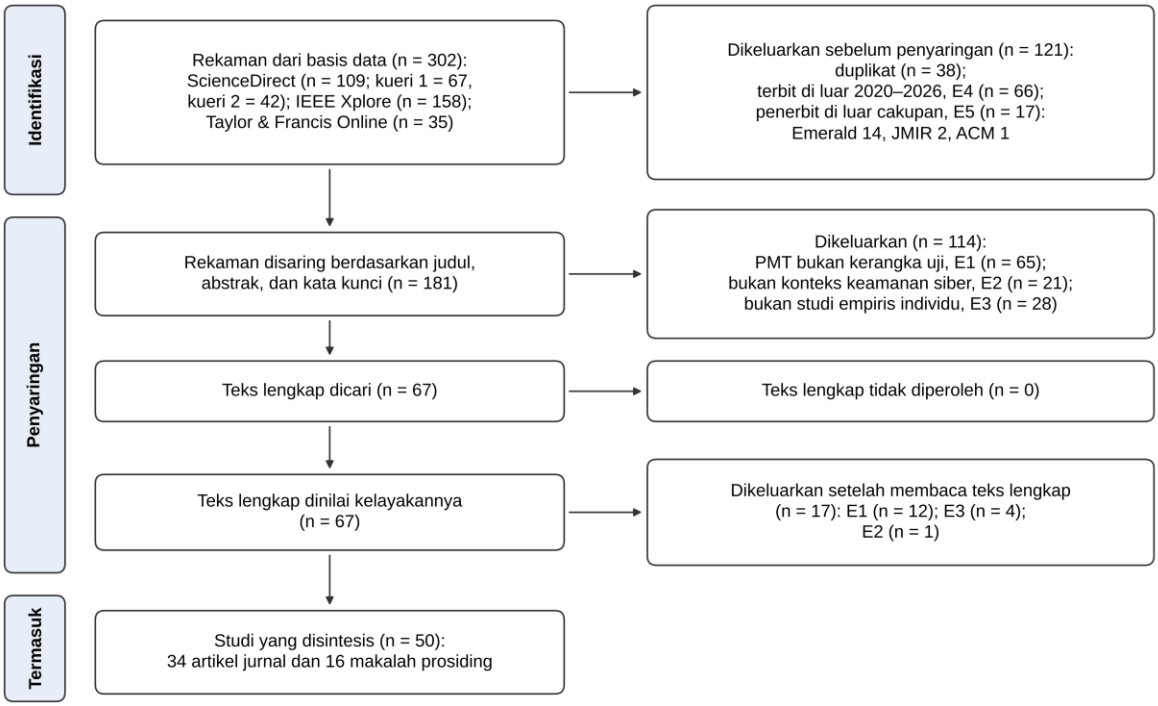
Setiap studi dikodekan menurut tahun, negara, setting, desain, analisis, konteks ancaman, dan jenis luaran (niat, perilaku dilaporkan, atau perilaku teramati). Hasil setiap konstruk dicatat sebagai signifikan sesuai arah teori, tidak signifikan, campuran antarmodel atau subsampel, atau berlawanan arah. Kelengkapan model dikodekan menjadi lengkap (lima konstruk inti: *severity*, *vulnerability*, *response efficacy*, *self-efficacy*, dan *response cost*), inti (empat konstruk tanpa *response cost*), parsial, agregat (penilaian ancaman atau penanggulangan diukur sebagai satu konstruk), dan intervensi (PMT sebagai dasar pesan atau pelatihan). Penyaringan dan pengodean dilakukan oleh satu penelaah, dan keputusan beserta alasannya dicatat untuk setiap rekaman. Data dianalisis dengan tabel frekuensi (RQ1), tabulasi silang hasil uji per konstruk (RQ2), dan sintesis naratif (RQ2 dan RQ3). Meta-analisis tidak dilakukan karena model dan ukuran efek antarstudi berbeda-beda.

HASIL DAN PEMBAHASAN

Sebanyak 50 studi dikaji, terdiri atas 34 artikel jurnal dan 16 makalah prosiding yang diterbitkan Elsevier (31 studi), IEEE (17 studi), dan Taylor & Francis (2 studi), dengan *Computers & Security* sebagai sumber terbanyak (15 studi). Karakteristik studi dirangkum pada Tabel 1, sedangkan sebaran studi menurut konteks ancaman dan setting disajikan pada Tabel 2. Studi kepatuhan kebijakan keamanan hampir seluruhnya dilakukan di organisasi, sedangkan studi *phishing*, kata sandi, dan penipuan siber umumnya meneliti pengguna individu.

Tabel 1. Karakteristik studi yang dikaji (n = 50)

Aspek	Sebaran studi, n (%)
Periode terbit	2020–2022 16 (32,0%); 2023–2024 16 (32,0%); 2025–2026 18 (36,0%)
Jenis publikasi	Artikel jurnal 34 (68,0%); makalah prosiding 16 (32,0%)
Wilayah asal data	Asia Tenggara 11 (22,0%), termasuk Indonesia 8; Asia lainnya 12 (24,0%); Amerika Utara 12 (24,0%); Eropa 7 (14,0%); Timur Tengah 3 (6,0%); Australia 3 (6,0%); lintas negara 2 (4,0%)
Setting	Individu 29 (58,0%); organisasi 21 (42,0%)
Desain dan analisis	Survei 41 (82,0%); eksperimen 8 (16,0%); campuran 1 (2,0%); PLS-SEM 32 (64,0%); CB-SEM 6 (12,0%); teknik lain 12 (24,0%)
Jenis luaran	Niat atau motivasi 24 (48,0%); perilaku dilaporkan 16 (32,0%); perilaku teramati 5 (10,0%); lainnya 5 (10,0%)
Kelengkapan model	Lengkap 21 (42,0%); parsial 10 (20,0%); inti 8 (16,0%); intervensi 6 (12,0%); agregat 5 (10,0%)



Gambar 1. Alur pemilihan artikel berdasarkan PRISMA 2020

Tabel 2. Sebaran studi menurut konteks ancaman dan setting

Konteks ancaman	Setting	n	Studi
Perilaku keamanan umum	Organisasi	9	Alshammari & Al-Mamary, 2026b; Bisma et al., 2021; Chongrui et al., 2021; Humaidi & Abdallah Alghazo, 2022; Lee et al., 2025; Li et al., 2022; Ma, 2022; Rahman et al., 2025; Vrhovec & Mihelič, 2021
	Individu	8	Khan et al., 2023; Kiran et al., 2025; Sahwahita & Utomo, 2024; Schneider & Rahman, 2021; Shang Ardhiyasa & Syamsuar, 2025; Tsai et al., 2022; van 't Hoff-de Goede et al., 2025; Wilke et al., 2026
Kepatuhan kebijakan keamanan	Organisasi	10	Aggarwal & Srivastava, 2024; Alrawhani et al., 2025; Alshammari & Al-Mamary, 2026a; Ameen et al., 2020; Ameen et al., 2021; Amir et al., 2026; Ogbanufe & Ge, 2023; Ogbanufe et al., 2023; Sharma & Aparicio, 2022; Wong et al., 2022
	Individu	1	McLeod & Dolezel, 2022
Phishing dan rekayasa sosial	Individu	8	Alsulami & Dupuis, 2024; Bax et al., 2021; Bourgeon et al., 2026; McGill et al., 2026; Ng et al., 2021; Putri Mazida & Sari, 2024; Thompson et al., 2024; Vrhovec et al., 2023
Kata sandi dan autentikasi	Organisasi	1	Wang et al., 2026
	Individu	6	Ekaputri et al., 2026; Jin & Dupuis, 2024; Nehme et al., 2024; Ogbanufe, 2023; Rani et al., 2024; Simon et al., 2025
Penipuan siber	Individu	4	Hassan et al., 2024; Naseer et al., 2026; Pramod et al., 2025; Tang et al., 2021
Malware, *ransomware*, dan perangkat lunak keamanan	Organisasi	1	Bekkers et al., 2023
	Individu	2	Kwon & Lee, 2024; Putra & Syamsuar, 2025

Untuk menjawab RQ1, penerapan PMT dipetakan menurut kelengkapan model. Sebanyak 21 studi (42,0%) menguji kelima konstruk inti, sedangkan 29 studi lainnya menguji model inti, parsial, agregat, atau memakai PMT sebagai dasar intervensi. *Fear* hanya diuji oleh 12 studi dan *maladaptive rewards* oleh 4 studi, sehingga model yang memuat seluruh konstruk revisi Rogers (1983) hanya ditemukan pada Bax et al. (2021), Ng et al. (2021), dan Wilke et al. (2026). Sebanyak 42 studi memperluas PMT dengan teori atau variabel lain, misalnya *theory of planned behavior* (Alshammari & Al-Mamary, 2026a; Vrhovec et al., 2023), *cultivation theory* (Tang et al., 2021), *routine activity theory* (Lee et al., 2025), teori identitas (Ogbanufe &

Ge, 2023), budaya dan iklim keamanan organisasi (Sharma & Aparicio, 2022; Chongrui et al., 2021), kesadaran keamanan (Wong et al., 2022; Alshammari & Al-Mamary, 2026b), atau kesediaan membayar perangkat lunak keamanan (Kwon & Lee, 2024).

Untuk menjawab RQ2, hasil uji setiap konstruk dirangkum pada Tabel 3. Konstruk penilaian penanggulangan lebih konsisten daripada konstruk penilaian ancaman, sejalan dengan simpulan Susyanto et al. (2026) pada konteks organisasi. *Response efficacy* signifikan pada 27 dari 36 studi, dan pada studi yang mengukur niat angkanya mencapai 18 dari 21 studi. *Self-efficacy* signifikan pada 27 dari 39 studi, tetapi tiga studi menemukan pengaruh negatif. Pada wirausaha Belanda, *self-efficacy* dan *response efficacy* justru menurunkan niat melindungi usaha dari *ransomware* (Bekkers et al., 2023); *self-efficacy* juga menurunkan perilaku pembuatan kata sandi karyawan (Humaidi & Abdallah Alghazo, 2022) dan menaikkan kecenderungan menyerah terhadap kepatuhan keamanan (McLeod & Dolezel, 2022).

Tabel 3. Hasil uji konstruk PMT pada studi yang dikaji

Konstruk	Diuji	Signifikan, n (%)	Tidak signifikan	Campuran	Berlawanan arah
Perceived severity	38	27 (71,1%)	9	2	0
Perceived vulnerability	39	23 (59,0%)	12	3	1
Response efficacy	36	27 (75,0%)	5	3	1
Self-efficacy	39	27 (69,2%)	6	3	3
Response cost	26	10 (38,5%)	12	3	1
Maladaptive rewards	4	3 (75,0%)	1	0	0
Fear	12	8 (66,7%)	3	1	0

Pada penilaian ancaman, *perceived severity* signifikan pada 27 dari 38 studi, sedangkan *perceived vulnerability* hanya pada 23 dari 39 studi. Inkonsistensi *vulnerability* mengikuti konteks ancaman: konstruk ini signifikan pada keenam studi *phishing* yang mengujinya, tetapi hanya pada 1 dari 5 studi kata sandi dan autentikasi serta 3 dari 9 studi kepatuhan kebijakan. Ancaman *phishing* menyasar pengguna secara langsung, sedangkan kerugian akibat pelanggaran kebijakan lebih banyak ditanggung organisasi; pola ini sejalan dengan Sommestad et al. (2015) dan Vrhovec & Mihelič (2021). Pengaruh *severity* dan *vulnerability* juga sering bekerja melalui *fear* (Bax et al., 2021; Thompson et al., 2024; Ma, 2022; McGill et al., 2026), sehingga pengaruh langsungnya tidak signifikan ketika *fear* dimasukkan ke model (Aggarwal & Srivastava, 2024; Ogbanufe et al., 2023).

Response cost merupakan konstruk yang paling lemah, yaitu signifikan pada 10 dari 26 studi, dan tidak satu pun dari enam studi kepatuhan kebijakan yang mengujinya menemukan pengaruh signifikan. Konstruk ini lebih sering berpengaruh pada adopsi alat, seperti autentikasi multifaktor (Ogbanufe, 2023) dan pengelola kata sandi (Nehme et al., 2024), tetapi arahnya dapat berbalik (Sahwahita & Utomo, 2024) dan berbeda menurut gender serta negara (Ameen et al., 2020; Ameen et al., 2021). *Maladaptive rewards* signifikan pada tiga dari empat studi, meskipun pada pengguna surel imbalan tersebut menaikkan perilaku maladaptif alih-alih menurunkan motivasi proteksi (Bax et al., 2021). Gambaran ini sejalan

dengan meta-analisis Mou et al. (2022), sehingga inkonsistensi *vulnerability* dan *response cost* tetap bertahan pada studi 2020–2026.

Jenis luaran juga membedakan hasil. Hanya lima studi mengukur perilaku teramati. Pada survei eksperimen berbasis populasi, penilaian ancaman dan penanggulangan berkaitan dengan perilaku yang dilaporkan, tetapi lemah atau berlawanan arah terhadap perilaku aktual (van 't Hoff-de Goede et al., 2025). Pelatihan berbasis PMT menaikkan persepsi dan pengetahuan peserta, tetapi efeknya diukur dari laporan diri (Tsai et al., 2022; Khan et al., 2023). Pesan berbasis PMT menaikkan niat dibandingkan pesan netral, tetapi tambahan komponen penanggulangan tidak mengungguli pesan ancaman saja (Wilke et al., 2026). Pada eksperimen lapangan terhadap 14.840 staf dan mahasiswa, variasi *severity* dan *susceptibility* dalam pesan tidak mengubah tingkat penggantian kata sandi (Wang et al., 2026). Pesan efikasi juga tidak menaikkan kognisi penanggulangan (Simon et al., 2025), dan edukasi maupun *fear appeal* tidak meningkatkan kemampuan mengenali *spear phishing* (Alsulami & Dupuis, 2024). Konsistensi PMT pada tingkat niat dengan demikian belum menjamin perubahan perilaku aktual.

Kedelapan studi Indonesia didominasi responden individu, yaitu mahasiswa, Gen Z, serta pengguna internet dan media sosial (Rani et al., 2024; Ekaputri et al., 2026; Shang Ardhiyasa & Syamsuar, 2025; Sahwahita & Utomo, 2024; Putra & Syamsuar, 2025; Putri Mazida & Sari, 2024). Hanya dua studi yang menyasar organisasi, yaitu pegawai kantor pertanahan (Amir et al., 2026) dan pelaku UMKM (Bisma et al., 2021). Pola hasilnya mirip dengan temuan global: *severity* signifikan pada kelima studi yang mengujinya, *vulnerability* pada empat dari enam studi, sedangkan *response cost* tidak signifikan pada tiga dari lima studi. Belum ditemukan studi Indonesia yang meneliti karyawan sektor keuangan, padahal sektor perbankan menjadi sasaran utama serangan (Infobanknews, 2024).

Untuk menjawab RQ3, temuan tersebut dikaitkan dengan komponen pengendalian internal COSO (COSO, 2013). Pada lingkungan pengendalian, konsistensi *response efficacy* dan *self-efficacy* menunjukkan bahwa manajemen perlu meyakinkan karyawan bahwa tindakan keamanan efektif dan dapat dijalankan; budaya organisasi dan kepercayaan pada manajemen terbukti menaikkan penilaian penanggulangan dan niat patuh (Sharma & Aparicio, 2022; Alshammari & Al-Mamary, 2026a). Pada penilaian risiko dan komunikasi, lemahnya *vulnerability* dalam studi kepatuhan menunjukkan bahwa risiko perlu dijelaskan secara spesifik bagi unit dan peran karyawan, dan pesan ancaman saja tidak cukup mengubah perilaku (Wang et al., 2026). Pada aktivitas pengendalian, kontrol teknis seperti autentikasi multifaktor perlu dibuat mudah dipakai agar biaya kepatuhan rendah. Pada pemantauan, kesenjangan antara niat dan perilaku teramati menunjukkan bahwa kepatuhan sebaiknya dipantau dari data perilaku aktual, seperti log sistem dan simulasi *phishing*.

Empat celah penelitian dapat dirumuskan. Pertama, hubungan PMT dengan perilaku aktual belum teruji secara memadai. Kedua, *maladaptive rewards* dan *fear* jarang diuji, sehingga PMT umumnya diterapkan dalam versi yang dipersempit. Ketiga, operasionalisasi *vulnerability* dan *response cost* perlu diseragamkan (Gerdin et al., 2025). Keempat, studi organisasi di Indonesia masih sedikit dan belum menyentuh sektor keuangan maupun fungsi akuntansi. Kajian ini terbatas pada tiga sumber penelusuran dan artikel berbahasa Inggris. Penyaringan dan pengodean dilakukan oleh satu penelaah, penilaian kualitas metodologis

tidak dilakukan, dan penghitungan signifikansi tidak memperhitungkan ukuran efek maupun ukuran sampel.

SIMPULAN

Studi PMT keamanan siber 2020–2026 didominasi survei yang mengukur niat dan jarang menguji model lengkap. *Response efficacy*, *severity*, dan *self-efficacy* paling konsisten, sedangkan *vulnerability* dan *response cost* tidak konsisten dan bergantung pada konteks ancaman, terutama pada studi kepatuhan kebijakan. Hubungan PMT dengan perilaku teramati lebih lemah daripada dengan niat. Peneliti disarankan mengukur perilaku aktual, menguji model lengkap, dan meneliti karyawan sektor keuangan di Indonesia. Organisasi disarankan merancang pengendalian yang menguatkan efikasi karyawan, mengomunikasikan risiko secara spesifik, dan memantau perilaku aktual.

DAFTAR PUSTAKA

Aggarwal, A. & Srivastava, S.K. 2024. Exploring Eustress And Fear: A New Perspective On Protection Motivation In Information Security Policy Compliance Within The Financial Sector. Computers & Security, 142: 103857.

Alrawhani, E.M., Romli, A. & Al-Sharafi, M.A. 2025. Evaluating The Role Of Protection Motivation Theory In Information Security Policy Compliance: Insights From The Banking Sector Using PLS-SEM Approach. Journal Of Open Innovation: Technology, Market, And Complexity, 11(1): 100463.

Alshammari, M.M. & Al-Mamary, Y.H. 2026a. Non-Technical Determinants Of Information Security Policy Compliance: An Integrated PMT-TPB Model With Psychological Ownership, Trust, And Social Influence. Computers In Human Behavior Reports, 21: 100947.

Alshammari, M.M. & Al-Mamary, Y.H. 2026b. Cybersecurity Awareness As A Mediating Factor In The Human Firewall System. Computers In Human Behavior Reports, 22: 101118.

Alsharida, R.A., Al-Rimy, B.A.S., Al-Emran, M. & Zainal, A. 2023. A Systematic Review Of Multi Perspectives On Human Cybersecurity Behavior. Technology In Society, 73: 102258.

Alsulami, S. & Dupuis, M. 2024. The Effectiveness Of Education And Fear Appeal To Prevent Spear Phishing Attacks. 2024 Cyber Awareness And Research Symposium (CARS): 1–8.

Ameen, N., Tarhini, A., Hussain Shah, M. & Madichie, N.O. 2020. Employees' Behavioural Intention To Smartphone Security: A Gender-Based, Cross-National Study. Computers In Human Behavior, 104: 106184.

Ameen, N., Tarhini, A., Shah, M.H., Madichie, N., Paul, J. & Choudrie, J. 2021. Keeping Customers' Data Secure: A Cross-Cultural Study Of Cybersecurity Compliance Among The Gen-Mobile Workforce. Computers In Human Behavior, 114: 106531.

Amir, S., Patria, N., Sensuse, D.I. & Lusa, S. 2026. Factors Influencing Employees' Information Security Awareness: Evidence From A Regional Land Administration Office In Indonesia. 2026 International Conference On Computer, Control, Informatics And Its Applications (IC3INA): 337–342.

Antara. 28 Juni 2024. Menkominfo Ungkap Pelaku Serangan Siber Ke Pusat Data Nasional. Antara News Manado.

Bax, S., Mcgill, T. & Hobbs, V. 2021. Maladaptive Behaviour In Response To Email Phishing Threats: The Roles Of Rewards And Response Costs. Computers & Security, 106: 102278.

Bekkers, L., Van 'T Hoff-De Goede, S., Misana-Ter Huurne, E., Van Houten, Y., Spithoven, R. & Leukfeldt, E.R. 2023. Protecting Your Business Against Ransomware Attacks? Explaining The Motivations Of Entrepreneurs To Take Future Protective Measures Against Cybercrimes Using An Extended Protection Motivation Theory Model. Computers & Security, 127: 103099.

Bisma, R., Winarto, S.R. & Puspita, Y.C. 2021. Investigating Cyber Security Factors Influencing The Perception Behavioral Intention Of Small And Medium Enterprise. 2021 Fourth International Conference On Vocational Education And Electrical Engineering (ICVEE): 1–7.

Bourgeon, S., Fitzhugh, E., Jansen, J. & Wash, R. 2026. Decoding Deception: An Integrated Cognitive Model Of User Response To Online Bank Fraud Attempts. Computers In Human Behavior: 109211.

Chongrui, L., Yan, L., Cong, W. & Hongjie, W. 2021. Exploring The Impact Of Information Security Climate And Information Security Training On Cybersecurity Behavior: Based On Protection Motivation Theory. 2021 6th International Symposium On Computer And Information Processing Technology (ISCIPT): 803–806.

COSO. 2013. Internal Control—Integrated Framework: Executive Summary. Committee Of Sponsoring Organizations Of The Treadway Commission.

Ekaputri, S.N., Utomo, R.G. & Insan, I.M. 2026. User Protection Motivation Toward Two-Factor Authentication (2FA) On Instagram: A Protection Motivation Theory Perspective. 2026 14th International Conference On Information And Communication Technology (Icoict): 1–6.

Gerdin, M., Grönlund, Å. & Kolkowska, E. 2025. Conceptual Inconsistencies In Variable Definitions And Measurement Items Within ISP Non-/Compliance Research: A Systematic Literature Review. Computers & Security, 152: 104365.

Gerdin, M., Karlsson, M., Kolkowska, E. & Grönlund, Å. 2026. You Get The Answers You Ask For: Experimental Evidence On The Influence Of Inconsistent Variable Definitions On Non-/Compliance Research Findings. Computers & Security, 171: 105065.

Haag, S., Siponen, M. & Liu, F. 2021. Protection Motivation Theory In Information Systems Security Research: A Review Of The Past And A Road Map For The Future. ACM SIGMIS Database: The DATABASE For Advances In Information Systems, 52(2): 25–67.

Hassan, S., Ahmad, R., Katuk, N., Ghazali, N.N., Aripin, J.A. & Ali, F. 2024. Staying One Step Ahead: Exploring Protection Motivation Theory To Combat Cyber-Fraud Among E-Services Users. Procedia Computer Science, 234: 1364–1371.

Humaidi, N. & Abdallah Alghazo, S.H. 2022. Procedural Information Security Countermeasure Awareness And Cybersecurity Protection Motivation In Enhancing Employee's

Cybersecurity Protective Behaviour. 2022 10th International Symposium On Digital Forensics And Security (ISDFS): 1–10.
Idayani, R.W., Pribadi Subriadi, A. & Setiawan, B. 2026. Towards An Extended Protection Motivation Theory For Personal Data Protection: A Systematic Literature Review. 2026 13th International Conference On ICT For Smart Society (ICISS): 1–6.
Infobanknews. 31 Oktober 2024. Ngeri! Ada 122,79 Juta Serangan Siber Ke RI, Sektor Ini Target Utamanya. Infobanknews.Com.
Jin, S. & Dupuis, M. 2024. Password Usage Behavior Of Online Users. 2024 Cyber Awareness And Research Symposium (CARS): 1–6.
Khan, N.F., Ikram, N., Murtaza, H. & Javed, M. 2023. Evaluating Protection Motivation Based Cybersecurity Awareness Training On Kirkpatrick's Model. Computers & Security, 125: 103049.
Kiran, U., Khan, N.F., Murtaza, H., Farooq, A. & Pirkkalainen, H. 2025. Explanatory And Predictive Modeling Of Cybersecurity Behaviors Using Protection Motivation Theory. Computers & Security, 149: 104204.
Kwon, S. & Lee, H. 2024. Willingness To Pay For Smart Car Security. IEEE Access, 12: 33867–33875.
Lee, J., Wang, J., De Guzman, M.C., Gupta, M. & Raghav Rao, H. 2025. Can I Help Prevent Data Breaches In The Workplace? From Routine Activities To Extra-Role Security Behaviors. IEEE Transactions On Technology And Society, 6(1): 90–101.
Li, L., Xu, L. & He, W. 2022. The Effects Of Antecedents And Mediating Factors On Cybersecurity Protection Behavior. Computers In Human Behavior Reports, 5: 100165.
Ma, X. 2022. IS Professionals' Information Security Behaviors In Chinese IT Organizations For Information Security Protection. Information Processing & Management, 59(1): 102744.
Mcgill, T., Thompson, N. & Narula, N. 2026. "Not All Bad": Determinants And Impacts Of Emotion-Focused And Problem-Focused Coping In Information Security Behavior. Computers & Security, 165: 104872.
Mcleod, A. & Dolezel, D. 2022. Information Security Policy Non-Compliance: Can Capitulation Theory Explain User Behaviors?. Computers & Security, 112: 102526.
Mou, J., Cohen, J.F., Bhattacherjee, A. & Kim, J. 2022. A Test Of Protection Motivation Theory In The Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach. Journal Of The Association For Information Systems, 23(1): 196–236.
Naseer, H., Wijayanayake, J. & Jayasinghe, S. 2026. Customer Awareness In Digital Banking: Antecedents And Implications For Information Security In Sri Lanka. 2026 IEEE International Research Conference On Smart Computing And Systems Engineering (SCSE), 9: 1–7.
Nehme, A., Li, M. & Warkentin, M. 2024. Adaptive And Maladaptive Factors Behind Password Manager Use: A Hope-Extended Protection Motivation Perspective. Computers & Security, 144: 103941.
Ng, K.C., Zhang, X., Thong, J.Y.L. & Tam, K.Y. 2021. Protecting Against Threats To Information Security: An Attitudinal Ambivalence Perspective. Journal Of Management Information Systems, 38(3): 732–764.

Ogbanufe, O. & Ge, L. 2023. A Comparative Evaluation Of Behavioral Security Motives: Protection, Intrinsic, And Identity Motivations. Computers & Security, 128: 103136.

Ogbanufe, O. 2023. Securing Online Accounts And Assets: An Examination Of Personal Investments And Protection Motivation. International Journal Of Information Management, 68: 102590.

Ogbanufe, O., Crossler, R.E. & Biros, D. 2023. The Valued Coexistence Of Protection Motivation And Stewardship In Information Security Behaviors. Computers & Security, 124: 102960.

Otoritas Jasa Keuangan. 2022. Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum. Jakarta: Otoritas Jasa Keuangan.

Page, M.J., Mckenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., Mcdonald, S., … Moher, D. 2021. The PRISMA 2020 Statement: An Updated Guideline For Reporting Systematic Reviews. BMJ, 372: N71.

Pramod, D., Patil, K.P. & Bharathi S, V. 2025. Is It Really Unreal? A Two-Theory Approach On The Impact Of Deepfakes Technology On The Protection Motivation Of Consumers. Cogent Business & Management, 12(1): 2461239.

Putra, R.R. & Syamsuar, D. 2025. Evolution Of Cyber Threats: The Critical Role Of Antivirus In Overcoming Current Digital Security Challenges Through Protection Motivation Theory (PMT) And UTAUT. 2025 11th International Conference On Wireless And Telematics (ICWT): 1–7.

Putri Mazida, A.Z. & Sari, P.K. 2024. How Social Engineering Information-Seeking Intention Mediating Information-Sharing Intention In Social Media. 2024 12th International Conference On Cyber And IT Service Management (CITSM): 1–6.

Rahman, K.M., Emon, M.M.H., Islam, M.S., Ahmed, M., Siam, S.A.J. & Rifat, H.H. 2025. Effect Of Intelligent Cybersecurity Systems On Data Protection And Breach Reduction In Bangladeshi IT Firms. 2025 IEEE 4th International Conference On Robotics, Automation, Artificial-Intelligence And Internet-Of-Things (RAAICON): 567–570.

Rani, A.S., Utomo, R.G. & Fathoni, M.F. 2024. Online Security Behavior Among Students: Factors Influencing Intention To Adopt Two-Factor Authentication (2FA) With Protection Motivation Theory. 2024 International Conference On Information Technology Systems And Innovation (ICITSI): 119–124.

Republik Indonesia. 2022. Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. Jakarta: Sekretariat Negara.

Rogers, R.W. 1975. A Protection Motivation Theory Of Fear Appeals And Attitude Change. The Journal Of Psychology, 91(1): 93–114.

Rogers, R.W. 1983. Cognitive And Physiological Processes In Fear Appeals And Attitude Change: A Revised Theory Of Protection Motivation. Dalam J.T. Cacioppo & R.E. Petty (Ed.). Social Psychophysiology: A Sourcebook: 153–176. New York: Guilford Press.

Sahwahita, R. & Utomo, R.G. 2024. Factors Influencing Gen Z Awareness Of Computer Security Using Protection Motivation Theory (PMT). 2024 International Conference On Information Technology Systems And Innovation (ICITSI): 374–379.

Schneider, M. & Rahman, S. 2021. Identifying Protection Motivation Theory Factors That Influence Smartphone Security Measures. 2021 IEEE International Conference On Big Data (Big Data): 3353–3359.

Sengati, F., Kanaan, A.M.J., Ayyasamy, R.K. & Senadjki, A. 2026. Policy, People, And Protection: A Decade Of Behavioral Cybersecurity Research In The Public Sector. 2026 1st International Conference On Innovations In Information And Communication Technologies (IICT): 1–10.

Shang Ardhiyasa, A.F. & Syamsuar, D. 2025. Assessing The Awareness And Preparedness Of Indonesian College Students Against Cyber Threats. 2025 12th International Conference On Electrical Engineering, Computer Science And Informatics (EECSI): 580–585.

Sharma, S. & Aparicio, E. 2022. Organizational And Team Culture As Antecedents Of Protection Motivation Among IT Employees. Computers & Security, 120: 102774.

Simon, J., Watson, S.J. & Van Sintemaartensdijk, I. 2025. Response-Efficacy Messages Produce Stronger Passwords Than Self-Efficacy Messages … For Now: A Longitudinal Experimental Study Of The Efficacy Of Coping Message Types On Password Creation Behaviour. Computers In Human Behavior Reports, 17: 100615.

Siponen, M., Rönkkö, M., Liu, F., Haag, S. & Laatikainen, G. 2024. Protection Motivation Theory In Information Security Behavior Research: Reconsidering The Fundamentals. Communications Of The Association For Information Systems, 53: 1136–1165.

Sommestad, T., Karlzén, H. & Hallberg, J. 2015. A Meta-Analysis Of Studies On Protection Motivation Theory And Information Security Behaviour. International Journal Of Information Security And Privacy, 9(1): 26–46.

Susyanto, Mulyanti, R.Y. & Rini, N. 2026. Extending Protection Motivation Theory To Explain Organizational Cybersecurity Behavior: A Systematic Literature Review. Jurnal Ilmiah Ilmu Terapan Universitas Jambi, 10(2): 1114–1131.

Tang, Z., Miller, A.S., Zhou, Z. & Warkentin, M. 2021. Does Government Social Media Promote Users' Information Security Behavior Towards COVID-19 Scams? Cultivation Effects And Protective Motivations. Government Information Quarterly, 38(2): 101572.

Thompson, N., Mcgill, T. & Narula, N. 2024. "No Point Worrying" – The Role Of Threat Devaluation In Information Security Behavior. Computers & Security, 143: 103897.

Tsai, C.-Y., Shih, W.-L., Hsieh, F.-P., Chen, Y.-A., Lin, C.-L. & Wu, H.-J. 2022. Using The ARCS Model To Improve Undergraduates' Perceived Information Security Protection Motivation And Behavior. Computers & Education, 181: 104449.

Van 'T Hoff-De Goede, M.S., Leukfeldt, E.R., Van De Weijer, S.G.A. & Van Der Kleij, R. 2025. Does Protection Motivation Predict Self-Protective Online Behaviour? Comparing Self-Reported And Actual Online Behaviour Using A Population-Based Survey Experiment. Computers In Human Behavior Reports, 18: 100649.

Verizon. 2025. 2025 Data Breach Investigations Report: Executive Summary. Verizon Business.

Vrhovec, S. & Mihelič, A. 2021. Redefining Threat Appraisals Of Organizational Insiders And Exploring The Moderating Role Of Fear In Cyberattack Protection Motivation. Computers & Security, 106: 102309.

Vrhovec, S., Bernik, I. & Markelj, B. 2023. Explaining Information Seeking Intentions: Insights From A Slovenian Social Engineering Awareness Campaign. Computers & Security, 125: 103038.

Wang, X., Zhang, Y., Siponen, M. & Zhang, N. 2026. The Power Of Persuasive Messaging On Improving Password-Change Behavior In University Information Systems: Evidence From A Large-Scale Field Experiment. Computers & Security, 169: 104933.

Wilke, A.J., Puikytė, M. & Meissner, F. 2026. Leveraging Protection Motivation Theory To Support Secure Online Behaviours: Two Experimental Studies With Vulnerable Age Groups. Computers In Human Behavior Reports, 24: 101374.

Wong, L.-W., Lee, V.-H., Tan, G.W.-H., Ooi, K.-B. & Sohal, A. 2022. The Role Of Cybersecurity And Policy Awareness In Shifting Employee Compliance Attitudes: Building Supply Chain Capabilities. International Journal Of Information Management, 66: 102520.