PERSEPTIF: Jurnal Ilmu Sosial dan Humaniora
2026, Vol. 4, No. 3, pp. 564-575
E-ISSN: 3025-9452

Efektivitas Pelatihan Security Awareness dalam Meningkatkan Keamanan dengan Mengaplikasikan Sistem Informasi pada Universitas Prasetiya Mulya

Khelik Adhi Prasetyo[1]✉, Mukrodi[2], Hamsinah B[3]
(1,2,3) Program Studi Magister Manajemen, Universitas Pamulang, Tangerang Selatan, Indonesia

Abstak: Transformasi digital perguruan tinggi meningkatkan ketergantungan pada sistem informasi sekaligus memperbesar risiko yang bersumber dari perilaku karyawan. Penelitian ini menganalisis efektivitas pelatihan security awareness dalam membentuk pemahaman, kesadaran, kepatuhan, dan perilaku keamanan informasi karyawan Universitas Prasetiya Mulya. Penelitian menggunakan pendekatan kualitatif dengan desain studi kasus tunggal. Data diperoleh melalui wawancara semi-terstruktur dengan delapan informan, expert judgement, FGD, observasi, dan dokumentasi, kemudian dianalisis melalui kondensasi data, penyajian data, serta penarikan dan verifikasi kesimpulan. Hasil penelitian mengindikasikan bahwa, dalam konteks kasus yang dikaji, pelatihan berkaitan dengan peningkatan pemahaman risiko, penguatan kesadaran bahwa keamanan merupakan tanggung jawab bersama, dan tumbuhnya kehati-hatian dalam menggunakan email, kata sandi, tautan, dan dokumen. Namun, perubahan perilaku belum konsisten karena cakupan peserta baru 135 dari 336 karyawan, beban kerja, kebiasaan lama, kurangnya penguatan pascapelatihan, evaluasi perilaku yang belum optimal, dan kanal pelaporan yang belum cukup jelas. Program perlu dijadikan wajib dan berkelanjutan, diintegrasikan dengan SDM dan onboarding, diperkuat microlearning serta simulasi phishing, dan dievaluasi menggunakan indikator perilaku.

Abstract: *The digital transformation of higher education has increased reliance on information systems while expanding risks arising from employee behaviour. This study examines the effectiveness of security awareness training in shaping employees' understanding, awareness, compliance, and information security behaviour at Universitas Prasetiya Mulya. A qualitative single-case design was employed. Data were collected through semi-structured interviews with eight informants, expert judgement, a focus group discussion, observation, and document analysis, and were analysed through data condensation, data display, and conclusion drawing and verification. The findings indicate that, within the case examined, training was associated with improved risk understanding, stronger awareness that security is a shared responsibility, and more cautious practices when handling email, passwords, links, and documents. Behavioural change, however, remained inconsistent because only 135 of 336 employees had completed the training, while workload, established habits, limited post-training reinforcement, underdeveloped behavioural evaluation, and unclear reporting channels constrained transfer to daily work. The programme should therefore become mandatory and continuous, be integrated with human-resource development and onboarding, use microlearning and phishing simulations, and be evaluated through behavioural indicators.*

Article history:
Received: 16 July 2026
Revised: 21 July 2026
Accepted: 19 August 2026
Published: 24 August 2026

Kata kunci:
Security Awareness, Perilaku Keamanan Informasi, Pelatihan Karyawan, Perguruan Tinggi, Budaya Keamanan Digital

Keyword:
Security Awareness, Information Security Behavior, Employee Training, Higher Education, Digital Security Culture

This is an open-access article under the CC-BY-SA License.

***How to cite*:** Prasetyo, K. A., Mukrodi, & Hamsinah. B. (2026). Efektivitas Pelatihan Security Awareness dalam Meningkatkan Keamanan dengan Mengaplikasikan Sistem Informasi pada Universitas Prasetiya Mulya. *PERSEPTIF: Jurnal Ilmu Sosial dan Humaniora*, *4*(3), 564–575. https://doi.org/10.70716/perseptif.v4i3.797

✉ *Corresponding author: khelik.prasetyo@gmail.com*

Copyright © 2026, the author(s)

PENDAHULUAN

Transformasi digital telah menempatkan sistem informasi sebagai infrastruktur utama perguruan tinggi. Email institusi, sistem akademik, aplikasi administrasi dan keuangan, layanan penyimpanan awan, serta kanal kolaborasi mempercepat proses kerja, tetapi sekaligus memperluas paparan risiko keamanan informasi. Dalam lingkungan semacam ini, kontrol teknis tidak cukup apabila karyawan masih mengklik tautan berbahaya, menggunakan kata sandi lemah, membagikan kredensial, salah mengatur akses dokumen, atau terlambat melaporkan aktivitas mencurigakan. Karyawan karena itu perlu diposisikan bukan hanya sebagai pengguna sistem, tetapi sebagai bagian dari mekanisme pertahanan organisasi. Dalam artikel ini, istilah karyawan digunakan sebagai istilah utama untuk merujuk profesional staf Universitas Prasetiya Mulya yang menggunakan sistem informasi institusi.

Security awareness merupakan upaya terencana untuk membangun pengetahuan, kesadaran, kepatuhan, dan tindakan aman pengguna. Dalam perspektif pengembangan sumber daya manusia, program ini seharusnya menghasilkan transfer pembelajaran ke pekerjaan, bukan berhenti pada penyampaian materi. Meta-analisis Prümmer et al. (2025) menunjukkan bahwa pelatihan keamanan siber secara umum berdampak positif pada pengguna akhir, tetapi pengaruhnya terhadap perilaku aktual lebih lemah daripada pengaruhnya terhadap pengetahuan dan sikap. Temuan tersebut menegaskan adanya awareness-behavior gap: seseorang dapat mengetahui tindakan yang benar tanpa selalu menerapkannya ketika menghadapi tekanan waktu, rutinitas, atau tuntutan operasional.

Efektivitas program juga dipengaruhi oleh desain dan lingkungan penerapannya. Chaudhary (2024) menekankan dukungan manajemen, keberlanjutan program, norma keamanan, pesan persuasif, metode inovatif, dan rekomendasi tindakan yang realistis. Alyami et al. (2023) memandang efektivitas Security Education, Training, and Awareness (SETA) sebagai siklus yang mencakup desain, pengembangan, implementasi, evaluasi, serta dukungan organisasi. Pada level intervensi, Khan et al. (2023) menunjukkan bahwa pelatihan berbasis Protection Motivation Theory dapat meningkatkan pengetahuan ancaman, pemahaman strategi perlindungan, dan self-efficacy, sedangkan Marshall et al. (2024) menemukan bahwa pelatihan phishing dipengaruhi oleh intensitas, pembelajaran aktif, umpan balik, dan kualitas evaluasi.

Konteks perguruan tinggi memerlukan perhatian khusus karena organisasi mengelola data akademik, administrasi, keuangan, SDM, penelitian, dan komunikasi dengan pihak eksternal dalam satu ekosistem digital. Penelitian pada universitas di Sumatera Barat memperlihatkan bahwa perilaku keamanan dipengaruhi faktor individu, organisasi, dan kebiasaan menggunakan teknologi (Gushelmi et al., 2024). Pada kelompok mahasiswa perguruan tinggi, perceived barriers, self-efficacy, dan perhatian terhadap privasi juga berhubungan dengan perilaku keamanan (Syed Zulkiplee et al., 2025). Bukti tersebut menguatkan bahwa intervensi tidak dapat diseragamkan; desain pelatihan harus memperhitungkan karakter pengguna, risiko pekerjaan, serta dukungan lingkungan.

Universitas Prasetiya Mulya telah menyelenggarakan pelatihan security awareness bagi karyawan. Namun, data awal dalam penelitian menunjukkan bahwa dari 336 karyawan, baru 135 orang yang mengikuti pelatihan secara penuh. Catatan agregat internal juga mencatat 41 kejadian password spraying dan 18 akses mencurigakan atau tidak dikenal selama Agustus-November 2025. Angka tersebut tidak digunakan untuk menyimpulkan hubungan sebab-akibat antara pelatihan dan insiden, tetapi menunjukkan bahwa cakupan program, perilaku karyawan, dan penguatan setelah pelatihan perlu dievaluasi secara lebih mendalam.

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

Literatur telah membahas kematangan information security awareness, strategi pencegahan phishing, dan cyber hygiene. Ahmad et al. (2024) menunjukkan bahwa kematangan awareness mencakup manajemen risiko, budaya organisasi, program pelatihan, kepatuhan kebijakan, dan dukungan teknis. Febriyani et al. (2023) menegaskan bahwa phishing perlu dihadapi melalui kombinasi penguatan sistem dan perilaku pengguna, sedangkan Armoogum et al. (2025) menempatkan kebiasaan kerja aman serta tanggung jawab bersama manajemen dan karyawan sebagai dasar cyber hygiene di tempat kerja. Meskipun demikian, kajian yang menghubungkan efektivitas pelatihan, hambatan transfer perilaku, dukungan DTI-SDM, dan pembentukan budaya keamanan dalam satu studi kasus karyawan perguruan tinggi di Indonesia masih terbatas.

Penelitian ini mengisi kesenjangan tersebut dengan memandang security awareness sebagai program pengembangan kompetensi kerja digital yang melibatkan fungsi teknologi informasi, sumber daya manusia, pimpinan unit, dan karyawan. Tujuan penelitian adalah menganalisis efektivitas pelatihan dalam meningkatkan pemahaman, kesadaran, kepatuhan, dan perilaku keamanan; mengidentifikasi faktor pendukung; menjelaskan hambatan penerapan perilaku aman; serta merumuskan strategi penguatan program. Kontribusi utamanya terletak pada kerangka penguatan yang menghubungkan pelatihan wajib dan kontekstual, penguatan pascapelatihan, evaluasi berbasis perilaku, dan budaya keamanan digital pada konteks karyawan perguruan tinggi.

METODE PENELITIAN

Penelitian menggunakan pendekatan kualitatif dengan desain studi kasus tunggal pada Universitas Prasetiya Mulya. Unit analisis adalah program pelatihan security awareness dan penerapan hasil pelatihan dalam praktik kerja karyawan. Batas kasus mencakup pelaksanaan program, dukungan lintas fungsi, dan perilaku keamanan karyawan ketika menggunakan email institusi, sistem akademik, aplikasi administrasi, layanan cloud, dokumen digital, dan platform kerja internal selama November 2025-Mei 2026. Studi kasus dipilih karena efektivitas pelatihan tidak dapat dilepaskan dari kebijakan organisasi, proses kerja, teknologi, budaya unit, dan pengalaman karyawan (Yin, 2018). Desain ini tidak menggunakan pengukuran sebelum-sesudah dan tidak dimaksudkan untuk mengestimasi besaran hubungan kausal; efektivitas ditafsirkan secara kualitatif melalui konvergensi pengalaman informan, observasi, dokumentasi, FGD, dan expert judgement.

Informan dipilih secara purposive berdasarkan pengalaman menggunakan sistem informasi, keikutsertaan atau keterlibatan dalam pelatihan, pengelolaan keamanan, pengembangan SDM, serta pengawasan perilaku kerja. Pemilihan ini tidak ditujukan untuk mencapai representasi statistik, melainkan untuk memperoleh variasi perspektif dari peserta, pengelola program, fungsi SDM, dan pimpinan unit. Wawancara individual melibatkan lima informan utama dan tiga key informan. Temuan diperkuat oleh satu expert judgement serta FGD yang melibatkan perwakilan informan dan/atau key informan. FGD diperlakukan sebagai teknik validasi kolektif, bukan sebagai tambahan jumlah informan individual. Komposisi sumber data ditampilkan pada Tabel 1.

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

Tabel 1. Sumber Data Penelitian

Kelompok	Jumlah	Unit/Fungsi	Kontribusi Data
Informan utama	5	MRA, kerja sama, administrasi akademik, dan DTI	Pengalaman karyawan, pemahaman, perilaku, hambatan, dan kebutuhan
Key informan	3	DTI, pimpinan unit, dan SDM	Desain program, kebijakan, pengawasan perilaku, pengembangan kompetensi, dan budaya
Expert judgement	1	Kepala bagian infrastruktur, keamanan jaringan, dan dukungan IT	Validasi interpretasi dan kelayakan rekomendasi
FGD	-	Perwakilan informan dan/atau key informan	Validasi kolektif atas kesamaan, perbedaan, dan prioritas strategi

Sumber: Data diolah peneliti (2026).

Data primer dikumpulkan melalui wawancara semi-terstruktur, observasi, dan FGD. Pedoman wawancara disusun berdasarkan empat fokus penelitian: efektivitas pelatihan; faktor pendukung keamanan; hambatan pelaksanaan dan penerapan perilaku aman; serta strategi peningkatan program. Masing-masing teknik digunakan secara komplementer: wawancara menggali pengalaman dan persepsi perilaku, observasi memberikan konteks praktik kerja, sedangkan FGD memeriksa kesamaan, perbedaan, dan prioritas interpretasi secara kolektif. Data sekunder meliputi materi pelatihan, rekap peserta, kebijakan atau SOP, komunikasi internal, pedoman penggunaan sistem, dan catatan insiden dalam bentuk agregat.

Analisis mengikuti model interaktif Miles et al. (2020), yaitu kondensasi data, penyajian data, serta penarikan dan verifikasi kesimpulan. Transkrip dan catatan lapangan dikodekan ke dalam tema pemahaman dan kesadaran, kepatuhan, perilaku, faktor individu, dukungan organisasi, teknologi, budaya, hambatan, serta strategi perbaikan. Pola temuan dibandingkan antar sumber dan dicocokkan dengan proposisi penelitian serta literatur terdahulu. Pernyataan informan mengenai perilaku tidak diperlakukan sebagai bukti langsung, melainkan sebagai data laporan diri yang perlu dibandingkan dengan observasi, dokumentasi, FGD, dan expert judgement.

Keabsahan data dijaga melalui triangulasi sumber, triangulasi teknik, pencocokan pola, FGD, dan expert judgement. Reliabilitas proses diperkuat dengan pedoman wawancara yang konsisten, kode tema yang terdokumentasi, dan penelusuran hubungan antara data mentah, hasil kondensasi, interpretasi, serta kesimpulan. Pertimbangan etis diterapkan melalui pembatasan data pada kebutuhan penelitian, penyamaran identitas personal dengan kode, penyajian catatan insiden secara agregat, dan pengatribusian kutipan berdasarkan kode informan. Penelitian tidak mengakses kata sandi, konfigurasi sistem, detail celah teknis, atau data pribadi sensitif, sedangkan nama unit hanya digunakan untuk menjelaskan konteks fungsi kerja.

HASIL DAN PEMBAHASAN

Analisis menghasilkan empat kelompok temuan. Pertama, informan melaporkan peningkatan pemahaman dan kesadaran awal yang disertai perubahan awal dalam praktik kerja. Kedua, perubahan

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

tersebut belum konsisten karena terdapat kesenjangan antara pengetahuan dan perilaku. Ketiga, dalam kasus yang dikaji, perilaku keamanan tampak dipengaruhi oleh keterpaduan faktor individu, organisasi, teknologi, proses pelaporan, dan budaya. Keempat, temuan mengarah pada kebutuhan untuk mengubah program dari kegiatan episodik menjadi siklus pengembangan kompetensi yang wajib, berkelanjutan, kontekstual, dan terukur. Ringkasan temuan disajikan pada Tabel 2.

Tabel 2. Ringkasan Temuan Utama

Tema	Bukti Empiris	Makna Analitis
Efektivitas awal	Pemahaman risiko meningkat; karyawan lebih waspada terhadap email, tautan, kata sandi, dan akses dokumen	Pelatihan menunjukkan efektivitas awal pada pengetahuan dan kesadaran serta disertai perubahan tindakan awal
Awareness-behavior gap	Perilaku aman melemah saat beban kerja tinggi; kebiasaan lama dan kurangnya pengingat tetap muncul	Pengetahuan belum otomatis menjadi kebiasaan; lingkungan kerja dan penguatan memengaruhi transfer
Faktor pendukung	Peran DTI, SDM, pimpinan, MFA, kontrol akses, kanal pelaporan, dan norma unit	Keamanan perlu dipahami sebagai hasil sistem sosio-teknis, bukan tanggung jawab karyawan atau DTI saja
Hambatan dan strategi	Cakupan 135 dari 336; evaluasi perilaku dan penguatan belum optimal	Program perlu wajib, berkelanjutan, kontekstual, terukur, dan terintegrasi dengan SDM

Sumber: Data diolah peneliti (2026).

Peningkatan Pemahaman, Kesadaran, dan Perilaku Awal

Sebelum mengikuti pelatihan, sebagian informan hanya memahami bahwa email dan kata sandi perlu dijaga. Setelah pelatihan, mereka mampu mengenali phishing, password spraying, akses mencurigakan, kebocoran kredensial, penggunaan kata sandi lemah, salah berbagi dokumen, dan penyalahgunaan akun. Materi yang paling mudah dipahami adalah phishing dan keamanan kata sandi karena dekat dengan aktivitas harian. Sebaliknya, konsep teknis seperti password spraying dan tanda aktivitas login mencurigakan masih memerlukan penjelasan yang lebih sederhana.

> *"Setelah pelatihan saya jadi lebih paham bahwa risiko keamanan tidak hanya soal virus komputer, tetapi juga bisa berasal dari kebiasaan pengguna, seperti klik tautan sembarangan atau memakai password yang lemah." (Informan 1).*

Data wawancara dan observasi menunjukkan munculnya pemaknaan baru bahwa keamanan informasi merupakan tanggung jawab bersama. Informan mulai melihat tindakan sederhana - memeriksa alamat pengirim, tidak membagikan kredensial, mengatur akses dokumen, menggunakan MFA, dan melaporkan aktivitas mencurigakan - sebagai bagian dari tanggung jawab profesional. Dari

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

sisi tindakan, karyawan menjadi lebih teliti saat membuka email, tautan, atau lampiran dan lebih sering meminta konfirmasi ketika menemukan komunikasi yang tidak wajar.

Temuan ini konsisten dengan Prümmer et al. (2025), yang menemukan efek positif pelatihan pada pengetahuan dan sikap, serta dengan Khan et al. (2023), yang menunjukkan peningkatan pengetahuan ancaman dan self-efficacy. Namun, data penelitian ini memberi ilustrasi kontekstual pada lingkungan karyawan perguruan tinggi: peningkatan pemahaman merupakan tahap awal, sedangkan efektivitas yang bermakna bagi organisasi perlu ditelaah dari kepatuhan dan perilaku kerja yang berulang.

Kualitas materi turut menentukan transfer pembelajaran. Contoh kasus yang menyerupai pekerjaan di unit penerimaan mahasiswa, kerja sama, administrasi akademik, atau DTI membuat risiko lebih mudah dipahami. Temuan ini sejalan dengan perbedaan tingkat awareness antarkelompok yang dilaporkan Fadli et al. (2025) dan perbedaan perilaku keamanan menurut karakter pengguna pada Candiwan et al. (2023). Artinya, materi inti dapat distandardisasi, tetapi kasus, bahasa, dan latihan perlu disesuaikan dengan data, sistem, dan risiko masing-masing fungsi kerja.

Kesenjangan antara Pemahaman dan Perilaku Nyata

Walaupun informan memahami risiko, perilaku aman belum selalu diterapkan secara konsisten. Beban kerja, tekanan penyelesaian tugas, keterbatasan waktu, kebiasaan lama, dan anggapan bahwa risiko tidak akan terjadi pada diri sendiri mengurangi ketelitian. Dalam kondisi sibuk, karyawan dapat langsung membuka lampiran, kurang memeriksa alamat pengirim, menggunakan kembali kata sandi, atau tidak meninjau hak akses dokumen secara cermat.

> *"Saat pekerjaan sedang padat, orang cenderung ingin cepat selesai sehingga kadang lupa mengecek detail seperti alamat email, tautan, atau hak akses dokumen." (Informan 1).*

Temuan tersebut mengindikasikan bahwa transfer perilaku belum berlangsung secara konsisten. Evaluasi yang dominan pada kehadiran atau pemahaman sesaat tidak cukup untuk memastikan bahwa perilaku aman bertahan di tengah rutinitas. Expert judgement menegaskan bahwa tujuan akhir security awareness bukan agar peserta sekadar mengetahui risiko, tetapi agar perilaku aman diterapkan secara konsisten.

Awareness-behavior gap dalam studi ini selaras dengan meta-analisis Prümmer et al. (2025). Penjelasan kontekstualnya adalah friksi operasional: prosedur keamanan bersaing dengan kebutuhan menyelesaikan pekerjaan secara cepat. Chaudhary (2024) menjelaskan bahwa perubahan perilaku memerlukan dukungan manajemen, norma keamanan, pesan persuasif, dan program berkelanjutan. Marshall et al. (2024) juga menunjukkan pentingnya latihan aktif, pengulangan, umpan balik, dan evaluasi pada pelatihan phishing. Dengan demikian, gap bukan semata-mata kekurangan pengetahuan individu, tetapi hasil interaksi antara kebiasaan, tekanan kerja, desain proses, dan dukungan organisasi.

Implikasinya, intervensi harus mengurangi beban kognitif ketika karyawan mengambil keputusan. Pedoman singkat, tombol pelaporan phishing, default akses yang aman, MFA, pengingat kontekstual, serta latihan berkala dapat menjadikan tindakan aman lebih mudah dilakukan. Pendekatan tersebut menggeser fokus dari menyalahkan karyawan menuju perancangan lingkungan kerja yang membantu mereka memilih tindakan aman.

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

Keamanan sebagai Ekosistem Lintas Fungsi

Dalam kasus yang dikaji, keamanan penggunaan sistem informasi dipengaruhi oleh interaksi beberapa faktor. Pada tingkat individu, pemahaman, kewaspadaan, motivasi, dan kemampuan mengenali risiko menjadi dasar. Pada tingkat organisasi, DTI menyediakan sistem, kebijakan, materi, data risiko, dukungan teknis, dan kanal pelaporan; SDM mengelola penjadwalan, pencatatan, onboarding, serta pengembangan kompetensi; pimpinan unit memberi contoh dan menguatkan norma kerja; sedangkan karyawan menerapkan perilaku aman dalam pekerjaan sehari-hari.

Dukungan teknologi juga berperan ganda sebagai kontrol dan media pembelajaran. MFA, kontrol akses, mekanisme pelaporan, e-learning, microlearning, kuis, dan simulasi phishing membantu mengurangi ketergantungan pada ingatan karyawan. Namun, teknologi hanya efektif apabila prosedurnya dipahami dan mudah digunakan. Sebagian informan mengetahui bahwa aktivitas mencurigakan perlu dilaporkan, tetapi belum seluruhnya yakin kapan, kepada siapa, dan melalui kanal apa laporan harus disampaikan.

Temuan mengenai keterpaduan faktor tersebut menguatkan model kematangan awareness dari Ahmad et al. (2024) dan temuan cyber hygiene Armoogum et al. (2025). Pada sektor jasa, nilai organisasi, perilaku rekan kerja, kemampuan mengambil keputusan, alat pendukung, dan relasi karyawan-organisasi berpengaruh terhadap perilaku keamanan (Gushelmi et al., 2023). Pada lingkungan pendidikan tinggi, hambatan yang dirasakan dan self-efficacy juga penting (Syed Zulkiplee et al., 2025). Dalam kasus ini, peran lintas fungsi DTI-SDM-pimpinan unit menjadi mekanisme yang menghubungkan faktor-faktor tersebut.

Budaya keamanan digital mulai terbentuk, tetapi belum merata antarunit. Unit yang memiliki pimpinan aktif dan komunikasi rutin menunjukkan penguatan yang lebih baik, sedangkan unit lain masih memandang keamanan sebagai domain DTI. Variasi ini menjelaskan mengapa satu materi pelatihan dapat menghasilkan tingkat penerapan yang berbeda. Pelatihan formal karena itu perlu diperkuat oleh norma sosial, teladan pimpinan, komunikasi berulang, dan respons positif terhadap pelaporan.

Hambatan Pelaksanaan dan Transfer Perilaku

Hambatan pertama adalah cakupan peserta. Hanya 135 dari 336 karyawan yang mengikuti pelatihan secara penuh, setara sekitar 40,2 persen. Kesenjangan cakupan membuat tingkat pemahaman dan kesiapan tidak seimbang. Karena satu akun atau satu karyawan yang tidak waspada dapat menjadi titik masuk serangan, pelatihan parsial membatasi manfaat program pada tingkat organisasi.

Hambatan kedua adalah desain penguatan yang belum konsisten. Informan menyatakan materi mudah terlupakan setelah kembali ke rutinitas kerja. Bentuk penguatan yang dianggap realistis meliputi email reminder, poster digital, video pendek, kuis, simulasi phishing, dan panduan pelaporan. Tanpa pengulangan, perilaku karyawan cenderung kembali ke kebiasaan lama.

Hambatan ketiga adalah evaluasi yang belum berorientasi pada perilaku. Kehadiran, penyelesaian modul, dan nilai kuis tetap berguna untuk memantau partisipasi dan pembelajaran, tetapi belum menunjukkan tindakan nyata. Indikator yang lebih relevan mencakup tingkat pelaporan email mencurigakan, hasil simulasi phishing, penggunaan MFA, kepatuhan pada kebijakan kata sandi dan

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

akses, kecepatan pelaporan, serta tren insiden akibat kelalaian karyawan. Indikator tersebut harus digunakan untuk pembelajaran dan perbaikan, bukan untuk menghukum pelapor.

Hambatan keempat adalah materi yang belum selalu kontekstual dan kanal pelaporan yang belum cukup jelas. Risiko pada administrasi akademik berbeda dari risiko pada rekrutmen mahasiswa, pengelolaan kerja sama, atau DTI. Contoh dan latihan berbasis unit membuat karyawan lebih mudah menghubungkan kebijakan dengan keputusan sehari-hari. Kejelasan kanal juga mengurangi keraguan saat karyawan menemukan email mencurigakan atau notifikasi login tidak dikenal.

Berbagai hambatan ini memperlihatkan bahwa masalah bukan hanya partisipasi individu. Program, proses, teknologi, dan budaya saling memengaruhi. Temuan tersebut konsisten dengan penelitian Gushelmi et al. (2024) mengenai faktor individu dan organisasi di perguruan tinggi serta dengan Febriyani et al. (2023) yang menekankan perlunya kombinasi perlindungan sistem dan penguatan perilaku untuk menghadapi phishing.

Strategi Penguatan Program

Strategi pertama adalah menjadikan pelatihan wajib, berjenjang, dan berkelanjutan bagi seluruh karyawan. Modul dasar diberikan kepada seluruh karyawan, sedangkan modul berbasis risiko disesuaikan dengan unit dan tingkat akses. Kewajiban perlu diintegrasikan ke proses SDM agar penjadwalan, pencatatan, pengingat, dan tindak lanjut memiliki pemilik yang jelas.

Strategi kedua adalah memasukkan security awareness ke onboarding. Karyawan baru perlu memahami sejak awal aturan akun, email, perangkat, jaringan, data, MFA, akses dokumen, dan pelaporan insiden. Integrasi ini memosisikan keamanan sebagai kompetensi kerja, bukan kegiatan teknis tambahan. Pendekatan tersebut sejalan dengan siklus SETA Alyami et al. (2023), yang menekankan keterhubungan desain, implementasi, evaluasi, dukungan organisasi, dan keberlanjutan.

Strategi ketiga adalah mengombinasikan sesi formal dengan microlearning, video singkat, kuis, studi kasus unit, simulasi phishing, dan pengingat berkala. Simulasi perlu disertai umpan balik segera dan materi remedial yang proporsional. Marshall et al. (2024) mendukung penggunaan latihan aktif dan pengulangan, sedangkan Khan et al. (2023) menunjukkan pentingnya membangun self-efficacy agar peserta yakin mampu merespons ancaman.

Strategi keempat adalah mengukur program sampai pada level perilaku dan hasil organisasi. Dashboard dapat memadukan penyelesaian modul, hasil kuis, tingkat pelaporan, performa simulasi, adopsi MFA, kepatuhan kebijakan, serta tren insiden agregat. Pengukuran harus dibaca sebagai rangkaian indikator, karena satu indikator tunggal dapat menyesatkan. Misalnya, peningkatan jumlah laporan mencurigakan pada tahap awal dapat menunjukkan kesadaran yang membaik, bukan memburuknya keamanan.

Strategi kelima adalah membangun budaya pelaporan yang jelas dan tidak menyalahkan. Kanal seperti helpdesk, email resmi, ticketing system, atau tombol pelaporan phishing perlu mudah ditemukan. Pimpinan unit harus mendorong pelaporan cepat dan memberi contoh kepatuhan. Rofiudin et al. (2025) menunjukkan bahwa perlindungan informasi memerlukan pertahanan berlapis yang menggabungkan kontrol teknis, pembaruan, dan pelatihan, sedangkan penelitian Pratama et al. (2025) memperlihatkan ruang inovasi teknologi untuk memperkuat user security awareness. Teknologi baru tetap harus digunakan berdasarkan kebutuhan dan diuji efektivitasnya, bukan sekadar karena tersedia.

Kerangka implementasi pada Tabel 3 merangkum pemilik, frekuensi, dan indikator minimum. Rangkaian ini membentuk siklus: pelatihan wajib dan kontekstual meningkatkan pemahaman;

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

penguatan serta kontrol yang mudah digunakan membantu mengubah pemahaman menjadi perilaku; evaluasi dan umpan balik menstabilkan perilaku; dan konsistensi lintas unit membentuk budaya keamanan digital.

Tabel 3. Kerangka Implementasi Program Security Awareness

Intervensi	Pemilik Utama	Frekuensi	Indikator Minimum
Pelatihan dasar wajib dan modul berbasis risiko unit	SDM dan DTI	Tahunan dan saat perubahan risiko	Cakupan, penyelesaian, dan pemahaman
Security awareness pada onboarding	SDM, DTI, pimpinan unit	Setiap karyawan baru	Penyelesaian modul dan aktivasi kontrol dasar
Microlearning, reminder, dan kampanye internal	DTI dan komunikasi internal	Bulanan/kuartalan	Jangkauan, respons, dan retensi pesan
Simulasi phishing dengan umpan balik	DTI	Kuartalan/semesteran	Tingkat klik, pelaporan, dan perbaikan berulang
Evaluasi perilaku dan budaya pelaporan	DTI, SDM, pimpinan unit	Kuartalan	MFA, kepatuhan, kecepatan pelaporan, dan tren insiden agregat

Sumber: Data diolah peneliti (2026).

Gambar 1. Kerangka Penguatan Pelatihan Security Awareness Berkelanjutan
Sumber: Diolah peneliti berdasarkan temuan penelitian (2026).

Gambar 1 memperlihatkan alur penguatan yang bergerak dari pelatihan wajib dan kontekstual menuju pemahaman dan kesadaran risiko, kemudian diterjemahkan menjadi perilaku aman yang terukur, hingga membentuk budaya keamanan digital. Alur tersebut tidak dipahami sebagai proses linear sekali jalan. Setiap tahap diperkuat secara lintas tahap oleh dukungan pimpinan, integrasi DTI-SDM, kontrol teknologi, pengingat dan umpan balik, serta kanal pelaporan. Hasil evaluasi perilaku dan

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

laporan insiden selanjutnya menjadi umpan balik untuk memperbarui materi, frekuensi, dan bentuk intervensi sehingga program berlangsung sebagai siklus perbaikan berkelanjutan.

Kontribusi dan Keterbatasan Penelitian

Secara teoretis, temuan penelitian ini menunjukkan bahwa efektivitas pelatihan perlu dipahami sebagai proses lintas level. Level individu mencakup pengetahuan, kesadaran, self-efficacy, dan kebiasaan; level pekerjaan mencakup beban, friksi proses, dan relevansi kasus; level organisasi mencakup kebijakan, kepemimpinan, koordinasi DTI-SDM, teknologi, serta budaya. Kontribusi analitis penelitian terletak pada penjelasan mengenai bagaimana awareness-behavior gap muncul dalam konteks karyawan perguruan tinggi dan bagaimana fungsi SDM dapat menjadi penghubung antara pelatihan teknis dan pembentukan kebiasaan kerja.

Secara praktis, hasil penelitian memberi arah perubahan dari program episodik menuju siklus kompetensi. Keberhasilan tidak cukup ditandai oleh selesainya kelas, tetapi oleh cakupan yang merata, tindakan aman yang lebih mudah, pelaporan yang cepat, pembelajaran dari simulasi dan insiden, serta norma lintas unit. Materi yang kontekstual dan evaluasi yang tidak menghukum penting agar program meningkatkan kapasitas tanpa menciptakan keengganan untuk melapor.

Penelitian ini memiliki keterbatasan. Studi dilakukan pada satu organisasi sehingga temuan dimaksudkan sebagai generalisasi analitis yang bergantung pada konteks, bukan generalisasi statistik. Perubahan perilaku ditafsirkan dari wawancara, observasi, dokumentasi, FGD, dan penilaian ahli; penelitian belum menggunakan pengukuran longitudinal atau desain sebelum-sesudah sehingga tidak dapat menetapkan besaran hubungan kausal. Wawancara mengenai kepatuhan keamanan juga berpotensi dipengaruhi social desirability bias karena informan dapat melaporkan perilaku yang dianggap benar secara normatif. Risiko tersebut dikurangi melalui perbandingan laporan diri dengan observasi, dokumentasi, FGD, dan expert judgement, tetapi tidak dapat dihilangkan sepenuhnya. Data insiden digunakan secara agregat dan tidak menjadi bukti kausal bahwa pelatihan menurunkan insiden. Penelitian selanjutnya dapat menguji kerangka ini melalui metode campuran, simulasi phishing berulang, pengukuran perilaku longitudinal, dan perbandingan antarinstitusi.

KESIMPULAN

Dalam konteks studi kasus Universitas Prasetiya Mulya, pelatihan security awareness menunjukkan efektivitas awal pada peningkatan pemahaman dan kesadaran karyawan serta disertai tumbuhnya kehati-hatian dalam menggunakan email, tautan, kata sandi, dokumen, dan akses sistem. Namun, perubahan perilaku belum konsisten dan temuan tidak dimaksudkan sebagai bukti mengenai besaran hubungan kausal. Efektivitas program dibatasi oleh cakupan peserta yang baru 135 dari 336 karyawan, tekanan dan beban kerja, kebiasaan lama, materi yang belum selalu kontekstual, penguatan pascapelatihan yang belum rutin, evaluasi yang masih berfokus pada kehadiran atau pemahaman, serta kanal pelaporan yang perlu diperjelas. Keamanan penggunaan sistem informasi karena itu perlu dibangun melalui keterpaduan faktor individu, kebijakan organisasi, dukungan DTI dan SDM, kepemimpinan unit, kontrol teknologi, proses pelaporan, dan budaya kerja. Program disarankan menjadi wajib, berkelanjutan, berbasis risiko unit, terintegrasi dengan onboarding dan pengembangan kompetensi, diperkuat microlearning serta simulasi phishing, dan dievaluasi menggunakan indikator perilaku. Dengan pendekatan tersebut, security awareness dapat berkembang dari kegiatan edukasi menjadi mekanisme pembentukan kompetensi dan budaya keamanan digital perguruan tinggi.

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

DAFTAR PUSTAKA

Ahmad, M. R., Osman, M. H., Abdullah, A., & Sharif, K. Y. (2024). Evolution of information security awareness towards maturity: A systematic review. *International Journal on Advanced Science, Engineering and Information Technology*, *14*(5), 1738-1747. https://doi.org/10.18517/ijaseit.14.5.20234

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2023). The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: A lifecycle model. *Information Technology & People*, *36*(8), 94-125. https://doi.org/10.1108/ITP-07-2022-0515

Armoogum, S., Armoogum, V., Chandra, A., Dewi, D. A., Kurniawan, T. B., Bappoo, S., Mohd Salikon, M. Z., & Alanda, A. (2025). A comprehensive review of cyber hygiene practices in the workplace for enhanced digital security. *JOIV: International Journal on Informatics Visualization*, *9*(1), 137-145. https://doi.org/10.62527/joiv.9.1.3787

Candiwan, Sudirman, B. P., & Sari, P. K. (2023). Differences in information security behavior of smartphone users in Indonesia using Pearson's chi-square and post hoc test. *International Journal on Advanced Science, Engineering and Information Technology*, *13*(2), 703-717. https://doi.org/10.18517/ijaseit.13.2.17975

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, *142*, 103858. https://doi.org/10.1016/j.cose.2024.103858

Fadli, R., Eliza, F., Sari, R. C., Surjono, H. D., Khulanthaivel, G., & Kartika, R. (2025). Comparison of cybersecurity awareness among vocational high school students. *International Journal on Advanced Science, Engineering and Information Technology*, *15*(6), 1747-1754. https://doi.org/10.18517/ijaseit.15.6.20304

Febriyani, W., Fathia, D., Widjajarto, A., & Lubis, M. (2023). Security awareness strategy for phishing email scams: A case study one of a company in Singapore. *JOIV: International Journal on Informatics Visualization*, *7*(3), 808-814. https://doi.org/10.30630/joiv.7.3.2081

Gushelmi, Latih, R., & Mohd Zin, A. (2023). Level of user security behavior in the service industry. *International Journal on Advanced Science, Engineering and Information Technology*, *13*(4), 1529-1536. https://doi.org/10.18517/ijaseit.13.4.18425

Gushelmi, Latih, R., & Mohd Zin, A. (2024). Cybersecurity behavior in the West Sumatra universities. *JOIV: International Journal on Informatics Visualization*, *8*(3-2), 1976-1986. https://doi.org/10.62527/joiv.8.3-2.3094

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. A. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's model. *Computers & Security*, *125*, 103049. https://doi.org/10.1016/j.cose.2022.103049

Marshall, N., Sturman, D., & Auton, J. C. (2024). Exploring the evidence for email phishing training: A scoping review. *Computers & Security*, *139*, 103695. https://doi.org/10.1016/j.cose.2023.103695

Miles, M. B., Huberman, A. M., & Saldaña, J. (2020). *Qualitative data analysis: A methods sourcebook (4th ed.).* SAGE Publications.

Pratama, I. P. A. E., Widyantara, I. M. O., Linawati, & Gunantara, N. (2025). Bibliometric analysis of AI-based prototype proposal for user security awareness in healthcare. *JOIV: International Journal on Informatics Visualization*, *9*(3), 982-994. https://doi.org/10.62527/joiv.9.3.3319

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License

Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers & Security*, *150*, 104206. https://doi.org/10.1016/j.cose.2024.104206

Rofiudin, A. S., Orvalamarva, & Saedudin, R. R. (2025). Comparative analysis of information security methods in e-commerce environment. *International Journal on Advanced Science, Engineering and Information Technology*, *15*(6), 1740-1746. https://doi.org/10.18517/ijaseit.15.6.20307

Syed Zulkiplee, S. M., Mohd Shukran, M. A., Mohd Isa, M. R., Adib Khairuddin, M., Wahab, N., & Hidayat, H. (2025). Examining the impact factors influencing higher education institution (HEI) students' security behaviours in cyberspace environment. *JOIV: International Journal on Informatics Visualization*, *9*(1), 146-152. https://doi.org/10.62527/joiv.9.1.2296

Yin, R. K. (2018). *Case study research and applications: Design and methods (6th ed.).* SAGE Publications.

Copyright © 2026, the author(s). This is an open access article under the CC-BY-SA License