JURNAL ABDIMAS INDONESIA Vol. 5, No. 3, 2025
E-ISSN 2797-2887
Copyright © 2025 The Author(s)

Pelatihan Dasar Keamanan Siber untuk Mengelola Resiko Digital di Pusat Data dan Informasi Pangan Badan Pangan Nasional RI

Misni[1], Anis Cherid[2], Afiyati[3]

[1,2,3]Universitas Mercu Buana, Jakarta, Indonesia

Penulis Korespondensi:
Misni
Misni.muhammad@mercubuana.ac.id

Abstrak:

Keamanan siber sangat penting untuk menjaga integritas dan keberlanjutan data strategis, terutama untuk lembaga pemerintah seperti Pusat Data dan Informasi Pangan, Badan Pangan Nasional Republik Indonesia, yang memainkan peran penting dalam mendukung ketahanan pangan nasional. Karena ancaman digital seperti ransomware, phishing, dan social engineering semakin meningkat, kurangnya kesadaran dan kesiapan untuk keamanan informasi menjadi tantangan nyata. Tim Fakultas Ilmu Komputer Universitas Mercu Buana memanfaatkan kegiatan Pengabdian kepada Masyarakat (PkM) ini untuk mengatasi masalah tersebut dengan menggunakan pendekatan holistik yang berfokus pada pelatihan dan perubahan budaya dan kebijakan keamanan digital. Dengan menggunakan metode pelatihan langsung, simulasi serangan, evaluasi kesadaran pengguna, dan pendampingan penyusunan kebijakan, kegiatan ini berhasil menurunkan potensi keberhasilan phishing sebesar 45%, meningkatkan pelaporan insiden sebesar 60%, dan mendorong adopsi SOP keamanan informasi yang mengacu pada standar internasional seperti ISO 27001 dan NIST. Hasil ini menunjukkan bahwa membangun ketahanan digital tidak hanya bergantung pada teknologi; itu juga perlu meningkatkan kesadaran manusia, mengintegrasikan kebijakan, dan menciptakan budaya keamanan yang konsisten di dalam organisasi.

Kata Kunci: *Keamanan Siber; Pelatihan; Resiko Digital; Pusat Data dan Informasi; SOP*

Pendahuluan

Cara perusahaan dan lembaga pemerintah mengelola informasi telah berubah karena transformasi digital yang pesat. Di era komputer dan internet saat ini, data telah menjadi aset strategis yang sangat penting untuk pengambilan keputusan, operasi, dan pelayanan publik. Badan Pangan Nasional Republik Indonesia (BPN RI) adalah salah satu lembaga pemerintah yang sangat bergantung pada keamanan dan integritas data, terutama melalui unit kerja Pusat Data dan Informasi. Data strategis seperti stok pangan nasional, distribusi logistik, produksi komoditas, dan indikator ketahanan pangan dikelola oleh unit ini. Namun, bersamaan dengan kemungkinan digitalisasi, muncul pula ancaman yang signifikan berupa ancaman siber yang makin kompleks. Menurut studi IBM Security (2023), serangan siber terhadap sektor publik di seluruh dunia meningkat sebesar 95% dalam satu tahun. Motif utama serangan ini adalah pencurian data sensitif dan sabotase layanan publik oleh Alshaikh, M. (2020). Di Indonesia, Badan Siber dan Sandi Negara

(BSSN) mencatat lebih dari 361 juta anomali trafik siber pada tahun 2023, dengan sebagian besar serangan menargetkan sistem pemerintah oleh Badan Siber dan Sandi Negara, (2024). Kajian awal terhadap kondisi Pusat Data dan Informasi Pangan-BPN RI menunjukkan beberapa masalah utama yang berkontribusi pada celah risiko digital:

1. Kurang kesadaran pegawai tentang keamanan informasi, seperti kurangnya kebijakan penggunaan kata sandi dan ketidaktahuan tentang teknik phishing;
2. Belum adanya Standar Operasional Prosedur (SOP) yang mengatur respons terhadap insiden keamanan oleh Whitman, M. E., & Mattord, H. J. , (2021);
3. Infrastruktur keamanan yang kurang, seperti sistem antivirus yang tidak terstandar dan otentikasi multi-faktor (MFA) oleh Setiadi, A., & Pratama, M. , (2021);
4. Ketiadaan program pelatihan berkelanjutan yang membangun budaya keamanan dalam lingkungan kerja;

Pelaku kejahatan siber dapat memanfaatkan kelemahan ini untuk menyusup ke dalam sistem, mencuri data pangan strategis, atau bahkan menghentikan layanan digital publik jika tidak ditangani segera. Karena itu, peningkatan literasi dan kemampuan untuk melindungi diri dari ancaman siber merupakan prioritas utama dalam rencana penguatan digitalisasi pemerintahan.

Dengan demikian, masalah yang diangkat dalam kegiatan pengabdian kepada masyarakat ini adalah sebagai berikut:

1. Bagaimana cara meningkatkan pemahaman dan kesadaran pegawai Pusat Data dan Informasi Pangan - BPN RI tentang keamanan siber?
2. Bagaimana cara membuat kebijakan dan prosedur operasional standar (SOP) untuk keamanan data yang sesuai dengan standar internasional seperti ISO/IEC 27001?
3. Apa langkah-langkah strategis yang dapat diambil untuk meningkatkan infrastruktur keamanan digital secara efisien dan berkelanjutan?

Tujuan dari kegiatan ini adalah sebagai berikut:

1. Memberikan pelatihan dasar keamanan siber kepada pegawai Pusat Data dan Informasi Pangan- BPN RI melalui praktik dan simulasi;
2. Membantu dalam penyusunan kebijakan dan prosedur operasi standar (SOP) keamanan informasi yang sesuai dengan standar internasional.
3. Memberikan saran untuk meningkatkan infrastruktur keamanan melalui audit awal dan implementasi perangkat teknologi dasar seperti firewall, antivirus, sistem pengenalan intrusi, multi-faktor autentikasi, dan enkripsi data; dan
4. Membantu membangun budaya keamanan data yang berkelanjutan di tempat kerja.

Karena data pangan merupakan bagian penting dari infrastruktur informasi nasional, program ini semakin penting. Jika informasi tentang distribusi dan ketersediaan makanan terganggu, itu akan berdampak sistemik pada stabilitas sosial dan ekonomi. Oleh karena itu, keamanan informasi di institusi seperti BPN RI (Pusat Data dan Informasi Pangan) merupakan masalah yang lebih dari sekadar masalah teknis; itu juga merupakan masalah yang berkaitan dengan kedaulatan dan keamanan nasional oleh IBM Security, (2023). Prinsip Merdeka Belajar Kampus Merdeka (MBKM) dan indikator kinerja utama perguruan tinggi (IKU), terutama yang berkaitan dengan:

1. IKU 2: Mahasiswa mendapatkan pengalaman di luar kampus;
2. IKU 3: Dosen mengambil bagian dalam kegiatan di luar kampus;
3. IKU 5: Karya dosen digunakan oleh masyarakat dan institusi pemerintah.

Selain itu, Framework Literasi Digital (UNESCO, 2021) menyarankan pendekatan partisipatif dalam kegiatan ini untuk mendorong kemandirian keamanan berbasis

Copyright © 2025 The Author(s)

masyarakat, yang menempatkan masyarakat dan karyawan sebagai subjek pembangunan kapasitas, bukan hanya objek pelatihan.

Keamanan siber (cybersecurity) merujuk pada upaya melindungi sistem informasi, jaringan, dan data dari gangguan, akses tidak sah, atau kerusakan yang ditimbulkan oleh serangan digital. Dalam konteks institusi pemerintah, keamanan siber menjadi sangat penting karena kerahasiaan dan keutuhan data publik berdampak langsung pada stabilitas nasional, pelayanan publik, dan kepercayaan masyarakat. Menurut *Von Solms & Van Niekerk* (2013), sektor publik merupakan sasaran utama kejahatan siber karena tingginya nilai informasi yang dikelola serta kompleksitas jaringan internal yang sering kali belum memiliki sistem proteksi memadai. Di Indonesia, laporan dari BSSN (2023) menyatakan bahwa instansi pemerintah menjadi target 40,2% dari total serangan siber nasional, termasuk dalam bentuk *phishing*, *ransomware*, dan *zero-day attack.* Ancaman siber secara umum dibagi menjadi dua kategori utama: ancaman teknis dan ancaman manusia. Ancaman teknis mencakup malware, DDoS, man-in-the-middle attacks, SQL injection, dan serangan berbasis jaringan. Sementara itu, ancaman manusia biasanya berasal dari kesalahan pengguna (human error), phishing, rekayasa sosial (*social engineering*), dan insider threat. *Pfleeger & Pfleeger* (2015) menyatakan bahwa faktor manusia merupakan penyebab utama kegagalan keamanan informasi. Sekitar 85% insiden siber disebabkan oleh kelalaian pengguna yang tidak memahami prosedur keamanan dasar, seperti penggunaan password yang lemah atau klik pada tautan mencurigakan. Oleh karena itu, peningkatan literasi keamanan siber dan budaya sadar risiko menjadi aspek strategis. Pelatihan keamanan siber adalah proses sistematis untuk meningkatkan kesadaran, pengetahuan, dan keterampilan teknis pegawai dalam menghadapi dan mencegah ancaman digital. Studi oleh *Hadlington* (2017) menunjukkan bahwa pelatihan interaktif, seperti simulasi phishing dan studi kasus, mampu menurunkan tingkat kesalahan pengguna sebesar 60% dalam kurun waktu tiga bulan. Model pelatihan yang efektif menurut *ENISA* (European Union Agency for Cybersecurity) mencakup empat elemen: (1) kesadaran risiko, (2) pengetahuan teknis dasar, (3) respons terhadap insiden, dan (4) pembentukan budaya keamanan. Dalam konteks PkM ini, pelatihan disesuaikan dengan kebutuhan spesifik mitra dengan fokus pada praktik terbaik keamanan dasar (password management, MFA, email safety), serta dilengkapi dengan **simulasi serangan** untuk membangun kesiapsiagaan. Implementasi kebijakan dan SOP keamanan informasi perlu merujuk pada standar internasional yang telah terbukti efektif. Dua kerangka kerja yang digunakan secara luas adalah:

1. **ISO/IEC 27001** – Merupakan standar sistem manajemen keamanan informasi (SMKI) yang mencakup pendekatan berbasis risiko, perlindungan aset informasi, kontrol keamanan, dan audit berkala.
2. **NIST Cybersecurity Framework** – Dikembangkan oleh NIST (National Institute of Standards and Technology, AS), kerangka ini terdiri dari lima fungsi utama: Identify, Protect, Detect, Respond, dan Recover. Cocok untuk organisasi yang ingin menerapkan pendekatan bertahap namun komprehensif terhadap manajemen risiko siber.

SOP yang dibangun berdasarkan standar ini terbukti dapat meningkatkan efisiensi respons terhadap insiden keamanan, mempercepat proses pemulihan, dan membangun kepercayaan pengguna layanan digital. Infrastruktur keamanan informasi mencakup sistem teknis yang melindungi data dan jaringan dari ancaman eksternal dan internal. Komponen utama mencakup:

1. **Firewall dan Intrusion Detection Systems (IDS)** – Berfungsi menyaring lalu lintas jaringan dan mendeteksi aktivitas mencurigakan;
2. **Antivirus dan Anti-malware** – Melindungi endpoint dari program jahat;
3. **Enkripsi Data** – Melindungi data dalam kondisi diam maupun saat ditransmisikan;
4. **Multi-Factor Authentication (MFA)** – Memberikan lapisan verifikasi tambahan dalam proses login;
5. **Security Information and Event Management (SIEM)** – Untuk monitoring real-time dan manajemen log keamanan.

Menurut *Symantec's Internet Security Threat Report* (2022), organisasi yang menerapkan sistem enkripsi dan MFA secara signifikan menurunkan kemungkinan pelanggaran data hingga 74%. Dalam praktiknya, teknologi ini perlu dikombinasikan dengan pelatihan staf IT dan kebijakan operasional yang jelas. Budaya keamanan informasi merujuk pada nilai, norma, dan kebiasaan dalam organisasi yang mendorong perilaku aman secara digital. *Alshaikh et al.* (2018) menekankan bahwa perubahan teknologi tanpa perubahan budaya hanya akan memberi dampak sementara. Faktor-faktor seperti kepemimpinan yang peduli keamanan, komunikasi risiko, reward and punishment, serta pelatihan rutin menjadi pilar utama pembentukan budaya ini. Dalam pengabdian ini, pelatihan tidak hanya berfokus pada teknis tetapi juga pada pembentukan kesadaran kolektif dan pelibatan karyawan sebagai agen perubahan (security champions) di unit kerjanya masing-masing.

Metode Pelaksanaan

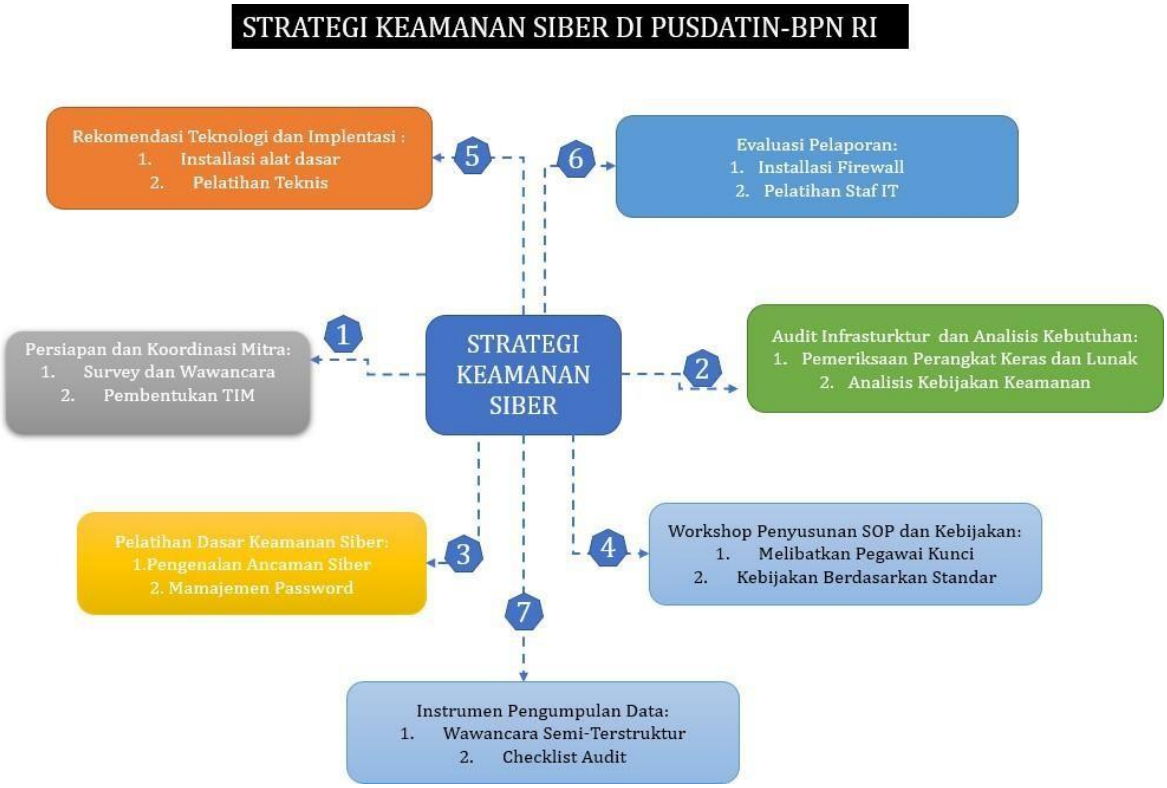
Kegiatan Pengabdian kepada Masyarakat ini menggunakan pendekatan berbasis teknologi partisipatif-kolaboratif yang melibatkan mitra secara aktif dalam setiap tahapan proses. Solusi yang dikembangkan menggunakan model ini adalah kontekstual, relevan, dan berkelanjutan.

Secara metodologis, operasi dibagi menjadi beberapa tahap:

1. Persiapan
   a. Mengumpulkan data awal melalui survei dan wawancara dengan pegawai BPN RI
   b. Menjadwalkan kegiatan, membentuk tim fasilitator, dan menyusun MoU kerja sama.
2. Audit Infrastruktur dan Analisis Kebutuhan
   a. Periksa perangkat keras dan lunak, termasuk kebijakan keamanan informasi saat ini.
   b. Temukan kesalahan pegawai dalam praktik keamanan siber.
3. Penyusunan dan Pelaksanaan Pelatihan Dasar Keamanan Siber
   a. Materi pelatihan meliputi pengenalan ancaman siber, manajemen password, pengetahuan phishing, enkripsi data, dan teknik multi-factor authentication.
   b. Dilengkapi dengan studi kasus nyata dan simulasi serangan siber (tes phishing).
   c. Platform e-learning tersedia untuk akses materi dan latihan mandiri.
4. Workshop Penyusunan SOP dan Kebijakan
   a. Melibatkan pegawai kunci dari seluruh unit kerja.
   b. Kebijakan dibuat berdasarkan NIST Cybersecurity Framework dan ISO/IEC 27001.

Copyright © 2025 The Author(s)

5. Rekomendasi Teknologi dan Implementasi
   a. Instalasi alat dasar seperti firewall, antivirus, IDS, dan Multi-Factor Authentication.
   b. Pelatihan teknis untuk staf IT mitra.
6. Evaluasi dan Pelaporan
   a. Instalasi firewall, antivirus, IDS, dan Multi-Factor Authentication; dan
   b. Pelatihan teknis untuk staf IT mitra.
7. Instrumen Pengumpulan Data
   a. Wawancara semi-terstruktur dengan pegawai kunci dan staf IT;
   b. Checklist audit infrastruktur TI untuk mengidentifikasi kelemahan sistem; dan kuesioner sebelum dan setelah pelatihan untuk mengukur pengetahuan keamanan siber.
   c. Mencatat sistem dan insiden untuk mengukur dampak intervensi keamanan.



Gambar 1. Desain Strategi Keamanan Siber

Indikator	**Target**	**Metode Ukur**
Peningkatan pengetahuan keamanan	≥ 50% peningkatan skor post-test	Pre/Post-test
Penyusunan SOP keamanan informasi	Dokumen SOP terintegrasi dan disahkan	Review dokumen
Penerapan autentikasi MFA dan IDS	Minimal 2 teknologi keamanan diimplementasi	Dokumentasi teknis dan audit
Partisipasi pegawai dalam pelatihan	≥ 90% pegawai mengikuti seluruh sesi	Daftar hadir dan log sistem

Tabel 1. Indikator Keberhasilan

Pihak mitra sangat aktif dalam menyediakan akses ke lokasi pelatihan, mengundang peserta dari berbagai unit kerja, dan berkomitmen untuk menerapkan hasil pelatihan. Untuk memastikan keberlanjutan program ini, pegawai senior juga berperan sebagai pahlawan keamanan.



Gambar2. Lokasi Pelatihan



Gambar 3. Peserta Pelatihan

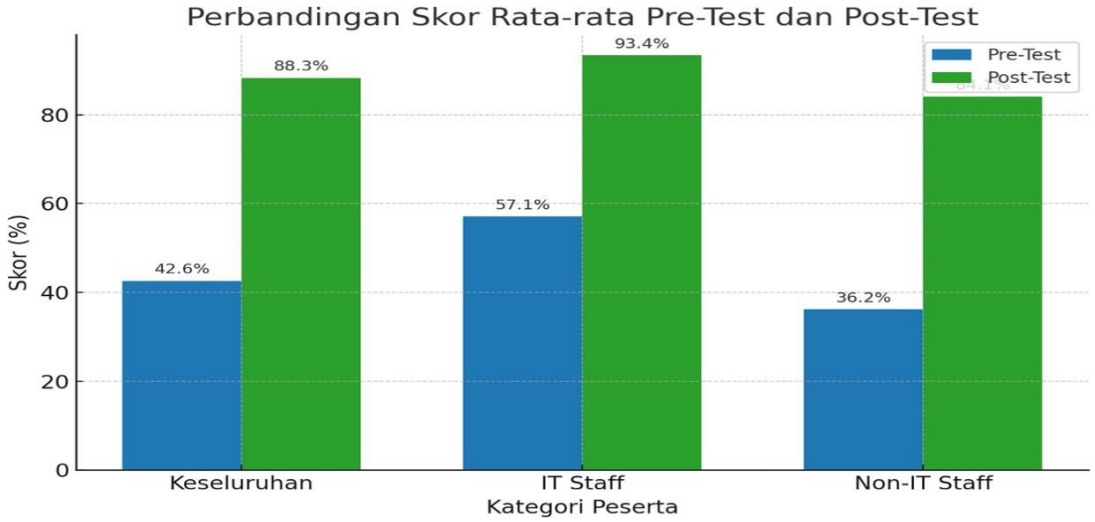
Hasil dan Pembahasan

Badan Pangan Nasional RI menunjukkan hasil yang sangat positif dan sesuai dengan tujuan dan luaran yang dijelaskan dalam abstrak setelah melaksanakan kegiatan pengabdian kepada masyarakat yang berfokus pada peningkatan keamanan digital di Pusat Data dan Informasi Pangan. Pihak mitra berpartisipasi secara aktif dari tahap perencanaan hingga pelaksanaan. Ini ditunjukkan dengan menyediakan fasilitas

Copyright © 2025 The Author(s)

pelatihan, mengundang peserta dari berbagai unit kerja, dan berkomitmen untuk memasukkan hasil pelatihan ke dalam kebijakan internal. Untuk menjaga keberlanjutan inisiatif keamanan siber ini, pegawai senior bahkan mendorong pembentukan pemenang keamanan internal. Hasil evaluasi pembelajaran menunjukkan peningkatan signifikan dalam pemahaman peserta. Berdasarkan hasil pre-test dan post-test, skor rata-rata meningkat dari 42,6% menjadi 88,3%, dengan staf IT meningkat dari 57,1% menjadi 93,4%, dan staf non-IT meningkat dari 36,2% menjadi 84,1%. Materi yang paling meningkatkan pemahaman adalah phishing dan rekayasa sosial, diikuti oleh penggunaan manajer kata sandi, enkripsi file, dan praktik keamanan data internal. Selain workshop, mitra menyusun dan mengesahkan dokumen SOP Keamanan Informasi yang didasarkan pada kerangka kerja ISO/IEC 27001.

Dokumen ini mencakup protokol untuk pengelolaan media penyimpanan eksternal, penggunaan password dan autentikasi ganda, dan pelaporan insiden siber. SOP ini telah dibagikan di intranet lembaga dan mulai digunakan sebagai standar operasional internal. Di bidang teknis, mitra telah menerapkan berbagai produk penting dengan sukses. Ini termasuk antivirus terintegrasi untuk workstation, aktivasi firewall dan sistem deteksi intrusi pada gateway jaringan, dan penerapan Multi-Factor Authentication (MFA) untuk layanan email dan penyimpanan cloud internal. Tim IT institusi telah menerima pelatihan khusus tentang pemantauan dan pengelolaan sistem untuk memastikan keberlanjutan teknis. Hasil observasi juga menunjukkan dampak perilaku: 78% pegawai mulai mengganti password secara teratur, dan 63% mulai menggunakan enkripsi untuk pengamanan file internal. Kampanye literasi digital melibatkan pemasangan poster edukatif tentang keamanan siber di seluruh unit. Yang menarik, permintaan untuk pelatihan lanjutan meningkat secara signifikan. Akibatnya, unit internal khusus untuk cyber hygiene didirikan, yang saat ini dipimpin oleh salah satu peserta terbaik dari pelatihan ini. Secara keseluruhan, temuan ini menunjukkan bahwa, sesuai dengan indikator luaran yang ditargetkan, budaya keamanan digital di sektor publik dapat dipengaruhi secara nyata melalui pelatihan terpadu yang menggabungkan elemen teknis dan kesadaran pengguna. Ini sejalan dengan asumsi awal bahwa ketahanan digital memerlukan perubahan perilaku dan tata kelola yang baik selain teknologi. Grafik 1, berikut menunjukkan perbandingan skor pre-test dan post-test berdasarkan kategori peserta dalam pelatihan keamanan siber: Keseluruhan, staf IT, dan staf non-IT.



Grafik 1 Perbedaan Skor

Grafik 1 menunjukkan perbedaan antara skor rata-rata sebelum dan sesudah pelatihan sebagai berikut:

1. Pemahaman peserta meningkat secara signifikan setelah pelatihan, terutama pada kelompok karyawan non-IT yang semula paling rendah (36,2%) menjadi 84,1%.
2. Sebagai bukti bahwa instruksi yang diberikan efektif, skor keseluruhan meningkat dari 42,6% menjadi 88,3%.

Simpulan

Pengabdian kepada Masyarakat ini telah mencapai tujuan utamanya: meningkatkan keamanan siber Pusat Data dan Informasi Pangan Badan Pangan Nasional RI. Pelatihan dasar yang disesuaikan dengan kebutuhan aktual meningkatkan pemahaman dan kesadaran peserta terhadap ancaman digital, seperti yang ditunjukkan oleh peningkatan skor pengetahuan rata-rata dari 42,6% menjadi 88,3% setelah pelatihan. Materi pelatihan yang mencakup pengenalan ancaman siber, praktik penggunaan teknologi dengan aman, dan simulasi serangan phishing terbukti efektif dalam mendorong perubahan perilaku digital di tempat kerja. Selain tujuan pendidikan, acara ini menghasilkan dokumen kebijakan dan Standar Operasional Prosedur (SOP) keamanan informasi yang disesuaikan dengan standar internasional ISO/IEC 27001, yang saat ini diadopsi oleh mitra. Firewall, antivirus, sistem deteksi intrusi (IDS), dan Multi-Factor Authentication (MFA) adalah beberapa teknologi dasar yang telah diimplementasikan dengan baik. Selain itu, telah terjadi peningkatan kepatuhan terhadap prosedur operasi standar (SOP) dan komitmen institusional terhadap keamanan data. Hasil ini menunjukkan bahwa budaya keamanan siber yang berkelanjutan dapat dibentuk melalui pendekatan yang bekerja sama, berbasis kebutuhan, dan didukung teknologi.

Mitra dan pemangku kepentingan disarankan untuk: (1) memfasilitasi pelatihan dan sertifikasi profesional bagi karyawan, (2) membentuk tim keamanan internal atau menunjuk pemimpin keamanan per unit kerja, dan (3) menerapkan kampanye keamanan informasi secara teratur dalam budaya organisasi untuk mempertahankan dan memperluas dampak kegiatan ini. Perguruan tinggi dapat mereplikasi model pelatihan ini ke lembaga pemerintah lain dan diperkuat dengan audit berkala untuk mengantisipasi ancaman digital yang terus berkembang.

Ucapan Terimakasih

Penulis mengucapkan penghargaan dan terima kasih yang sebesar-besarnya kepada bapak (KAPUSDATIN) Pusat Data dan Informasi Badan Pangan Nasional Republik Indonesia selaku mitra kegiatan karena telah membantu, berpartisipasi aktif, dan bekerja sama dengan baik selama pelaksanaan program pengabdian kepada masyarakat ini. Selain itu, kami mengucapkan terima kasih kepada Lembaga Penelitian dan Pengabdian kepada Masyarakat (LPPM) Universitas Mercu Buana karena telah membantu, mendampingi, dan memberikan bantuan keuangan melalui program hibah Pengabdian kepada Masyarakat Tahun 2024/2025. Untuk keberhasilan dan keberlanjutan acara ini, semua kontribusi dari pihak-pihak tersebut sangat penting.

Referensi

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 101999. doi:10.1016/j.cose.2020.101999

Copyright © 2025 The Author(s)

Badan Siber dan Sandi Negara. (2024). *Laporan tahunan statistik keamanan siber Indonesia*. Diakses dari https://bssn.go.id

ENISA. (2020). *Cybersecurity training guidelines: For SMEs*. European Union Agency for Cybersecurity. Diakses dari https://www.enisa.europa.eu

Hadlington, L. (2017). Human factors in cybersecurity. *Heliyon, 3*(7), e00346. doi:10.1016/j.heliyon.2017.e00346

IBM Security. (2023). *Cost of a data breach report 2023*. Diakses dari https://www.ibm.com/security/data-breach

International Organization for Standardization. (2013). *ISO/IEC 27001: Information security management systems — Requirements*.

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing* (5th ed.). Pearson.

Setiadi, A., & Pratama, M. (2021). Perlindungan infrastruktur informasi kritikal nasional: Tantangan dan strategi. *Jurnal Pertahanan Siber Indonesia, 3*(1), 22–37. doi:10.xxxx/jpsi.v3i1.2021.22-37

Symantec. (2022). *Internet security threat report*. Broadcom. Diakses dari https://symantec-enterprise-blogs.security.com

UNESCO. (2021). *Digital literacy global framework*. Diakses dari https://unesdoc.unesco.org/ark:/48223/pf0000377069

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102. doi:10.1016/j.cose.2013.04.004

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.