JIPITI: Jurnal Pengabdian kepada Masyarakat
Vol. 2, No. 1, Februari 2025, pp. 50~55
ISSN: 3063-573X (Media Online)

Pelatihan Kesadaran Keamanan Informasi bagi Karyawan PT. Wijaya Kesuma Segara untuk Mencegah Ancaman Siber

Ellanda Purwawijaya [1], Dinur Syahputra [2], Roy Nuary Singarimbun [3], Aripin Rambe [4], Baginda Harahap [5], Auliana Nasution [6]
[1,2,3,4,5,6] Fakultas Teknologi, Universitas Battuta
e-mail: [1] ellanda.purwa.wijaya@gmail.com , [2] dinsyahui12@gmail.com, [3] roy90singarimbun@gmail.com, [4] arambedigital@gmail.com, [5] profesionalbaginda@gmail.com, [6] auliana@battuta.ac.id

Abstrak

Dalam era digital yang semakin berkembang, ancaman siber menjadi risiko yang signifikan bagi perusahaan, termasuk PT. Wijaya Kesuma Segara. Banyak serangan siber yang terjadi akibat kurangnya pemahaman dan kesadaran karyawan terhadap keamanan informasi, seperti phishing, malware, dan kebocoran data. Oleh karena itu, kegiatan pengabdian masyarakat ini bertujuan untuk meningkatkan kesadaran dan pemahaman karyawan mengenai keamanan informasi guna mengurangi risiko serangan siber. Metode yang digunakan dalam kegiatan ini meliputi sosialisasi, pelatihan interaktif, serta simulasi ancaman siber untuk mengidentifikasi pola serangan dan langkah mitigasinya. Evaluasi dilakukan melalui pre-test dan post-test guna mengukur peningkatan pemahaman peserta. Hasil dari kegiatan ini menunjukkan bahwa terjadi peningkatan kesadaran dan kemampuan karyawan dalam mengenali serta mencegah ancaman siber. Dengan demikian, diharapkan PT. Wijaya Kesuma Segara dapat menerapkan kebijakan keamanan informasi yang lebih baik dan mengurangi risiko serangan siber yang dapat merugikan perusahaan.

***Kata kunci**: Keamanan Informasi, Kesadaran Siber, Pelatihan, Ancaman Siber.*

Abstract

In the growing digital era, cyber threats are a significant risk for companies, including PT Wijaya Kesuma Segara. Many cyber attacks occur due to a lack of employee understanding and awareness of information security, such as phishing, malware, and data leakage. Therefore, this community service activity aims to increase employee awareness and understanding of information security to reduce the risk of cyber attacks. The methods used in this activity include socialization, interactive training, and cyber threat simulations to identify attack patterns and mitigation steps. Evaluation was conducted through pre-test and post-test to measure the improvement of participants' understanding. The results of this activity show that there is an increase in employee awareness and ability to recognize and prevent cyber threats. Thus, it is expected that PT Wijaya Kesuma Segara can implement better information security policies and reduce the risk of cyber attacks that can harm the company.

***Keywords**: Information Security, Cyber Awareness, Training, Cyber Threats.*

1. PENDAHULUAN

Di era digital yang semakin maju, keamanan informasi menjadi aspek krusial dalam keberlangsungan operasional sebuah perusahaan. [1] PT. Wijaya Kesuma Segara, sebagai salah satu perusahaan yang mengandalkan sistem digital dalam kegiatan bisnisnya, menghadapi tantangan besar dalam melindungi data dan sistem dari berbagai ancaman siber, seperti phishing, malware, serangan ransomware, serta kebocoran data akibat kelalaian manusia. Serangan siber tidak hanya dapat mengakibatkan kerugian finansial, tetapi juga dapat merusak reputasi perusahaan dan menurunkan kepercayaan pelanggan.[2]

Berdasarkan berbagai penelitian, salah satu penyebab utama terjadinya serangan siber adalah kurangnya kesadaran dan pemahaman karyawan terhadap pentingnya keamanan informasi. [3] Banyak kasus pelanggaran keamanan terjadi akibat kelalaian individu, seperti penggunaan kata sandi yang lemah, mengakses situs tidak aman, atau tidak mengenali email

berbahaya yang berisi phishing. [4] Oleh karena itu, upaya peningkatan kesadaran keamanan informasi bagi karyawan menjadi langkah strategis dalam mencegah serangan siber dan menjaga integritas data perusahaan. [5]

Sebagai bentuk kontribusi akademisi dalam upaya peningkatan literasi digital dan keamanan informasi, kegiatan pengabdian masyarakat ini bertujuan untuk memberikan pelatihan kepada karyawan PT. Wijaya Kesuma Segara mengenai pentingnya keamanan informasi dan langkah-langkah yang dapat dilakukan untuk melindungi data perusahaan. Pelatihan ini akan mencakup pemahaman dasar tentang ancaman siber, praktik terbaik dalam pengelolaan informasi, serta simulasi kasus nyata untuk meningkatkan kesiapan karyawan dalam menghadapi potensi serangan siber. [6]

Diharapkan melalui kegiatan ini, karyawan PT. Wijaya Kesuma Segara dapat memiliki pemahaman yang lebih baik mengenai keamanan informasi serta mampu menerapkan langkah-langkah mitigasi risiko secara proaktif. Dengan demikian, perusahaan dapat membangun budaya keamanan siber yang lebih kuat dan mengurangi potensi ancaman terhadap sistem digital yang digunakan dalam operasional bisnisnya. [7]

2. METODE

Kegiatan pengabdian masyarakat ini dilaksanakan melalui beberapa tahapan strategis guna memastikan efektivitas pelatihan dalam meningkatkan kesadaran keamanan informasi bagi karyawan PT. Wijaya Kesuma Segara. Adapun metode pelaksanaan yang diterapkan meliputi perencanaan, pelaksanaan, serta evaluasi hasil pelatihan.

1. Tahap Perencanaan

Pada tahap ini, dilakukan analisis kebutuhan pelatihan berdasarkan kondisi perusahaan dan tingkat pemahaman karyawan terhadap keamanan informasi. Data dikumpulkan melalui survei awal dan wawancara dengan pihak manajemen guna mengidentifikasi potensi risiko siber yang sering terjadi di lingkungan kerja. Selain itu, dilakukan penyusunan materi pelatihan yang mencakup aspek fundamental keamanan informasi, jenis-jenis ancaman siber, teknik pencegahan, serta studi kasus terkait serangan siber yang relevan dengan sektor industri perusahaan.

2. Tahap Pelaksanaan Pelatihan

Pelatihan dilaksanakan secara interaktif melalui beberapa pendekatan, yaitu:

a. Sesi Sosialisasi dan Presentasi: Penyampaian materi mengenai dasar-dasar keamanan informasi, ancaman siber yang umum terjadi, serta langkah-langkah mitigasi risiko.

b. Workshop dan Simulasi Keamanan Siber: Karyawan akan diberikan pelatihan berbasis praktik untuk mengidentifikasi email phishing, penggunaan kata sandi yang kuat, serta simulasi serangan sosial (social engineering) guna meningkatkan kewaspadaan terhadap ancaman siber.

c. Diskusi dan Tanya Jawab: Memberikan ruang bagi peserta untuk berbagi pengalaman serta mendiskusikan tantangan yang mereka hadapi terkait keamanan informasi di lingkungan kerja mereka.

3. Tahap Evaluasi dan Tindak Lanjut

Untuk mengukur efektivitas pelatihan, dilakukan pre-test sebelum pelatihan dan post-test setelah pelatihan guna menilai peningkatan pemahaman peserta. Selain itu, peserta akan diberikan studi kasus untuk menguji kemampuan mereka dalam mengidentifikasi dan menanggapi ancaman siber secara tepat. Sebagai tindak lanjut, perusahaan akan diberikan rekomendasi kebijakan terkait penguatan keamanan informasi, seperti penerapan autentikasi dua faktor (2FA), regulasi penggunaan perangkat kerja, serta kebijakan akses data yang lebih aman.

Melalui metode ini, diharapkan karyawan PT. Wijaya Kesuma Segara dapat memiliki kesadaran yang lebih tinggi terhadap pentingnya keamanan informasi serta mampu menerapkan

langkah-langkah preventif dalam aktivitas kerja sehari-hari, sehingga dapat mengurangi potensi ancaman siber terhadap perusahaan.

3. HASIL DAN PEMBAHASAN

Kegiatan pelatihan kesadaran keamanan informasi bagi karyawan PT. Wijaya Kesuma Segara telah dilaksanakan sesuai dengan metode yang dirancang. Pelatihan ini diikuti oleh 50 orang karyawan dari berbagai divisi yang memiliki akses terhadap sistem informasi perusahaan. Hasil pelatihan ini dapat dilihat dari beberapa aspek utama:

1. Peningkatan Pemahaman Keamanan Informasi

Hasil pre-test menunjukkan bahwa mayoritas peserta memiliki pemahaman yang masih terbatas mengenai ancaman siber, dengan skor rata-rata (nilai pre-test). Setelah sesi pelatihan dan simulasi, hasil post-test menunjukkan peningkatan signifikan, dengan rata-rata skor mencapai (nilai post-test). Peningkatan pemahaman terutama terlihat dalam aspek mengenali email phishing, penggunaan kata sandi yang kuat, dan kesadaran terhadap social engineering.

Tabel 1. Perbandingan Hasil Pre-Test dan Post-Test

No	Aspek yang Dinilai	Rata-rata Pre-Test (%)	Rata-rata Post-Test (%)	Peningkatan (%)
1	Pemahaman tentang ancaman siber (phishing, malware, ransomware)	55%	85%	**30%**
2	Kemampuan mengenali email phishing	50%	88%	**38%**
3	Kesadaran akan pentingnya kata sandi yang kuat	60%	90%	**30%**
4	Pemahaman tentang social engineering	45%	83%	**38%**
5	Pemahaman tentang enkripsi data dan akses aman	40%	80%	**40%**
6	Kepatuhan terhadap kebijakan keamanan informasi	58%	87%	**29%**

Dari tabel di atas, terlihat adanya peningkatan signifikan dalam pemahaman dan kesadaran karyawan terhadap keamanan informasi setelah mengikuti pelatihan. Aspek dengan peningkatan tertinggi adalah pemahaman tentang enkripsi data dan akses aman (+40%) serta kemampuan mengenali email phishing (+38%). Hasil ini menunjukkan bahwa metode pelatihan yang diterapkan efektif dalam meningkatkan kesadaran keamanan siber di lingkungan kerja PT. Wijaya Kesuma Segara.

2. Efektivitas Simulasi dan Studi Kasus

Dalam sesi simulasi, peserta diberikan berbagai skenario serangan siber, seperti email phishing dan akses tidak sah terhadap sistem perusahaan. 66.6% peserta berhasil mengidentifikasi email phishing dengan benar setelah mengikuti pelatihan. Studi kasus yang diberikan juga membantu peserta memahami risiko keamanan informasi yang sering terjadi dalam operasional perusahaan.

JIPITI: Jurnal Pengabdian kepada Masyarakat
Vol. 2, No. 1, Februari 2025, pp. 50~55
ISSN: 3063-573X (Media Online)

3. Perubahan Perilaku Karyawan dalam Mengelola Keamanan Informasi

Sebelum pelatihan, banyak peserta menggunakan kata sandi yang mudah ditebak dan tidak mengganti kata sandi secara berkala. Setelah pelatihan, lebih dari 60% peserta mulai menerapkan praktik keamanan seperti penggunaan autentikasi dua faktor (2FA), menghindari akses ke situs tidak terpercaya, dan meningkatkan kehati-hatian dalam membuka email dari sumber yang tidak dikenal.

Pelatihan ini memberikan dampak positif bagi perusahaan dalam meningkatkan kesadaran keamanan informasi di lingkungan kerja. Beberapa perubahan yang mulai diterapkan setelah pelatihan, antara lain:

1. Penerapan Kebijakan Keamanan Informasi

Manajemen perusahaan mulai mempertimbangkan penerapan kebijakan keamanan siber yang lebih ketat, seperti regulasi penggunaan perangkat kerja, akses data terbatas, serta penyuluhan keamanan secara berkala.

2. Meningkatnya Budaya Keamanan Siber di Perusahaan

Kesadaran akan pentingnya keamanan informasi tidak hanya diterapkan oleh tim IT, tetapi juga oleh seluruh karyawan. Hal ini berkontribusi dalam mengurangi risiko serangan siber di masa mendatang.

3. Pengurangan Risiko Ancaman Siber

Dengan meningkatnya kesadaran dan pemahaman karyawan, risiko terjadinya insiden keamanan informasi di PT. Wijaya Kesuma Segara dapat ditekan.

Gambar 1. Dokumentasi Hasil Kegiatan Pengabdian

4. KESIMPULAN

Pelaksanaan kegiatan pengabdian masyarakat dengan judul "Pelatihan Kesadaran Keamanan Informasi bagi Karyawan PT. Wijaya Kesuma Segara untuk Mencegah Ancaman Siber" telah berhasil meningkatkan pemahaman dan kesadaran peserta terhadap pentingnya keamanan informasi. Berdasarkan hasil evaluasi pre-test dan post-test, terjadi peningkatan pemahaman rata-rata sebesar 34.17%, dengan tingkat keberhasilan pelatihan mencapai 66.6%. Pelatihan ini memberikan dampak positif, terutama dalam beberapa aspek utama, seperti:

1. Peningkatan Kesadaran Keamanan Siber : Peserta lebih memahami jenis-jenis ancaman siber, seperti phishing, malware, ransomware, dan social engineering.
2. Kemampuan Mengidentifikasi Ancaman – Setelah pelatihan, karyawan lebih waspada terhadap potensi serangan siber, terutama dalam mengenali email phishing dan penggunaan kata sandi yang lebih aman.
3. Perubahan Perilaku dalam Keamanan Informasi : Banyak peserta mulai menerapkan praktik keamanan yang lebih baik, seperti penggunaan autentikasi dua faktor (2FA) dan meningkatkan kepatuhan terhadap kebijakan keamanan perusahaan.
4. Dukungan terhadap Kebijakan Keamanan Perusahaan : Pelatihan ini mendorong PT. Wijaya Kesuma Segara untuk lebih memperhatikan penerapan kebijakan keamanan informasi yang lebih ketat dan berkelanjutan.
5. Meskipun pelatihan ini berjalan dengan baik, terdapat beberapa tantangan yang perlu diperhatikan, seperti rendahnya kesadaran awal karyawan dan perlunya pelatihan berkelanjutan agar pemahaman keamanan siber tetap terjaga seiring dengan perkembangan teknologi dan ancaman baru. Oleh karena itu, direkomendasikan agar pelatihan ini dilakukan secara berkala, didukung dengan kebijakan keamanan yang lebih ketat, serta penyediaan modul pembelajaran digital untuk memperkuat kesadaran keamanan informasi di lingkungan kerja.

Dengan adanya kesadaran yang lebih tinggi dan dukungan kebijakan yang tepat, PT. Wijaya Kesuma Segara diharapkan dapat mengurangi risiko ancaman siber, menjaga keamanan data perusahaan, serta menciptakan lingkungan kerja yang lebih aman di era digital.

DAFTAR PUSTAKA

[1] F. Anita and K. Tanujaya, “Pengaruh Kejahatan Siber terhadap Kinerja Organisasi dengan Moderasi Kesadaran Keamanan Informasi di Sektor Perbankan Kota Batam,” *Jurnal Ekuilnomi*, vol. 5, no. 2, pp. 266–275, Nov. 2023, doi: 10.36985/CT1N3819.

[2] A. A. Nasution *et al.*, “Analisis Keamanan Informasi dalam Sistem Informasi Manajemen: Tantangan dan Solusi di Era Cybersecurity,” *Journal Of Informatics And Busisnes* , vol. 2, no. 2, pp. 168–170, Jul. 2024, Accessed: Feb. 18, 2025. [Online]. Available: https://jurnal.ittc.web.id/index.php/jibs/article/view/1215

[3] E. Susanto *et al.*, “Analisis Keamanan Informasi PT. Indofood Sukses Makmur, Tbk : Studi Kasus tentang Peran Objek Vital, Pengamanan File, dan Pengamanan Cyber,” *Jurnal Manajemen dan Ekonomi Kreatif*, vol. 1, no. 3, pp. 79–87, Jun. 2023, doi: 10.59024/JUMEK.V1I3.116.

[4] E. Susanto, DenyaSaputri, D. A. Prasetya, I. Arbatona, J. C. Marpaung5, and S. H. Rahadian, “Pengamanan Objek Vital, Keamanan File, Dan Keamanan Cyber Pada Pt Pos Indonesia,” *Jurnal Mutiara Ilmu Akuntansi*, vol. 1, no. 3, pp. 163–174, Jun. 2023, doi: 10.55606/JUMIA.V1I3.1516.

[5] T. G. Laksana and S. Mulyani, “Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan,” *Jurnal Ilmiah Multidisiplin*, vol. 3, no. 01, pp. 109–122, Jan. 2024, doi: 10.56127/JUKIM.V3I01.1143.

[6] A. Z. Kamalia, H. R. Herlianto, Z. Rozikin, and A. Suwarno, "Pelatihan Cyber Security untuk Perlindungan Data dan Privasi Pada Karyawan PT CKD Manufacturing Indonesia," *Madaniya*, vol. 5, no. 3, pp. 1181–1186, Aug. 2024, doi: 10.53696/27214834.905.

[7] "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity | Jurnal Sains dan Teknologi." Accessed: Feb. 18, 2025. [Online]. Available: https://ejournal.sisfokomtek.org/index.php/saintek/article/view/2347