Vol. 14 No. 1, hal. 219 - 227
pISSN: 2302-3937 eISSN: 2745-4223
url. https://jurnal.uns.ac.id/jurnal-semar/article/view/99770
DOI. https://doi.org/10.20961/semar.v14i1.99770

Pelatihan Keamanan Siber Sebagai Pengetahuan Dasar Keamanan Untuk Peningkatan *Security Awarness*

Winarno*, Wiranto, Bambang Harjito, Heri Prasetyo, Sari Widya Sihwi
Informatika, Fakultas Teknologi Informasi dan Sains Data, Universitas Sebelas Maret, Indonesia
*Email : win@staff.uns.ac.id

Submitted: 22 Februari 2025, Revised: 23 April 2025, Accepted: 28 April 2025, Published: 1 Mei 2025

Abstrak

Dalam beberapa tahun terakhir di tahun 2024 banyak terjadi insiden keamanan, baik kebocoran, *hacking*, *defacing* dan lain-lainnya. Hal ini terjadi dikarenakan masyarakat di Indonesia banyak yang kurang akan *security awarness*. Kesadaran keamanan siber yang masih kurang ini menjadi permasalahan serius. Seperti yang disampaikan oleh Bapak Sandi Indonesia yaitu ingatlah bahwa kekhilafan satu orang saja cukup sudah menyebabkan keruntuhan negara. Hal tersebut juga terjadi di Lembaga pemerintah, banyak organisasi perangkat daerah yang portal websitenya terkena *defacing*. Hampir 90% website pemerintah daerah kabupaten/kota di Jawa Tengah terkena defacing. Oleh karena itu karena pentingnya hal tersebut, sebagai solusi untuk peningkatannya adalah menyelenggarakan pelatihan *cyber security*. Dalam pelaksanaan kegiatan ini menggandeng beberapa lembaga dalam negeri dan luar negeri yaitu Diskominfo SP Kota Surakarta, UPTD Solo Technopark dan Rapixus. Inc. Taiwan. Pelatihan meliputi pemberian teori dasar mengenai *cyber security* dan praktik melakukan penetrasi, *attack* dan menanggulangi serangan. Hasil dari pelatihan ini didapat bahwa 87,9% peserta mendapatkan kebaruan pengetahuan, 87,9% mendapatkan kemanfaatan dan 61,4% peserta merasakan kemudahan menerima materi.

Kata kunci : keamanan siber, pelatihan, *security awarness*, insiden keamanan

Abstract

In recent years, specifically in 2024, there has been a notable increase in security incidents, encompassing breaches, hacking, defacements, and various other forms of cyberattacks. This phenomenon can be attributed to a significant deficiency in security awareness among the populace in Indonesia. Such a lack of cybersecurity awareness constitutes a critical issue of considerable magnitude. As articulated by Mr. Sandi Indonesia, it is imperative to recognize that the error of a singular individual can precipitate the downfall of an entire nation. This predicament is also prevalent within governmental entities, where numerous regional apparatus organizations have experienced the defacement of their website portals. Alarmingly, nearly 90% of district and city government websites in Central Java have been subjected to defacement. Consequently, in light of the gravity of this situation, a viable solution to ameliorate it involves implementing cybersecurity training programs. The execution of this initiative involves collaboration with several domestic and international institutions, including Diskominfo SP Surakarta City, UPTD Solo Technopark, and Rapixus, Inc., Taiwan. The training curriculum encompasses the dissemination of foundational theories about cybersecurity, alongside practical exercises involving penetration testing, attack simulations, and countermeasures against such attacks. The outcomes of this training indicated that 87.9% of participants acquired new knowledge, 87.9% perceived the training as beneficial, and 61.4% reported an ease of comprehension regarding the material presented.

Keyword : *cybersecurity, training, security awareness, security incidents*

Cite this as: Rinanto Y., Winarno W., Wiranto W., Harjito B., Prasetyo H., Sihwi S W., 2025. Pelatihan Keamanan Siber Sebagai Pengetahuan Dasar Keamanan Untuk Peningkatan Security Awarness. *Jurnal SEMAR (Jurnal Ilmu Pengetahuan, Teknologi, dan Seni bagi Masyarakat), 14*(1). 219-227. doi: https://doi.org/10.20961/semar.v14i1.99770

Pendahuluan

Keamanan siber telah muncul sebagai perhatian kritis dalam ekosistem digital kontemporer, ditandai dengan eskalasi frekuensi dan kecanggihan ancaman *cyber*. Entitas di berbagai sektor mengakui keharusan untuk mengalokasikan sumber daya ke inisiatif keamanan siber untuk melindungi aset digital mereka dan mempertahankan ketahanan operasional. Komitmen ini tidak hanya di bagian aset atau keuangan saja, namun juga mencakup spektrum kegiatan yang luas, termasuk penyebaran teknologi keamanan canggih, perumusan kebijakan keamanan yang kuat, dan penyediaan pelatihan karyawan yang bertujuan untuk meningkatkan kesadaran keamanan siber dan mempromosikan praktik baik (Rattanapong and Ayuthaya, 2025). Menurut Khaw et al (2024), perumusan kebijakan keamanan siber yang kuat sangat penting untuk mengurangi kerentanan yang teridentifikasi dan untuk memastikan sinkronisasi mereka dengan tujuan menyeluruh organisasi. Kebijakan ini berfungsi sebagai kerangka dasar untuk pelestarian keamanan sistem dan perlindungan informasi rahasia.

Program pelatihan sangat penting dalam meningkatkan budaya keamanan siber dalam organisasi. Irwandy et. al (2024) menekankan perlunya inisiatif pelatihan ekstensif yang menargetkan kekurangan pengetahuan di antara karyawan, terutama di industri seperti perawatan kesehatan, di mana personel sering merupakan penghubung paling rentan dalam perlindungan keamanan siber. Pembentukan protokol keamanan siber yang eksplisit dan dapat ditegakkan, dalam hubungannya dengan budaya kesadaran keamanan yang kuat, sangat penting untuk mitigasi risiko yang efektif.

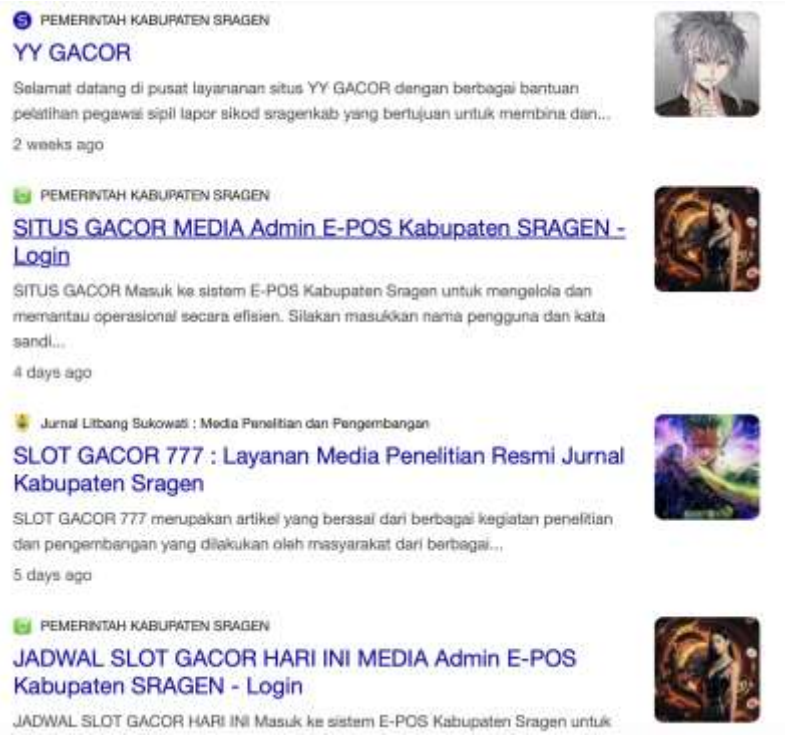
Selain itu, pembentukan kerangka pelatihan keamanan siber yang komprehensif, seperti yang dianjurkan oleh Nair (2023) memiliki potensi untuk secara nyata meningkatkan kesadaran dan kesiapan di antara personel. Kerangka kerja ini harus sesuai dengan standar yang diakui, termasuk yang ditetapkan oleh National Institute of Standards and Technology (NIST), untuk menjamin kemanjurannya.

Selain itu, pentingnya memahami dan mengatasi ancaman keamanan siber sangat penting. Disarankan agar organisasi menerapkan kerangka kerja manajemen risiko yang mencakup proses identifikasi, evaluasi, dan pengurangan kerentanan keamanan (Sun *et al.*, 2022). Metodologi antisipatif ini sangat penting untuk tujuan kesiapan, pengamanan, dan reaksi terhadap ancaman cyber. Pentingnya faktor manusia dalam domain keamanan siber sama pentingnya, seperti yang sampaikan oleh Dikito et al. (2024), yang menggambarkan kesadaran, dukungan manajerial, dan penyebaran informasi sebagai komponen penting yang mempengaruhi kemanjuran langkah-langkah keamanan siber. Mitigasi faktor manusia ini melalui program pendidikan khusus dan kampanye kesadaran memiliki potensi untuk meningkatkan kerangka kerja keamanan siber yang komprehensif dari institusi.

Keharusan untuk peningkatan berkelanjutan dalam metodologi keamanan siber lebih lanjut ditekankan oleh penelitian yang dilakukan oleh Neri et al. (2024), yang menunjukkan bahwa terlepas dari kemajuan dalam dimensi teknis, kekurangan substansial dalam kesiapan organisasi tetap ada. Ini menggarisbawahi perlunya pendidikan dan pelatihan berkelanjutan untuk menumbuhkan lingkungan yang kondusif bagi kesadaran keamanan siber (Neri, Niccolini and Martino, 2024).

Pemerintah daerah saat ini masih banyak hal yang harus dibenahi, terutama mengenai keamanan siber. Banyak portal pemerintah daerah yang mengalami serangan siber pada tahun 2024 seperti terlihat pada Gambar 1. Hal ini dikarenakan belum banyak pemerintah daerah yang menguasai bagaimana cara kerja serangan siber dan menjaga

untuk menghindari serangan siber. Di sekitar wilayah karesidenan Surakarta masih terdapat banyak kasus serangan siber. Di Pemerintah Kota Surakarta pada tahun 2024 sering terjadi serangan siber seperti yang disampaikan oleh Kepala Dinas Komunikasi, Informasi, Statistik dan Persandian Kota Surakarta dalam acara pembukaan pelatihan *cyber security* di Solo Technopark. Dalam pengabdian ini dilakukan beberapa pelatihan yang terkait dengan cara kerja serangan siber dan bagaimana menghindari serangan-serangan tersebut.



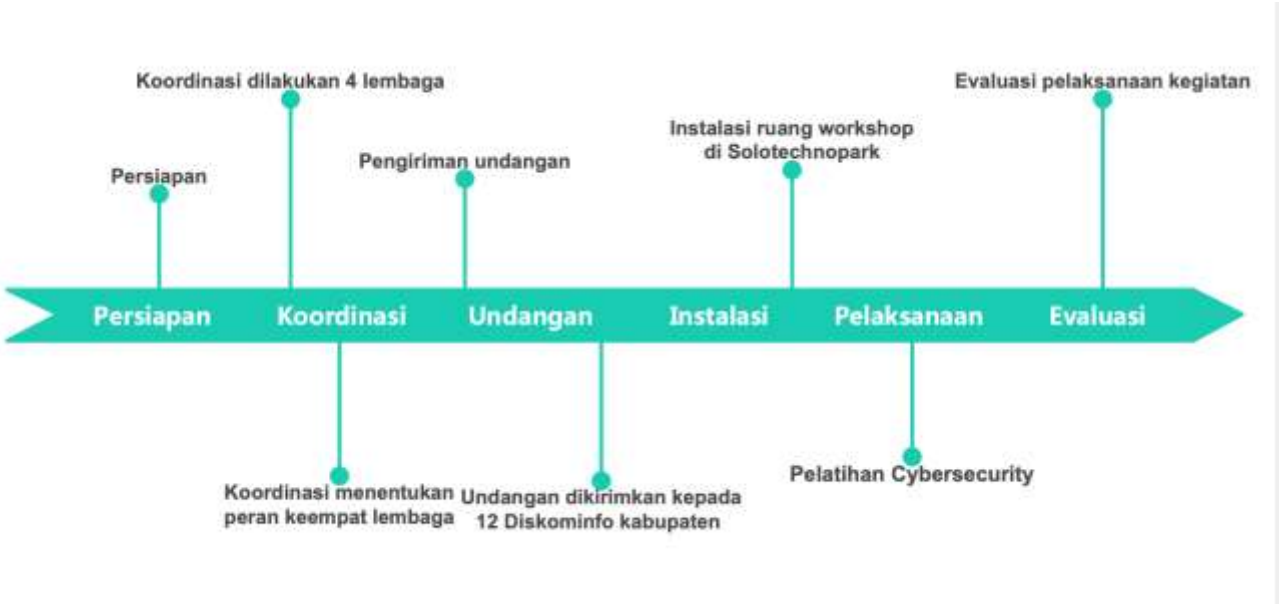
Gambar 1. Laman Website Pemerintah Daerah yang Terkena *Hacking*

.

Metode Pelaksanaan

Kegiatan ini dilakukan dengan metode seperti Gambar 2. Dari setiap tahapan tersebut membutuhkan beberapa peralatan dan bahan seperti alat tulis kantor, komputer klien, komputer *server* target, *virtual machine*, Kali Linux OS dan Windows OS. Urutan kegiatan ini dijelaskan sebagai berikut ini

1. Persiapan: merupakan kegiatan yang dilakukan untuk mempersiapkan kegiatan ini dengan menggandeng empat lembaga yaitu Universitas Sebelas Maret, Dinas Komunikasi, Informasi, Statistik dan Persandian, Solo Technopark dan Rapixus. Inc.
2. Koordinasi: merupakan kegiatan mensikronkan empat lembaga dengan membagi peran apa saja yang menjadi hak dan tanggung jawab. Hal ini dilakukan karena koordinasi mampu meningkatkan sinergi antar anggota, meningkatkan pengelolaan sumber daya, meningkatkan transparansi, pengambilan Keputusan lebih baik dan peningkatan kinerja(Chang, Lee and Leu, 2011; Dietrich, Kujala and Artto, 2013; Braka *et al.*, 2023; Panday, Wang and Spasova, 2023; Mojidra *et al.*, no date).
3. Undangan: merupakan kegiatan mengundang lembaga Dinas Komunikasi dan Informasi dari 12 kabupaten kota di sekitar karesidenan Surakarta. Walaupun perkembangan teknologi undangan dapat dikirimkan melalui email hal ini dikarenakan undangan memberikan perhatian besar, mampu membangun kepercayaan, membangun komunikasi efektif, dan mampu meningkatkan partisipasi (Tinmouth *et al.*, 2014; Senore *et al.*, 2015; Twenge, Spitzberg and Campbell, 2019; Dahl *et al.*, 2021).



Gambar 2. Metode Pelaksanaan Pengabdian

4. Instalasi: merupakan kegiatan mempersiapkan computer klien dan server dengan instalasi beberapa software yaitu virtual machine versi 10, Kali Linux. Dipilih Kali Linux karena merupakan sistem terintegrasi dengan alat penetrasi, memiliki komunitas dukungan yang besar, lebih fleksibel, mendukung berbagai macam pengujian (Hassan, Muzaffar and Ahmad, 2021; Lu and Yu, 2021; Akhtar and Rawol, 2024; Ritzkal *et al.*, 2024).
5. Pelatihan: merupakan kegiatan inti yang berupa penjelasan dan praktik menggunakan komputer klien dan mengelola server, menggunakan Kali Linux dan computer klien.
6. Evaluasi: merupakan kegiatan mengukur efektivitas kegiatan dengan melakukan penyebaran kuesioner dan mengolah data yang diolah dengan Microsoft Excel dan dianalisis. Evaluasi dilakukan dengan alasan karena mampu mengidentifikasi capaian, sebagai bukti pengambilan keputusan program selanjutnya, memberikan kontribusi positif terhadap akuntabilitas, dan mampu memberikan pembelajaran dari pengalaman (Hemingway, Douville and Fierro, 2022; Maccalla *et al.*, 2022; Da Silva, Sá Guerreiro and Malta, 2023; Milosek, Eady and Moreau, 2023).

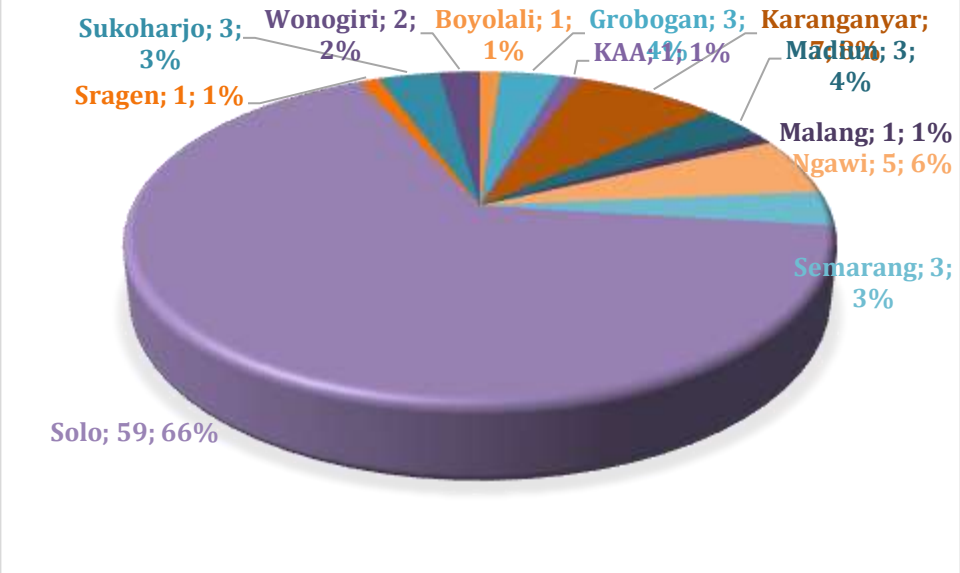
.

Hasil Dan Pembahasan

Pelaksanaan kegiatan dilaksanakan sebanyak tiga batch secara bertahap yaitu pada tanggal 21-22 Juni 2024, 28-29 Juni 2024 dan 5-6 Juli 2024. Untuk persiapan kegiatan tersebut dilakukan beberapa hal yaitu membuat memorandum of aggreement(MoA). Lembaga yang terlibat dalam kegiatan ini tidak hanya melibatkan lembaga dari dalam negeri namun juga melibatkan sebuah perusahaan dari Taiwan yaitu Rapixus, Inc. Lembaga kedua adalah Dinas Komunikasi, Informasi, Statistik dan Persandian Kota Surakarta, UPTD Kawasan Sains dan Teknologi Solo Techno Park. Peserta yang diundang berasal dari 2 perwakilan staff dari Dinas Komunikasi dan Informatika 15 kabupaten/kota, mahasiswa dan masyarakat umum.

Tabel I. Distribusi Asal Peserta Pelatihan

Asal Daerah	**Jumlah**
Boyolali	1
Grobogan	3
KAA	1
Karanganyar	7
Madiun	3
Malang	1
Ngawi	5
Semarang	3
Solo	59
Sragen	1
Sukoharjo	3
Wonogiri	2
Total	89



Gambar 1. Peta Sebaran Distribusi Peserta

Rekapitulasi pendaftaran seperti pada Tabel 1 dan Gambar 1. Sebagian besar peserta berasar dari Kota Surakarta. Pendaftaran dibuka dengan mengirimkan undangan kepada 15 Dinas kabupaten/kota dan menyampaikan dalam sosial media di beberapa instansi salah satunya adalah Solo Techno Park. Pendaftaran dilakukan dengan pengisian online pada formulir yang sudah disiapkan. Dari 89 peserta yang mengisi pendaftaran, jumlah peserta yang hadir sebanya 83 orang, sehingga terdapat 6 orang yang tidak hadir membatalkan kepesertaanya.

Secara umum peserta yang paling banyak adalah dari staff Diskominfo perwakilan kabupaten/kota, selanjutnya diikuti oleh mahasiswa dan yang paling sedikit adalah dari masyarakat umum. Pelaksanaan kegiatan dibuka oleh Dekan Fakultas Teknologi Informasi dan Sains Data (Fatisda) dan dihadiri oleh Kepala Dinas Komunikasi, Informasi, Statistik dan Persandian Kota Surakarta seperti terlihat di Gambar 2. Untuk pelaksanaan pelatihan diawali dengan penjelasan materi teori oleh Winarno, S.Si., M.Eng dari Informatika , dilanjutkan dengan praktik oleh Bagus

Setiawan, S.Si. dan diakhiri oleh Ievan Anthonio Thonka dari Rapixus, Inc. Taiwan. Pelaksanaan seperti terlihat di Gambar 3.

Tabel 2.Rekapitulasi Peserta Pelatihan Keamanan Siber

Batch	Hari 1			Hari 2		
	Staff	Mahasiswa	Umum	Staff	Mahasiswa	Umum
Batch 1	31	2	0	24	2	0
Batch 2	0	30	0	0	26	0
Batch 3	14	9	6	12	7	4
Total	44	41	6	36	35	4

Gambar 2. Pembukaan Pelatihan *Cyber Security*

Gambar 3. Pelaksanaan Pelatihan *Cyber Security*

Pelatihan diberikan di ruang *Cyber Security* hub di Solo Technopark Kota Surakarta. Materi yang diberikan berupa materi teori dasar mengenai dasar keamanan siber, sumber-sumber kerentanan, motivasi serangan siber, jenis-jenis serangan, cara menghindari serangan siber dan perkembangan serangan di era *artificial intelligence*. Materi praktik peserta diberikan materi simulasi menggunakan komputer dengan sistem operasi Kali Linux. Untuk materi praktik meliputi proses *penetration testing* dalam website, *penetration testing* dalam *database*, *brute force password* aplikasi dan *brute force* akses WIFI. Semua kegiatan praktik dilakukan secara langsung dalam pelatihan dengan

menggunakan komputer yang disediakan oleh Solo Technopark. Hari kedua kegiatan pelatihan dengan materi infrastructure asset management(ITAM) yang meliputi pengenalan dasar *software Vans*, instalasi server *Vans*, instalasi agent pada komputer *client*, manajemen dan monitoring aset elektronik. Setelah pelatihan peserta diberikan pertanyaan evaluasi mengenai pelaksanaan pelatihan dengan jawaban berupa pilihan sangat tidak setuju (STS), tidak setuju (TS), agak setuju (AS), setuju (S), sangat setuju (SS). Hasil kuesioner disajikan dalam uraian di bawah ini.

Tabel 3. Hasil Kuesioner Peserta Dalam Hal Pengetahuan Baru

Jenis Kepesertaan	AS	S	SS	Total
Mahasiswa: 21-22 Mei 2024	4	8	23	35
Staff Pemerintah Daerah: 28-29 Mei 2024	5	8	13	26
Umum: 5-6 Juni 2024	1	6	15	22
Total	10	22	51	83

Dari Tabel 3 didapat informasi bahwa dari 83 peserta sebanyak 51 orang (61,4%) sangat setuju bahwa pelatihan ini memberikan pengetahuan baru bagi mereka. Sedangkan untuk yang setuju sebanyak 22 orang (26,5%) bahwa pelatihan ini memberikan pengetahuan baru dan hanya 12,1% saja yang menjawab agak setuju. Hal ini berarti 87,9% peserta setuju bahwa kegiatan ini mampu meningkatkan pengetahuan dan wawasan peserta.

Tabel 4. Hasil Kuesioner Kemudahan Materi Diterima

Jenis Kepesertaan	TS	AS	S	SS	Total
Mahasiswa	2	15	10	8	35
Staff Pemerintah Daerah	3	6	8	9	26
Umum		6	10	6	22
Grand Total	5	27	28	23	83

Dari Tabel 4 didapat informasi bahwa bahwa dari 83 peserta terdapat 23 orang (27,7%) yang sangat setuju jika materi mudah diterima. Untuk yang setuju bahwa materi pelatihan mudah diterima sebanyak 28 orang (33,7%), kemudian 27 orang (32.5%) agak setuju jika materi pelatihan mudan diterima dan 5 orang (6%) menganggap bahwa materi sulit diterima. Terkait dengan kemanfaatan pelatihan disajikan dalam Tabel IV. Sebanyak 43 orang (51,8%) sangat setuju bahwa kegiatan ini bermanfaat, kemudian 30 orang (36,1%) memberikan respon setuju jika kegiatan ini bermanfaat, sembilan orang (10,8%) agak setuju dan satu orang (1,2%) tidak setuju memberikan manfaat.

Tabel 5. Hasil Kuesioner Kemanfaatan Pelatihan

Jenis Kepesertaan	TS	AS	S	SS	Total
Mahasiswa	1	3	13	18	35
Staff Pemerintah Daerah		4	10	12	26
Umum		2	7	13	22
Total	1	9	30	43	83

Dari Tabel 5 didapat bahwa 43 orang (51,8%) peserta sangat setuju mendapatkan manfaat kegiatan, 30 orang (36,1%) peserta setuju bahwa kegiatan ini bermanfaat, sedangkan 9 orang (10,8%) agak setuju jika kegiatan ini bermanfaat dan 1 orang (1,2%) merasa tidak setuju jika bermanfaat.

Tabel 6. Rekapitulasi Hasil Kuesioner

Jenis	TS(%)	AS(%)	S(%)	SS(%)
Kebaruan pengetahuan	0	12,1	26,5	61,4
Kemudahan materi diterima	6	32,5	33,7	27,7
Kemanfaatan kegiatan	1,2	10,8	36,1	51,8

Secara umum hasil setuju dan sangat setuju jika dijumlahkan maka di atas 60% di semua aspek. Hal ini dapat simpulkan bahwa 87,9% peserta mendapatkan kebaruan pengetahuan 87,9% mendapatkan kemanfaatan dan 61,4% peserta merasakan kemudahan menerima materi.

Tabel 7. Indeks Kepuasan Peserta

Jenis Peserta	Indeks Kepuasan	Responden (orang)
Mahasiswa	4,543	35
Staff Pemerintah Daerah	4,308	26
Umum	4,636	22
Rerata	4.494	83

Dari pelaksanaan kegiatan pelatihan ini sebenarnya masih banyak materi yang perlu didalami, karena pelaksanaan kegiatan ini merupakan kegiatan pengenalan keamanan siber dasar. Dari cara penyajian dan penyelenggaraan yang sudah dilaksanakan banyak peserta yang tertarik untuk mengikuti kembali. Hasil survey terkait dengan hal ini dapat dilihat di Tabel 8.

Tabel 8. Ketertarikan Peserta Mengikuti Pelatihan Selanjutnya

Jenis Kepesertaan	Tidak tertarik	Belum pasti	Tertarik ikut	Total
Mahasiswa		9	26	35
Staff Pemerintah Daerah	1	3	22	26
Umum		1	21	22
Grand Total	1	13	69	83

Dari Tabel 8 dapat diketahui bahwa 69 orang (83.1%) tertarik untuk mengikuti pelatihan selanjutnya, sedangkan 13 orang (15,7%) belum pasti ikut dan satu orang (1,2%) tidak tertarik ikut lagi.

Kesimpulan

Dari uraian pembahasan di atas dapat disimpulkan bahwa kegiatan pelaksanaan pelatihan *cyber security* merupakan kegiatan yang masih jarang dilaksanakan sehingga banyak orang yang mencari dan ingin mengikutinya. Selanjutnya dari kegiatan ini 87,9% peserta mendapatkan kebaruan pengetahuan 87,9% mendapatkan kemanfaatan dan 61,4% peserta merasakan kemudahan menerima materi. Aspek dalam *transfer knowledge* ini menjadi aspek paling kecil mendapatkan respon, maka untuk penyelenggaraan selanjutnya dapat disarankan untuk meningkatkan terkait pemberian materi.

Ucapan Terima Kasih

Kegiatan ini dapat terselenggara dengan baik berkat pembiayaan dan dukungan dari Lembaga Penelitian dan Pengabdian kepada Masyarakat Universitas Sebelas Maret Tahun 2025.

Daftar Pustaka

Akhtar, Z.B. and Rawol, A.T. (2024) ‘Uncovering Cybersecurity Vulnerabilities: A Kali Linux Investigative Exploration Perspective’, *International Journal of Advanced Network, Monitoring and Controls*, 9(2), pp. 11–22. Available at: https://doi.org/10.2478/ijanmc-2024-0012.

Braka, F. *et al.* (2023) 'The role of polio emergency operations centers: perspectives for future disease control initiatives in Nigeria', *The Pan African Medical Journal*, 45. Available at: https://doi.org/10.11604/pamj.supp.2023.45.2.41308.

Chang, A.S., Lee, C.H. and Leu, W.H. (2011) 'Coordination Needs and Performance for Manufacturing Process Improvement Projects', *Advanced Materials Research*, 311–313, pp. 2239–2244. Available at: https://doi.org/10.4028/www.scientific.net/AMR.311-313.2239.

Da Silva, A.G., Sá Guerreiro, C. and Malta, D.C. (2023) 'Meta-evaluation of studies on community physical activity programs in Brazil', *The International Journal of Health Planning and Management*, 38(1), pp. 252–264. Available at: https://doi.org/10.1002/hpm.3585.

Dahl, M. *et al.* (2021) 'Involving people with type 2 diabetes in facilitating participation in a cardiovascular screening programme', *Health Expectations*, 24(3), pp. 880–891. Available at: https://doi.org/10.1111/hex.13228.

Dietrich, P., Kujala, J. and Artto, K. (2013) 'Inter-Team Coordination Patterns and Outcomes in Multi-Team Projects', *Project Management Journal*, 44(6), pp. 6–19. Available at: https://doi.org/10.1002/pmj.21377.

Dikito, A.R., Kaiser, M.S. and Vincent, J.P. (2024) 'Factors Influencing Cybersecurity: A Focus Group Approach', *International Journal of Academic Research in Progressive Education and Development*, 13(4), p. Pages 754-767. Available at: https://doi.org/10.6007/IJARPED/v13-i4/23539.

Hassan, S.Z. ul, Muzaffar, Z. and Ahmad, S.Z. (2021) 'Operating Systems for Ethical Hackers - A Platform Comparison of Kali Linux and Parrot OS', *International Journal of Advanced Trends in Computer Science and Engineering*, 10(3), pp. 2226–2233. Available at: https://doi.org/10.30534/ijatcse/2021/1041032021.

Hemingway, B.L., Douville, S. and Fierro, L.A. (2022) 'Aligning Public Health Training and Practice in Evaluation: Implications and Recommendations for Educators', *Pedagogy in Health Promotion*, 8(4), pp. 324–331. Available at: https://doi.org/10.1177/23733799211033621.

Irwandy, I. *et al.* (2024) 'Cybersecurity Culture Among Healthcare Workers in Indonesia: Knowledge Gaps, Demographic Influences, and Strategic Policy Solutions'. Available at: https://doi.org/10.21203/rs.3.rs-5421169/v1.

Khaw, T.Y., Amran, A. and Teoh, A.P. (2024) 'Building a thematic framework of cybersecurity: a systematic literature review approach', *Journal of Systems and Information Technology*, 26(2), pp. 234–256. Available at: https://doi.org/10.1108/JSIT-07-2023-0132.

Lu, H.-J. and Yu, Y. (2021) 'Research on WiFi Penetration Testing with Kali Linux', *Complexity*. Edited by M.I. Uddin, 2021(1), p. 5570001. Available at: https://doi.org/10.1155/2021/5570001.

Maccalla, N.M.G. *et al.* (2022) 'Gauging treatment impact: The development of exposure variables in a large-scale evaluation study', *New Directions for Evaluation*, 2022(174), pp. 57–68. Available at: https://doi.org/10.1002/ev.20509.

Milosek, J., Eady, K. and Moreau, K.A. (2023) 'Program Evaluation Activities in Competence by Design: A Survey of Specialty/Subspecialty Program Directors'. Available at: https://doi.org/10.21203/rs.3.rs-3369555/v1.

Mojidra, M. *et al.* (no date) 'The Impact of Stakeholder Communication and Coordination on Project Outcome – IJSREM'. Available at: https://ijsrem.com/download/the-impact-of-stakeholder-communication-and-coordination-on-project-outcome/ (Accessed: 21 February 2025).

Nair, P. (2023) 'Enhancing Cybersecurity Awareness Training through the NIST Framework', *IJARCCE*, 12(12). Available at: https://doi.org/10.17148/IJARCCE.2023.121203.

Neri, M., Niccolini, F. and Martino, L. (2024) 'Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment', *Information & Computer Security*, 32(1), pp. 38–52. Available at: https://doi.org/10.1108/ICS-05-2023-0084.

Panday, M.S., Wang, P.N. and Spasova, I.H. (2023) 'Participatory Project Planning and Performance of Donor Funded Projects in Khulna, Bangladesh', *Journal of Entrepreneurship & Project Management*, 7(5), pp. 1–11. Available at: https://doi.org/10.53819/81018102t5193.

Rattanapong, P. and Ayuthaya, S.D.N. (2025) 'Influential factors of cybersecurity investment: A quantitative SEM analysis', *Management Science Letters*, 15(1), pp. 31–44. Available at: https://doi.org/10.5267/j.msl.2024.3.005.

Ritzkal *et al.* (2024) 'Enhancing Cybersecurity Through Live Forensic Investigation of Remote Access Trojan Attacks using FTK Imager Software', *International Journal of Safety and Security Engineering*, 14(1), pp. 217–223. Available at: https://doi.org/10.18280/ijsse.140121.

Senore, C. *et al.* (2015) 'Optimising colorectal cancer screening acceptance: a review', *Gut*, 64(7), pp. 1158–1177. Available at: https://doi.org/10.1136/gutjnl-2014-308081.

Sun, N. *et al.* (2022) 'How Do Organizations Seek Cyber Assurance? Investigations on the Adoption of the Common Criteria and Beyond'. Available at: https://doi.org/10.48550/ARXIV.2203.01526.

Tinmouth, J. *et al.* (2014) 'Using physician-linked mailed invitations in an organised colorectal cancer screening programme: effectiveness and factors associated with response', *BMJ Open*, 4(3), p. e004494. Available at: https://doi.org/10.1136/bmjopen-2013-004494.

Twenge, J.M., Spitzberg, B.H. and Campbell, W.K. (2019) 'Less in-person social interaction with peers among U.S. adolescents in the 21st century and links to loneliness', *Journal of Social and Personal Relationships*, 36(6), pp. 1892–1913. Available at: https://doi.org/10.1177/0265407519836170.

