Indonesian Journal of Community Service and Innovation (IJCOSIN)
Vol. 4, No. 1, Januari 2024, Hal. 29-35
e-ISSN: 2807 - 6370
http://journal.ittelkom-pwt.ac.id/index.php/ijcosin

Peningkatan Kesadaran Keamanan Informasi Siswa SMK Telkom Purwokerto Melalui Pelatihan *Footprinting* dan *Reconnaissance*

Wahyu Adi Prabowo[1*], Rifki Adhitama[2], Auliya Burhanuddin[3], Paradise[4], Khusnul Fauziah[5], Aufa Salsabila Nahrowi[6]

Institut Teknologi Telkom Purwokerto, Jl DI Panjaitan 128 Purwokerto[123]
Email: wahyuadi@ittelkom-pwt.ac.id*

Received 06 Desember 2023, Revised 02 Januari 2024, Accepted 08 Januari 2024

ABSTRAK

Kegiatan pengabdian masyarakat ini bertujuan untuk mendalami konsep *footprinting* dan *reconnaissance* dalam *cybersecurity* dengan fokus pada siswa SMK Telkom Purwokerto. Dipandu oleh dosen dan mahasiswa, kegiatan ini bertujuan untuk meningkatkan pemahaman peserta didik tentang teknik analisis dan pengumpulan informasi awal yang vital dalam ranah keamanan siber. Metode pelaksanaan mencakup pembelajaran daring dan sesi praktik langsung di kelas, yang memungkinkan peserta untuk mampu mengimplementasikan konsep-konsep tersebut. Manfaat dari pelatihan ini mencakup peningkatan pemahaman tentang ancaman keamanan sistem, pengembangan keterampilan analisis teknis, dan kemampuan menerapkan langkah-langkah perlindungan yang lebih baik. Hasil pelaksanaan menunjukkan partisipasi aktif peserta dan peningkatan pemahaman siswa tentang pentingnya *footprinting dan reconnaissance* dalam mengelola risiko keamanan informasi. Terdapat peningkatan kesadaran sebesar 90% setelah peserta mengikuti pelatihan, menunjukkan dampak positif dari kegiatan ini terhadap pemahaman siswa tentang keamanan informasi. Dengan demikian, kegiatan ini tidak hanya mendukung tridharma perguruan tinggi, tetapi juga memperkuat hubungan antara Institut Teknologi Telkom Purwokerto dan masyarakat dalam meningkatkan keamanan siber di tingkat lokal.

Kata kunci: *footprinting, reconnaissance,* keamanan informasi, pendidikan keamanan siber.

ABSTRACT

The community service activity aims to delve into the concept of footprinting and reconnaissance in cybersecurity focusing on students at SMK Telkom Purwokerto. Guided by lecturers and students, the activity aims to enhance participants' understanding of vital early information analysis and gathering techniques in the realm of cybersecurity. Implementation methods include online learning and direct practical sessions in the classroom, enabling participants to implement these concepts. The training benefits encompass an improved understanding of system security threats, the development of technical analysis skills, and the ability to implement better protective measures. The results demonstrate active participation and an enhanced understanding of the importance of footprinting and reconnaissance in managing information security risks among the participants. There was a 90% increase in awareness after the participants underwent the training, indicating a positive impact of this activity on students' comprehension of information security. Therefore, this activity not only supports the tridharma of higher education but also strengthens the relationship between the Telkom Purwokerto Institute of Technology and the community in enhancing local cybersecurity.

Keywords : *footprinting, reconnaissance, information security, cybersecurity education.*

PENDAHULUAN

Keamanan informasi menjadi hal yang semakin krusial di era digital yang terus berkembang(Muni et al., 2023). Pemahaman mendalam terhadap teknik *footprinting* dan *reconnaissance* menjadi kunci penting dalam melindungi sistem informasi. *Footprinting*, sebagai langkah awal dalam penelusuran informasi (Alwi & Ilmawan, 2021), memungkinkan para profesional keamanan untuk memahami secara mendalam infrastruktur dan kerentanan yang mungkin dimanfaatkan oleh pihak yang tidak sah (Flores et al., 2016). Sementara itu, *Reconnaissance* memberikan pemahaman lebih lanjut melalui pengumpulan data menyeluruh, dengan menyertakan network scanning baik secara internal maupun eksternal yang bersumber dari internet dan sumber-sumber *offline* (Styugin, 2019). Tahapan awal dalam siklus serangan, seperti *footprinting, scanning,* dan *enumeration*, memegang peranan kritis dalam upaya mencegah serangan dari pihak yang tidak bermaksud baik. Oleh karena itu, upaya proaktif dalam memahami dan melindungi sistem informasi menjadi sangat penting (Sutejo et al., 2021). Masalah yang timbul dari kurangnya pemahaman mendalam terhadap teknik-teknik *footprinting* dan *reconnaissance* di lingkungan pendidikan dapat menjadi celah bagi para pelaku jahat untuk mengeksploitasi dan mengancam keamanan sistem informasi. Adapun kebutuhan akan pendekatan khusus dalam memberikan pemahaman dan ketrampilan kepada siswa di lingkungan sekolah teknologi informasi menjadi esensi, mengingat peran vital siswa sebagai generasi penerus dalam menghadapi kompleksitas ancaman siber masa depan.

Pelatihan ini dirancang khusus untuk siswa SMK Telkom Purwokerto, mempertimbangkan kebutuhan dan kepentingan unik dari latar belakang pendidikan dan lingkungan sekolah. Pelatihan ini berfokus pada teknik *footprinting* dan *reconnaissance* untuk mengidentifikasi potensi risiko keamanan informasi. *Footprinting*, sebagai langkah pertama, melibatkan pengumpulan informasi terinci tentang organisasi (Dinis & Serrão, 2014), termasuk infrastruktur jaringan, layanan yang digunakan, dan kebijakan keamanan yang diterapkan. *Reconnaissance*, sebagai kelanjutan dari *footprinting*, mencakup pencarian aktif terhadap celah dan kelemahan yang mungkin dapat dimanfaatkan (Lenjani et al., 2020).

Lingkungan sekolah teknologi informasi seperti SMK Telkom Purwokerto, siswa memiliki peluang besar untuk mendalami konsep keamanan informasi sejak dini. Pelatihan ini bertujuan memberikan pemahaman praktis dan aplikatif tentang teknik *footprinting* dan *reconnaissance*, dengan penekanan pada situasi dan tantangan dunia nyata. Dengan memperhatikan konteks dunia nyata, siswa tidak hanya diperkenalkan secara teoritis mengenai dasar keamanan informasi, tetapi juga diberikan pengalaman praktis mengenai teknik-teknik *footprinting* dan *reconnaissance* melalui simulasi dan latihan langsung. Sehingga, para siswa dapat mengembangkan keterampilan mereka dalam mengidentifikasi potensi ancaman, menganalisis kerentanan, dan merancang strategi keamanan yang efektif.

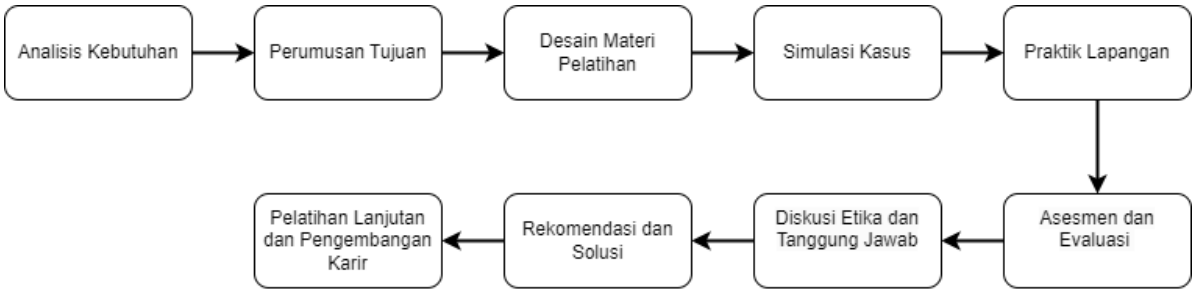
Tujuan utama pelatihan ini adalah meningkatkan pemahaman siswa tentang pentingnya keamanan informasi, dan memberikan dasar yang kokoh untuk merancang dan mengimplementasikan langkah-langkah keamanan yang efektif. Eksplorasi terhadap metode dan alat *footprinting* yang relevan dengan kebijakan keamanan informasi, serta memberikan wawasan mendalam tentang proses *reconnaissance* yang dapat diaplikasikan dalam konteks pengembangan keamanan siber. Melalui pemahaman mendalam tentang teknik ini, siswa SMK diharapkan dapat memperkuat lapisan pertahanan sistem yang dimiliki oleh siswa, mampu mengidentifikasi potensi risiko (Soesanto et al., 2023), dan memitigasi celah keamanan sebelum dapat dieksploitasi oleh pihak yang tidak bertanggung jawab(Alsmadi, 2023). Sehingga, siswa dapat menerapkan prinsip-prinsip keamanan informasi yang berlaku dan mengeksplorasi alat-alat terkini yang digunakan dalam menganalisis *footprinting* dan *reconnaissance* (Edgar & Manz, 2017; Ghonge et al., 2021) . Pelatihan ini dapat menjadi langkah awal yang bermanfaat dalam membentuk generasi yang memiliki kesadaran tinggi

Vol.4 No.1 Januari 2024 ISSN 2807 - 6370 (Online)
DOI: 10.20895/ijcosin.v4i1.1346

terhadap keamanan informasi di era digital ini. Kegiatan ini akan memberikan wawasan praktis tentang langkah-langkah yang dapat diambil untuk meningkatkan keamanan informasi dalam menghadapi ancaman yang terus berkembang (Thoyyibah, 2018).

METODE

Perancangan kegiatan pengabdian Masyarakat yang dilakukan memiliki kerangka pemecahan masalah yang terstruktur untuk memastikan pencapaian tujuan pelatihan. Berikut adalah langkah-langkah dalam kerangka pemecahan masalah keamanan informasi, khususnya pada teknik *footprinting* dan *reconnaissance*, yang dilakukan pembimbingan dan pemberdayaan siswa SMK Telkom Purwokerto seperti yang terlihat pada gambar 1.



Gambar 1. Kerangka Masalah

Langkah pertama, analisis kebutuhan yaitu sebelum kegiatan dilakukan, langkah awal yang harus dilakukan adalah mengidentifikasi kebutuhan dan tantangan yang dihadapi siswa SMK Telkom Purwokerto dalam konteks keamanan informasi. Proses ini melibatkan pemahaman mendalam terhadap tingkat pemahaman siswa tentang keamanan informasi dan menentukan kompetensi yang diinginkan setelah pelatihan. Selanjutnya langkah kedua, perumusan tujuan yaitu kegiatan ini bertujuan untuk menetapkan spesifik pelatihan, baik dari segi pengetahuan maupun keterampilan dan memastikan tujuan tersebut sesuai dengan kurikulum dan tingkat kemampuan siswa. Proses perumusan tujuan ini akan memastikan bahwa setiap elemen pelatihan dirancang untuk mencapai hasil yang diinginkan, dengan merinci kompetensi yang diharapkan dan menyesuaikannya dengan kemampuan serta kebutuhan siswa di SMK Telkom Purwokerto.

Langkah ketiga, desain materi pelatihan yaitu mengembangkan materi pelatihan yang terstruktur, mulai dari konsep dasar hingga teknik pelatihan dan menyesuaikan materi dengan konteks sekolah dan siswa, dan memastikan penggunaan metode pembelajaran yang interaktif dan relevan. Proses desain ini akan memastikan bahwa materi pelatihan tidak hanya relevan tetapi juga mampu menggugah minat siswa, mempertimbangkan keunikan lingkungan belajar mereka. Selain itu, penggunaan metode pembelajaran yang interaktif dan relevan akan diintegrasikan, memastikan siswa tidak hanya memahami konsep-konsep keamanan informasi secara teoritis tetapi juga dapat mengaplikasikannya dalam situasi praktis.

Langkah keempat, simulasi kasus yaitu menyertakan simulasi kasus keamanan informasi yang mencerminkan situasi dunia nyata. Ini membantu siswa untuk mengaplikasikan pengetahuan yang didapat dalam konteks yang nyata dalam menghadapi tantangan yang mungkin mereka temui di masa depan. Setelah itu, praktik lapangan yaitu merencanakan sesi praktik lapangan yang memungkinkan siswa untuk langsung mengaplikasikan teknik *footprinting* dan *reconnaissance*. Pelatihan ini dalam pengawasan yang cermat dan dapat memberikan umpan balik yang konstruktif. Selanjtnya, asesmen dan evaluasi yaitu menggunakan metode asesmen yang bervariasi, termasuk ujian tertulis, proyek lapangan, dan

Vol.4 No.1 Januari 2024 ISSN 2807 - 6370 (Online)
DOI: 10.20895/ijcosin.v4i1.1346

presentasi. Evaluasi ini membantu mengukur pemahaman siswa dan keberhasilan implementasi teknik keamanan informasi.

Langkah ketujuh, diskusi etika dan tanggung jawab yaitu menyisipkan sesi diskusi tentang etika keamanan informasi dan tanggung jawab siswa dalam menggunakan pengetahuan yang didapatkan. Menekankan pentingnya penggunaan keterampilan ini untuk kebaikan dan keamanan bersama. Selanjutnya, rekomendasi dan solusi yaitu memberikan kesempatan kepada siswa untuk merumuskan rekomendasi dan solusi terhadap potensi risiko keamanan yang diidentifikasi dan mendorong siswa untuk berpikir proaktif dalam memberikan solusi preventif. Dan terakhir, pelatihan lanjutan dan pengembangan karir yaitu menginformasikan kepada siswa mengenai peluang pelatihan lanjutan dan pengembangan karir dalam bidang keamanan informasi. Kegiatan ini membantu siswa dalam merencanakan langkah-langkah selanjutnya setelah menyelesaikan pelatihan ini.

Melalui kerangka pemecahan masalah ini, diharapkan siswa dapat mengoptimalkan pembelajaran mereka tentang *footprinting* dan *reconnaissance*, memahami konsep keamanan informasi, dan siap menghadapi tantangan di dunia teknologi informasi.

HASIL, PEMBAHASAN, DAN DAMPAK

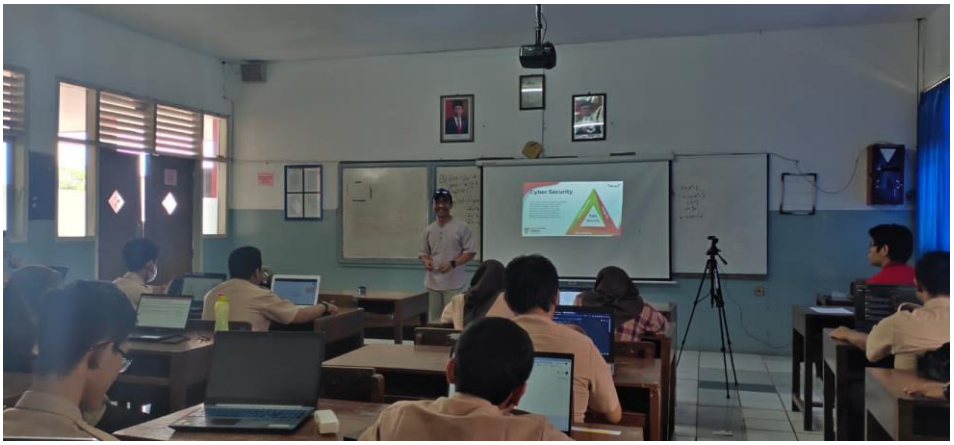
Fase analisis kebutuhan pada pelatihan ini mengambil pendekatan yang komprehensif dengan meneliti secara cermat tantangan dan kebutuhan khusus yang dihadapi siswa SMK Telkom Purwokerto dalam memahami konsep keamanan informasi. Proses ini melibatkan serangkaian metode, termasuk survei kebutuhan yang melibatkan siswa secara langsung dan konsultasi mendalam dengan para guru. Hasilnya memberikan gambaran yang akurat tentang tingkat pemahaman dan minat siswa, menjadi landasan utama dalam merancang pelatihan yang responsif.

Berdasarkan perumusan tujuan pelatihan kemudian menjadi langkah yang sangat penting. Dengan merinci tujuan spesifik, baik dalam hal pengetahuan maupun keterampilan dan memastikan bahwa pelatihan ini sejalan dengan kurikulum sekolah dan dapat diukur keberhasilannya. Poin-poin tujuan ini menciptakan kerangka evaluasi yang jelas, memandu arah dan pencapaian pelatihan. Desain materi pelatihan dilakukan dengan memperhatikan struktur terstruktur dari konsep dasar hingga teknik *hacking* yang dapat diterapkan dalam keseharian. Kehadiran materi yang disesuaikan dengan konteks sekolah dan siswa memastikan relevansi dan daya serap dapat maksimal diterima oleh para siswa. Metode pembelajaran yang interaktif dan mengajak siswa berpartisipasi aktif turut mendukung pemahaman yang mendalam. Simulasi kasus keamanan informasi diintegrasikan dalam pelatihan untuk memberikan siswa pengalaman yang terlihat dalam konteks dunia nyata.

Pelatihan ini bukan hanya menguji materi secara praktis, tetapi juga mempersiapkan siswa dalam menghadapi permasalahan sehari-hari yang mungkin dihadapi dalam praktik keamanan informasi. Sesi praktek lapangan didesain agar siswa dapat mengaplikasikan langsung teknik *footprinting* dan *reconnaissance* yang telah dipelajari. Pengawasan yang cermat dan umpan balik yang diberikan melalui sesi ini menjadi poin kunci dalam membentuk keterampilan siswa dengan efektif. Tahap asesmen dan evaluasi memanfaatkan pendekatan yang beragam, termasuk ujian tertulis, proyek lapangan, dan presentasi. Kombinasi metode ini membantu dalam mengukur pemahaman siswa dan sejauh mana mereka berhasil mengimplementasikan teknik keamanan informasi yang dipelajari. Diskusi etika dan tanggung jawab menjadi aspek yang tidak terpisahkan dari pelatihan, menyoroti pentingnya penggunaan keterampilan keamanan informasi dengan etika dan kepedulian terhadap dampaknya. Pada saat merumuskan rekomendasi dan solusi, pelatihan yang telah dilakukan ini diharapkan dapat memberikan siswa mampu berperan aktif dalam mengidentifikasi dan merespons potensi risiko keamanan yang mereka temukan. Melalui cara ini, siswa tidak hanya mengembangkan

Vol.4 No.1 Januari 2024 ISSN 2807 - 6370 (Online)
DOI: 10.20895/ijcosin.v4i1.1346

pemahaman tetapi juga memberikan kontribusi nyata dalam upaya mencegah ancaman keamanan. Pada tahap akhir, siswa diinformasikan tentang peluang pelatihan lanjutan dan pengembangan karir di bidang keamanan informasi. Langkah ini dirancang untuk membantu siswa merencanakan langkah selanjutnya setelah menyelesaikan pelatihan, membuka pintu untuk pengembangan karir yang lebih lanjut dalam dunia keamanan informasi. Melalui pendekatan holistik, pelatihan ini diharapkan memberikan kontribusi substansial dalam memperkaya pemahaman dan keterampilan siswa SMK Telkom Purwokerto, memberikan para siswa fondasi yang kokoh untuk menghadapi dinamika keamanan informasi di era digital.



Gambar 2. Sesi Pelatihan

Pentingnya dampak positif dari kegiatan ini seperti yang dapat dilihat pada gambar 2 tidak hanya terbatas pada peningkatan pengetahuan dan keterampilan siswa dalam keamanan informasi. Analisis awal sebelum pelaksanaan kegiatan menunjukkan bahwa tingkat kesadaran peserta terhadap keamanan informasi sebesar 40%. Setelah kegiatan pelatihan selesai, dilakukan pengukuran ulang yang menunjukkan peningkatan yang signifikan dalam kesadaran yang dimiliki oleh para siswa mencapai tingkat 90%. Hal ini berarti terjadi peningkatan sebesar 50% dari tingkat kesadaran awal. Hasil dari kegiatan pelatihan yang diperoleh dari pengukuran ini secara signifikan menjelaskan bahwa kegiatan pelatihan *footprinting* dan *reconnaissance* dalam *cybersecurity* memberikan dampak yang besar terhadap pemahaman dan kesadaran peserta tentang keamanan informasi. Peningkatan kesadaran sebesar ini tidak hanya mencerminkan hasil yang menggembirakan, tetapi juga menegaskan keberhasilan metodologi pelatihan yang kami terapkan dalam meningkatkan pemahaman siswa terhadap ranah keamanan siber. Dampak jangka panjangnya mencakup peningkatan kesadaran siswa terhadap risiko keamanan, yang membantu menciptakan lingkungan sekolah yang lebih aman dan responsif terhadap tantangan keamanan siber. Dengan meningkatnya pemahaman dan keterampilan siswa, diharapkan akan muncul generasi yang lebih mampu menghadapi dan mencegah ancaman keamanan informasi di masa depan. Selain itu, kolaborasi dengan para guru dan ahli keamanan informasi lokal dapat membuka peluang kerjasama yang berkelanjutan, memperkuat hubungan antara pendidikan dan industri di bidang keamanan informasi. Secara keseluruhan, pelatihan ini diharapkan memberikan kontribusi yang berkelanjutan terhadap peningkatan keamanan informasi di lingkungan SMK Telkom Purwokerto dan dapat dijadikan model bagi institusi pendidikan lainnya.

SIMPULAN

Pelatihan ini membawa dampak positif yang signifikan dalam memperkuat pemahaman dan keterampilan siswa SMK Telkom Purwokerto dalam keamanan informasi. Melalui

Vol.4 No.1 Januari 2024 ISSN 2807 - 6370 (Online)
DOI: 10.20895/ijcosin.v4i1.1346

pendekatan analisis kebutuhan yang terperinci, pelatihan ini berhasil mengidentifikasi tantangan dan kebutuhan unik siswa, membentuk dasar kuat untuk merumuskan tujuan dan desain materi pelatihan yang sesuai. Pelaksanaan simulasi kasus, praktek lapangan, dan berbagai metode asesmen memastikan siswa terlibat aktif dan mendapatkan pengalaman langsung dalam penerapan teknik *footprinting* dan *reconnaissance*. Sesi diskusi etika dan tanggung jawab memberikan dimensi etis yang diperlukan dalam penggunaan keterampilan keamanan informasi. Siswa tidak hanya dilatih untuk menjadi praktisi keamanan informasi yang kompeten tetapi juga untuk menjalankan tanggung jawab dengan penuh kesadaran terhadap dampaknya. Hasilnya, siswa tidak hanya meningkatkan pengetahuan mengenai keamanan informasi, tetapi juga mampu mengidentifikasi potensi risiko keamanan dan memberikan solusi proaktif. Dengan demikian, pelatihan ini bukan hanya merespon kebutuhan pendidikan, tetapi juga membuka ruang bagi pengembangan karakter dan tanggung jawab siswa dalam penggunaan teknologi informasi. Pentingnya pelatihan ini tidak hanya terbatas pada manfaat langsung bagi siswa, tetapi juga menciptakan dampak jangka panjang dalam meningkatkan kesadaran dan keamanan siber di lingkungan sekolah. Kolaborasi dengan guru dan ahli keamanan informasi membuka peluang untuk kerjasama yang berkelanjutan dan membangun jembatan antara pendidikan dan industri keamanan informasi. Sebagai kesimpulan, pelatihan ini berhasil mencapai tujuan-tujuan yang ditetapkan, memberikan kontribusi positif pada tingkat pengetahuan, keterampilan, dan sikap siswa terkait keamanan informasi. Kegiatan ini memberikan pengetahuan dan memberikan landasan yang kokoh untuk peningkatan kesadaran dan keamanan informasi di masa depan.

UCAPAN TERIMAKASIH

Wiwid Widiyantoro, S.Si., M.pd yang telah mengundang kami sebagai pembicara di SMK Telkom Purwokerto.

DAFTAR PUSTAKA

Alsmadi, I. (2023). The NICE Cyber Security Framework. In *The NICE Cyber Security Framework*. https://doi.org/10.1007/978-3-031-21651-0

Alwi, E. I., & Ilmawan, L. B. (2021). Analisis Keamanan Sistem Informasi Akademik (SIAKAD) Universitas XYZ Menggunakan Metode Vulnerability Assessment. *INFORMAL: Informatics Journal*, *6*(3). https://doi.org/10.19184/isj.v6i3.27053

Dinis, B., & Serrão, C. (2014). Using PTES and open-source tools as a way to conduct external footprinting security assessments for intelligence gathering. *Journal of Internet Technology and Secured Transaction*, *3*(3), 271–279. https://doi.org/10.20533/jitst.2046.3723.2014.0035

Edgar, T. W., & Manz, D. O. (2017). Research Methods for Cyber Security. In *Research Methods for Cyber Security*. https://doi.org/10.1016/s1353-4858(18)30053-9

Flores, F., Paredes, R., & Meza, F. (2016). Procedures for mitigating Cybersecurity risk in a Chilean Government Ministry. *IEEE Latin America Transactions*, *14*(6), 2947–2950. https://doi.org/10.1109/TLA.2016.7555280

Ghonge, M. M., Pramanik, S., Mangrulkar, R., & Le, D. N. (2021). Cyber Security and Digital Forensics. In *Cyber Security and Digital Forensics*. https://doi.org/10.1002/9781119795667

Lenjani, A., Dyke, S. J., Bilionis, I., Yeum, C. M., Kamiya, K., Choi, J., Liu, X., & Chowdhury, A. G. (2020). Towards fully automated post-event data collection and analysis: Pre-event and post-event information fusion. *Engineering Structures*, *208*. https://doi.org/10.1016/j.engstruct.2019.109884

Muni, A., Sudeska, E., Crismondari, C., Jalil, M., & Bayu Rianto. (2023). OPTIMALISASI IT DALAM ERA LITERISASI DIGITAL. *SWARNA: Jurnal Pengabdian Kepada Masyarakat*, *2*(1). https://doi.org/10.55681/swarna.v2i1.263

Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen*, *1*(2).

Styugin, M. (2019). Protection from reconnaissance for establishing information security systems. *Information Security Journal*, *28*(1–2), 46–54. https://doi.org/10.1080/19393555.2019.1630528

Sutejo, S., Prasetijo, A. B., & Agushyban, F. (2021). The Role of Information System for Risk Management in Hospital: A Narrative Review. *Jurnal Aisyah : Jurnal Ilmu Kesehatan*, *6*(3). https://doi.org/10.30604/jika.v6i3.1014

Thoyyibah, T. (2018). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013 Pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X. *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer Dan Teknologi Informasi*, *4*(2), 72. https://doi.org/10.24014/coreit.v4i2.6292