Jurnal Abmas - *p-ISSN 1412-1891 & e-ISSN 2798-1436*
Volume 25 No 1 (2025) 29-38

JURNAL UPI

Jurnal Abmas

Media Informasi Pengabdian Kepada Masyarakat

https://ejournal.upi.edu/index.php/ABMAS

Role of HR in strengthening cyber security on the social media platform of the Teratai Putih Foundation, Yogyakarta

Idam Wahyudi[1], Anggun Sulistyowati[2], Bikorin[3]
[1,2,3]Universitas AKPRIND Indonesia, Kota Yogyakarta, Indonesia
iwahyudi@akprind.ac.id[1] , anggun_sulistyowati@akprind.ac.id[2] , bikorin@akprind.ac.id[3]

ABSTRACT

In the increasingly advanced digital era, social media has become a primary tool for organizations, including Yayasan Teratai Putih Yogyakarta, to disseminate information, build networks, and enhance community engagement. As an institution engaged in social and educational activities, the foundation heavily relies on social media to implement various programs and social campaigns. However, alongside the benefits it offers, there are significant cybersecurity challenges that must be taken seriously. This community service program (Abdimas) aims to enhance the capacity and awareness of human resources (HR) at Yayasan Teratai Putih Yogyakarta in strengthening cybersecurity on the social media platforms they manage. The target participants of this initiative include social media administrators of the foundation, including staff and volunteers responsible for information management and digital interactions. As a result of this socialization activity, participants gained an in-depth understanding of data protection strategies, security policies, and preventive measures against cyber threats. With increased awareness and skills in managing digital security, the foundation can minimize the risk of cyberattacks while maintaining its credibility and public trust in the information it shares.

ARTICLE INFO

Article History:
Received: 15 Feb 2025
Revised: 11 Mei 2025
Accepted: 19 Mei 2025
Available online: 27 Mei 2025
Publish: 27 Jun 2025

Keywords:
cyber security; digital era; human resource

Open access
Jurnal Abmas
is a peer-reviewed open-access journal

ABSTRAK

Dalam era digital yang semakin maju, media sosial telah menjadi alat utama bagi organisasi, termasuk Yayasan Teratai Putih Yogyakarta, untuk menyebarkan informasi, membangun jejaring, dan meningkatkan keterlibatan masyarakat. Sebagai lembaga yang bergerak di bidang sosial dan pendidikan, yayasan ini sangat bergantung pada media sosial untuk menjalankan berbagai program dan kampanye sosial. Namun, di balik manfaat yang ditawarkan, terdapat tantangan besar dalam hal keamanan siber yang harus diperhatikan secara serius. Kegiatan pengabdian kepada masyarakat (Abdimas) ini bertujuan untuk meningkatkan kapasitas dan kesadaran Sumber Daya Manusia (SDM) di Yayasan Teratai Putih Yogyakarta dalam memperkuat keamanan siber pada platform media sosial yang mereka kelola. Sasaran kegiatan ini adalah pengelola media sosial Yayasan Teratai Putih Yogyakarta, termasuk staf dan relawan yang bertanggung jawab atas pengelolaan informasi serta interaksi digital. Hasil dari kegiatan sosialisasi ini peserta memperoleh pemahaman mendalam mengenai strategi perlindungan data, kebijakan keamanan, serta langkah-langkah pencegahan ancaman siber. Dengan meningkatnya kesadaran dan keterampilan dalam mengelola keamanan digital, yayasan dapat meminimalkan risiko serangan siber serta menjaga kredibilitas dan kepercayaan publik terhadap informasi yang disampaikan.

Kata Kunci: *Era digital; keamanan siber; manajemen sumber daya manusia*

How to cite (APA Style)
Wahyudi, I., Sulistyowati, A., & Bikorin, B. (2025). Role of HR in strengthening cyber security on the social media platform of the Teratai Putih Foundation, Yogyakarta. *Jurnal Abmas, 25*(1), 29-38.

Peer review
This article has been peer-reviewed through the journal's standard double-blind peer review, where both the reviewers and authors are anonymised during review.

https://doi.org/10.17509/abmas.v25i1.83473

INTRODUCTION

Dalam era digital yang semakin maju, media sosial telah menjadi alat utama bagi organisasi, termasuk Yayasan Teratai Putih Yogyakarta, untuk menyebarkan informasi, membangun jejaring, dan meningkatkan keterlibatan masyarakat. Sebagai lembaga yang bergerak di bidang sosial dan pendidikan, yayasan ini sangat bergantung pada media sosial untuk menjalankan berbagai program dan kampanye sosial. Namun, di balik manfaat yang ditawarkan, terdapat tantangan besar dalam hal keamanan siber yang harus diperhatikan secara serius (Prasepta & Subakti, 2024). Ancaman siber seperti peretasan akun, pencurian data, penyebaran hoaks, serta penyalahgunaan akses menjadi risiko yang dapat berdampak negatif terhadap operasional yayasan. Jika akun media sosial yayasan tidak dikelola dengan sistem keamanan yang baik, potensi serangan dari pihak tidak bertanggung jawab dapat mengancam kredibilitas serta efektivitas komunikasi yayasan dengan masyarakat. Kejadian seperti pengambilalihan akun secara ilegal atau penyebaran informasi palsu atas nama yayasan dapat menyebabkan dampak serius, termasuk hilangnya kepercayaan publik (Napu *et al.,* 2024).

Sumber Daya Manusia (SDM) yang terlibat dalam pengelolaan media sosial memiliki peran strategis dalam menjaga keamanan siber. Kesadaran serta keterampilan dalam menerapkan kebijakan dan prosedur keamanan digital sangat diperlukan agar platform media sosial yayasan tetap terlindungi dari ancaman siber (Kristianti & Kurniasi., 2024). Tanpa pemahaman yang baik mengenai praktik keamanan digital, pengelola akun media sosial rentan melakukan kesalahan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab (Anugrah *et al*., 2024).

Tabel 1. Permasalahan dan Program untuk Mitra

No	Permasalahan	Uraian
1	Rendahnya kesadaran SDM mengenai ancaman keamanan siber pada media sosial.	Edukasi mengenai jenis ancaman siber dan cara pencegahannya bagi pengelola media sosial yayasan.
2	Tidak adanya kebijakan dan prosedur standar dalam mengelola keamanan akun media sosial.	Membantu yayasan dalam merancang kebijakan dan SOP untuk pengelolaan keamanan akun media sosial.
3	Kurangnya literasi digital bagi anggota yayasan yang terlibat dalam pengelolaan media sosial.	Program Literasi Digital: Peningkatan keterampilan digital untuk mengelola media sosial dengan aman dan efektif.

Sumber : Yayasan Teratai Putih Yogyakarta

Untuk itu, diperlukan langkah-langkah preventif dalam memperkuat keamanan siber pada media sosial Yayasan Teratai Putih Yogyakarta. Penyusunan kebijakan keamanan digital, penerapan standar operasional yang jelas, serta edukasi bagi pengelola akun media sosial menjadi bagian penting dalam membangun sistem pertahanan yang kokoh (Kristianti & Kurniasi., 2024). Dengan adanya kebijakan yang jelas, setiap anggota tim dapat memahami peran dan tanggung jawabnya dalam menjaga keamanan informasi yayasan di ranah digital (Effendy & Oktiani, 2024). Selain itu, penggunaan teknologi keamanan yang tepat seperti autentikasi dua faktor (2FA), enkripsi data, serta pemantauan aktivitas akun juga dapat membantu meningkatkan perlindungan terhadap ancaman siber. Tidak hanya itu, peningkatan kapasitas SDM melalui pelatihan keamanan siber yang berkelanjutan juga menjadi langkah strategis dalam memastikan bahwa setiap individu yang terlibat dalam pengelolaan media sosial yayasan memiliki keterampilan yang memadai dalam menghadapi ancaman digital (Irawan *et al*., 2024).

Untuk memperkuat keamanan siber pada platform media sosial Yayasan Teratai Putih Yogyakarta, diperlukan langkah-langkah preventif yang sistematis dan komprehensif. Langkah awal adalah menyusun kebijakan keamanan digital yang terstruktur, mencakup pedoman pengelolaan akun, klasifikasi data, dan protokol tanggap insiden siber. Dengan kebijakan yang jelas, seluruh anggota tim dapat memahami peran, tanggung jawab, dan mekanisme eskalasi ketika terjadi potensi pelanggaran keamanan. Selanjutnya, penerapan standar operasional prosedur (SOP) yang detail menjadi pondasi bagi konsistensi pelaksanaan kebijakan. SOP ini mencakup proses autentikasi, otorisasi, serta tata cara penggunaan alat bantu keamanan seperti *firewall* dan sistem deteksi intrusi (IDS) untuk memantau lalu lintas

https://doi.org/10.17509/abmas.v25i1.83473

data. Studi literatur menunjukkan bahwa kombinasi firewall, intrusion detection/prevention, enkripsi, dan *multi-factor authentication* (MFA) secara signifikan meningkatkan ketahanan sistem dari serangan siber (Imran *et al.,* 2024).

Selain kebijakan dan SOP, edukasi berkelanjutan bagi pengelola akun media sosial adalah langkah strategis yang tidak kalah penting. Program pelatihan keamanan siber sebaiknya mengadopsi kerangka kerja adaptif, menyesuaikan materi dengan kebutuhan dan latar belakang pengguna. Model ACSTF-SMR *(Adaptive Cybersecurity Training Framework for Social Media Risks)* yang diuji pada beberapa organisasi mampu meningkatkan pemahaman peserta terhadap kebijakan dan meningkatkan kesadaran akan ancaman di ranah digital (Ben-Salamah *et al.,* 2023). Dukungan manajemen puncak dan komitmen organisasi menjadi faktor kunci keberhasilan. Perlu dibentuk tim *task force* keamanan digital yang lintas fungsi, termasuk perwakilan manajemen, tim IT, dan humas. Tim ini bertanggung jawab menyusun *road map* penerapan kebijakan, mengawasi hasil audit keamanan, serta memutakhirkan mitigasi ancaman siber secara proaktif (Creese *et al*., 2021).

Dengan meningkatnya kesadaran dan kesiapan SDM dalam menghadapi tantangan keamanan siber, Yayasan Teratai Putih Yogyakarta dapat lebih percaya diri dalam memanfaatkan media sosial sebagai sarana komunikasi dan penyebaran informasi. Keamanan yang terjaga dengan baik tidak hanya melindungi yayasan dari ancaman digital, tetapi juga memperkuat kredibilitas dan kepercayaan publik terhadap yayasan di dunia maya (Aditya, 2024). Keseluruhan upaya ini diharapkan dapat menciptakan ekosistem digital yang lebih aman bagi yayasan dalam menjalankan misinya, sehingga media sosial dapat terus digunakan sebagai alat yang efektif dalam mendukung program-program sosial yang bermanfaat bagi masyarakat luas. Kegiatan pengabdian kepada masyarakat (Abdimas) ini bertujuan untuk meningkatkan kapasitas dan kesadaran Sumber Daya Manusia (SDM) di Yayasan Teratai Putih Yogyakarta dalam memperkuat keamanan siber pada platform media sosial yang mereka kelola.

Literature Review

Manajemen SDM

Sumber daya manusia (SDM) adalah salah satu faktor dalam suatu perusahaan selain faktor lain seperti modal. Suparmi *et al*. dalam buku "*Manajemen Sumber Daya Manusia (Prinsip - Prinsip dan Praktik dalam Mengelola Organisasi)*" berpendapat bahwa SDM harus dikelola dengan baik untuk meningkatkan efektitivitas dan efisiensi organisasi, sebagai salah satu fungsi dalam perusahaan yang dikenal dengan manajemen sumber daya manusia (MSDM).

Manajemen Sumber Daya Manusia (MSDM) dapat diartikan sebagai serangkaian kegiatan, kebijakan, dan program yang dirancang serta dilaksanakan untuk memperoleh, mengembangkan, dan mempertahankan tenaga kerja guna meningkatkan kontribusinya terhadap efektivitas organisasi. Seluruh proses ini dilaksanakan dengan cara yang dapat dipertanggungjawabkan secara etis dan sosial. Kegiatan tersebut mencakup berbagai tindakan seperti perencanaan, pengorganisasian, pengarahan, pengawasan, analisis jabatan, proses rekrutmen dan seleksi, orientasi karyawan baru, serta upaya memotivasi tenaga kerja. Penetapan kebijakan mencerminkan arah strategis, misalnya memberikan prioritas pada sumber daya internal untuk pengisian jabatan kosong atau memberikan kesempatan yang merata bagi semua individu. Sementara itu, Sumitra *et al.* dalam buku "*Manajemen (Prinsip, Proses dan Praktik)*" menyatakan bahwa program-program dapat meliputi pelatihan kerja yang mencakup metode pelaksanaan, pihak yang terlibat, dan aspek-aspek terkait lainnya.

Berdasarkan rujukan di atas, sumber daya manusia (SDM) merupakan salah satu elemen kunci dalam perusahaan selain faktor modal. Peran penting SDM menuntut pengelolaan yang optimal guna mencapai efektivitas dan efisiensi organisasi. Oleh karena itu, Manajemen Sumber Daya Manusia (MSDM) hadir sebagai fungsi strategis dalam perusahaan yang bertujuan mengelola SDM secara terarah dan profesional.

https://doi.org/10.17509/abmas.v25i1.83473

MSDM mencakup berbagai kegiatan, kebijakan, dan program yang dirancang untuk memperoleh, mengembangkan, dan mempertahankan tenaga kerja. Proses ini dilakukan secara etis dan bertanggung jawab secara sosial, melalui tahapan seperti perencanaan, rekrutmen, orientasi, hingga pelatihan dan motivasi kerja. Kebijakan yang diambil dalam MSDM juga mencerminkan strategi perusahaan, sementara program pelatihan menjadi bagian penting dalam meningkatkan kompetensi karyawan. Dengan demikian, MSDM bukan hanya berfokus pada operasional semata, tetapi juga berperan dalam menciptakan nilai strategis bagi keberlanjutan organisasi.

Keamanan Siber

Keamanan siber adalah serangkaian teknologi, kebijakan, proses, dan praktik terintegrasi yang dirancang untuk mencegah, mendeteksi, dan merespons ancaman digital termasuk *malware*, *phishing*, peretasan, dan akses tidak sah serta untuk melindungi sistem komputer, jaringan, perangkat elektronik, dan data organisasi atau individu dari gangguan, pencurian, kerusakan, dan penyalahgunaan (Lumintosari *et al.,* 2024; Laksana & Mulyani, 2024).

Seiring dengan meningkatnya ketergantungan terhadap teknologi digital, pentingnya keamanan siber pun semakin meningkat. Serangan siber berpotensi menimbulkan dampak serius, seperti kerugian finansial besar, penurunan reputasi, hingga membahayakan keamanan suatu negara. Karena itu, upaya untuk melindungi infrastruktur digital dan informasi sensitif kini menjadi fokus utama berbagai negara dan institusi (Kristianti & Kurniasi., 2024; Dinda, 2024).

Keamanan siber mencakup rangkaian tindakan teknis dan non-teknis untuk memastikan bahwa aset digital seperti server, aplikasi, dan data terlindungi dari upaya akses tidak sah, pencurian data, serta gangguan layanan. Menurut Undang-Undang dan regulasi nasional, kerangka kerja keamanan siber harus meliputi tiga pilar utama: kerahasiaan, integritas, dan ketersediaan, yang sering disebut TRIAD CIA. Kerahasiaan memastikan hanya pihak berwenang yang dapat mengakses informasi; integritas menjaga agar data tidak diubah atau dirusak tanpa izin; sedangkan ketersediaan menjamin bahwa sistem dan informasi tetap dapat diakses saat dibutuhkan.

Dari sisi regulasi, Indonesia terus memperkuat kerangka hukum melalui pembentukan Badan Siber dan Sandi Negara (BSSN) dan penerbitan Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Regulasi ini menekankan pentingnya sertifikasi keamanan, pelaporan insiden siber, dan perlindungan data pribadi sebagai hak warga negara (Aji, 2023).

Dari rujukan di atas, keamanan siber saat ini menjadi aspek krusial dalam melindungi infrastruktur digital dari berbagai ancaman yang kian kompleks. Keamanan siber bukan hanya sekadar perlindungan teknis, melainkan juga mencakup kebijakan, prosedur, dan praktik yang saling mendukung untuk mencegah, mendeteksi, dan merespons serangan digital seperti *malware, phishing*, dan peretasan. Dalam konteks ini, keamanan siber tidak hanya penting bagi organisasi, tetapi juga bagi individu dan negara, mengingat kerugian yang ditimbulkan oleh serangan siber bisa bersifat sistemik dan berdampak luas. Dari perspektif regulasi, penulis memandang bahwa langkah-langkah yang diambil oleh pemerintah Indonesia, seperti pembentukan BSSN dan penerbitan regulasi tentang penyelenggaraan sistem elektronik, merupakan bentuk keseriusan negara dalam menghadapi tantangan keamanan digital. Penekanan pada sertifikasi keamanan, pelaporan insiden, dan perlindungan data pribadi menjadi indikator bahwa keamanan siber tidak hanya menjadi tanggung jawab teknis, tetapi juga bagian dari pemenuhan hak warga negara di era digital.

Media Sosial

Media sosial merupakan suatu platform digital berbasis internet yang memfasilitasi interaksi sosial antar pengguna, sekaligus memungkinkan mereka untuk menghasilkan, menyebarluaskan, dan mengonsumsi berbagai bentuk informasi secara *real-time* (Zed *et al.,* 2025).

https://doi.org/10.17509/abmas.v25i1.83473

Media sosial adalah kumpulan aplikasi dan layanan berbasis internet yang dibangun di atas fondasi Web 2.0, dirancang untuk memfasilitasi penciptaan, pertukaran, dan interaksi konten di antara pengguna. Platform ini meliputi fitur pembuatan profil, jaringan pertemanan, percakapan dua arah, serta mekanisme kolaborasi *real-time*, sehingga memungkinkan pengguna untuk menghasilkan, menyebarkan, dan mengonsumsi informasi tanpa batasan ruang dan waktu, sekaligus membentuk ikatan sosial virtual yang dinamis (Situmorang & Hayati, 2023).

Media sosial membentuk sebuah ekosistem digital yang memadukan unsur jaringan *(network)*, interaktivitas *(interactivity),* dan arsip *(archive)*, di mana setiap aktivitas terekam dan dapat diakses kembali kapan saja. Karakteristik jaringan menciptakan koneksi antara pengguna, grup, atau komunitas berdasarkan minat dan tujuan bersama. Interaktivitas memfasilitasi dialog dua arah, baik berupa komentar, reaksi, maupun pertukaran pesan pribadi. Sedangkan arsip memastikan bahwa informasi tersimpan dengan rapi dalam basis data, memungkinkan penelusuran dan analisis konten secara berkelanjutan (Liedfray *et al*., 2022; Syaddam *et al.,* 2024).

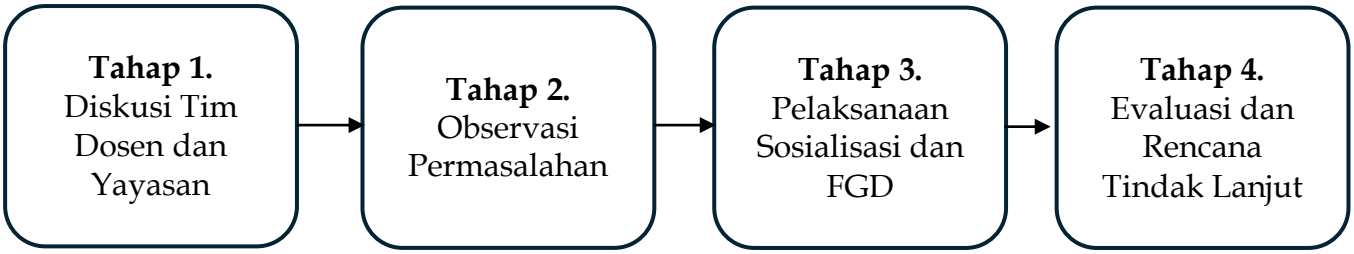
Media sosial memberi peluang bagi organisasi untuk membangun narasi kolektif dan memperkuat *branding* melalui kampanye digital. Fitur *like, share,* dan *follow* turut memperluas jangkauan pesan, sementara algoritma berbasis data membantu mempersonalisasi konten sesuai preferensi audiens. Namun, dinamika ini juga menimbulkan tantangan baru, seperti penyebaran informasi salah (hoaks), privasi data, dan keamanan akun, yang menuntut kerangka kebijakan dan edukasi berkelanjutan bagi pengelola *platform* (Yusuf *et al.,* 2023).

Dari referensi di atas, media sosial merupakan suatu platform digital berbasis internet yang tidak hanya memungkinkan pengguna untuk berinteraksi secara sosial, tetapi juga memberikan kebebasan dalam menciptakan, menyebarluaskan, dan mengakses informasi secara *real-time*. Platform ini berlandaskan teknologi Web 2.0 yang menekankan partisipasi aktif pengguna dalam berbagai bentuk komunikasi dan pertukaran konten. Oleh karena itu, penggunaan media sosial secara optimal memerlukan kebijakan yang kuat, edukasi literasi digital, serta pengelolaan yang bijak agar manfaatnya dapat dirasakan tanpa mengabaikan risikonya.

METHODS

Sasaran kegiatan ini adalah pengelola media sosial Yayasan Teratai Putih Yogyakarta, termasuk staf dan relawan yang bertanggung jawab atas pengelolaan informasi serta interaksi digital. Kegiatan ini dilaksanakan pada Senin, 10 Maret 2025, dengan metode presentasi untuk memperkenalkan konsep keamanan siber dalam pengelolaan media sosial. Acara diawali dengan pemaparan mengenai pentingnya peran Sumber Daya Manusia (SDM) dalam menjaga keamanan siber, khususnya dalam mencegah ancaman seperti peretasan, *phishing*, dan penyebaran informasi palsu. Interaksi antara narasumber dan peserta berlangsung secara aktif melalui sesi diskusi dan tanya jawab untuk mengidentifikasi tantangan serta kendala yang dihadapi dalam menerapkan langkah-langkah keamanan digital.

Sebagai penutup, dilaksanakan *Focus Group Discussion* (FGD) yang membahas hambatan dalam implementasi kebijakan keamanan siber serta harapan peserta terhadap pengembangan strategi perlindungan data dan informasi di masa mendatang. Tim dosen dari Universitas AKPRIND Indonesia juga mengundang peserta untuk memberikan masukan mengenai bentuk dukungan lanjutan yang dapat diberikan dalam upaya memperkuat keamanan siber pada platform media sosial yayasan. Alur pelaksanaan kegiatan ditunjukkan pada **Gambar 1**.



Gambar 1. Alur Pelaksanaan Kegiatan
Sumber : Wahyudi et al. (2025)

https://doi.org/10.17509/abmas.v25i1.83473

RESULTS AND DISCUSSION

Setelah dilaksanakan sosialisasi Peran SDM Dalam Memperkuat Keamanan Siber Pada Platform Media Sosial, peneliti dapat merangkum dalam **Tabel 2**.

Tabel 2. Target dan Persentase Ketercapaian

No.	Keterangan	Persentase Ketercapaian
1	Keberhasilan jumlah target peserta	98 %
2	Ketercapaian tujuan pelatihan	100 %
3	Ketercapaian target materi yang direncanakan	95 %
4	Peningkatan pemahaman pengurus yayasan teratai putih	Ada

Sumber: Data diolah peneliti, 2025

Dalam pelaksanaan pelatihan ini, panitia menargetkan 20 orang peserta. Berdasarkan daftar hadir tercatat bahwa 19 peserta (98% dari target) telah mengikuti seluruh rangkaian sesi, sehingga hanya satu peserta yang berhalangan hadir. Setiap peserta kemudian menjalani *post training evaluation* berupa kuis dan kuesioner *pre test* dan *post test* dengan *passing grade* yang telah ditetapkan; hasilnya menunjukkan 100% peserta berhasil mencapai atau melampaui skor minimal, menandakan bahwa semua tujuan pembelajaran telah tercapai. Dengan memadukan data kuantitatif absensi, evaluasi, log penyampaian materi dan data kualitatif dari FGD, keempat indikator keberhasilan pelatihan ini dapat diverifikasi secara komprehensif. Efektivitas metode kolaboratif dan *active learning*, tetapi juga menjadi dasar rekomendasi penyusunan SOP respons insiden dan pengembangan program pelatihan berkala bagi SDM organisasi (Rozikin & Suyati, 2023).

Pelatihan bertema "Peran Strategis Sumber Daya Manusia dalam Keamanan Siber pada Platform Media Sosial Yayasan Teratai Putih Yogyakarta" berhasil menarik partisipasi aktif dari seluruh peserta. Materi yang disampaikan oleh pemateri memfokuskan pada urgensi perlindungan data digital serta peningkatan kapasitas SDM dalam menghadapi berbagai jenis ancaman siber yang semakin kompleks dan dinamis. Selama sesi penyampaian materi, peserta terlihat aktif menyimak dan mencatat penjelasan mengenai pentingnya strategi pertahanan siber yang holistik, terutama dalam konteks organisasi nirlaba seperti yayasan. Pemateri menghadirkan berbagai studi kasus aktual yang menggambarkan situasi nyata kebocoran data, serangan siber berbasis rekayasa sosial *(social engineering)*, hingga implikasi hukum dan reputasi terhadap organisasi.

Sesi dilanjutkan dengan pelaksanaan *Focus Group Discussion* (FGD) seperti yang terlihat pada **Gambar 2**, yang memperdalam pemahaman peserta terhadap isu-isu keamanan digital melalui dialog terbuka dan berbasis pengalaman pribadi. Peserta saling berbagi praktik terbaik dalam pengelolaan data sensitif, serta secara kolektif mengidentifikasi kelemahan sistem yang ada di internal yayasan, termasuk kurangnya prosedur standar untuk mitigasi insiden siber, serta rendahnya literasi digital di kalangan pengurus dan staf operasional.

https://doi.org/10.17509/abmas.v25i1.83473

Gambar 2. Sosialisasi dan FGD
Sumber: Dokumentasi Penulis, 2024

Pelatihan juga menghasilkan beberapa keluaran konkret, yaitu: 1) draft *Standard Operating Procedure* (SOP) tentang pengelolaan data digital yayasan; 2) pengembangan modul pelatihan berkelanjutan untuk seluruh anggota yayasan; serta 3) usulan kebijakan keamanan digital yang mencakup penggunaan autentikasi ganda, rotasi sandi berkala, dan peningkatan kontrol akses data berbasis peran.

Hasil ini didukung dengan penelitian sebelumnya yang menunjukkan bahwa dalam era digital yang terus berkembang, keamanan informasi menjadi krusial (Sunarso, 2024). Sistem keamanan informasi tidak hanya bergantung pada teknologi, tetapi juga pada faktor organisasi, sosial, dan manusia. Integrasi yang efektif antara teknologi, organisasi, dan sumber daya manusia menjadi kunci utama dalam menciptakan lingkungan keamanan informasi yang kuat dan adaptif. Kemudian penelitian lain menjelaskan bahwa tujuan strategis Strategi Keamanan Siber Indonesia adalah tercapainya ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber dan keamanan siber pada ekonomi digital (Ginanjar, 2022). Strategi Keamanan Informasi Indonesia ini diharapkan dapat menjadi salah satu fondasi kepercayaan dunia kepada Indonesia dalam berbagai forum keamanan siber internasional. Pendapat lain menekankan penting bagi profesional Sumber Daya Manusia untuk memahami kegunaan perangkat dan meninjau risiko dan prospek yang mungkin ditimbulkannya bagi suatu organisasi (Andrabi, 2020).

Discussion

Hasil kegiatan pelatihan menunjukkan bahwa pendekatan kolaboratif dalam edukasi keamanan siber sangat efektif dalam meningkatkan kesadaran dan kompetensi SDM organisasi. Peningkatan kesadaran ini sangat penting mengingat bahwa ancaman siber tidak hanya bersifat teknis, tetapi juga menyangkut faktor perilaku manusia sebagai titik masuk utama *(human error)*. Oleh karena itu, pelatihan yang menekankan aspek peran SDM menjadi sangat relevan dan strategis. Temuan dalam sesi diskusi menyatakan bahwa keberhasilan implementasi keamanan siber tidak dapat bergantung sepenuhnya pada teknologi, melainkan juga pada partisipasi aktif dari seluruh individu dalam organisasi. Kebijakan pelatihan kolaboratif mampu memperkuat pemahaman konsep *Protect Detect Respond Recover* secara holistik (Wright, 2023). Dalam konteks Yayasan Teratai Putih Yogyakarta, terdapat kesadaran baru bahwa keamanan digital adalah tanggung jawab kolektif, bukan hanya milik tim IT. Hal ini menandakan terjadinya *paradigm shift* dalam pendekatan keamanan informasi yang lebih holistik dan berbasis budaya organisasi. Hal ini didukung oleh penelitian lain bahwa pelatihan berbasis simulasi, sertifikasi profesional, serta program kesadaran keamanan siber secara berkelanjutan berkontribusi signifikan terhadap peningkatan kompetensi kapasitas SDM (Yusron, 2025).

https://doi.org/10.17509/abmas.v25i1.83473

Pendekatan ini mendukung efektivitas *active learning* yang menyatakan bahwa pembelajaran berbasis pengalaman dapat meningkatkan retensi pengetahuan dan keterampilan praktis. Pendekatan *active learning* misalnya *embedded training* yang langsung men-*trigger* pelatihan saat pengguna hendak melanggar kebijakan dibuktikan mampu meningkatkan retensi pengetahuan hingga 75% dibanding metode pasif (Doolittle *et al.,* 2023).

Lebih lanjut, hasil FGD mengungkapkan bahwa meskipun peserta memiliki semangat tinggi untuk meningkatkan keamanan digital, masih ditemukan kendala seperti keterbatasan sumber daya teknis, belum tersedianya kebijakan tertulis tentang manajemen data, serta belum optimalnya pelatihan keamanan digital secara berkala. Oleh karena itu, rekomendasi kebijakan yang dihasilkan selama pelatihan termasuk pembuatan SOP dan pembentukan tim respons insiden merupakan langkah awal yang signifikan dalam menciptakan sistem manajemen keamanan siber yang berkelanjutan. Pembuatan SOP penanganan insiden, eskalasi insiden, hingga penutupan insiden guna mempermudah evaluasi pasca-insiden untuk memperbaiki proses penanganan insiden di masa yang akan datang (Padel & Sutabri, 2023).

Pendapat lain menjelaskan penting untuk memperkuat penerapan Undang-Undang Perlindungan Data Pribadi (UU PDP) dengan mengintegrasikan langkah - langkah penegakan hukum yang efektif (Sorisa *et al.,* 2024). Upaya ini diharapkan dapat memitigasi risiko kebocoran data di masa depan dan membangun kembali kepercayaan masyarakat terhadap layanan publik. Dalam penelitian lain, strategi nasional pembangunan SDM BSSN melalui aksi kolaborasi dan peta okupasi mempertegas bahwa investasi pada pelatihan berkelanjutan merupakan fondasi budaya keamanan kolektif, bukan sekadar tanggung jawab tim IT (Rai *et al*., 2022).

Implikasi dari kegiatan ini menunjukkan bahwa yayasan sosial atau lembaga nirlaba pun tidak dapat mengabaikan pentingnya investasi pada pelatihan SDM terkait keamanan siber. Mengingat tingginya potensi risiko serangan terhadap organisasi yang menyimpan data sensitif, maka keberlanjutan dari inisiatif seperti ini sangat disarankan, tidak hanya untuk kepentingan keamanan, tetapi juga untuk menjaga kepercayaan publik terhadap integritas yayasan.

CONCLUSION

Kegiatan pengabdian masyarakat ini menegaskan pentingnya peran SDM dalam memperkuat keamanan siber pada platform media sosial Yayasan Teratai Putih Yogyakarta. Peserta memperoleh pemahaman mendalam mengenai strategi perlindungan data, kebijakan keamanan, serta langkah-langkah pencegahan ancaman siber. Dengan meningkatnya kesadaran dan keterampilan dalam mengelola keamanan digital, yayasan dapat meminimalkan risiko serangan siber serta menjaga kredibilitas dan kepercayaan publik terhadap informasi yang disampaikan. Yayasan perlu menerapkan kebijakan keamanan siber yang lebih ketat dan konsisten, termasuk pelatihan berkala bagi pengelola media sosial untuk mengantisipasi ancaman terbaru. Selain itu, investasi dalam teknologi keamanan serta kerja sama dengan pakar di bidang siber akan membantu meningkatkan perlindungan data secara berkelanjutan. Dengan langkah-langkah ini, Yayasan Teratai Putih Yogyakarta dapat menciptakan lingkungan digital yang lebih aman, profesional, dan terpercaya.

AUTHOR'S NOTE

Penulis menegaskan bahwa tidak terdapat konflik kepentingan dalam proses penulisan dan publikasi artikel ini. Selain itu, penulis memastikan bahwa seluruh data dan konten dalam artikel ini disusun secara orisinal dan terbebas dari unsur plagiarisme.

https://doi.org/10.17509/abmas.v25i1.83473

REFERENCES

Aditya, A. (2024). Upaya preventif cegah kejahatan siber dan penyalahgunaan transaksi elektronik melalui sosialisasi UU ITE. *Jurnal AbdiMas Nusa Mandiri*, 6(1), 22-27.

Aji, M. P. (2023). Sistem keamanan siber dan kedaulatan data di Indonesia dalam perspektif ekonomi politik (studi kasus perlindungan data pribadi). *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 13(2), 222-238.

Andrabi, U. (2020). The impact of social media on human resource intervention and social engineering. *Journal of Emerging Technologies and Innovative Research, 5*(4), 187-190.

Anugrah, R., Nugroho, D., & Nuche, A. (2024). Pengaruh sistem informasi manajemen dalam pembentukan kinerja organisasi bisnis di Indonesia. *Jurnal Mentari: Manajemen, Pendidikan dan Teknologi Informasi, 2*(2), 134-141.

Ben-Salamah, F., Palomino, M. A., Craven, M. J., Papadaki, M., & Furnell, S. (2023). An adaptive cybersecurity training framework for the education of social media users at work. *Applied Sciences (Switzerland), 13*(17), 1-18.

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. *Personal and Ubiquitous Computing*, 25(5), 941-955.

Dinda, A. L. S. (2024). Efektivitas penegakan hukum terhadap kejahatan siber di Indonesia. *Al-Dalil: Jurnal Ilmu Sosial, Politik, dan Hukum*, 2(2), 69-77.

Doolittle, P., Wojdak, K., & Walters, A. (2023). Defining active learning: A restricted systematic review. *Teaching and Learning Inquiry, 11*(1), 1-24.

Effendy, M. Y., & Oktiani, H. (2024). Literasi digital keamanan siber pada remaja menghadapi social engineering. *Wacana Publik, 18*(1), 35-42.

Ginanjar, Y. (2022). Strategi indonesia membentuk cyber security dalam menghadapi ancaman cyber crime melalui badan siber dan sandi negara. *Jurnal Dinamika Global, 7*(2), 291-312.

Imran, M. F., Gunawan, H., & Asmoro, D. (2024). Addressing the hurdles: Enhancing better policies in Indonesia cyber security management amidst uncertainty. *Jurnal Manajemen Pelayanan Publik*, 8(2), 275-290.

Irawan, A., Fadholi, W. H. N., Erikamaretha, Z., & Sinlae, F. (2024). Tantangan dan strategi manajemen keamanan siber di Indonesia berbasis IoT. *Journal Zetroem, 6*(1), 114-119.

Kristianti, N., & Kurniasi, R. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. Satya Dharma: Jurnal Ilmu Hukum, 7(1), 297-310.

Laksana, T. G., & Mulyani, S. (2024). Pengetahuan dasar identifikasi dini deteksi serangan kejahatan siber untuk mencegah pembobolan data perusahaan. *Jurnal Ilmiah Multidisiplin, 3*(1), 109-122.

Liedfray, T., Waani, F. J., & Lasut, J. J. (2022). Peran media sosial dalam mempererat interaksi antar keluarga di Desa Esandom Kecamatan Tombatu Timur Kabupaten Minasa Tenggara. *Jurnal Ilmiah Society, 2*(1), 1-13.

Napu, I. A., Supriatna, E., Safitri, C., & Destiana, R. (2024). Analisis peran keamanan siber dan keterampilan digital dalam pertumbuhan usaha kecil menengah di era ekonomi digital di Indonesia. *Sanskara Ekonomi dan Kewirausahaan, 2*(3), 156-167.

Padel, P. M. A., & Sutabri, T. (2023). Analisis Standard Operating Procedure (SOP) manajemen insiden menggunakan Framework ITIL V3 dengan metode analisis gap layanan pada PT Lingkaran Sistem Intelektual. *Indonesian Journal of Multidisciplinary on Social and Technology, 1*(2), 61-68.

https://doi.org/10.17509/abmas.v25i1.83473

Surbakti, F. P. S. (2024). Edukasi keamanan siber berdigital dengan aman. *Prima Abdika: Jurnal Pengabdian Masyarakat, 4*(4), 868-878.

Rai, I. N. A. S., Heryadi, D., & Kamaluddin N., A. (2022). Peran Indonesia dalam membentuk keamanan dan ketahanan di ruang siber. *Jurnal Politica Dinamika, 13*(1), 43-66.

Rozikin, A. Z., & Suyati, E. S. (2023). Pengaruh media sosial dan efikasi diri terhadap perilaku konsumsi siswa SMAN 3 Palangka Raya. *Jurnal Pendidikan Ekonomi Undiksha, 15*(1), 28-35.

Situmorang, W., & Hayati, R. (2023). Media sosial Instagram sebagai bentuk validasi dan representasi diri. *Jurnal Sosiologi Nusantara, 9*(1), 111-118.

Sorisa, C., Kiareni, C. L., & Parsuhip, J. (2024). Etika keamanan siber: Studi kasus kebocoran data BPJS kesehatan di Indonesia. *Jurnal Sains Student Research, 2*(6), 586-593.

Sunarso, B. (2024). Organizational and social factor analysis: The role of human resources in the success of information security systems in the digital business context. *Technology and Society Perspectives (TACIT), 2*(1), 165-192.

Syaddam, S., Febrianti, Z., Christian, M., & Samuel, H. (2024). Perancangan database sistem kearsipan di SMP 13 Negeri Tarakan menggunakan DBLC. *Jurnal Dialektika Informatika (Detika), 5*(2), 55-71.

Wahyudi, I., Sulistyowati, A., & Bikorin. (2025). Pemanfaatan Sistem Informasi Manajemen (SIM) untuk optimalisasi administrasi Kalurahan Imogiri. *Jurnal Pengabdian West Science, 4*(2), 230-236.

Wright, C. H. (2023). A collaborative cybersecurity training policy for future space endeavors. *Amos Conference, 52*(1), 153-192.

Yusron, M. (2025). Pembinaan peningkatan kapasitas SDM tim tanggap insiden siber pemerintah Daerah Provinsi Banten. *Jurnal Cahaya Nusantara, 1*(2), 86-92.

Yusuf, F., Rahman, H., Rahmi, S., & Lismayani, A. (2023). Pemanfaatan media sosial sebagai sarana komunikasi, informasi, dan dokumentasi: Pendidikan di Majelis Taklim Annur Sejahtera. *JHP2M: Jurnal Hasil-Hasil Pengabdian dan Pemberdayaan Masyarakat, 2*(1), 1-8.

Zed, E. Z., Apriliasari, D. F., Nursaidah, H., Sulastri, I., Triantoro, T., & Bangsa, P. (2025). Pengaruh strategi pemasaran melalui media sosial terhadap penjualan pada usaha dadar beredar di Cikarang Bekasi. *Stratēgo: Jurnal Manajemen Modern, 7*(1), 218-229.

https://doi.org/10.17509/abmas.v25i1.83473