JPMB: Jurnal Pemberdayaan Masyarakat Berkarakter
e-ISSN 2622-6928 | p-ISSN 2622-5387
Vol. 3 No.2 (Agustus-Desember) 2020, Hal. 121-132

Data *Security Awareness* sebagai Upaya Peningkatan Literasi Tentang *Cyber Attacks* dan *Threats*

Khairunnisak Nur Isnaini[1], Dina Fajar Sulistiyani[2], Manut Sutrisno[3]

Abstrak: Tujuan kegiatan pengabdian yang dilaksanakan adalah untuk meningkatkan kewaspadaan terhadap perlindungan dan keamanan data bagi guru terutama di lingkungan sekolah. Upaya konkret yang ditempuh adalah menerapkan langkah-langkah yang tepat dan solutif. Tahap pelaksanaan dibagi menajdi 3 tahap yaitu pra-pelaksanaan, pelaksanaan, dan pasc-pelaksanaan. Tahap-tahap tersebut dituangkan dalam kegiatan seminar dalam bentuk ceramah dan diskusi serta workshop dalam bentuk demonstrasi dan praktikum. Seminar dan workshop dibantu dengan handout materi dan modul praktikum untuk memudahkan peserta dalam menggunakan software pemulihan data yaitu Recuva. Hasil yang diperoleh dilihat pada tahap pasca-pelaksanaan yaitu pada evaluasi akhir kegiatan. Hasilnya yaitu guru-guru masih kurang mengetahui pentingnya sebuah aset informasi (data) untuk dilindungi. Hasil tersebut dilihat dari jawaban post-test pada Google Form yang tertuang dalam gambar grafik menunjukaan jawaban salah sebesar 60%. Namun ketika mempraktikkan penggunaan software recuva hampir semua peserta dapat mengoperasikannya. Secara garis besar dapat dikatakan bahwa pengetahuan dan kewaspadaan tentang pengamanan dan perlindungan aset informasi masih tergolong minim. Oleh karena itu diperlukan tindak lanjut konkrit dan tepat agar hal-hal yang tidak diinginkan dapat diminimalisir risikonya.

Kata kunci : *Data Security; CIA; Backup and Recovery; Physical Security; Logical Password*

Abstract: *The service activity is conducted to increase awareness of data protection and security for teachers, especially in the school environment. The threat that may happen is losing important data related to the learning process. This can occur due to hardware failure, software failure, human resource failure, natural, financial, external, and internal. The concrete effort taken is to*

[1] Universitas Amikom Purwokerto, Jl. Letjend Pol. Soemarto, Watumas, Purwanegara, Purwokerto, Indonesia, nisak@amikompurwokerto.ac.id
[2] Universitas Amikom Purwokerto, Jl. Letjend Pol. Soemarto, Watumas, Purwanegara, Purwokerto, Indonesia, fajardinasulistiyani@gmail.com
[3] Universitas Amikom Purwokerto, Jl. Letjend Pol. Soemarto, Watumas, Purwanegara, Purwokerto, Indonesia, manutsutrisno13@gmail.com

implement appropriate and solution steps. The implementation stage is divided into 3 stages, namely pre-implementation, implementation, and post-implementation. These stages are outlined in seminar and workshop, which assisted with handout materials and practicum models to make it easier for participants to use data recovery software, namely Recuva. The result obtained was seen in the post-assessment stage at the final evaluation of the activity. The result is that teachers are still not prepared to protect an information asset (data). These results are seen from the post-test answers on the Google Form which are contained in the graphic image showing 60% wrong answers. However, when practicing the use of software which is recognized almost all participants can operate it. Generally, it can be said that knowledge and awareness about information security and assurance are still relatively lacking. Therefore, concrete and precise follow-up is needed so that things that are undesirable can be minimized.

Keywords: *Data Security; CIA; Backup and Recovery; Physical Security; Logical Password*

A. Pendahuluan

Keamanan informasi adalah proses langsung yang terdiri dari dominan keamanan fisik dan skema klasifikasi dokumen sederhana (Whitman & Mattord, 2011). Perlindungan terhadap keamanan informasi dapat dilakukan dengan beragam cara dengan tujuan untuk menyakinkan intergritas, kerahasiaan, kekonsistenan data yang diolah. Tujuan lain dari perlindungan terhadap keamanan informasi yaitu dapat meminimalisir risiko yang dapat terjadi sewaktu-waktu apabila apabila terdapat hal-hal yang dapat mengancam keberlangsungan suatu sistem dalam perusahaan atau lembaga. Reputasi sebuah organisasi akan dicermati dan dinilai oleh masyarakat apabila dapat diyakini oleh integritas informasi, kerahasiaan informasi, dan ketersediaan informasi(IBISA, 2011).

Ancaman-ancaman yang dapat mengganggu kelangsungan bisnis suatu organisasi dapat terjadi karena banyak faktor yang mempengaruhinya. Oleh karena itu perlindungan terhadap keamanan informasi penting untuk dilakukan. Ancaman (IBISA, 2011) adalah aksi atau kejadian yang dapat merugikan perusahaan yang mengakibatkan kerugian berupa biaya, tenaga upaya, reputasi nama baik, dan paling parah adalah dapat membuat organisasi pailit. Ancaman tersebut dapat berupa *hardware failure, software failure*, kegagalan sumber daya manusia, alam, keuangan, eksternal, dan internal.

Menurut (Katadata, 2015), saat ini pengguna *smartphone* secara umum di Indonesia pada Tahun 2016-2019 sebanyak 92 juta pengguna dan khususnya terdapat 73% dari pengguna tersebut merupakan Android *user*. Artinya, guru di SMP Negeri 3 Purbalingga adalah beberapa pengguna yang masuk ke dalam daftar tersebut. Di dalam penggunaan akun dan internet, terkadang pengguna mengabaikan aspek-aspek keamanan informasi. Aspek-aspek keamanan informasi tersebut antara lain kerahasiaan, ketersediaan, dan integritas. Seringkali pengguna tidak sadar untuk menjaga itu semua. Seperti halnya seringkali terjadi di sekolah-sekolah maupun instansi lain tidak mengunci perangkat ponsel, personal computer maupun laptop dengan kata sandi. Kasus lain dapat terjadi misalnya mengakses situs pendidikan namun tidak sengaja menge-klik iklan dan tiba-tiba muncul yang dimungkinkan iklan tersebut mengandung virus maupun akses yang dapat menyebabkan hilangnya sebuah data. Serangan terhadap kontrol akses, kata sandi, maupun situs yang disisipi virus dan lainnya sering disebut *Cyber Attacks and Threats*.

Beberapa kasus yang pernah terjadi akibat cyber attacks and threats antara lain (Wardani, 2018) melaporkan, bahwa sejak Tahun 2013 tedapat data yang dibobol mencapai 6,9 juta per harinya. Data yang hilang beberapa di antaranya berasal dari sosial media sebanyak 56,11% dan diikuti oleh data instansi 26,62%. Tipe pelanggaran yang ada diklasifikasikan menjadi pencurian data (64,55%), akses akun (17,47 %), akses finansial (13,02%), berbagai gangguan, hingga data eksistensial. Fakta lain mengungkap bahwa hanya 4% dari jumlah tersebut yang dilindungi enkripsi oleh pemiliknya. Kasus lain(Online, 2019) yang terjadi yaitu adanya pencurian data siswa di suatu sekolah di Distrik Washoe County School. Pelanggaran yang terjadi adalah pencurian data siswa yang terdaftar pada Tahun 2001-2016 dan informasi yang bocor salah satunya adalah tanggal lahir para siswa. Secara umum kedua hal tersebut dapat terjadi karena kurangnya kesadaran menjaga keamanan informasi dari pemilik data tersebut maupun secara organisasi masih belum memiliki perangkat perlindungan keamanan informasi yang lengkap dalam menghadapi cyber attacks and threats.

Kasus lain cyber attacks and threats dapat berupa Social engineering. Social engineering sendiri berarti pelaku Social Engineering untuk melakukan hal-hal yang illegal seperti mencuri informasi yang tidak seharusnya diketahui olehnya. (Widodo & Gunawan, 2017)**.** Tentunya pengetahuan tentang *cybersecurity awareness* atau keamanan siber sangat diperlukan pada saat ini bagi organisasi, perusahaan ataupun individu saat menggunakan internet untuk menghindari adanya gangguan, ancaman

siber (*cyber threat*), serangan siber (*cyber attack*) yang sewaktuwaktu bisa terjadi kepada mereka.(Ramadhani & Raf, 2020)

Ancaman keamanan informasi dapat pula menganggu kinerja dan aktivitas para guru. Menurut (Admin, 2020) Guru-guru yang mengajar di SMP Negeri 3 Purbalingga berjumlah 41 orang. Tentunya guru dalam aktivitas digitalnya tidak lepas dari internet. Di dalamnya, lebih jauh lagi guru memanfaatkan akses internet tersebut untuk membuka akun dan data-data yang berkaitan dengan data akademik. Seperti contohnya data soal dan kunci jawaban atau data akun pribadi yang ter integrasi dengan data institusi seperti data pada mobile banking atau sosial media. Serangan dan ancaman terhadap keamanan informasi dapat terjadi kapanpun dan dimanapun. Selain aktivitas digital, aktivitas fisik pun tidak luput dari upaya pencurian data. Misalnya berkas-berkas yang tertinggal di meja kerja dan berkas tersebut merupakan informasi penting terkait dengan data akademik ataupun data institusi.

Pentingnya penerapan keamanan logis dan keamanan fisik yaitu untuk mencegah adanya upaya serangan dan ancaman terhadap keamanan informasi, khususnya keamanan data untuk guru. Selain itu upaya pencegahan dengan melakukan tindakan preventif adalah dengan untuk menjaga ketersediaan, integritas, dan kerahasiaan suatu informasi (secara pribadi maupun melibatkan institusi) akibat human *error* maupun *hardware/software failure* maupun bencana alam. Contohnya adalah penyadapan akun yang berisi data pribadi yang ter integrasi dengan akun mobile banking untuk penerimaan honor guru per bulan dapat dengan disadap dan diakses secara ilegal oleh orang yang tidak bertanggungjawab. Akses tersebut dapat menemukan data pribadi seperti nomor induk kependudukan, alamat dan nomor telfon korban. Tentunya hal tersebut dapat menganggu aktivitas para guru secara umum dan merugikan nama pribadi maupun institusi apabila disebarkan di dunia sosial mengenai hal pribadi lainnya seperti foto dan video. Contoh lain adalah adanya bencana alam dapat memporak porandakan sebagian maupun keseluruhan fasilitas umum, kantor termasuk sekolah yang terdapat berkas-berkas penting tertentu yang tidak sempat diamankan atau dibackup. Hal tersebut dapat terjadi karena kurangnya kesadaran mengenai keamanan informasi dilingkungan sekitar guru dan karyawan adminitrasi sekolah.

Keamanan fisik merupakan aspek yang terlihat tidak dapat diukur dengan besaran uang (intangible) namun sebenarnya kerugian yang ditimbulkan dari sistem keamanan yang lemah dapat dihitung dalam besaran uang. Manajemen dapat menghitung besarnya kerugian yang ditimbulkan, contohnya kerugian saat kehilangan data dapat

direpesentasikan dari jumlah biaya yang dibutuhkan untuk recovery data yang hilang tersebut.(Priatmoko, 2016)

Menurut (IBISA, 2013) sistem komputer memiliki empat parameter keamanan yang sangat penting antara lain *physical security, system security, application security*, dan *data security*. *Physical security* merupakan perlindungan pertama yang langsung berhubungan dengan dunia luar. Sedangkan aspek setelahnya merupakan logical security yang membahas mengenai pengguna dapat masuk ke sistem, tingkat otoritas kepada masing-masing pengguna (sistem, program, dan data). *Logical security* menurut (IBISA, 2011) penting untuk dilakukan karena bertujuan untuk melindungi data atau informasi dari perusakan atau penghancuran yang dilakukan baik secara sengaja maupun secara tidak sengaja dan menghindari serta mendeteksi perubahan terhadap informasi yang dilakukan oleh yang tidak berwenang. *Physical security* dilakukan agar organisasi dapat membuat langkah-langkah seperti meminimalkan risiko-risiko yang sewaktu-waktu dapat terjadi misalkan kebakaran, memiliki *physical security* yang memadai, dan memiliki program *recovery* yang memadai dan dapat dipertanggungjawabkan.

Maka dari itu, permasalahan yang muncul terkait potensi serangan dan ancaman keamanan informasi, yang dapat mengancam data maupun informasi yang dimiliki guru perlu ditanggulangi dengan tepat. Prioritas solusi yang akan dituntaskan yaitu upaya meningkatkan kesadaran tentang keamanan data secara fisik maupun digital untuk guru dan karyawan. Upaya penaggulangan tersebut dapat dilakukan dengan beragam cara salah satunya mengadakan seminar mengenai keamanan data khususnya pada materi beragam aset keamanan informasi, cyber security ataacks and threats dilingkungan guru ataupun sekolah pda umumnya serta workshop menggunakan bantuan tools recovery data yaitu Recuva.

B. Metode Pelaksanaan

Pengabdian Masyarakat ini dilaksanakan di SMP Negeri 3 Purbalingga yang ber-alamat di. Adapun metode pelaksanaan dibagi menjadi 3 bagian yaitu pra-pelaksanaan, pelaksanaan, dan pasca-pelaksanaan. Penjabarannya antara lain:

1. Pra-Pelaksanan
    a. Membuat bahan materi berupa handout teori dan modul praktikum.
    b. Cek lokasi mitra pengabdian untuk memastikan persiapan ruangan untuk melakasanakan seminar dan *workshop* serta

jaringan internet yang memadai dengan kapasitas yang sesuai dengan jumlah peserta.

c. Instalasi software yang akan digunakan.

2. Pelaksanaan

a. Metode Seminar

Metode seminar yang dimaksud adalah ceramah dan diskusi. Pemateri akan menjelaskan beberapa materi dasar terkait keamanan data.

b. Metode demonstrasi dan praktik

Demonstrasi dan praktik diberikan untuk menjelaskan setiap proses yang ditempuh dari tahap awal hingga akhir. Proses-proses tersebut diterjemahkan ke dalam beberapa kegiatan antara lain

1) Demonstrasi contoh studi kasus *cyber attacks and threat* pada *email*, *world wide web*, dan data yang tersimpan di *personal computer* atau *usb flashdisk drive*.
2) Demonstrasi studi kasus *control access, management password*, dan *logical security*.
3) Praktik yang akan dilakukan adalah praktik *backup* and *recovery* data menggunakan tools Recuva.

3. Pasca-Pelaksanan

a. Evaluasi hasil akhir kegiatan

Evaluasi yang akan dilakukan adalah mengadakan post-test dalam bentuk tes *online* dan hasilnya digunakan untuk menjadi dasar pengambilan kesimpulan dari kegiatan yang telah di laksanakan.

b. Tindak lanjut kegiatan pengabdian dengan mitra

Hasil evaluasi post-test akan dianalisis oleh narasumber untuk mendapatkan saran atau rekomendasi yang tepat dalam rangka upaya meningkatkan *security awareness* pengguna (peserta seminar dan workshop) dari bahaya ancaman dan serangan yang menyerang data.

C. Hasil dan Pembahasan

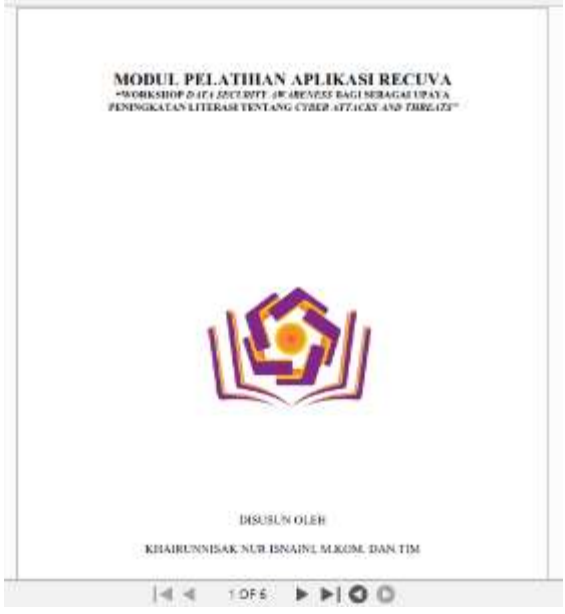
1. Pra pelaksanaan

Tahap awal pada kegiatan ini adalah tahap persiapan. Tahap persiapan berjalan sesuai dengan rencana yang telah dirancang oleh tim pengabdian. Pada tahap pra-pelaksanaan terdapat tiga aktivitas

antara lain membuat bahan materi materi berupa handout teori dan modul praktikum, kedua cek lokasi mitra untuk memastikan fasilitas yang akan digunakan telah memadai, dan terakhir dalah instalasi software yang digunakan. Visualisasi handout dan praktikum dapat dilihat dari gambar 1 dan gambar 2.

Gambar 1. Salah satu handout materi

Pada gambar 1 adalah handout materi yang berisikan macam-macam pengetahuan dasar tentang keamaanan informasi (data seacra khusus).



Gambar 2. Pelaksanaan praktikum penggunaan Recuva

Pada gambar 2 praktik tersebut akan dilengkapi dengan modul praktikum dari instalasi hingga penggunaanya software tersebut. Software tersebut berfungsi sebagai upaya penanggulangan hilangnya data akibat berbagai macam alasan keamanan informasi.

Maka dari itu, workhsop yang diselenggarakan menjadi hal yang penting bagi guru di lingkungan sekolah secara pribadi maupun umum dalam mengamankan sebuah aset keamanan informasi berupa data dan informasi.

2. Pelaksanaan

Tahap pelaksanaan kegiatan dibagi menjadi dua aktivitas yaitu seminar dan demonstrasi juga praktik. Tahap pertama yaitu pemaparan materi dalam bentuk seminar. Materi yang disampaikan yaitu Keamanan Informasi secara umum, aset keamanan informasi khusunya di lingkungan sekolah dan guru, serangan mapun ancaman terhadap aset keamanan informasi, dan perlindungan aset secara fisik. Adapun penjabaran materinya antara lain

a. Konsep dasar keamanan informasi (tujuan dan konsep CIA(*Confidentiality, Integrity, Availability*)
b. Aset Keamanan informasi (*personel, hardware, software, data*, fasilitas, dan penunjang)
c. *Cyber Security Attacks and Threats* (kegagalan sistem/hardware software failure, kegagalan sumber daya manusia/minimnya *security awareness, virus, phising*, sabotase, bencana alam)
d. Keamanan fisik/*Physical Security* pada lingkup sekolah dan aktivitas guru (akses ilegal, serangan pada perangkat keras, kesadaran dan kepedulian “insider”, aturan *clean desk policy*)
e. *Recovery data*

Semua pemahaman materi peserta akan diukur melalui post-test melalui Google Form (berbentuk pilihan ganda) untuk mengukur peningkatan pengetahuan tentang *data security awareness* guru setelah diberikan pemaparan materi. Post-test merupakan bentuk luaran konkrit dan terukur secara kuantitatif sebagai hasil dari proses penyampaian materi yang disampaikan oleh dosen kepada mitra pengabdian yaitu guru SMP Negeri 3 Purbalingga.

Tahap kedua adalah demonstrasi dan praktik. Demontrasi yang dilakukan untuk dua materi utama yaitu studi kasus cyber attacks and threat dan studi kasus control access dan management password. Adapun penjabarannya yaitu

a. Demonstrasi contoh studi kasus *cyber attacks and threat* pada *email*, *world wide web*, dan data yang tersimpan di *personal*

computer atau *usb flashdisk drive*. Contoh studi kasus dihubungkan dengan persoalan keamanan informasi yang sering terjadi dilingkungan sekolah secara pribadi maupun institusi. Misalnya hilangnya data di *personal computer* maupun *usb flashdisk drive*, situs yang terindikasi menyebarkan virus atau penyadapan informasi.

b. Demonstrasi studi kasus *control access, management password*, dan *logical security*. Contoh studi kasus dihubungkan dengan persoalan keamanan informasi yang sering terjadi dilingkungan sekolah secara pribadi maupun institusi. Misalnya pembuatan *password* yang baik dan benar sesuai acuan *control password*, cara pengamanan dan studi kasus yang berkaitan dengan akun.
c. Praktik recovery data menggunakan software Recuva. Visualisasi software Recuva dan kegiatan praktik tersebut dapat dilihat pada gambar 3

Gambar 3. Pelaksanaan praktikum

Pada gambar 3 narasumber sedang menjelaskan langkah-langkah dalam pemulihan data menggunakan software Recuva. Praktik tersebut di awali dengan membuat simulasi data yang akan disimpan disebuah flasdisk drive yang kemudian dihapus. Kemudian, peserta membuka aplikasi recuva dan mencari tempat/drive dimana data tersebut hilang. Selanjutnya mengikuti arahan sesuai yang tertera dimodul dan juga narasumber hingga menemukan data yang hilang tersebut kembali. Pada saat akan mengembalika data yang hilang pemakai/user diarahkan untuk tidak menyimpan data yang hilang tersebut ke tempat semula melainkan di tempat atau drive yang lain.

3. Pasca-Pelaksanaan

Tahap terakhir dalam kegiatan pengabdian adalah evaluasi. Pasca-pelaksanaan ini dibagi menjadi aktivitas ayitu evaluasi ahsil akir kegiatan dan tindak lanjut kegiatan penagbdia dengan mitra. Penjabaran aktivutas tersebut antara lain

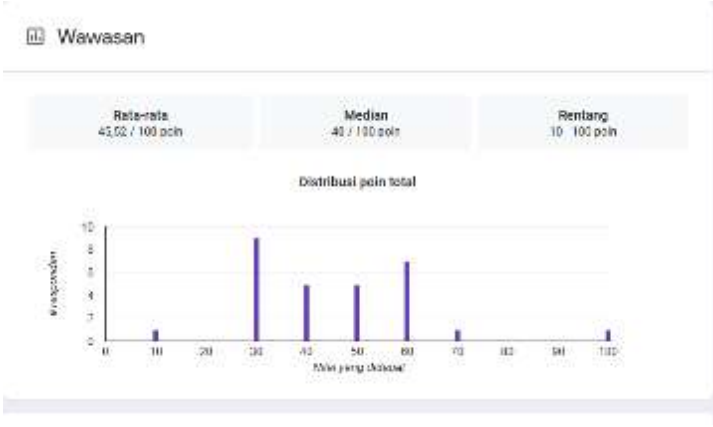
a. Evaluasi hasil akhir kegiatan

Bentuk evaluasi hasil akhir kegiatan adalah mengadakan post-test dalam bentuk tes *online* yang berisi materi pada saat seminar hingga *workshop* menggunakan Google Form. Pelakasanaan post-test berlangsung di hari yang sama dalam waktu 15 menit. Hasil pengukuran didapatkan dari isian jawaban google form pertanyaan seputar materi yang telah disampaikan menjadi dasar pengambilan kesimpulan dari kegiatan yang telah di laksanakan. Penggunaan Google Form dengan pemberian skor mempermudah evaluator yaitu narasumber untuk mengetahui sejauh mana pemahaman peserta selain itu juga dapat menambah ilmu pengetahuan baru kepada peserta dengan jawaban benar yang telah disediakan. Pertanyaan yang digunakan dalam post-test tersebut terdapat pada tabel 1.

Tabel 1. Daftar Tema Pertanyaan

No	Daftar Tema Pertanyaan
1	Keamanan Informasi
2	Aset Informasi
3	Ancaman sebuah informasi
4	Akses Kontrol
5	Parameter sebuah keamanan
6	mekanisme keamanan fisik
7	Insider akses informasi
8	Jenis informasi
9	Aspek keamanan fisik
10	Ancaman terhadap penggunaan PC

Pada tabel 1 terdapat 10 pertanyaan yang dijawab oleh guru-guru. Pertanyaan tersebut berasal dari materi semianar yang disampaikan pada awal kegiatan. Selanjutnya adalah mengukur pemahaman peserta. Hasil yang diperoleh dapat dilihat pada grafik 1.



Grafik 1. Pemahaman Peseta

Dari grafik 1 dapat dilihat bahwa rata-rata nilai yang diperoleh ada pada rentang 30-60 artinya peserta masih belum memahami tentang perlindungan dan kewaspadaan mengenai aset informasi.

b. Tindak lanjut kegiatan pengabdian dengan mitra
Berdasarkan pada grafik 1 masih banyak peserta yang masih belum memahami pentingnya sebuah keamanan informasi untuk aset-aset yang dimiliki oleh guru maupun sekolah. Oleh karena itu tindak lanjut setelah kegiatan pengabdian selesai dilaksanakan pengabdian selanjutnya dengan salah satu subbab secara spesifik dibahas dengan mitra untuk turut membantu menyelesaikan persoalan tersebut.

D. Simpulan

Berdasarkan hasil dan maka diambil kesimpulan sebagai berikut: (1) Kegiatan tersebut telah menambah ilmu pengetahuan guru-guru di SMP Negeri 3 Purbalingga akan berbagai macam hal yang masuk ke dalam aset keamanan informasi, perlindungan secara fisik, bahaya akibat adanya cyber attacks and threat, serta cara pemulihan data menggunakan salah satu software recovery data yaitu recuva; (2) Kegiatan pengabdian dapat meningkatkan kemampuan guru-guru di SMP Negeri 3 Purbalingga dalam mengamankan data-data pribadi maupun yang berkaitan dengan sekolah misalnya memperketat management password; (3) kegiatan pengabdian juga telah meningkatkan *awareness* tentang pentingnya menjaga akun dan password email yang sedang digunakan sebagai pintu masuk ke hampir semua akses aplikasi maupun website. Selain itu perlindungan terhadap

personal komputer dan ruangan kerja yang berhubungan dengan data digital maupun fisik.

Ucapan Terima Kasih

Tim pengabdian masyrakat mengucapkan terima kasih kepada Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Amikom Purwokerto dan SMP Negeri 3 Purbalingga sebagai mitra pengabdian. Suksesnya kegiatan pengabdian masyarakat tentunya tidak lepas dari bantuan kedua instansi tersebut dan antuasiasme peserta dala mengikuti keseluruhan acara.

Daftar Pustaka

Admin. (2020). Data Guru SMP N 3 Purbalingga. Retrieved from http://sekolah.data.kemdikbud.go.id/index.php/chome/profil/D0111D5A-2DF5-E011-842F-C30817A7FE4F

IBISA. (2011). *Keamanan Sistem Informasi*. Yogyakarta: ANDI OFFSET.

IBISA. (2013). *Physical Security*. Yogyakarta: CV ANDI OFFSET.

Katadata. (2015). *pengguna-smartphone-di-indonesia-2016-2019.pdf*. Retrieved from https://databoks.katadata.co.id/datapublish/2016/08/08/pengguna-smartphone-di-indonesia-2016-2019

Online, R. W. (2019). Bahaya, Belasan Ribu Data Siswa Dicuri. Retrieved March 3, 2020, from Warta Ekonomi website: https://www.wartaekonomi.co.id/read239371/bahaya-belasan-ribu-data-siswa-dicuri.html

Priatmoko, D. B. (2016). UNTUK MELINDUNGI DATA ORGANISASI (Studi Kasus Pada Unit Penerimaan Mahasiswa Baru Dan Sistem Informasi (PMBSI) IKIP PGRI MADIUN). *Jurnal Administrasi Bisnis (JAB)*, *40*(1), 160–169.

Ramadhani, M. R., & Raf, A. (2020). Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia. *AUTOMATA*, *1*(2).

Wardani, A. S. (2018). 4,5 Miliar Data Dicuri Selama 6 Bulan Pertama 2018. Retrieved March 3, 2020, from Liputan 6 website: https://www.liputan6.com/tekno/read/3665291/45-miliar-data-dicuri-selama-6-bulan-pertama-2018

Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security Fourth Edition. In *Course Technology*.

Widodo, P., & Gunawan, D. (2017). Efektivitas keamanan informasi dalam menghadapi ancaman social engineering effectiveness of information security threats facing social engineering. *Peperangan Asimetris*, 73–90.