e-ISSN : 2964 - 4533

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95

Cyber Security Awareness di Lingkungan Sekolah Menengah Pertama (SMP) Negeri 215 DKI berdasarkan ISO 27001:2013

Rahmat Rian Hidayat *[1], Muhammad Rifqi[2],
[1,2,*]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana
*e-mail: rahmat.rian@mercubuana.ac.id[1],m.rifqi@mercubuana.ac.id[2],

ABSTRACT

The utilization of technology in various sectors of the organization is no longer "just" a factor in increasing competitiveness. But in addition, it has become an existential threat. Information (data) is a valuable asset, so information protection is very important for an organization. Seeing the increasing importance of the role of information in the organization, information threats and vulnerabilities are increasing with the emergence of certain information hacks / leaks that have an impact on the organization. The rapid development of technology has led to a rise in cybercrime. In the future, an organization's business processes will rely more on ICT. It is feared that personnel in the organization still lack IT literacy and information security awareness, or the use of information technology or information systems does not meet the organization's internal standards. In every organization's efforts to protect information, security awareness is a very important role. Unfortunately, this aspect often gets less attention. As a result, it can lead to the threat of total failure of all efforts and energy expended to protect the organization's information. Therefore, awareness is a starting point for all employees in the organization to pursue or understand information technology security knowledge. With information security awareness, employees can focus on one or more possible problems or threats. In addition, it is necessary to raise the awareness of all employees, teachers and even students. Community service that will be carried out at SMPN 215 DKI Jakarta Barat is expected to improve IT literacy and information security awareness even better.

Keywords: Awareness, Cyber, Data, Information, Security

ABSTRAK

Pemanfaatan teknologi di berbagai sektor organisasi tidak lagi “hanya” menjadi faktor peningkatan daya saing. Tapi di samping itu, telah menjadi ancaman eksistensial. Informasi (data) merupakan aset yang berharga, sehingga perlindungan informasi sangat penting bagi suatu organisasi. Melihat semakin pentingnya peran informasi dalam organisasi, ancaman dan kerentanan informasi semakin meningkat dengan munculnya peretasan/bocoran informasi tertentu yang berdampak pada organisasi. Perkembangan teknologi yang pesat menyebabkan meningkatnya kejahatan dunia maya. Ke depan, proses bisnis organisasi akan lebih bergantung pada TIK. Dikhawatirkan personel dalam organisasi masih kurang melek IT dan kesadaran keamanan informasi, atau penggunaan teknologi informasi atau Sistem informasi tidak memenuhi standar internal organisasi. Dalam upaya setiap organisasi untuk melindungi informasi, kesadaran keamanan adalah peran yang sangat penting. Sayangnya, aspek ini seringkali kurang mendapat perhatian. Akibatnya, hal itu dapat menyebabkan ancaman kegagalan total dari semua upaya dan energi yang dikeluarkan untuk melindungi informasi organisasi. Oleh karena itu, kesadaran merupakan titik awal atau starting point bagi seluruh pegawai dalam organisasi untuk menekuni atau memahami pengetahuan keamanan teknologi informasi. Dengan kesadaran keamanan informasi, pegawai dapat fokus pada satu atau lebih kemungkinan masalah atau ancaman. Selain itu, perlu meningkatkan kesadaran seluruh karyawan, guru bahkan siswa. Pengabdian kepada masyarakat yang akan dilaksanakan di SMPN 215 DKI Jakarta Barat ini diharapkan dapat meningkatkan literasi IT dan kesadaran keamanan informasi lebih baik lagi.

Kata kunci:, Awareness, Cyber, Data, Informasi, Security

e-ISSN : 2964 - 4533
PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95

1. PENDAHULUAN

Transformasi digital yang pesat yang dibawa oleh Revolusi Industri 4.0 memang telah mengubah dunia. Konstelasi aplikasi teknologi secara fundamental telah mengubah semua bidang bisnis dan kehidupan. Ini termasuk organisasi yang bergerak di bidang pendidikan tinggi. Merebaknya pandemi COVID-19 sejak awal tahun 2020 telah mempercepat perubahan mendasar ini. Tidak hanya harus berubah dengan cepat, tetapi juga harus berubah sekarang.

Pemanfaatan teknologi di berbagai sektor organisasi tidak lagi "hanya" menjadi faktor peningkatan daya saing. Di samping itu, itu telah menjadi ancaman eksistensial. Banyak organisasi dan perusahaan terpaksa tutup karena tidak siap mengikuti proses penggunaan teknologi saat menjalankan bisnisnya. Tentu ada faktor lain, namun penggunaan teknologi merupakan salah satu faktor kunci yang dapat digunakan untuk menjawab tantangan tersebut.

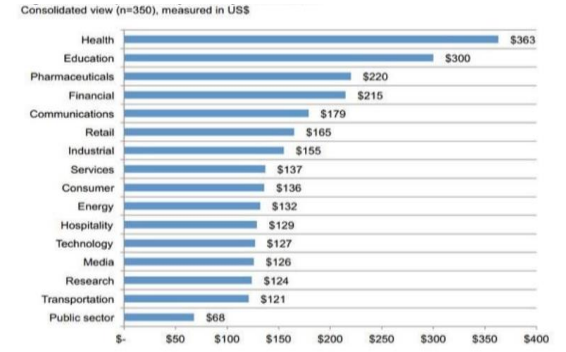
Informasi dan data merupakan aset yang berharga, sehingga perlindungan informasi sangat penting bagi suatu organisasi. Keamanan informasi adalah untuk melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan operasi sebuah organisasi, meminimalkan kerusakan yang disebabkan oleh ancaman, dan mempercepat pemulihan alur kerja organisasi.

Melihat semakin pentingnya peran informasi dalam organisasi, ancaman dan kerentanan informasi semakin meningkat dengan munculnya peretasan/bocoran informasi tertentu yang berdampak pada sebuah organisasi. Pengamanan informasi sangat dibutuhkan supaya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi dapat terjaga sehingga tidak mengganggu kinerja dan operasional organisasi.

Misalnya data akademik yang merupakan data yang sangat penting di dalam dinas pendidikan Dengan data tersebut akan melancarkan berbagai urusan baik siswa, guru dan pegawai sekolah. Jika dirusak oleh orang yang tidak bertanggung jawab, sekolah akan kewalahan dalam memulihkan data tersebut. Bisa jadi data itu akan hilang selamanya tidak bisa diperbaiki kembali.

Baru-baru ini data sebanyak 815 data pribadi milik guru sekolah menengah atas (SMA) di Kabupaten Tangerang, Banten, bocor. Adapun data pribadi yang biasanya mengalami kebocoran itu meliputi nama lengkap, identitas nama gadis ibu, KTP dan nomor rekening. Disinyalir data tersebut bocor setelah diunggah ke situs vbook.pub yang mana situs ini sebagai penyedia e-book secara gratis. Menurut Ombudsman RI Perwakilan Banten menilai bahwa kebocoran data guru tersebut dikarenakan sumber daya manusia (SDM) yang tidak paham. Sehingga evaluasi secara menyeluruh terkait dengan bocornya ratusan data guru tersebut.(Budi, 2021)

Pendidikan adalah industri yang berada pada posisi tengah yang terkena dampak COVID-19. Ini berarti bahwa pendidikan mungkin menjadi pemenang dan pecundang. Itu tergantung pada bagaimana *stakholder* mempersiapkan dan bagaimana menghadapi kondisi yang berubah ini. Menurut survey Ponemon Institute, sektor pendidikan merupakan sektor dengan dampak biaya yang tertinggi kedua setelah sektor kesehatan jika terjadi insiden keamanan informasi padanya.



Gambar 1 : *Biaya per kapita insiden keamanan berdasarkan Industri*

e-ISSN : 2964 - 4533
PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95

Guru/pegawai bahkan Siswa wajib memiliki awareness yang tinggi akan keamanan informasi organisasinya. Hal ini bukan tanpa alasan mengingat meningkatnya kecondongan ancaman keamanan informasi di dunia. Informasi semakin memiliki nilai secara material sehingga menjadi target serangan siber. Perkembangan teknologi yang semakin pesat memicu peningkatan *cybercrime*, semakin tingginya tingkat ketergantungan proses bisnis organisasi terhadap TIK kedepannya, dikhawatirkannya personal dalam organisasi masih memiliki IT *Literacy* dan *information security awareness* yang rendah, atau penggunaan sistem informasi yang belum sesuai standar dalam internal organisasi (Pratama, 2020). Kegagalan dalam menerapkan *Information Security* akan berdampak buruk pada organisasi yang dapat berupa terganggunya kegiatan operasional/pelayanan organisasi, menurunnya reputasi organisasi dan kepercayaan dari stakeholder, kerugian finansial organisasi, bocornya rahasia organisasi, atau dampak buruk lainnya terhadap organisasi.(Umar Alhabsyi, 2020)

Perlu kita ketahui bahwa serangan keamanan informasi bisa dari dalam dan dari luar, adapun penyebab terbanyak adalah manusia baik secara personal maupun berkelompok dari sini kita menilai bahwa bisa jadi memungkikan pelanggaran paling besar justru dilakukan oleh pegawai, karena disebabkan oleh faktor kelalaian yang tak disengaja atau memang disengaja *(criminal)*. Manusia memegang peran penting dalam menerapkan sistem keamanan informasi. Simon dan Mitnick mengemukakan manusia merupakan faktor utama dan penting dalam pengamanan informasi selain teknologi, karena manusia merupakan rantai terlemah dalam rantai keamanan. Maka dari itu, dimensi manusia perlu selalu dibimbing dengan baik supaya segala bentuk ancaman dapat dihindari. Adapun upaya yang dapat dilakukan dengan menumbuhkan kesadaran akan pentingnya keamanan informasi.

Kesadaran terhadap keamanan informasi hal yang sangat krusial kontribusinya dalam usaha pengamanan informasi pada setiap organisasi. Namun, dimensi ini seringkali kurang mendapatkan kepedulian yang memadai. Risikonya dapat menyebabkan segala upaya yang telah dikeluarkan untuk pengamanan informasi pada sebuah organisasi terancam sia-sia.

Maka dari itu kesadaran merupakan poin atau titik awal untuk seluruh pegawai di suatu organisasi dalam mengejar atau memahami pengetahuan mengenai keamanan teknologi informasi.(Imam Suhartadi, 2021) Dengan adanya kesadaran pengamanan, seorang pegawai dapat memfokuskan perhatiannya pada sebuah atau sejumlah permasalahan atau ancaman-ancaman yang mungkin terjadi. Selanjutnya untuk menumbuhkan kesadaran seluruh pegawai, Guru bahkan siswa salah satu Universitas terbaik di Jakarta yaitu Mercu Buana melalui kegiatan Pengabdian Masyarakat mengangkat tema keamanan informasi.

2. METODE

Pengabdian kepada masyarakat adalah usaha untuk menyebarluaskan ilmu pengetahuan, teknologi, dan seni kepada masyarakat. Kegiatan tersebut harus mampu memberikan suatu nilai tambah bagi masyarakat, baik dalam kegiatan ekonomi, kebijakan, dan perubahan perilaku (sosial). Kegiatan ini terdiri dari beberapa dosen sebagai narasumber dan sesuai dengan judul yang diajukan pada proposal maka saya menyampaikan presentasi tentang Cyber Security Awareness di Lingkungan SMPN 215 Jakarta Barat berdasarkan ISO 27001:2013.

Kegiatan pengabdian masyarakat mengusung tema “Pengenalan Media Online pada masa pandemi dalam meningkatkan kinerja dan kesadaran keamanan informasi Guru Sekolah SMPN 215 Jakarta Barat”

Kegiatan pengabdian masyarakat ini dilaksanakan secara Hybrid yang mana peserta ada yang bergabung di lokasi sekolah dan ada yang bergabung secara online melalui zoom. Kegiatan ini didukung dengan menggunakan komputer, infocus dan layar besar.

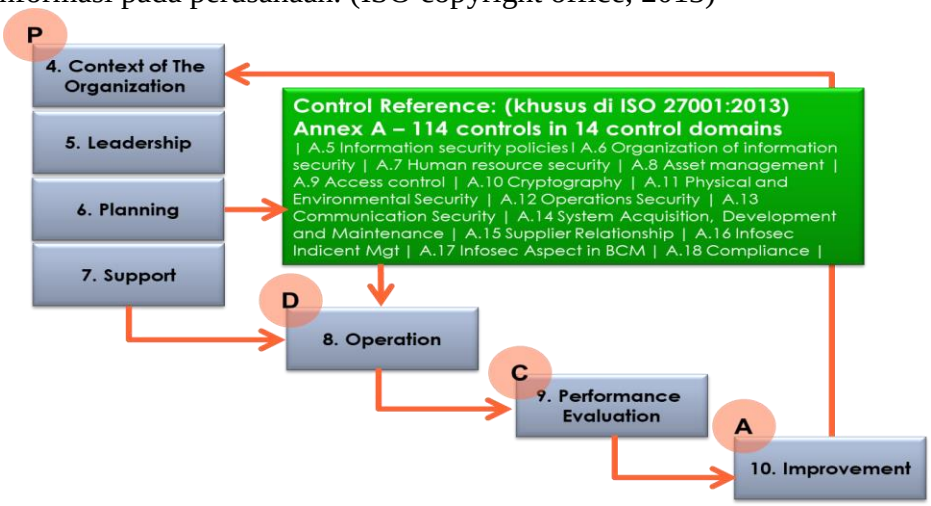
Indikator ketercapaian tujuan pengabdian kepada masyarakat ini adalah menumbuhkan kesadaran atau mengubah perilaku terhadap keamanan informasi, mendapatkan tambahan

e-ISSN : 2964 - 4533
PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95

wawasan dan ide baru yang berguna dalam membantu organisasi dalam melakukan pengamanan informasi, Dapat mendorong SDM dibidang keamanan siber untuk dapat memiliki kompetensi yang lebih baik dalam bidang keamanan siber dan Menumbuhkan keterikatan kepada siswa untuk memilih keamanan siber sebagai bidang karirnya dan membantu lebih banyak untuk bisa menjadi pemimpin dalam industri ini. (BUANA, 2022)

3. HASIL DAN PEMBAHASAN

ISO 27001:2013 adalah standar internasional yang diakui secara global untuk mengelola risiko terhadap keamanan informasi. Standar ini mengadopsi pendekatan proses untuk menetapkan, menerapkan, operasi, pemantauan, pengkajian, memelihara, dan meningkatkan keamanan informasi pada perusahaan. (ISO copyright office, 2013)



Gambar 2. Struktur ISO 27001:2013

Informasi adalah salah satu aset penting dan sangat berharga bagi kelangsungan hidup bisnis dan disajikan dalam berbagai format berupa: catatan, lisan, elektronik, pos, dan audio visual. Oleh karena itu, manajemen informasi penting untuk meningkatkan kesuksesan yang kompetitif dalam semua sektor ekonomi. Tujuan manajemen informasi adalah untuk melindungi kerahasiaan, integritas dan ketersediaan informasi.

Keamanan Informasi berarti melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran yang tidak sah untuk menyediakan: (Arianto, n.d.)

1. Kerahasiaan (Confidentiality), yang berarti menjaga pembatasan resmi atas akses dan pengungkapan, termasuk cara untuk melindungi privasi pribadi dan informasi hak milik

2. Integritas (Integrity), yang berarti menjaga dari modifikasi atau perusakan informasi yang tidak tepat, dan termasuk memastikan informasi non-penyangkalan, keakuratan, dan keaslian;

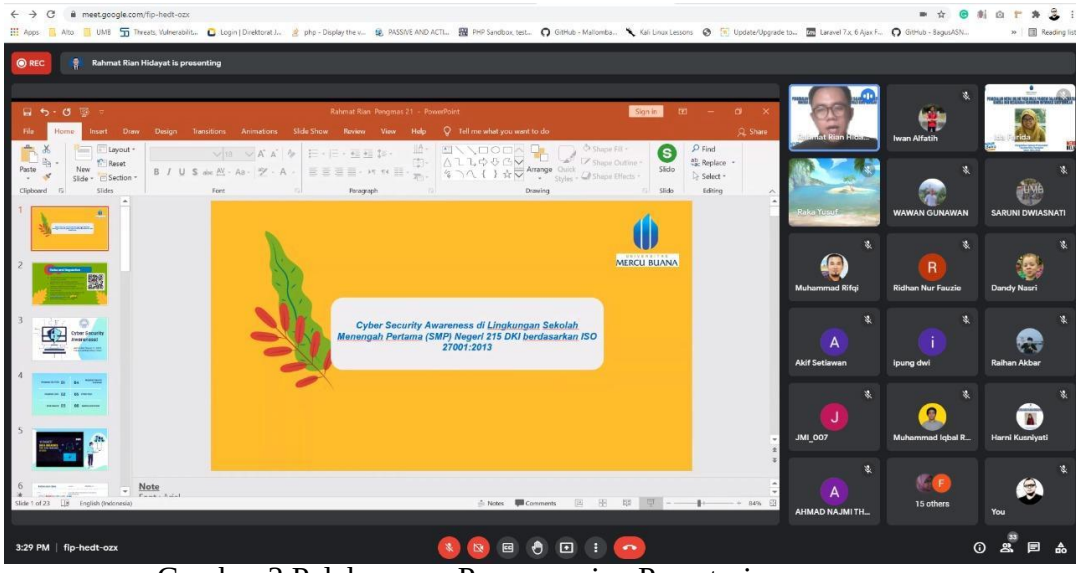
3. Ketersediaan (Availability), yang berarti memastikan akses yang tepat waktu dan dapat diandalkan ke, dan penggunaan, informasi.

Cyber security atau disebut sebagai pengaman siber merupakan praktik melindungi komputer, perangkat seluler, *server*, sistem elektronik, dan data dari risiko serangan jahat

e-ISSN : 2964 - 4533

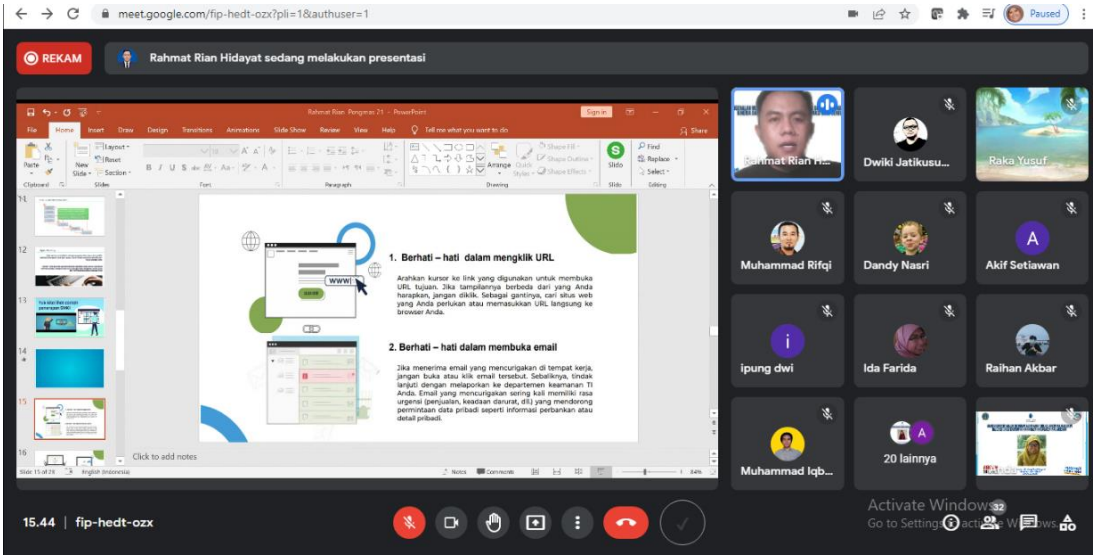
PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95

Manfaat yang diperoleh yaitu memastikan keamanan suatu bisnis, melindungi informasi pribadi, mengantisipasi situs web agar tidak mengalami sistem *down*, dan meningkatkan produktivitas karyawan.
Berikut ini adalah salah satu dari slide dari profil pembicara pada saat presentasi materi.



Gambar 3 Pelaksanaan Penyampaian Pemateri

Begitu juga dengan Gambar 4 dibawah ini adalah suasana pada saat penyampaian materi yang dilakukan dengan penuh antusias dan terlihat para peserta sangat fokus dalam menyimak penjelasan dari pemateri.

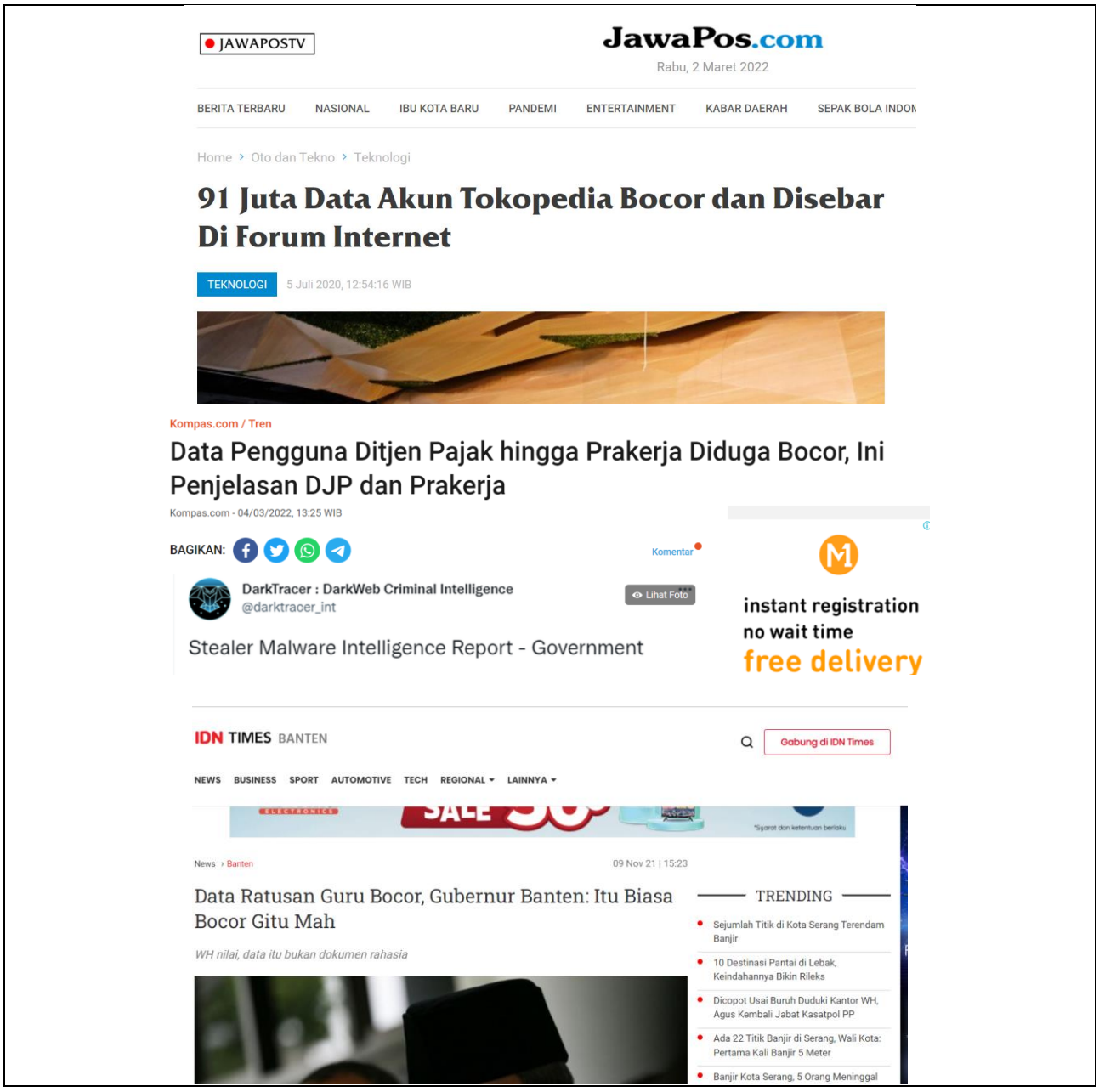


Gambar 4 Peserta menyimak pemaparan materi

e-ISSN : 2964 - 4533

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95

Berikut ini penjelasan dari materi yang disampaikan:
Berawal dari memberikan informasi bahwa ada beberapa kasus yang dialami akibat kebocoran data, sebagai berikut:

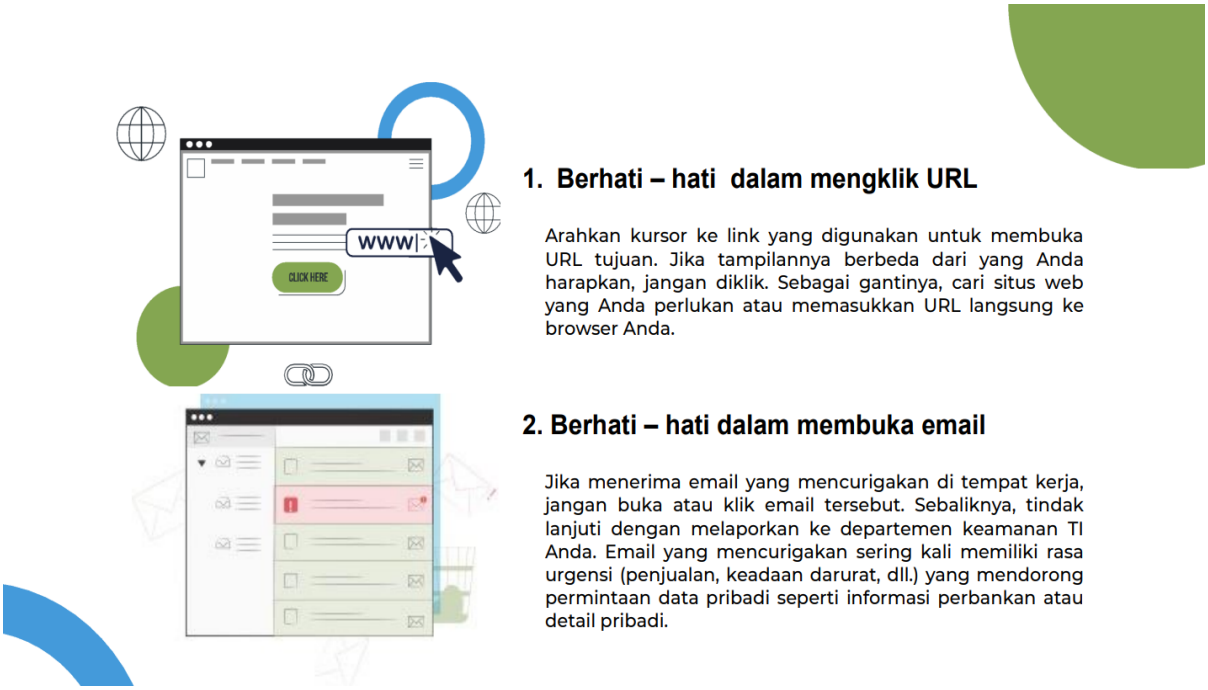


e-ISSN : 2964 - 4533

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95

Gambar 5 Contoh kasus Kebocoran Data

Dari penjelasan diatas tentang ISO 27001 dapat kita gunakan untuk membuat c*ampaign* secara rutinitas seperti *Security Awareness*. Berikut ini contohnya.



e-ISSN : 2964 - 4533

PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95

3. Gunakan frasa password yang kuat

Coba gunakan frasa password dengan huruf dan angka dibandingkan dengan kata password sederhana. Pendekatan unik ini dapat membantu Anda mengingat string panjang untuk keamanan tambahan. Pertimbangkan kata password yang lemah "keju" dibandingkan dengan frasa password yang rumit "1l0v3ch33s3" atau "m0r3ch33s3pl3as3."

4. Selalu lakukan pembaharuan

Selalu pasang pembaruan terbaru untuk sistem operasi, browser, dan aplikasi apa pun yang diinstal pada perangkat. Penjahat dunia maya mencari sistem yang sudah ketinggalan zaman dan belum ditambal untuk memanfaatkan kerentanan yang diketahui. Jangan biarkan diri Anda (atau organisasi Anda) menjadi sasaran empuk.

5. Berhati – hati saat melakukan sambungan Wi-Fi

Sebelum Anda terhubung ke jaringan Wi-Fi yang tidak dikenal, pikirkan tentang risikonya. Data apa yang mungkin dibagikan melalui koneksi? Menggunakan VPN dapat membantu melindungi Anda dengan membuat koneksi pribadi terenkripsi ke internet.

6. Belanja dengan bijak dan aman

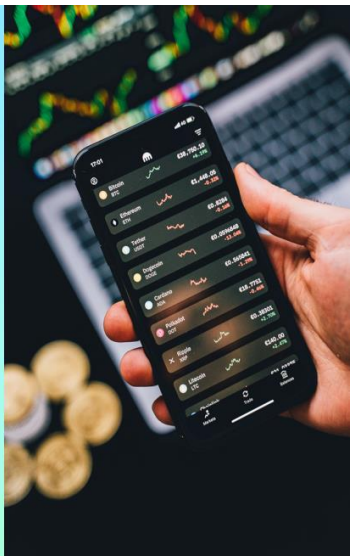
Belanja online telah menjadi kenyamanan sehari-hari di dunia modern. Lindungi data perbankan sensitif dengan hanya berbelanja di situs yang Anda percaya. Jangan pernah menyimpan informasi kartu Anda di tempat yang dapat dicuri dan digunakan nanti.

7. Tidak membagikan data pribadi.

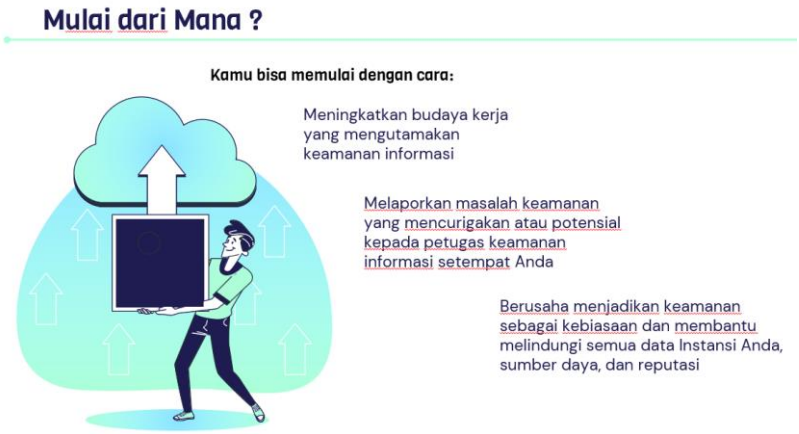
Saat melakukan bisnis atau urusan pribadi secara online, ingatlah untuk bijaksana dan menggunakan bahasa yang sopan. Ingatlah bahwa membagikan informasi pribadi seseorang secara online, tidak pernah diperbolehkan dan dapat membuat anda terkena masalah hukum

Beberapa tindakan spesifik yang dapat Anda ambil.

1. Perbarui Perangkat Lunak Anti-virus Dan Anti-malware
2. Jangan Menginstal Perangkat Lunak Yang Tidak Disetujui
3. Jaga Agar Sistem Operasi Komputer Anda Tetap Mutakhir/Update
4. Log Off Atau Kunci Layar Komputer Anda Saat Tidak Digunakan
5. Pastikan Untuk Menggunakan Screensaver Yang Dilindungi Kata Sandi
6. Mengunci Dokumen Secara Fisik Yang Berisi Informasi Sensitif Saat Tidak Digunakan
7. Mengadopsi Clean Screen, Clear Desk
8. Jangan Pernah Menuliskan Kata Sandi Tertulis Di Catatan Dan Tempel Di Monitor Anda
9. Jangan Pernah Membuka Lampiran Email Yang Datang Dari Orang Yang Tidak Anda Kenal
10. Jaga OTP atau PIN transaksi Perbankan anda

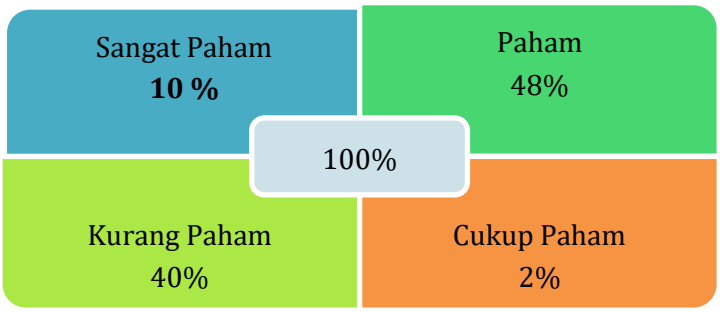


e-ISSN : 2964 - 4533
PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95



Gambar 6 Materi Security Awareness (SEVIMA, 2020)

Adapun hasil Feedback dari Peserta atas kegiatan:



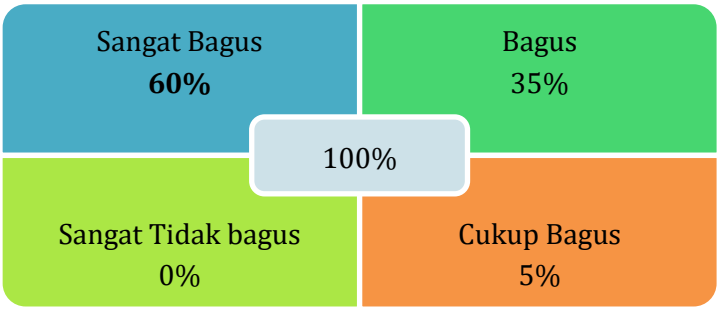
Gambar 7 hasil Evaluasi pemahaman peserta sebelum pemateri

Pada Gambar 7 diatas merupakan hasil evaluasi atas pemahaman peserta mengenai materi cyber security yang memang dianggap belum begitu familiar.

Gambar 8 hasil Evaluasi relevansi materi

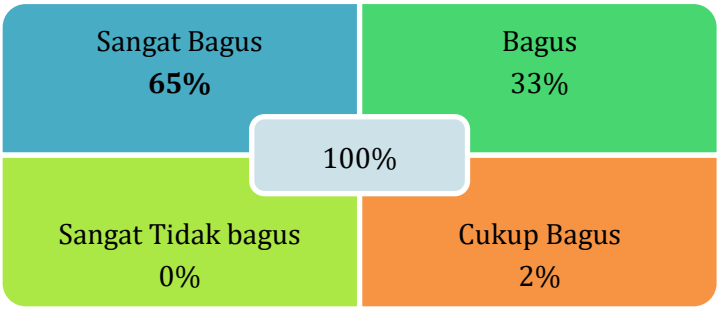
e-ISSN : 2964 - 4533
PEMANAS: Jurnal Pengabdian Masyarakat Nasional
Vol. 2, No. 2 November 2022, Hal 85 - 95

Pada Gambar 6 diatas merupakan hasil evaluasi pada relevansi materi yang disampaikan untuk lingkungan SMP 512



Gambar 9. Hasil Evaluasi isi materi

Pada Gambar 9 diatas merupakan hasil evaluasi pada isi materi yang disampaikan oleh narasumber.



Gambar 10. Hasil Evaluasi setelah menerima materi

Pada Gambar 8 diatas merupakan hasil evaluasi pada perbandingan pemahaman sebelum dan sesudah materi disampaikan.

4. KESIMPULAN

Berdasarkan kegiatan yang telah dilaksanakan dan hasil evaluasi selama kegiatan pengabdian masyarakat ini, dapat kami simpulkan bahwa program pengabdian masyarakat telah mampu memberikan manfaat bagi Guru dan Staff di Sekolahan SMPN 215 Jakarta terutama dalam membangun kesadaran dalam keamanan informasi di lingkungan sekolahan baik dari Guru, siswa dan para staff begitu juga para mahasiswa yang ikut serta dalam pengabdian ini. Peserta dapat menyimak dengan baik. Jadi dapat dinyatakan “BERHASIL” selama proses kegiatan PKM online dengan Judul: Cyber Security Awareness di Lingkungan SMPN 215 Jakarta Barat berdasarkan ISO 27001:2013

.

5. UCAPAN TERIMAKASIH

Terima kasih yang sebesar-besarnya kami sampaikan kepada segenap civitas akademika SMPN 215 Jakarta Barat yang sudah menjadi mitra dalam kegiatan PKM Internal dan terimakasih kepada PPM Universitas Mercu Buana karena sudah mendukung kegiatan ini sehingga bisa terlaksana dengan baik.

REFERENSI

Arianto, A. R. (n.d.). *Membangun pertahanan dan keamanan siber nasional indonesia guna menghadapi ancaman siber global melalui*. 13–30.

Pratama, M. rifqi R. & A. R. (2020). Analisis Kecerdasan Cybersecurity pada pengguna Media Sosial di Indonesia. *Jurnal Universita Islam Indonesia*. https://journal.uii.ac.id/AUTOMATA/article/view/15426/10219

Biro Hukum dan Hubungan Masyarakat – BSSN. (2021). *Tanggapi Urgensi Kebutuhan Kompetensi Pengelolaan Keamanan Siber Sektor TIK, BSSN Selenggarakan Cyber Security Awaraness di Yogyakarta*. https://bssn.go.id/tanggapi-urgensi-kebutuhan-kompetensi-pengelolaan-keamanan-siber-sektor-tik-bssn-selenggarakan-cyber-security-awaraness-di-yogyakarta/

BUANA, A. A. (2022). Pengenalan Pentingnya Cyber Security Awareness Pada UMKM. *Made Suartana, Ricky Eka Putra, Rahadian Bisma, Aditya Prapanca.*, *5*.

Budi, C. S. (2021). *Fakta Data 815 Guru di Banten Bocor, Pelaku Ternyata Orang Dalam, Diperiksa Polisi*. Kompas.Com. https://regional.kompas.com/read/2021/11/09/113200978/fakta-data-815-guru-di-banten-bocor-pelaku-ternyata-orang-dalam-diperiksa

Imam Suhartadi. (2021). *Webinar Cybersecurity Ignite 2021 Menambah Wawasan Keamanan Siber*. Https://Investor.Id/. https://investor.id/it-and-telecommunication/267079/webinar-cybersecurity-ignite-2021-menambah-wawasan-keamanan-siber

ISO copyright office. (2013). *Information technology — Security techniques — Information security management systems — Requirements*.

SEVIMA, A. (2020). *Cara dan Tips Melindungi Data Sistem Informasi Kampus*. SEVIMA.CO.ID. https://sevima.com/cara-dan-tips-melindungi-data-sistem-informasi-kampus/

Umar Alhabsyi. (2020). *Security Awareness Pada Institusi Pendidikan Tinggi*. Https://Wakool.Id/. https://wakool.id/blog/235-security-awareness-pada-institusi-pendidikan-tinggi