Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta

Ala Aprila Ipungkarti[1]

[1]Mahasiswa, *Universitas Pendidikan Indonesia*
Purwakarta (Telp. (0855) 59157905; e-mail: ala.aprila19@upi.edu)

(Received: November 2022, Revised : Januari 2023, Accepied : April 2023)

Abstract—**Penerapan IT Security Awareness merupakan faktor penting di organisasi, perusahaan dan lembaga pemerintah saat ini karena ancaman serangan kebocoran data terus terjadi. Hal ini juga memperjelas bahwa adanya kebutuhan untuk membangun minimnya kesadaran para pegawai dalam meningkatkan keamanan data dan informasi perusahaan salah satunya di BPJS Ketenagakerjaan Kantor Cabang Purwakarta. Oleh karena itu, perlu adanya upaya dalam meningkatkan Penerapan IT Security Awareness pada pegawai BPJS Ketenagakerjaan dengan harapan dapat meningkatkan kesadaran serta pemahaman para pegawai mengenai Pentingnya Penerapan IT Security Awareness dengan menggunakan standar keamanan ISO 27001. Dan kajian yang diusulkan ini menggunakan metode kualitatif yang menguraikan penelitian untuk mengukur tingkat kesadaran pegawai BPJS Ketenagakerjaan cabang purwakarta dengan melakukan sebuah tes pemahaman para pegawai terhadap penerapan IT Security Awareness dengan standar keamanan ISO 27001. Maka dari itu adanya Penerapan IT Security Awareness ini juga bertujuan agar para pegawai lebih berhati-hati terhadap keamanan data diri sendiri dan data perusahaan. Dan tulisan ini dilatarbelakangi oleh adanya langkah meningkatkan penerapan IT Security Awareness di BPJS Ketenagakerjaan Kantor Cabang Purwakarta.**

Keyword: ***IT Security Awareness, Keamanan Data, ISO 27001***

***Intisari*— Implementation of IT Security Awareness is an important factor in today's organizations, companies and government agencies because the threat of data leak attacks continues to occur. This also clarifies that there is a need to build the lack of awareness of employees in improving the security of company data and information, one of which is at the BPJS Ketenagakerjaan Purwakarta Branch Office. Therefore, efforts are needed to increase the Implementation of IT Security Awareness for BPJS Ketenagakerjaan employees in the hope of increasing awareness and understanding of employees regarding the Importance of Implementing IT Security Awareness using ISO 27001 security standards. And this proposed study uses a qualitative method that describes the research to measure the level of awareness of BPJS Ketenagakerjaan employees in the Purwakarta branch by conducting a test of employee understanding of the implementation of IT Security Awareness with ISO 27001 security standards. Therefore the Implementation of IT Security Awareness also aims to make employees more careful about the security of their own data and company data. And this article is motivated by steps to increase the implementation of IT Security Awareness at BPJS Ketenagakerjaan at the Purwakarta Branch Office.**

***Kata Kunci*: *IT Security Awareness, Data Security, ISO 27001*.**

I. PENDAHULUAN

Pada saat ini, penerapan penggunaan teknologi di Indonesia sudah mulai banyak digunakan untuk mempermudah dalam berkomunikasi baik itu di lingkup privat, maupun di ruang publik. Dalam Hal ini tidak menutup kemungkinan akan ada terjadinya kebocoran data dan informasi atau serangan siber baik di lingkungan pemerintahan maupun di lingkup swasta. salah satu perusahaan keamanan internet internasional yaitu Eset Indonesia menyatakan bahwa Indonesia mendapat sekitar 1,225 miliar serangan siber setiap harinya, Malware masih mendominasi serangan siber di Indonesia pada tahun 2018, dan virus ransomware akan terus menjadi tantangan keamanan dan ketahanan siber bagi setiap perusahaan dan sektor pemerintahan di Indonesia.

Kebanyakan serangan atau insiden siber yang berlangsung di perusahaan maupun pemerintahan Indonesia karena kurangnya pemahaman para pegawai juga masyarakat di Indonesia akan kerentanan di dunia oleh karenanya masih mudah dimanfaatkan oleh serangan siber untuk setiap perusahaan maupun sektor pemerintahan di Indonesia. Seperti yang kita telah ketahui, IT Security Awareness merupakan Salah satu yang dapat menggerakkan seseorang untuk melakukan tindakan pencegahan dengan membangun awareness atau kewaspadaan terhadap segala macam kemungkinan ancaman yang mengintainya. Sehingga pengguna dapat secara sadar dan konsisten mengetahui berbagai ancaman keamanan yang dihadapi oleh teknologi informasi yang digunakannya. Maka dari itu keamanan informasi sangat penting untuk mengelola data dan informasi tentang

p-ISSN 1858-2680
e-ISSN 2723-4673

pelayanan publik. Dan Penerapan IT Security Awareness merupakan faktor penting yang harus diperhatikan saat ini.

Selanjutnya, pada penelitian ini kami mendapatkan data hasil dari pengukuran kesadaran informasi mengenai keamanan data yang dilakukan oleh 34 responden pegawai BPJS Ketenagakerjaan Kantor Cabang Purwakarta dengan cara mengukur pengetahuan terhadap aspek-aspek it security Awareness. Hasil pengukuran pengetahuan It Security Awareness tersebut didapatkan nilai cukup memuaskan. Dimana dari hasil data penilaian pengisian tes pemahaman It Security Awareness semua para pegawai BPJS Ketenagakerjaan Purwakarta sudah cukup memahami pengetahuan tentang It Security Awareness. rata-rata nilai yang didapatkan oleh para pegawai BPJS Ketenagakerjaan Purwakarta 100% menjawab benar.

Adapun tujuan dari penelitian ini yaitu untuk mengetahui seberapa tingkat kesadaran para pegawai BPJS Ketenagakerjaan Kantor cabang Purwakarta terhadap pemahaman dan meningkatkan terhadap Penerapan IT Security Awareness. Isi kajian ini pun terkait dengan penerapan IT Security Awareness yang ada dalam system BPJS Ketenagakerjaan Kantor cabang Purwakarta. Pada kajian ini akan dijelaskan beberapa yaitu seperti, Penerapan Security Awareness di Perusahaan, Pentingnya Penerapan Security Awareness, dan IT Security Awarenees dengan Standar keamanan ISO 27001.

II. TINJUAN PUSTAKA

a. IT Security Awareness

IT Security Awareness adalah kesadaran yang dimiliki individu atau kelompok, yang diikuti dengan tindakan untuk melindungi diri dan aset, khususnya data atau teknologi informasi yang dimiliki, dari berbagai ancaman, serangan, atau kejadian yang menyebabkan kerusakan atau cedera, baik fisik maupun non fisik. Jadi security awareness pada dasarnya adalah awareness atau kesadaran akan adanya ancaman di sekitar kita dan tingkat keamanan yang kita miliki. Sehingga pengguna dapat secara sadar dan konsisten mengetahui berbagai ancaman keamanan yang dihadapi oleh teknologi informasi yang digunakannya.

b. Keamanan Informasi Data

Keamanan data adalah melindungi informasi data dari berbagai ancaman untuk menjamin kelangsungan operasi organisasi, meminimalkan kerusakan akibat ancaman, dan mempercepat pemulihan alur kerja organisasi. Atau dengan kata lain, keamanan informasi adalah upaya untuk melindungi informasi data dan sistem informasi agar tidak dapat diakses, digunakan, diungkapkan, diganggu, dimodifikasi atau dihancurkan oleh orang yang tidak bertanggung jawab untuk menjaga keutuhan, kerahasiaan dan ketersediaan informasi. Setiap orang dalam suatu organisasi memiliki peran yang berbeda sehubungan dengan informasi, dan penting bagi semua anggota organisasi untuk memahami peran dan tanggung jawab mereka terhadap informasi. Setiap orang dalam organisasi memiliki peran informasi yang berbeda. Unsur utama yang menjadi subjek informasi adalah peran pengguna, pemilik atau pemelihara informasi tersebut.

1) Owner /Pemilik

Pemilik bertanggung jawab atas informasi yang harus dilindungi. Pemilik informasi pada akhirnya bertanggung jawab atas perlindungan data, dan menurut konsep pencegahan, pemilik mungkin bertanggung jawab atas kelalaian atau kegagalan melindungi informasi sensitif. Namun, fungsi perlindungan data sehari-hari ditugaskan kepada penjaga. Tugas penting pemilik adalah menentukan tingkat klasifikasi informasi yang diperlukan berdasarkan kebutuhan organisasi untuk melindungi data dan memastikan bahwa setiap tingkat klasifikasi informasi tunduk pada kontrol keamanan yang sesuai.

2) Custodian

Custodian adalah pihak yang bertanggung jawab untuk menjaga informasi yang diberikan oleh pemilik. Kustodian bertanggung jawab untuk menjaga tiga aspek mendasar dari informasi, yaitu kerahasiaan, integritas, dan ketersediaannya. Dalam penerapannya, kustodian harus dapat menentukan teknologi keamanan yang tepat, baik secara fisik (firewall, kontrol akses) maupun logis (enkripsi, autentikasi), berdasarkan klasifikasi informasi yang dilindungi. Untuk meningkatkan efisiensi dan

p-ISSN 1858-2680
e-ISSN 2723-4673

efektifitas pengamanan, kustodian harus dapat mengembangkan prosedur operasi standar berdasarkan kebijakan dan aturan yang ditetapkan oleh pemilik.

3) User /Pengguna

Pengguna adalah pihak yang dianggap secara teratur menggunakan informasi dalam menjalankan pekerjaannya. Pengguna juga dapat dianggap sebagai konsumen data yang membutuhkan akses ke informasi setiap hari untuk melakukan tugas. Pengguna harus mengikuti prosedur operasi yang ditentukan dalam kebijakan keamanan organisasi, serta harus mematuhi prosedur yang telah dipublikasikan. Selain itu, pengguna harus benar-benar peduli untuk mengamankan informasiyang sensitif sesuai dengan kebijakan keamananinformasi dan penggunaannya.

c. Informasi Kesadaran

Awareness merupakan starting point atau titik awal bagi seluruh karyawan suatu organisasi untuk mengejar atau memahami pengetahuan keamanan teknologi informasi Dengan kesadaran keamanan, karyawan dapat fokus pada satu atau lebih kemungkinan masalah atau ancaman. Tujuan adanya Security Awareness adalah untuk meningkatkan keamanan dengan melakukan hal berikut:

1) Pemilik, pengguna, dan pemelihara/ custodian informasi memahami tanggung jawab mereka untuk sistem keamanan informasi dan mengajari mereka cara mengadopsi bentuk keamanan yang sesuai, sehingga membantu mereka mengubah perilaku untuk meningkatkan kesadaran keamanan.

2) Mengembangkan keterampilan dan pengetahuan yang memungkinkan pemilik, pengguna, dan informasi informasi penjaga dapat melakukan pekerjaan mereka dengan lebih aman.

3) Pelajari apa yang perlu Anda ketahui untuk merancang, menerapkan, atau menjalankan program kesadaran keamanan informasi untuk organisasi Anda.

d. ISO/IEC 27001:2013

ISO/IEC 27001 adalah rangkaian standar yang diterbitkan oleh International Organization for Standardization yang memuat spesifikasi atau persyaratan yang harus dipenuhi ketika membangun Sistem Manajemen Keamanan Informasi (ISMS) (ISO/IEC, 2013). Standar ini tidak bergantung pada produk teknologi informasi, memerlukan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk memastikan bahwa kontrol keamanan yang dipilih oleh perusahaan dapat melindungi aset informasi dari berbagai risiko dan memberikan kepercayaan kepada pihak yang berkepentingan pada tingkat keamanan.

Menurut (Chazar, 2015) ISO/IEC 27001 merupakan standar yang biasa digunakan untuk menentukan kebutuhan dalam menerapkan keamanan sistem informasi[4]. Implementasi ISO/IEC 27001 melindungi semua aspek keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan. Penerapan ISO/IEC 27001 disesuaikan dengan maksud, tujuan dan kebutuhan organisasi. ISO/IEC 27001 menguraikan persyaratan yang dibutuhkan perusahaan/organisasi saat mereka berusaha menerapkan konsep keamanan informasi. Pendekatan proses menekankan hal-hal berikut:

1) Memahami persyaratan keamanan informasi organisasi dan kebutuhan akan kebijakan dan tujuan keamanan informasi,
2) Menerapkan dan mengoperasikan kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis keseluruhan organisasi,
3) Memantau dan meninjau kinerja dan efektivitas SMKI, dan
4) Perbaikan berkelanjutan berdasarkan pengukuran tingkat pencapaian tujuan

III.METODE PENELITIAN

Sesuai dengan tujuan penelitian di atas, maka metode yang digunakan dalam penelitian ini adalah metode kualitatif. Pendekatan kualitatif ini dilakukan terhadap pokok bahasan kajian di lapangan berupa teori dengan data yang memuat fakta tentang implementasi IT Security Awareness di BPJS Ketenagakerjaan Purwakarta.

Dari penggunaan metode ini, sumber data yang diambil adalah lembar data yang berisi kutipan jurnal yang terkait dengan topik penelitian, dan data valid dari survei

p-ISSN 1858-2680
e-ISSN 2723-4673

penelitian saya berdasarkan judul topik yang diambil. Data tersebut diperoleh melalui survei berupa Google Form yang respondennya adalah pegawai BPJS Ketenagakerjaan cabang Purwakarta.

Penggunaan data survey pada google form ini dilaksanakan selama 8 (Delapan) hari dengan kriteria yang diambil dalam sebuah metode penelitian pada survei kali ini merujuk pada judul penelitian saat ini yaitu mengenai seberapa pahamkah pegawai BPJS Ketenagakerjaan dalam IT Security Awarenees, tingkat kesadaran para pegawai BPJS Ketenagakerjaan cabang Purwakarta dalam penerapan IT Security Awareness dengan Standar keamanan ISO 27001, pentingnya penerapan IT Security Awarenees, dan beberapa kriteria lainnya yang diambil dalam metode penelitian kali ini.

Dari sebuah hasil survey yang dilakukan selama 8 (Delapan) hari, akan mengambil sebuah data dari hasil survey dengan berupa grafik serta penjelasan untuk menarik kesimpulan dari hasil pengisian oleh para responden di mana mereka semua merupakan para pegawai BPJS Ketenagakerjaan Cabang Purwakarta yang telah bersedia mengisi kuesioner yang ada di google form.

IV. HASIL DAN PEMBAHASAN

Penerapan IT Security Awareness di Perusahaan

Pada dasarnya sistem informasi itu terintegrasi, teknologi informasi dibangun berbasis sistem yang dirancang untuk dapat mendukung kerja, manajemen dan pengambilan keputusan dalam organisasi.Dari 175 negara yang diinvestigasi, Indonesia berkonstribusi sebanyak 38 (Tiga Puluh Delapan) persen dari total sasaran trafik hacking di internet. Angka tersebut meningkat seiring dengan meningkatnya kecepatan internet di Indonesia. Oleh karena itu, penerapan teknologi informasi di berbagai bidang semakin luas, dan risiko keamanan informasi yang terancam juga semakin meningkat. Bukti meningkatnya ancaman keamanan informasi baik jumlah maupun kecanggihannya dapat dilihat dari berbagai sumber.

Koherensi diperlukan dalam pengembangan dan penerapan peraturan dan kebijakan ini, agar tidak menjadi bumerang bagi perusahaan itu sendiri mengenai keamanan informasi. Apalagi di era Revolusi Industri, berbagai proses di dalam perusahaan juga mengalami perubahan Di luar perusahaan, pemerintah membantu dengan mengoordinasikan aturan dan kebijakan untuk mendukung daya saing industri dan memastikan koordinasi keamanan informasi data perusahaan yang baik dengan pembuat kebijakan. Dan adapun beberapa konsep keamanan informasi yang dipaparkan oleh Chan dan Mubarak (2011) yang antara lain:

1. Phishing adalah perilaku umum yang mengancam keamanan dan kerahasiaan informasi dengan menggunakan email palsu atau situs web yang meniru alamat situs atau alamat email asli untuk mendapatkan informasi rahasia atau melakukan pencurian identitas. Itu juga dapat dilakukan melalui cara non-teknis seperti rekayasa sosial, atau dengan spam sebagai mod phishing.
2. Spam adalah surat atau pesan elektronik komersial yang tidak diinginkan penerimanya. Mungkin terlihat sepele, namun spam tidak hanya mengganggu penerima, tetapi berpotensi menimbulkan bencana atau kerusakan sistem. Misalnya, kode berbahaya seperti virus atau trojan horse sering kali menggunakan spam sebagai alat distribusi. Kode berbahaya dapat menurunkan kinerja sistem dan membatasi akses pengguna sehingga mengganggu aspek ketersediaan informasi. Selain itu, email spam terkadang berisi tautan ke situs phishing. Sementara kontrol teknis yang dilakukan organisasi untuk mencegah spam memasuki sistem email organisasi mungkin tidak 100% terselesaikan. Oleh karena itu, sangat penting bagi karyawan atau individu untuk memahami konsep spam dan bahaya yang terkait dengannya.
3. Rekayasa sosial, dalam konteks keamanan informasi, mengacu pada penggunaan sarana non-teknis untuk melakukan pencurian identitas atau memperoleh informasi rahasia. Dalam kasus seperti itu, penyerang dapat menggunakan kombinasi manipulasi psikologis dan peniruan identitas untuk memikat korban yang tidak bersedia memberikan informasi rahasia. Karena aspek rekayasa sosial yang sangat manusiawi, tidak

p-ISSN 1858-2680
e-ISSN 2723-4673

mungkin menggunakan kontrol teknis untuk mencegah serangan. Mitigasi rekayasa sosial sangat bergantung pada kesadaran karyawan akan konsep dan penegakan kebijakan organisasi terkait keamanan dan privasi.

4. Kata sandi yang kuat adalah kunci untuk mengautentikasi pengguna dan mencegah akses tidak sah ke sistem. Selain rekayasa sosial dan phishing, dua serangan yang disebut peretasan kata sandi dapat digunakan untuk mendapatkan kata sandi secara ilegal. Tidak masalah apakah Anda dapat memecahkan kodenya, yang penting adalah berapa lama waktu yang dibutuhkan untuk memecahkan kombinasi kode tersebut. Kata sandi yang kuat akan mengurangi kemungkinan penyerang melakukan serangan kata sandi. Kontrol teknis yang ada mampu membuat kata sandi yang kuat, tetapi tidak semua sistem informasi memiliki kontrol ini, sehingga diperlukan kesadaran karyawan untuk memastikan kata sandi mereka cukup kuat. Penting untuk memahami konsep kata sandi ini. Kata sandi yang kuat harus terdiri dari kombinasi huruf, angka, dan simbol yang cukup panjang.
5. Integritas data atau informasi ditandai dengan akurasi dan keaslian, keandalan, penerapan dan ketepatan waktu. Dari segi akurasi dan kebenaran yaitu informasi harus kuat dan benar, karena data harus akurat dan sesuai dengan kenyataan, misalnya data tanggal lahir yang dimasukkan ke dalam sistem harus bebas dari kemungkinan kesalahan. Dan kemudian kepercayaan, memastikan keakuratan dan keaslian akan memastikan bahwa informasi yang disimpan dalam sistem adalah representasi dari kenyataan sehingga seseorang dapat mempercayai informasi tersebut. Selain validitas dan ketepatan waktu, mengambil tanggal lahir sebagai contoh, tanggal lahir yang tepat adalah variabel yang berubah dari waktu ke waktu. Kesesuaian informasi tunduk pada perubahan realitas dari waktu ke waktu dan harus diikuti.
6. Social Networking adalah jenis media sosial atau situs jejaring, seperti Facebook dan Twitter, yang semakin penting dalam beberapa tahun terakhir sebagai sumber informasi rahasia yang bocor. Media sosial dapat menjadi sumber pelanggaran data ketika karyawan mengungkapkan informasi pribadi dan terkait tempat kerja di situs media sosial. Oleh karena itu, media sosial adalah bagian penting dari setiap rencana atau kebijakan keamanan. Penting untuk menyadari bahaya jejaring sosial dalam hal keamanan informasi.

Pentingnya Penerapan IT Security Awareness

Menurut (Alkhudayr et al., 2019) pentingnya perlindungan informasi perusahaan, yang menyatakan bahwa melindungi informasi perusahaan dan menjaga keamanan informasi sangatlah penting. Keamanan informasi didefinisikan sebagai perlindungan informasi, sistem dan perangkat keras yang menggunakan, menyimpan, dan mengirimkan informasi untuk memastikan integritas, kerahasiaan, dan ketersediaan data.

Dalam hal ini, sekalipun dengan teknologi yang kompleks yang tidak melibatkan faktor keamanan, semuanya menjadi tidak berarti, karena tidak pernah ada keamanan tanpa memperhatikan kerahasiaan, integritas dan ketersediaan pada umumnya dan keamanan pada khususnya setiap informasi atau data yang dihasilkan dalam teknologi dunia dapat menjadi bencana, sehingga setiap informasi yang dimiliki memang dianggap sebagai aset berharga dari suatu lembaga atau perusahaan.

Keamanan sistem informasi tidak hanya melibatkan kontrol keamanan teknis, tetapi juga kontrol administratif, prosedural, dan manajemen (Papagiannakis, Pijl, & Visser, 2011). Cara pengguna (karyawan, manajer, personel TI) menggunakan sistem informasi organisasi memainkan peran penting dalam menjaga kelangsungan aset informasi perusahaan. Kesadaran keamanan adalah bidang ilmu keamanan yang terkait erat dengan faktor manusia keamanan aset informasi. Pengetahuan yang diperoleh dari sekolah merupakan elemen kunci dalam mengembangkan kesadaran keamanan. Kesadaran keamanan dan program pelatihan dapat dipecah menjadi tiga bagian yang berbeda (Schlienger & Teufel, 2003):

p-ISSN 1858-2680
e-ISSN 2723-4673

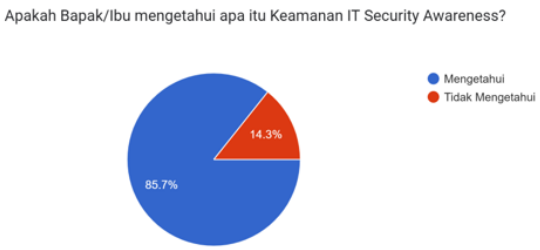
1. Pendidikan: seperti karyawan harus memahami mengapa keamanan informasi penting bagi organisasi. Kita semua perlu memahami bahwa kita semua bertanggung jawab atas keamanan yang memengaruhi lingkungan kita. Pendidikan dapat diberikan melalui kursus keamanan informasi.
2. Pelatihan: Karyawan harus tahu bagaimana mereka bisa merasa aman. Mereka harus mengetahui cara menggunakan fitur keamanan dalam aplikasi dan alur kerja. Perlu memberikan pelatihan tentang peralatan atau fitur keamanan dalam aplikasi.
3. Kesadaran: Pendidikan dan pelatihan merupakan dasar dari program keselamatan. Namun, ini tidak menjamin perilaku aman dalam kehidupan sehari-hari. Langkah-langkah keamanan di luar ruang kelas mengingatkan staf akan pelajaran yang dipetik. Perkakas seperti poster dengan slogan keselamatan, alas mouse, dan pulpen membantu mendemonstrasikan tema keselamatan di mana-mana. Program insentif akan mendorong partisipasi karyawan. Kontrol, kewajiban, dan penalti menyoroti pentingnya keamanan informasi.

IT Security Awareness Berstandar ISO 27001

ISO (Organisasi Standar Internasional) atau Organisasi Standar Internasional adalah badan penetapan standar internasional yang terdiri dari perwakilan badan standar nasional dari berbagai negara. ISO 27001 adalah dokumen standar untuk Sistem Manajemen Keamanan Informasi atau Sistem Manajemen Keamanan Informasi – ISMS, yang memberikan gambaran umum tentang apa yang harus dilakukan perusahaan ketika mereka mencoba menerapkan konsep keamanan informasi perusahaan. Secara umum, terdapat 11 area atau biasa disebut dengan kontrol yang harus ada di setiap perusahaan dalam upaya menerapkan konsep keamanan informasi.

Dalam konteks ini, kontrol adalah hal-hal yang dapat berupa proses, prosedur, kebijakan, atau alat, yang digunakan sebagai sarana untuk mencegah hal-hal yang tidak diperlukan oleh konsep keamanan informasi, seperti melarang akses ke data atau informasi rahasia. informasi perusahaan. Herny Februariyanti dalam Standar dan Manajemen Keamanan Komputer (2006) mengatakan bahwa terdapat 11 control keamanan informasi standar ISO 27001 tersebut adalah sebagai berikut: Security policy,organization of information security, Assetmanagement, Human resources security,Physical and environmental security,Communications and operationsmanagement, Access control, Informationsystem acquisition, development, andmaintenance, Information security incidentmanagement, Business continuity management, Compliance.

Standar Nasional Indonesia (SNI) 27001 yang mengadopsi ISO 27001 telah mensyaratkan kebutuhan pencapaian ambang batas minimum dan meminta semua pengamanan wajib dan control yang relevan diterapkan secara konsisten dan efektif oleh institusi/instansi dalam proses pengamanan informasi. Dalam tulisan ini proses penerapan ISO 27001 digunakan untuk evaluasi yang dilakukan terhadap kelengkapan dan konsistensi bentuk pengamanan informasi sesuai dengan ISO 27001. Dan dalam sebuah penelitian yang dijalani selama 8 (Delapan) hari ini, kami mendapatkan hasil sebagai berikut:



Gambar 1. Pertanyaan IT Security Awareness

Pada pertanyaan pertama, sebanyak 85,7% responden menjawab mengetahui dan 14,3% tidak mengetahui. Dari beberapa responden tersebut mengatakan bahwa terdapat jenis keamanan it security awarenes yang diketahui nya yakni seperti Batasan Penggunaan email korporasi, Pulse secure, Penggantian password secara berkala.

p-ISSN 1858-2680
e-ISSN 2723-4673

Gambar 2. Pertanyaan Standar Keamanan ISO 27001

Di pertanyaan selanjutnya, kebanyakan para responden mengaku tidak mengetahui apa itu standar keamanan ISO 27001. Responden hanya mengetahui keamanan security Awareness yang diterapkan di perusahaan saat ini. Dan responden yang menjawab mengetahui dan pernah menerapkannya namun tidak tahu jenis standar iso apa yang telah digunakan.

Dan selanjutnya terdapat pemahaman IT Security Awareness responden yang dibuat dengan menggunakan standar ISO 270001.

No	Pertanyaan Pemahaman	Persentase		
		Tidak Mengetahui	Mengetahui	Sangat Mengetahui
1.	Apakah Bapak/Ibu mengetahui panduan keamanan informasi yang disesuaikan dengan peran perusahaan? (Information Security Policies)	0	57.1%	42.9%
2.	Apakah Bapak/Ibu mengetahui prosedur dasar keamanan informasi (seperti laporan insiden keamanan informasi) dan baseline controls (seperti keamanan password, malware controls,& clear desk)? (Organisation of Information Security)	14.3%	42.9%	42.9%
3.	Apakah Bapak/Ibu mengetahui proses tata tertib terkait tindakan pelanggaran pegawai pada keamanan informasi? (Organisation of Information Security)	14.3%	42.9%	42.9%
4.	Apakah Bapak/Ibu mengetahui penetapan dan penyimpanan fasilitas utama pengolah informasi Perusahaan dan fasilitas lainnya? (Physical and Environmental Security)	0	71.4%	28.6%
5.	Apakah Bapak/Ibu mengetahui prosedur jika komputer ditinggalkan dalam keadaan terdapat data perusahaan yang sensitive? (Operations Security)	0	57.1%	42.9%
6.	Apakah Bapak/Ibu mengetahui kebijakan keamanan informasi berdasarkan dengan peraturan, dan undang-undang yang berlaku di perusahaan? (Information Security Policies)	0	57.1%	42.9%
7.	Apakah Bapak/Ibu mengetahui penyediaan menu untuk akses kontrol terhadap fungsi sistem aplikasi? (Access Control)	14.3%	42.9%	42.9%
8.	Apakah Bapak/Ibu mengetahui kebijakan mengontrol hak akses pengguna (Access Control)	14.3%	57.1%	28.6%
9.	Apakah Bapak/Ibu mengetahui seperti apa pembatasan pada instalasi software berisiko tinggi dan mengurangi celah dari kesempatan akses yang tidak berhak? (Operations Security)	14.3%	57.1%	28.6%
10	Apakah Bapak/Ibu mengetahui bentuk perlindungan jika adanya pertukaran informasi sensitif dalam bentuk lampiran? (Communications Security)	14.3%	28.6%	57.1%

Gambar 3. Pemahaman IT Security Awareness Standar ISO 27001

Dari hasil tabel pemahaman responden diatas memiliki hasil pemahaman yang cukup bagus dengan hasil rata-rata 51.42% responden untuk mengetahui, presentase dari kategori sangat mengetahui yaitu rata-rata 40.035%, dan kategori presentase tidak mengetahui yaitu dengan rat-rata 8.58%.

V. KESIMPULAN

KESIMPULAN

Berdasarkan hasil penelitian dan survey yang telah dilakukan selama 8 hari, didapatkan sebuah hasil yang selaras yang dimana hal tersebut ditunjukkan dari sebuah hasil data Primer mengenai tes pengetahaun para pegawai BPJS Ketenagakerjaan yang menunjukkan hasil cukup bagus untuk pengetahuan para tentang IT Security Awarenes. Dan di hasil survey yang kami lakukan menunjukan hasil bahwa untuk pemehaman dan pengetahuan tentang IT Security Awareness standar keamanan ISO 27001 ini masih banyak yang belum mengatahuinya. Namun untuk penerapan IT Security Awareness standar keamanan ISO 27001 sudah ada beberapa yang mengetahui dan menerapkan serta ada juga beberapa pegawai yang belum menerapkannya.

Kemudian dapat ditarik kesimpulan bahwa pemahaman serta pengetahuan para pegawai BPJS Ketenagakerjaan mengenai IT Security Awareness sudah cukup bagus, namun jika menggunakan standar keamanan ISO 270001 masih perlu adanya pemahaman yang mendalam seperti pelatihan bagi para pegawai untuk IT Security Awareness standar keamanan ISO 27001. Dan jika IT Security Awareness dengan standar keamanan ISO 27001 ini diterapakan di BPJS Ketenagakerjaan bisa digunakan namun masih ada beberapa yang perlu diperhatikan baik pemahaman serta penerapan para pegawainya. Dan dari penelitian ini merekomendasikan peningkatan keamanan untuk BPJS Ketenagakerjaan Cabang Purwakarta dari jenis control keamanan informasi standar ISO 27001 yakni mulai dari Organisation of Information Security, Access Control, Operations Security, dan Communications Security.

SARAN

Berdasakan kesimpulan diatas, terdapat saran dari penelitian diantarannya untuk para peneliti selanjutnya diharapkan dapat melanjutkan penelitian ini untuk dapat

p-ISSN 1858-2680
e-ISSN 2723-4673

mengetahui perkembangan terbaru dari judul topik yang sedang diteliti ini. Juga diharapkan dari kesimpulan penelitian di atas dapat diperbaharui dari sisi penerapan IT Security Awareness menggunakan standar ISO yang lain misalkan seperti standar ISO 27002 dan peneliti selanjutnya juga dapat mengevaluasi kembali dari IT Security Awareness dengan 11 jenis control keamanan informasi standar ISO 27001 di BPJS Ketenagakerjaan Cabang Purwakarta.

DAFTAR PUSTAKA

[1] Aloul, F. A. (2013). The Need for Effective Information Security Awareness. *JOURNAL OF ADVANCES IN INFORMATION TECHNOLOGY*, VOL. 3, NO. 3.

[2] Batmetan, J. R., Kariso, B., Moningkey, M., & Tumembow, A. (2018). Tingkat Kesadaran Privasi Atas Masalah Keamanan Informasi.

[3] Februariyanti, H. (2006). Standar dan Manajemen Keamanan Komputer. *Jurnal Teknologi Informasi DINAMIK*, Vol XI, pp 134-142.

[4] Fitroh, Seputra, M. R., Ramadhan, G., Hersyaf, T. N., & Rokhman, A. N. (2017). PENTINGNYA IMPLEMENTASI ISO 27001 DALAM MANAJEMEN KEAMANAN : SISTEMATIKA REVIEW. *Seminar Nasional Sains dan Teknologi*, pp. 1-6.

[5] Hansch, N., & Benenson, Z. (2014). Specifying IT security awareness. 328-330.

[6] Juliharta, I. P. (2019). ANALISA TINGKAP KESIAPAN PENERAPAN KEAMANAN TEKNOLOGI INFORMASI DALAM PELAKSANAAN e-GOVERNMENT BERBASIS INDEKS KEAMANAN INFORMASI (KAMI) STUDI KASUS PEMERINTAH KOTA KEDIRI. *Jurnal Teknologi Informasi dan Komputer*, Volume 5, Nomor 1, pp 21-27.

[7] Jumiati, Indarjani, S., & Sofiana, D. D. (2011). Pembinaan Kesadaran Keamanan Informasidi Lingkungan Sekolah Tinggi Sandi NegaraBerdasarkan National Institute of Standard and Technology (NIST). *e-Indonesia Initiative Forum*, 1-7.

[8] Octariza, N. F. (2019). Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dan ISO/IEC 27002 Pada Kantor Pusat PT Jasa Marga.

[9] Persadha, P. D., Waskita, A. A., Fadhila, M. I., Kamal, A., & Yazid, S. (2016). How inter-organizational knowledge sharing drives national cyber security awareness?: A case study in Indonesia. *2016 18th International Conference on Advanced Communication Technology (ICACT)*. PyeongChang, Korea (South): IEEE.

[10] Prasetyowati, D. D., Gamayanto, I., wibowo, S., & Suharnawi. (2019). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang. *Journal of Information System*, Vol. 4, No. 1, hlm. 65-75.

[11] Puspitaningrum, E. A., Devani, F. T., Putri, Q. V., Hidayanto, A. N., Solikin, & Hapsari, I. C. (2018). Measurement of Employee Information Security Awareness: Case Study at A Government Institution. *IEEE Xplore*. Palembang, Indonesia: 2018 Third International Conference on Informatics and Computing (ICIC).

[12] Rinaldi, R., & Krisnadi, I. (2019). ANALISIS DAMPAK REVOLUSI INDUSTRI 4.0 TERHADAP KEAMANAN DATA DIGITAL. *Universitas Mercubuana, Manajemen ICT*.

[13] Sembiring, S., & Lubis, S. A. (2014). PENERAPAN INDEKS KEAMANAN INFORMASI BERBASIS ISO 27001 UNTUK MENGUKUR TINGKAT KESIAPAN PENGAMANAN INFORMASI PADA INSTITUSI PENDIDIKAN TINGGI. Vol-2.

[14] Sonnenschein, R., Loske, A., & Buxmann, P. (2017). The Role of Top Managers' IT Security Awareness in Organizational IT Security Management.

[15] Wadah, R. (2016). EFFECT OF QUALITY MANAGEMENT SYSTEM ISO 9001: 2008 ON THE PERFORMANCE. *Jurnal Syarikah*, Vol 2, Nomor 1.

p-ISSN 1858-2680
e-ISSN 2723-4673