JTERA (Jurnal Teknologi Rekayasa), Vol. 7, No. 1, Juni 2022, Hal. 73-82
Terakreditasi "**Peringkat 3**" oleh Kemenristek/BRIN, Nomor SK: 85/M/KPT/2020
DOI: 10.31544/jtera.v7.i1.2022.73-82
p-ISSN 2548-737X
e-ISSN 2548-8678

Kajian Dimensi Budaya Keamanan Informasi dalam Berbagai Organisasi

Nur Andita Prasetyo[#], Bambang Setiawan
Institut Teknologi Sepuluh Nopember
Jl. Teknik Kimia, Keputih, Kec. Sukolilo, Kota Surabaya, Jawa Timur 60111, Indonesia
[#]nurandita.prasetyo69@gmail.com

Abstrak

Budaya keamanan informasi yang sangat diperlukan dalam mengamankan data pribadi maupun data perusahaan. Penilaian tingkat budaya umumnya dilakukan dengan menghitung nilai indeks (indikator komposit) yang dibentuk dari dimensi-dimensi atau faktor-faktor yang mempengaruhi budaya tersebut. Penelitian ini bertujuan untuk mendapatkan faktor-faktor budaya keamanan informasi yang dapat digunakan untuk membentuk indeks tingkat budaya keamanan informasi. Metode yang digunakan adalah *Sistematic Literature Review* (SLR). SLR digunakan untuk mengidentifikasi, mengkaji, membahas, dan membahas semua penelitian yang tersedia dengan bidang fenomena yang menarik, dengan pertanyaan penelitian tertentu yang relevan. Penelitian ini mempelajari 39 makalah penelitian terkait budaya keamanan informasi pada organisasi dan individu antara tahun 2012 hingga 2021. Ada sembilan jenis organisasi yang dibahas, antara lain kesehatan, pemerintahan, Industri Kecil dan Menengah, organisasi publik, finansial, organisai umum, perusahaan perdagangan, telekomunikasi, dan akademik. Hasil penelitian menunjukkan bahwa ada 11 faktor yang digunakan dalam penilaian budaya keamanan informasi, yaitu kesadaran, kebijakan, pelatihan, pemantauan, kepatuhan, pengetahuan, pendidikan, perilaku, strategi, manajemen perubahan dan komunikasi. Dimana ada empat faktor yang digunakan lebih dari 25% makalah, yaitu kesadaran, kebijakan, pelatihan dan pemantauan.

Kata kunci: dimensi, budaya keamanan informasi, organisasi, keamanan informasi

Abstract

Information Security Culture is indispensable in securing personal data and company data. The assessment of the cultural level is generally done by calculating the index value (composite indicator) which is formed from the dimensions or factors that influence the culture. This study aims to obtain information security culture factors that can be used to form an index of the level of information security culture. The method used is Systematic Literature Review (SLR). The SLR is used to identify, review, discuss and discuss all available research on the phenomenon area of interest, with specific relevant research questions. This study examines 39 research papers related to information security culture in organizations and individuals between 2012 and 2021. There are nine types of organizations discussed, including: health, government, Small and Medium industrial, public organizations, finance, general organizations, trading companies, telecommunications, and academics. The results showed that there were 11 factors used in the assessment of information security culture, namely awareness, policy, training, monitoring, compliance, knowledge, education, behavior, strategy, change management and communication. Where there are four factors used by more than 25% of papers, namely awareness, policy, training and monitoring.

Keywords: *dimensions, information security culture, organization, information security*

I. PENDAHULUAN

Di era milenial yang sarat teknologi saat ini, proses organisasi erat kaitannya dengan penggunaan sistem informasi (SI), yang mengarahkan organisasi pada risiko dan ancaman keamanan informasi. [1]. Kondisi ini dibuktikan dengan banyaknya ancaman dan risiko keamanan yang tidak dapat dihindari secara efektif hanya dengan menggunakan sumber daya teknis dan manusia dalam organisasi. [2]. Sehingga segala aspek yang mempengaruhi keamanan informasi harus diperhatikan. Meskipun organisasi sudah memiliki sumber daya yang baik dan berkualitas, organisasi juga harus memiliki pedoman praktis yang mendukung kinerjanya [3]. Pedoman biasanya

Diterima: 13 April 2022; Direvisi: 27 Mei 2022; Disetujui: 1 Juni 2022
JTERA, Vol. 7, No. 1, Juni 2022

disebut kerangka kerja untuk mengelola sumber daya ini. Dalam suatu kerangka keamanan informasi, umumnya terdapat beberapa dimensi yang dijadikan pedoman atau penilaian. Pemangku kepentingan harus menyadari hal ini karena jika suatu organisasi menggunakan kerangka kerja untuk keamanan informasi, maka dia harus bisa mengontrol implementasi dari kerangka kerja tersebut [4]. Keamanan informasi organisasi dapat aman ketika sumber daya manusia dan kerangka kerja diselaraskan [5].

Ada beberapa pernyataan terkait dengan definisi dimensi keamanan informasi. Dimensi mewakili aspek tertentu dari keamanan informasi dan didasarkan pada budaya organisasi dan konsep keamanan informasi yang diterima secara luas [6]. Dimensi merupakan salah satu aspek yang ditunjukkan oleh anggota organisasi dalam praktiknya, dalam hal ini terkait dengan keamanan informasi [7]. Keamanan informasi memiliki dimensi yang berbeda-beda sehingga tidak ada standar khusus mengenai hal ini. Salah satu alasannya adalah bidang organisasi yang berbeda. Semua ini menimbulkan konflik dan masalah bagi para peneliti di bidang ini dalam mengidentifikasi bagaimana konsep keamanan informasi sebenarnya. Praktisi bidang ini juga merasa kesulitan untuk mengembangkan dan menilai keamanan informasi dalam suatu organisasi, sehingga ada keterbatasan bagi praktisi dan peneliti di bidang keamanan informasi. [8].

Ada banyak makalah yang membahas budaya keamanan informasi, misalnya referensi [6] membahas berbagai dimensinya, referensi [9] membahas penilaian budaya keamanan Informasi, referensi [10] mendiskusikan metode arus utama apa yang digunakan untuk menilai budaya keamanan informasi. Pada penelitan ini dilakukan pencarian faktor-faktor yang mempengaruhi budaya keamanan pada berbagai bidang organisasi. Sehingga faktor-faktor tersebut dapat digunakan untuk pembuatan indeks pengukuran tingkat budaya keamanan informasi yang menggunakan indikator komposit yang berbasis metode multiple criteria decision analysis.

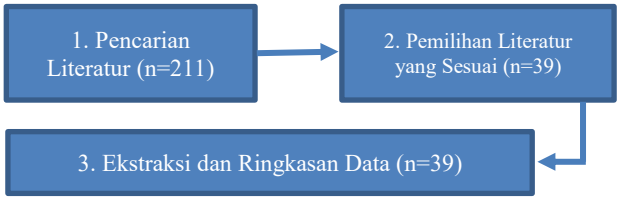
II. METODE PENELITIAN

Penelitian ini menggunakan metode *Preferred Reporting Items for Systematic Review and Meta-Analysis* (PRISMA). Metode ini memiliki dua bagian utama, yang terdiri dari meta-analisis dan tinjauan sistematis. Tinjauan sistematis memberikan ringkasan objektif dari topik penelitian. Metode ini bermanfaat di berbagai bidang penelitian, dengan banyak publikasi yang berfokus pada setiap objek secara sempit. Meta-analisis mengacu pada penggunaan teknik statistik dalam tinjauan sistematis untuk mengintegrasikan hasil studi yang dipilih sebagai tinjauan literatur dalam penelitian terkait. Tujuan dari metode ini adalah untuk mengintegrasikan tinjauan literatur yang ada secara transparan. Dalam metode ini terdapat tiga tahapan yaitu pencarian literatur, pemilihan literatur dan ekstraksi data [8].

1) Pencarian Literatur: Pada tahap pertama, peneliti mencari jurnal yang akan digunakan untuk literatur. Pencarian ini dilakukan di Science Direct, google Scholar, research gate, dan web journal lainnya. Kata kunci yang digunakan adalah "budaya keamanan informasi", "dimensi keamanan informasi" dan "keamanan informasi". Pencarian dilakukan dengan tahun terbit tidak lebih dari 10 tahun, dengan asumsi lebih dari 10 tahun terlalu lama dan tidak relevan dengan masa sekarang. Filter juga dilakukan dalam penelitian ini, jenis artikel penelitian dan artikel review. Sebanyak 2.048 artikel diekstraksi berdasarkan strategi pencarian. Setelah penghapusan literatur yang terdapat duplikasi, 231 artikel potensial telah dipilih. Judul dan abstrak kemudian disaring dan literatur yang tidak relevan dihapus, hal tersebut menghasilkan literatur yang akan diteliti menjadi 211.

2) Pemilihan Literatur yang Sesuai: Tahap selanjutnya adalah pemilihan artikel yang akan digunakan dalam penelitian ini. Artikel teks lengkap ditinjau dan dianalisis untuk kelayakan. Artikel yang dipilih terkait dengan dimensi keamanan informasi. Tahap ini menghasilkan 39 artikel yang memenuhi syarat untuk topik penelitian yang akan dilakukan.

3) Ekstraksi dan Ringkasan Data: Tahap terakhir adalah ekstraksi data dan ringkasan. Tahapan ini dilakukan pada 39 artikel yang dipilih dari ribuan artikel terkait budaya keamanan informasi. Pada tahap ini, setiap data penelitian diekstraksi dan dirangkum. Peneliti berfokus pada dimensi keamanan informasi. Selanjutnya, setiap artikel akan menyebutkan dimensinya dalam satu tabel.



Gambar 1. Tahapan penelitian

III. HASIL DAN PEMBAHASAN

Keamanan informasi adalah seperangkat metodologi, praktik, atau proses yang dapat dilakukan untuk melindungi informasi digital yang ada [1]. Keamanan informasi bertujuan untuk melindungi data pada berbagai tahapan, baik selama proses input, output, dan manajemen [11]. Selama pandemi ini, sebagian besar organisasi telah beralih menggunakan platform digital untuk melakukan banyak sisi baik dan buruk. Serangan digital yang dapat mengancam keamanan informasi merupakan salah satu kelemahan dari platform digital [12], [13]. Namun, sisi baiknya dapat meningkatkan produktivitas organisasi itu sendiri. Manajemen harus berperan aktif dalam masa transisi platform digital, terutama kebijakan keamanan informasi untuk melindungi informasi atau data penting yang dimiliki organisasi. Prosedur ini harus diterapkan di semua lapisan struktur organisasi [1].

Tabel 1 menunjukkan daftar dimensi yang terkait dengan keamanan informasi menurut berbagai penelitian yang digunakan sebagai literatur dalam penelitian ini. Kolom pertama pada Tabel 1 berisi penulis literatur, kolom kedua berisi dimensi dimana terdapat dua jenis yaitu organisasi dan individu serta kolom ketiga berisi bidang organisasi.

Tabel 1. Kajian dimensi budaya keamanan informasi tahun 2012-2021

Literatur	Dimensi		Bidang organisasi
	Organisasi	Individu	
[14]	Manajemen Perubahan, Sistem Organisasi, Persyaratan Keamanan	Perilaku, Kesadaran Keamanan Informasi, Pengetahuan	Kesehatan
[15]	Dukungan Manajemen Puncak, Penegakan Kebijakan	Pelatihan, Kesadaran, Kepemilikan	Pemerintah
[10]	Nilai yang Dianut, Artefak, Asumsi Diam-diam Bersama	Pengetahuan keamanan informasi	Organisasi Publik
[16]	Informasi yang berkaitan dengan insiden dan kerentanan, analisis dan manajemen risiko, strategi dan perencanaan, kebijakan dan standar, proses dan prosedur, metodologi dan kerangka kerja, audit dan kontrak	Pengetahuan dan pengalaman, kesadaran, pelatihan dan outsourcing	Industri Kecil dan Menengah
[17]	Aturan	Kepatuhan, kesadaran	Pemerintah
[11]	Kepemimpinan Keamanan Informasi, Manajemen Aset Informasi, Manajemen Perubahan, Manajemen Keamanan Informasi, Manajemen Pengguna, Program Keamanan Informasi, Kebijakan Keamanan Informasi	Kepercayaan	Keuangan
[18]	Pemantauan Keamanan, Komitmen Manajemen Puncak	Komunikasi Keamanan	Umum
[3]	Manajemen Pengguna, Manajemen Aset Informasi, Manajemen Keamanan Informasi, Program Keamanan Informasi, Manajemen Perubahan, Kebijakan Keamanan Informasi, Kepemimpinan Keamanan Informasi	Kepercayaan, Pelatihan, dan Kesadaran,	Keuangan
[19]	Budaya Keamanan, Pemantauan Keamanan, Kebijakan Keamanan	SETA (Pendidikan, Pelatihan, dan Kesadaran Keamanan)	Umum
[5]	Organisasi, Strategi, Teknologi	Orang, Lingkungan	Umum
[20]	Sanksi, Penghargaan, Jumlah Karyawan	Peran Pekerjaan	Umum
[21]	Strategi, Teknologi, Organisasi,	Orang, Lingkungan	Pemerintah, Industri Kecil dan Menengah, perusahaan dagang
[22]	Kebijakan Keamanan, Manajemen Puncak	Perilaku keamanan, Kesadaran dan Pendidikan Keamanan, Penerimaan Keamanan	Umum

[23]	Kepemimpinan Keamanan Informasi, Manajemen Aset Informasi, Kebijakan Keamanan Informasi, Manajemen Pengguna, Manajemen Perubahan, Program Keamanan Informasi, Manajemen Keamanan Informasi	Kepercayaan, Pelatihan, dan Kesadaran	Umum
[24]	Teknologi, Organisasi, Strategi	Lingkungan, Orang	Pemerintah, Industri Kecil dan Menengah, perusahaan dagang
[25]	Komitmen Manajemen Puncak, Akuntabilitas	Kesadaran Keamanan Informasi	Pemerintah
[26]	Kepatuhan, Akuntabilitas, Tata Kelola	Komunikasi	Umum
[27]	Asosiasi, Subsistensi, Biseksualitas, Teritorial, Temporalitas, Eksploitasi, Rekreasi dan Humor, Pertahanan,	Belajar, Interaksi	Telekomunikasi
[28]	Kebijakan Keamanan Informasi, Sikap Manajerial	Kepatuhan dengan praktik terbaik, Pelatihan, dan Kesadaran keamanan informasi	Organisasi Publik
[29]	Artefak, nilai yang dianut, asumsi diam-diam bersama, strategi, manajemen perubahan, Kebijakan, Kontrol	pengetahuan, persepsi, motivasi, pelatihan	Umum
[4]	Kebijakan Keamanan Informasi, Manajemen Risiko, Manajemen Puncak, Pemantauan	Pengetahuan Keamanan Informasi, Berbagi Pengetahuan Keamanan Informasi, SETA	Umum
[30]	Evaluasi risiko keamanan, Biaya kepatuhan keamanan, Evaluasi kepatuhan keamanan formal, Pengaruh sosial	Efikasi diri keamanan	Umum
[31]	kebijakan, standar, prosedur, kontrol		Umum
[32]	Manajemen Sistem, Dimensi Kebijakan dan Kelembagaan dan Dimensi Budaya	Kesadaran	Umum
[33]	Budaya, Pengambilan Keputusan, Manajemen, Strategi, Kebijakan, Kompetensi	Kesadaran, Peran dan Tanggung Jawab	Pemerintah
[7]	Masalah Keamanan Informasi Umum, Komitmen Manajemen, Budaya Pelaporan Dan Reaksi terhadap Pelaporan Insiden,	Sikap Karyawan, Pelatihan dan Pendidikan Keamanan	Umum
[34]	Komitmen Keamanan Informasi, Pentingnya Keamanan Informasi, Efektivitas Kebijakan Keamanan Informasi, Arahan Keamanan Informasi, Kepatuhan Pemantauan Keamanan Informasi, Konsekuensi Keamanan Informasi, Praktik Anggaran Keamanan Informasi, Investasi Keamanan Informasi, Kemampuan Teknologi Informasi, Kompatibilitas Teknologi Informasi	Tanggung Jawab Keamanan Informasi, Pelatihan Keamanan Informasi	Organisasi Publik
[35]	Kebijakan Insentif dan Disinsentif, Ketidaktahuan dan Kelalaian, Anggaran, Pengembalian Investasi Keamanan Informasi, Budaya, Iklim Keamanan dan Keamanan Informasi, Penegakan Kebijakan Keamanan, Dukungan Manajemen, Dasbor Bisnis Keamanan Informasi, dan Bias Pemrosesan Informasi, Proses Audit dan Kepatuhan	Kegunaan, Kesadaran Keamanan, Pelatihan dan Pendidikan, Keterampilan, Pengalaman, Keterlibatan Karyawan, Stres Individu, Perilaku Keamanan, Komunikasi, Persepsi Risiko	Industri Kecil dan Menengah

[6]	Prosedur penanggulangan, Manajemen risiko, Manajemen puncak komitmen, Pemantauan,	Pendidikan keamanan, pelatihan dan kesadaran, Informasi keamanan pengetahuan, berbagi pengetahuan keamanan informasi	Akademi
[36]	Dukungan manajemen, kebijakan keamanan informasi	pendidikan, pelatihan, dan kesadaran keamanan informasi	Umum
[37]		Kurangnya Motivasi, Kurangnya Kesadaran, Keyakinan, Perilaku, Penggunaan Teknologi yang Tidak Memadai, Risiko Keamanan Komputer	Umum
[38]		Perceived information security knowledge (PISK), Perceived social competence (PSC), Perceived information security problem-solving skills (PSPS)	Umum
[39]	Manajemen Puncak, Kontrol Keamanan	Kepatuhan, Kesadaran	Industri Kecil dan Menengah
[40]	Aset, Kontinuitas, Akses dan Kepercayaan, Operasi, Pertahanan, Tata Kelola Keamanan	Sikap, Kesadaran, Perilaku, Kompetensi	Umum
[41]	Artefak dan kreasi, Nilai, Organisasi, Lindungi informasi, Manajemen, Kebijakan, Perubahan.	Perilaku, Manusia, norma dan pengetahuan, Asumsi dan keyakinan dasar, Sikap/persepsi,	Akademi, Industri Kecil dan Menengah
[42]	Komitmen Manajemen Puncak terhadap Keamanan, Pemantauan	Komunikasi	Umum
[43]	Dukungan manajemen puncak, Kemampuan tempat kerja, Faktor risiko dan respons, Manajemen operasional, Manajemen perubahan, Budaya organisasi, Masalah lunak dan kemandirian tempat kerja, Kebijakan Keamanan Informasi,	Pengetahuan, Kepatuhan keamanan, Perilaku keamanan, Pelatihan dan kesadaran	Kesehatan
[44]	Manajemen Puncak, Kebijakan Keamanan, Penilaian Risiko, Perilaku Etis, Kepuasan Kerja,	Pendidikan & Pelatihan Keamanan Informasi, Sifat Kepribadian, Kesadaran Keamanan, Kepemilikan Keamanan, Kepatuhan Keamanan	Umum
[45]	Dukungan manajemen senior, dan kebijakan keamanan informasi.	Budaya organisasi yang berorientasi pada karyawan versus pekerjaan, pelatihan & kampanye kesadaran, kepercayaan antarpribadi,	Pemerintah

Pada Tabel 1 di atas, tingkat organisasi dimaksudkan untuk mencakup semua faktor yang terkait dengan infrastruktur, operasi, kebijakan, dan prosedur teknologi keamanan organisasi sedangkan tingkat individu ditujukan pada atribut dan karakteristik karyawan yang berdampak langsung pada sikap keamanan mereka dan perilaku [40].

1) Individu: Keamanan informasi tergantung pada sikap orang-orang yang terlibat dalam proses di dalamnya [28] [7] [40] [41]. Namun, bahkan jika manusia yang terlibat memiliki sikap positif terhadap keamanan informasi, informasi organisasi tidak akan aman jika manusia yang sama tidak memiliki pengetahuan yang diperlukan. [14] [16] [29] [4]. Jadi pengguna individu harus memahami peran dan tanggung jawab yang bergantung pada perilaku mereka [22] [35]. Untuk memastikan tingkat pengetahuan, kesadaran, pelatihan, dan program pendidikan yang diperlukan telah terpenuhi [19] [4]. Faktor manusia meliputi perilaku, tanggung jawab, keahlian, pelatihan, sikap atau etika, kesadaran, kepercayaan, motivasi, kolaborasi, komunikasi, operasi, motivasi, pengetahuan, peran, dan interaksi.

2) Organisasi: Budaya organisasi merupakan salah satu dimensi yang biasa ditemukan dalam penelitian tentang keamanan informasi [26] [29]. Budaya perusahaan dibentuk oleh perilaku anggota perusahaan yang dominan seperti pendiri dan manajer puncak. Jadi budaya organisasi dapat memiliki aspek yang berbeda dari satu organisasi ke organisasi lainnya berdasarkan anggota perusahaan yang dominan. Contoh budaya organisasi adalah kebijakan dan struktur administrasi [43]. Budaya organisasi meliputi kebijakan, struktur organisasi, pengendalian, komitmen manajemen, operasi, sistem, regulasi, lingkungan, sanksi dan penghargaan.

Teknologi merupakan salah satu kunci sukses dalam pengelolaan keamanan informasi. Praktisi IS percaya pada hubungan yang kuat antara kontrol keamanan, termasuk sosial, kontrol keamanan teknologi dan budaya keamanan. Beberapa peneliti juga mengatakan bahwa ketika membangun budaya keamanan informasi, kita perlu menggabungkan aspek-aspek berikut secara harmonis: sumber daya manusia, proses, dan teknologi [5]. Dimensi teknologi terdiri dari teknologi yang digunakan untuk keamanan informasi termasuk perangkat keras, perangkat lunak, layanan aplikasi dimana semua dimensi ini untuk melindungi aset informasi [11].

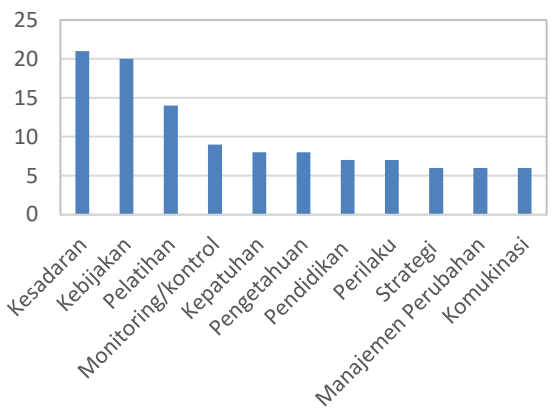
Organisasi yang memiliki komitmen jangka panjang dan manajemen strategis yang baik dapat menjadi organisasi dengan keamanan informasi yang berkualitas tinggi. Ada kecenderungan untuk merombak total manajemen keamanan/struktur tata kelola ketika perlindungan tidak lagi memadai atau biaya pemeliharaan terlalu tinggi. Namun, tidak ada bukti bahwa mereka telah mempertimbangkan strategi jangka panjang dan rencana apa yang harus dilakukan di masa depan. Strategi jangka panjang yang jelas bertujuan untuk menyelaraskan keamanan organisasi dan budaya organisasi [26]. Beberapa dimensi yang dikelompokkan ke dalam tata kelola antara lain manajemen, koordinasi, tata kelola, dan kepemimpinan.

Strategi dalam konteks ini berkaitan dengan penerapan keamanan informasi yang tepat sesuai kebutuhan, seperti rencana tindakan, tujuan, praktik terbaik, standar, pedoman, dan prioritas yang dirancang untuk memandu organisasi anggota untuk mencapai tujuan melindungi aset Informasi [24]. Sedangkan kelompok Strategi meliputi audit, orientasi, strategi, artefak, program, dan persyaratan.

Gambar 2 menunjukkan bahwa 11 dimensi terbanyak pada Tabel 1 adalah kesadaran yang digunakan pada 21 studi, kebijakan digunakan pada 20 studi, pelatihan digunakan dalam 14 studi, pemantauan/kontrol digunakan dalam 9 studi, kepatuhan dan pengetahuan digunakan dalam 8 studi, pendidikan dan perilaku digunakan dalam 7 studi, sedangkan strategi, manajemen perubahan, dan komunikasi masing-masing digunakan dalam 6 studi.

Tabel 1 juga memberikan informasi terkait jenis organisasi yang dibahas dalam 39 literatur yang dipelajari pada penelitian ini. Ada 9 jenis organisasi yang meliputi kesehatan, pemerintahan, industri kecil dan menengah, organisasi publik, keuangan, umum, perusahaan perdagangan, telekomunikasi dan akademi.

Organisasi bidang Kesehatan menggunakan dimensi-dimensi keamanan informasi berikut: sistem organisasi, persyaratan keamanan perilaku, manajemen perubahan, kesadaran keamanan informasi, pengetahuan, dukungan manajemen puncak, kemampuan tempat kerja, faktor risiko dan respons, manajemen operasional, manajemen perubahan, budaya organisasi, masalah lunak dan kemandirian tempat kerja, kebijakan keamanan informasi, kepatuhan keamanan, perilaku keamanan, pelatihan dan kesadaran.



Gambar 2. 11 dimensi terbanyak

Berikut dimensi-dimensi keamanan Informasi yang digunakan pada organisasi Pemerintah: penegakan kebijakan, dukungan manajemen puncak, pelatihan, kesadaran, kepemilikan, kebijakankepatuhan, kesadaran, strategi, teknologi, organisasi, orang, lingkungan, komitmen manajemen puncak, akuntabilitas kesadaran keamanan informasi, dukungan manajemen senior, dan kebijakan keamanan informasi, budaya organisasi yang berorientasi pada karyawan versus pekerjaan, kampanye pelatihan dan kesadaran, kepercayaan antar pribadi.

Organisasi publik menggunakan dimensi-dimensi keamanan informasi berikut: nilai-nilai yang dianut, artefak, asumsi tacit bersama, pengetahuan keamanan informasi, kebijakan keamanan informasi, sikap manajerial kepatuhan terhadap praktik terbaik system informasi, pelatihan dan kesadaran, komitmen keamanan informasi, pentingnya keamanan informasi, efektivitas kebijakan keamanan informasi, arahan keamanan informasi, kepatuhan pemantauan keamanan informasi, konsekuensi keamanan informasi, praktik anggaran keamanan informasi, investasi keamanan informasi, kemampuan teknologi informasi, informasi kompatibilitas teknologi tanggung jawab keamanan informasi, dan pelatihan keamanan informasi.

Organisasi di bidang Industri Kecil dan Menengah menggunakan dimensi-dimensi keamanan informasi berikut: informasi yang berkaitan dengan insiden dan kerentanan, analisis dan manajemen risiko, strategi dan perencanaan, kebijakan dan standar, proses dan prosedur, metodologi dan kerangka kerja, audit dan kontrak pengetahuan dan pengalaman, kesadaran, pelatihan dan outsourcing, budaya, pengambilan keputusan, manajemen, strategi, kebijakan, kompetensi, peran dan tanggung jawab, kebijakan insentif, dan disinsentif, ketidaktahuan dan kelalaian, anggaran, pengembalian investasi keamanan informasi, budaya, keamanan dan iklim keamanan informasi, penegakan kebijakan keamanan, dukungan manajemen, dasbor bisnis keamanan informasi, dan bias pemrosesan informasi, audit dan proses kepatuhan, kegunaan, pelatihan dan pendidikan, keterampilan, pengalaman, keterlibatan karyawan, stres individu, keamanan perilaku, komunikasi, persepsi risiko, teknologi, organisasi, orang, lingkungan, manajemen puncak dan kontrol keamanan.

Organisasi di bidang Keuangan menggunakan dimensi-dimensi keamanan informasi berikut: kepemimpinan keamanan informasi, manajemen aset informasi, manajemen perubahan, manajemen keamanan informasi, manajemen pengguna, program keamanan informasi, kebijakan keamanan informasi, manajemen pengguna, manajemen aset informasi, manajemen keamanan informasi, program keamanan informasi, manajemen perubahan, kebijakan keamanan informasi, kepemimpinan keamanan informasi, pelatihan, dan kesadaran.

Berikut dimensi-dimensi keamanan Informasi yang digunakan pada organisasi umum: pemantauan keamanan, komitmen manajemen puncak, komunikasi, budaya keamanan, kebijakan keamanan, seta (pendidikan keamanan, pelatihan, dan kesadaran), organisasi, strategi, teknologi, orang, lingkungan, sanksi, penghargaan, jumlah karyawan, peran pekerjaan, perilaku keamanan, kesadaran dan pendidikan keamanan, penerimaan keamanan, kepemimpinan keamanan informasi, manajemen aset informasi, manajemen pengguna, manajemen perubahan, program keamanan informasi, manajemen keamanan informasi, kepercayaan, kepatuhan, akuntabilitas, tata kelola, artefak, nilai-nilai yang dianut, asumsi diam-diam bersama, strategi, pengetahuan, persepsi, motivasi, pelatihan, manajemen risiko, berbagi pengetahuan keamanan informasi, evaluasi risiko keamanan, biaya kepatuhan keamanan, evaluasi kepatuhan keamanan formal, pengaruh sosial, efikasi diri keamanan, standar, prosedur, manajemen sistem, masalah keamanan informasi umum, komitmen manajemen, budaya pelaporan dan reaksi terhadap pelaporan insiden, sikap karyawan, kurangnya motivasi, kurangnya kesadaran, keyakinan, perilaku, penggunaan teknologi yang tidak memadai, risiko keamanan komputer, perceived information security knowledge (pisk), perceived social competence (psc), perceived information security problem-solving skills (psps), aset, kontinuitas, akses dan kepercayaan, operasi, pertahanan, sikap, kompetensi, perilaku etis, kepuasan kerja, sifat kepribadian, kepemilikan keamanan.

Perusahaaan perdagangan menggunakan dimensi-dimensi keamanan informasi berikut: strategi, teknologi, organisasi, orang, dan lingkungan.

Perusahaaan telekomunikasi menggunakan dimensi-dimensi keamanan informasi berikut: asosiasi, subsistensi, biseksualitas, teritorial, temporalitas, eksploitasi, rekreasi dan humor, pertahanan, pembelajaran, dan interaksi.

Sedangkan organisasi di bidang Akademi menggunakan dimensi-dimensi keamanan informasi berikut: prosedur penanggulangan, manajemen risiko, manajemen puncak, komitmen, pemantauan, pendidikan keamanan, pelatihan, dan kesadaran, pengetahuan keamanan informasi, berbagi

pengetahuan keamanan informasi, artefak dan kreasi, nilai, organisasi, lindungi informasi, manajemen, kebijakan, perubahan, perilaku, manusia, norma dan pengetahuan, asumsi dan keyakinan dasar, dan sikap/persepsi.

IV. KESIMPULAN

Kami telah mendemonstrasikan dan mendiskusikan studi terbaru tentang budaya keamanan informasi pada dimensinya sesuai dengan bidang organisasinya. Ada beberapa bidang organisasi yaitu kesehatan, pemerintahan, Industri Kecil dan Menengah, organisasi publik, keuangan, umum, perusahaan perdagangan, telekomunikasi dan akademi. Secara umum, studi ini mengkaji 39 makalah antara tahun 2012 dan 2021. Kesebelas dimensi yang sering digunakan adalah kesadaran (21 studi), kebijakan (20 studi), pelatihan (14 studi), monitoring/kontrol (9 studi), Kepatuhan (8 studi). studi), pengetahuan (8 studi), Pendidikan (7 studi), perilaku (7 studi), Strategi (6 studi), manajemen perubahan (6 studi) dan komunikasi (6 studi). Penelitian selanjutnya dapat menggunakan berbagai macam dimensi ini untuk pengukuran indeks budaya keamanan informasi.

REFERENSI

[1] N. S, Safa, M. Sookhaka, R. V. Solms, S. Furnell, N. A. Ghania and T. Herawana, "Information security conscious care behaviour formation in organizations," *Computers & Security*, pp. 65-78, 2015.

[2] A. A. Maidabino and A.N. Zainab, "A holistic approach to collection security implementation in university libraries," *Library Collections, Acquisitions, & Technical Services*, pp. 107-120, 2012.

[3] A. da Veiga and N. Martins, "Improving the information security culture through monitoring and implementation actions illustrated through a case study," *Computers & Security*, pp. 162-176, 2015.

[4] A. Nasir, R. A. Arshah and M. R. A. Hamid, "Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture: A Conceptual Framework," *Information System and Data Mining*, pp. 56-60, 2017.

[5] A. Al Hogail, "Design and validation of information security culture framework," *Computers in Human Behavior*, pp. 567-575, 2015.

[6] A. Nasir, R. A. Arshah and M. R. A. Hamid, "A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions," *Information Security Journal: A Global Perspective*, vol. 28, no. 3, pp. 55-80, 2019.

[7] T. O. Nævestad, S. F. Meyer and J. H. Honerud, "Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information security," in *Safety and Reliability*, London, Taylor & Francis Group, pp. 3021-3029, 2018.

[8] A. Nasir, R. A. Arshah, M. R. A. Hamid and S. Fahmy, "An analysis on the dimensions of information security culture concept: A review," *Journal of Information Security and Applications*, pp. 12-22, 2019.

[9] S. Orehek and G. Petrič, "A systematic review of scales for measuring information security culture," *Information and Computer Security*, pp. 133-158, 2021.

[10] I. Okere, J. van Niekerk and M. Carroll, "Assessing Information Security Culture: A Critical Analysis of Current Approaches," *Information Security for South Africa (ISSA)*, pp. 136-143, 2012.

[11] A. da Veiga and N. Martins, "Information Security Culture: A Comparative Analysis of Four Assessments," *European Conference on Information Management and* Evaluation, pp. 49-57, 2014.

[12] J. Valuch, T. Gábriš and O. Hamulak, "Cyber Attacks, Information Attacks, and Postmodern Warfare," *Baltic Journal of Law & Politics*, vol. 10, iss. 1, pp. 63-89, 2017.

[13] S. Kim, G. Heo, E. Zio, J. Shin and Jae-guSong, "Cyber attack taxonomy for digital environment in nuclear power plants," *Nuclear Engineering and Technology*, pp. 995-1001, 2020.

[14] N. H. Hassan and Z. Ismail, "A conceptual model for investigating factors influencing information security culture in healthcare environment," *International Congress on Interdisciplinary Business and Social Science 2012 (ICIBSoS 2012)*, pp. 1007 – 1012, 2012.

[15] M. A. Alnatheer, "Understanding and Measuring Information Security Culture in Developing Countries: Case of Saudi Arabia," *PhD diss., Queensland University of Technology*, 2012.

[16] A. Fagerström, "Creating, Maintaining and Managing an Information Security Culture," *KPMG Oy Ab*, 2013.

[17] I. Al-Mayahi and S. P. Mansoor, "Information Security Culture Assessment: Case Study," In *2013 IEEE Third International Conference on Information Science and Technology (ICIST)*, pp. 789-792. IEEE, 2013.

[18] J. D'Arcy and G. Greene, "Security culture and the employment relationship as drivers of employees' security compliance," *Information Management & Computer Security*, pp. 474 - 489, 2014.

[19] Y. Chen, K. (Ram) Ramamurthy and K. Wen, "Impacts of Comprehensive Information Security Programs on Information Security Culture," *Journal of Computer Information Systems*, pp. 11-19, 2015.

[20] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson and C. Jerram, "The Influence of Organizational Information Security Culture on Information Security Decision Making," *Journal of Cognitive Engineering and Decision Making*, pp. 117-129, 2015.

[21] A. AlHogail and A. Mirza, "Organizational Information Security Culture Assessment," *International Conference on Security and Management SAM 2015*, pp. 286-292, 2015.

[22] E. Sherif and S. Furnell, "A Conceptual Model for Cultivating an Information Security Culture," *International Journal for Information Security Research (IJISR)*, pp. 565-573, 2015.

[23] A. Da Veiga and N. Martins, "Information security culture and information protection culture: A validated assessment instrument," *Computer Law & Security Review*, pp. 243-256, 2015.

[24] A. Al-Hogail, "Cultivating and Assessing an Organizational Information Security Culture; an Empirical Study," *International Journal of Security and Its Applications*, pp. 163-178, 2015.

[25] A. Al Kalbani, H. Deng and B. Kam, "Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure," *Pacific Asia Conference on Information Systems (PACIS 2015)*, pp. 1-11. RMIT University, 2015.

[26] M. Tang, M. Li and T. Zhang, "The impacts of organizational culture on information security culture: a case study," *Information Technology and Management*, vol. 17, no. 2: 179-186. 2015

[27] G. Dhillon, R. Syed and C. Pedron, "Interpreting information security culture: An organizational transformation case study," *Computers & Security*, pp. 63-69, 2016.

[28] F. Al-Izki and G. R. S. Weir, "Management Attitudes Toward Information Security in Omani Public Sector Organisations," *Cybersecurity and Cyberforensics Conference (CCC)*, pp. 107-112, 2016.

[29] S. Govender, E. Kritzinger and M. Loock, "The Influence of National Culture on Information Security Culture," In *2016 IST-Africa Week Conference*, pp. 1-9. IEEE, 2016.

[30] H. C. Pham, D. D. Pham, L. Brennan and J. Richardson, "Information Security and People: A Conundrum for Compliance," *Australasian Journal of Information Systems*, vol. 21, 2017.

[31] A. G. Bello, D. Murray and J. Armarego, "A systematic approach to investigating how information security and privacy can be achieved in BYOD environments," *Information & Computer Security*, pp. 475-492, 2017.

[32] W. Sung and S. Kang, "An Empirical Study on the Effect of Information Security Activities: Focusing on Technology, Institution, and Awareness," *Digital Government Research*, pp. 84-93, 2017.

[33] T. R. Vinnakota and N. G. P. L Mandaleeka, "Assessing an Information Security Governance of an Enterprise," *US Patent*, 2017.

[34] M. N. Masrek, Q. N. Harun and M. K. Zaini, "The Development of an Information Security Culture Scale for the Malaysian Public Organization," *International Journal of Mechanical Engineering and Technology (IJMET)*, p. 1255–1267, 2018.

[35] Choe, A. I. Al-Darwish and Pilsung, "A Framework of Information Security Integrated with Human Factors," *International Conference on Human-Computer Interaction*, p. 217–229, 2019.

[36] K. Arbanas and N. Z. Hrustek, "Key Success Factors of Information Systems Security," *Journal of Information and Organizational Sciences*, pp. 131-144, 2019.

[37] Z. Shouran, T. K. Priyambodo and A. Ashari, "Information System Security: Human Aspects," *International Journal of Scientific & Technology Research*, pp. 111-115, 2019.

[38] H. L. Kim, A. Hovav and J. Han, "Protecting intellectual property from insider threats," *Journal of Intellectual Capital*, pp. 181-202, 2019.

[39] A. Ključnikov, L. Mura and D. Sklenár, "Information Security Management in SMEs: Factors of Success," *Journal of Entrepreneurship and Sustainability Issues*, pp. 2081-2094, 2019.

[40] A. Georgiadou, S. Mouzakitis, K. Bounas and D. Askounis, "A Cyber-Security Culture Framework for Assessing Organization Readiness," *Journal of Computer Information Systems*, pp. 1-11, 2020.

[41] A. da Veiga, L. V. Astakhova, A. Botha and M. Herselman, "Defining organisational information security culture – Perspectives from academia and industry," *Computers & Security*, 2020.

[42] G. Solomon and I. Brown, "The influence of organisational culture and information security culture on employee compliance behaviour," *Journal of Enterprise Information Management*, 2020.

[43] P. K. Sari, A. Prasetio, Candiwan, P. W. Handayani, A. N. Hidayanto, S. Syauqina, E. F. Astuti and F. P. Tallei, "Information security cultural differences among health care facilities in Indonesia," *Heliyon*, vol. 7, no. 6, 2021.

[44] A. Tolah, S. M. Furnell and M. Papadaki, "An Empirical Analysis of the Information Security Culture Key Factors Framework," *Computers & Security*, 2021.

[45] S. Tenzin, "An Investigation of the Factors that Influence Information Security Culture in Government Organisations in Bhutan," *Doctoral Dissertation, Murdoch University*, 2021.