KEMAHIRAN LITERASI DIGITAL DAN TINGKAH LAKU KESELAMATAN MAKLUMAT DI KALANGAN PEKERJA DALAM PERSEKITARAN KERJA SECARA ATAS TALIAN BAGI MEMUPUK BUDAYA KESELAMATAN MAKLUMAT

Mohd Sharulnizam Kamarulzaman [1]*; Shamila Mohamed Shuhidan[2]; Khalid Abdul Wahid[3] dan Abdul Jalil Toha[4]
*Email: sharul.aimer@gmail.com

[1,2]Faculty of Information Management & Universiti Teknologi MARA Puncak Perdana Campus, Seksyen U10, 40150, Shah Alam, Selangor, Malaysia

[3]Universiti Teknologi MARA Cawangan Kelantan, Bukit Ilmu, 18500 Machang, Kelantan, Malaysia

[4]Bahagian Pembangunan Kurikulum Kementerian Pendidikan Malaysia, Aras 4-8, Blok E9, Kompleks Kerajaan Parcel E, Pusat Pentadbiran Kerajaan Persekutuan, Presint 1, 62000 Putrajaya

Abstrak: Budaya Keselamatan Maklumat (BKM) telah dicadangkan sebagai cara untuk mengukuhkan keselamatan maklumat pekerja di tempat kerja. Walau bagaimanapun, peranan pekerja dan kemahiran digital mereka dalam proses itu telah banyak diabaikan terutamanya dalam persekitaran kerja atas talian. Mempunyai pekerja yang celik digital dapat mempengaruhi pengwujudan bu- daya keselamatan maklumat, serta memberi pengaruh ke atas tingkah laku pekerja berkenaan keselamatan siber dalam sesebuah organisasi dan merupakan salah satu langkah yang dapat mengurangkan risiko yang disebabkan oleh manu- sia. Sejak tercetusnya pandemik, kebanyakan pekerja dikehendaki bekerja secara atas talian, sekali gus meningkatkan bahaya ancaman keselamatan siber pada aset maklumat organisasi. Oleh itu, budaya keselamatan maklumat sesebuah organ- isasi adalah penting dengan memahami literasi digital (LD) dan kesan tingkah laku keselamatan maklumat (TLKM) terhadap pekerja di persekitaran kerja atas talian. Inisiatif ini akan memberikan pemahaman lanjut tentang isu-isu dan men- jadi sebahagian daripada penyelesaian dengan menyumbang kepada literatur ba- haru dan dalam mempertingkatkan inisiatif, rangka kerja dan garis panduan se- masa yang telah sedia ada. Ia akan meningkatkan pemetaan rangka kerja keceka- pan LD pekerja Malaysia dengan budaya keselamatan maklumat dan rangka kerja tingkah laku dalam persekitaran kerja atas talian, serta memberikan pema- haman dan pengetahuan kepada kerajaan, penggubal dasar dan organisasi mengenai jurang itu. Kepen- tingan kajian ini ialah ia akan meningkatkan tahap LD dan TLKM dalam kalangan pekerja yang terlibat terutamanya dalam melaksanakan rancangan pembangunan negara, seperti meningkatkan fungsi pentadbiran, infrastruktur sosial, dan prestasi pertumbuhan ekonomi negara selaras dengan inisiatif MyDigital, serta sebagai menambah baik BKM dalam organisasi.

Kata Kunci: Literasi digital, budaya keselamatan siber, tingkah laku keselamatan maklumat, kerja atas talian.

Pendahuluan

Keselamatan maklumat adalah komponen penting dalam kehidupan seharian dalam era moden. Maklumat digunakan dalam semua aspek kehidupan profesional dan peribadi kita. Menurut Alhogail, 2015, berdasarkan penyelidikan oleh Van Niekerk dan Von Solms (2010), mengekalkan aset maklumat mesti menjadi perhatian utama kerana banyak organisasi tidak dapat berfungsi tanpa data mereka. Menurut penyelidikan 2018 oleh PriceWaterhouseCoopers, kira-kira 30 peratus kebimbangan keselamatan dicetuskan oleh pekerja, 27 peratus oleh bekas pekerja, dan 23 peratus oleh penggodam yang tidak diketahui. Pelanggaran keselamatan boleh mengakibatkan kehilangan atau kerosakan data sensitif. Walaupun hakikat bahawa kesilapan manusia menyumbang sebahagian besar insiden, hanya 34% daripada organisasi telah menyediakan program untuk mengajar kakitangan tentang kebimbangan keselamatan. Selain itu, hanya 31% organisasi mengatakan bahawa dasar keselamatan data adalah mandatori dan latihan amalan terbaik perlu dilaksanakan (PriceWaterhouseCoopers, 2019). Menurut petikan Nel dan Drevin berdasarkan kajian Thomson, von Solms, dan Louw (2006), komitmen syarikat terhadap keselamatan maklumat adalah sangat penting (Nel & Drevin,2019).

Di samping itu, penyelidikan lepas telah menunjukkan bahawa majoriti pelanggaran data disebabkan oleh pekerja yang tidak bertanggungjawab (Cheng et al., 2017; MyCert, 2017). Ini menyerlahkan lagi keperluan pentingnya bagi pekerja Malaysia untuk membina budaya keselamatan maklumat. Alhogail, 2015, memetik kajian Schlienger & Teufel, 2003, menyatakan bahawa budaya keselamatan maklumat merangkumi semua teknik sosiobudaya yang menyokong langkah keselamatan teknologi dalam usaha untuk mengintegrasikan keselamatan maklumat ke dalam aktiviti harian pekerja (Alhogail, 2015). Ia juga konsisten dengan penyelidikan mengenai budaya keselamatan maklumat yang dijalankan oleh Ramachandran, Rao, dan Goles pada tahun 2008, yang menunjukkan bahawa pemahaman terhadap kepercayaan, sikap dan nilai berkaitan keselamatan dapat membentuk dan mengarahkan tingkah laku berkaitan keselamatan. Menurut penyelidikan Alhogail, yang memetik hujah oleh Malcolmson, 2009, "Budaya keselamatan" boleh mempengaruhi cara pekerja berinteraksi dengan sistem dan proses organisasi pada bila- bila masa, yang membawa kepada tingkah laku yang boleh diterima atau tidak boleh diterima. Budaya keselamatan maklumat ditakrifkan sebagai "kumpulan persepsi, nilai, sikap, andaian, pengetahuan, dan kemahiran yang mengawal penglibatan manusia

dengan aset maklumat dalam organisasi dalam usaha untuk mempengaruhi tingkah laku keselamatan pekerja bagi mengekalkan keselamatan maklumat" (Alhogail & Mirza, 2014b). BKM diterangkan lebih lanjut oleh Masrek et al. (2018) sebagai keadaan di mana kakitangan bukan sahaja memiliki kesedaran dan kebolehan yang diperlukan untuk keselamatan maklumat, tetapi juga mempunyai pemahaman tentang proses dan prosedur yang memastikan keselamatan maklumat. Organisasi dilihat mempunyai BKM yang baik jika ia melengkapkan kakitangannya dengan latihan, pengetahuan dan kemahiran yang diperlukan.

Penggunaan teknologi telah membawa kebimbangan baharu tentang cara melindungi privasi dan keselamatan maklumat peribadi dalam mengambil kesempatan daripada faedah dan kemudahan yang berkaitan. Pertimbangan juga mesti diberikan kepada literasi digital. Dari segi sejarah, hanya profesional yang mempunyai akses kepada teknologi; namun, ini telah berubah secara drastik dari semasa ke semasa. Peningkatan zaman maklumat dan perkembangan pesat media digital akan mengubah interaksi pekerja dengan maklumat secara dramatik selama-lamanya. Teknologi baharu, seperti komputer dan peranti mudah alih, telah membentuk semula cara orang menerima maklumat. Memandangkan teknologi maklumat dan komunikasi (ICT) telah maju, begitu juga konsep yang digunakan untuk mentakrifkan literasi. Idea ini telah dirujuk pada masa lalu dan sekarang sebagai "celik ICT", "celik komputer", "celik elektronik", "celik rangkaian", "celik maklumat", dan "celik media". Secara amnya dipersetujui bahawa konsep literasi harus berkembang seiring dengan evolusi ICT, dan penyelidikan lepas telah menunjukkan bahawa kedua-dua perkataan dan kriteria penilaian telah disesuaikan dengan perubahan landskap (Ng, 2012). Literasi perlu berubah mengikut definisi untuk menjadi berkesan dalam dunia di mana maklumat terus berkembang. Namun begitu, kajian kesusasteraan kontemporari mengenai subjek ini mendedahkan bahawa 'literasi digital' telah menggantikan 'literasi maklumat' sebagai titik fokus baharu wacana. Disebabkan oleh perkembangan pesat teknologi maklumat dan percambahan sumber dan sistem maklumat baharu, pengguna dijangka meningkatkan carian maklumat, tingkah laku dan kebolehan mereka, di samping menyesuaikan diri dengan budaya keselamatan maklumat.

Sesungguhnya, integrasi teknologi ke dalam kewujudan manusia telah meningkat. Untuk pekerja menjadi berkesan dan produktif dalam kerjaya mereka, mereka mesti memiliki atau mencapai tahap pengetahuan tertentu. Dalam era maklumat yang pantas, privasi dan keselamatan data sentiasa berisiko. Akibatnya, organisasi bertanggungjawab untuk mematuhi undang-undang yang mengawal perlindungan aset maklumat dengan memupuk budaya berpaksikan keselamatan maklumat. Kakitangan juga diperlukan untuk beroperasi dalam rangka kerja tertentu organisasi, yang menonjolkan isu literasi digital dalam tenaga kerja untuk mencapai matlamat yang dinyatakan. Keselamatan maklumat mesti diperiksa untuk memastikan pematuhan dengan rangka kerja sistem maklumat organisasi. Seperti yang dinyatakan dalam istilah tersebut, melindungi privasi maklumat memerlukan pengekalan kerahsiaan sebarang butiran yang boleh mendedahkan identiti individu dan juga organisasi. Privasi adalah berkenaan dengan pemeliharaan hak dan keistimewaan individu berbanding data yang serupa, manakala keselamatan adalah berkenaan dengan perlindungan sumber maklumat dan matlamat korporat (Burkell, 2015).

Menurut huraian sebelum ini, adalah penting untuk memahami cara pekerja berkelakuan dengan betul semasa mengurus maklumat sebagai individu yang celik digital semasa bekerja bukan sahaja di pejabat tetapi juga secara atas talian, terutamanya dari rumah. Untuk memahami tingkah laku pekerja, adalah perlu untuk mengkaji budaya keselamatan maklumat yang telah ditubuhkan oleh organisasi, kerana tingkah laku keselamatan maklumat pekerja membentuk budaya keselamatan maklumat organisasi. Disebabkan kepentingan keselamatan maklumat, penyelidikan dan kajian terdahulu mengenai literasi digital tertumpu terutamanya pada sektor pendidikan, dengan hanya sejumlah kecil literatur menangani masalah dari sudut organisasi.

Ia harus dipandang serius kerana dalam situasi keadaan semasa, yang menyokong kerja secara atas talian dan bekerja dari rumah, pekerja bersendirian tanpa sebarang pemantauan atau langkah keselamatan, berbanding ketika mereka bekerja di pejabat. Dengan cara ini, tingkah laku keselamatan maklumat pekerja mungkin berdasarkan pengetahuan dan tingkah laku mereka sendiri, khususnya kemahiran literasi digital mereka dan budaya keselamatan maklumat organisasi mereka sendiri. Disebabkan kekurangan kawalan dalaman dan pengurusan, adalah jauh lebih sukar bagi sesebuah organisasi untuk memastikan kakitangannya mengamalkan amalan keselamatan maklumat yang betul. Untuk memahami tingkah laku keselamatan maklumat pekerja, organisasi mesti memupuk budaya keselamatan maklumat. Ini memerlukan pengajaran satu set nilai dan sikap yang sama dalam diri pekerja untuk membantu mereka dalam mewujudkan persekitaran maklumat yang selamat.

Kajian Literatur

Keselamatan Maklumat dalam Konteks Malaysia

Risiko dan serangan keselamatan, seperti ancaman yang timbul daripada faktor luaran atau diiktiraf sebagai ancaman luaran yang dikaitkan dengan orang luar yang melanggar keselamatan maklumat organisasi, boleh menambahkan ketidakcekapan dan kekurangan produktiviti organisasi. Malah pengurusan dan kakitangan mungkin terdedah kepada bahaya dalaman.

Mengenai isu ini, Malaysia telah pun mengeluarkan dasar keselamatan siber yang praktikal; diarahkan oleh Majlis Keselamatan Negara (MKN), Strategi Keselamatan Siber Malaysia 2020-2024 bertujuan memastikan keselamatan maklumat di samping menggalakkan kemajuan ekonomi dan kebajikan awam serta memperkukuh rangkaian pertukaran maklumat, saluran dan rujukan untuk agensi kerajaan, syarikat dan orang awam mengenai keselamatan dan bahaya siber (Majlis Keselamatan Negara, 2020). Selain itu, kesedaran situasi, kerjasama, dan kapasiti untuk mengurangkan bahaya mesti dipertingkatkan. Di samping memberi penerangan tentang keperluan mengutamakan keselamatan di peringkat nasional, kajian ini menunjukkan kepentingan melaksanakan pendekatan atas ke bawah termasuk semua warganegara Malaysia dari segi keselamatan maklumat.

Memandangkan krisis kesihatan global ini, kepentingan teknologi di tempat kerja telah meningkat. Covid-19 memerlukan perniagaan celik digital agar mereka berkembang maju (Siti Aiysyah Tumin, 2020). Sebelum wabak, banyak insentif dilaksanakan untuk menggalakkan firma mengguna pakai inovasi teknologi terutamanya inisiatif Revolusi Perindustrian Keempat (Revolusi 4.0). Manakala inisiatif MyDIGITAL menghasilkan Pelan Tindakan Ekonomi Digital Malaysia untuk memastikan tiada rakyat Malaysia yang ketinggalan dalam revolusi digital dan mewujudkan asas bagi peralihan negara kepada ekonomi digital yang maju. Asas ini terdiri daripada rangka kerja untuk pertumbuhan infrastruktur, merangsang inovasi, dan menyediakan suasana di mana semua rakyat Malaysia boleh menyumbang untuk mencapai taraf hidup yang lebih tinggi. Takrif MyDIGITAL dalam Pelan Tindakan Ekonomi Digital Malaysia adalah berobjektif untuk mempercepatkan peralihan Malaysia kepada ekonomi berteknologi maju. Pada abad baru ini akan membina asas bagi kedudukan strategik Malaysia sebagai kuasa berdaya saing. MyDIGITAL merupakan pemangkin yang amat diperlukan bagi pelaksanaan Rancangan Malaysia Kedua Belas, 2021-2025 (RMKe-12), yang bertujuan merealisasikan Wawasan Kemakmuran Bersama 2030 (Unit Perancang Ekonomi, Jabatan Perdana Menteri, 2020).

Inisiatif MyDigital ini disasarkan untuk menggalakkan rakyat Malaysia menggunakan teknologi digital dalam kehidupan seharian mereka. Sebagai sebahagian daripada Teras 1 Pelan Tindakan Ekonomi Digital Malaysia: untuk memacu transformasi digital dalam sektor awam dengan matlamat untuk mendidik semua peringkat kakitangan kerajaan, daripada kakitangan peringkat permulaan kepada kakitangan peringkat atasan, mengenai celik digital; dan Teras 6: untuk membina persekitaran digital yang dipercayai, selamat, beretika dengan matlamat meningkatkan kesedaran keselamatan siber dan memastikan semua rakyat Malaysia mempunyai kemahiran dan pengetahuan yang diperlukan untuk memerangi serangan siber, program literasi digital nasional akan dilaksanakan. (Unit PerancangEkonomi, Jabatan Perdana Menteri, 2020). Inisiatif MyDigital ini akan menyiasat hubungan antara celik digital dan budaya keselamatan maklumat, serta pengaruh budaya keselamatan maklumat terhadap tingkah laku keselamatan maklumat pekerja jauh.

Budaya Keselamatan Maklumat

Organisasi harus memberikan penekanan yang lebih tinggi pada tingkah laku pekerja untuk mengurangkan kemungkinan berlakunya pelanggaran keselamatan maklumat. Dengan membina budaya yang mementingkan keselamatan, risiko kepada aset maklumat akan berkurangan (Da Veiga dan Eloff, 2010). Di sebalik risiko ini, pekerja mempunyai keupayaan untuk menjadi aset yang berharga dalam mengurangkan risiko kepada aset maklumat. Kunci untuk meningkatkan keselamatan maklumat ialah pematuhan pekerja kepada dasar dan prosedur keselamatan (Bulgurcu et al., 2010). Kakitangan yang terlatih dengan betul mempunyai potensi untuk menjadi penghubung terkuat organisasi dalam seni binanya (Thomson et al., 2006). Kakitangan sesebuah organisasi harus memiliki tahap literasi digital yang diperlukan untuk memastikan bahawa mereka cukup bersedia untuk mematuhi peraturan dan perundangan keselamatan maklumat, seterusnya memupuk budaya keselamatan maklumat yang sihat.

(Bulgurcu et al., 2010). Pekerja harus melihat keselamatan maklumat sebagai sifat kedua dan bahagian intrinsik dalam kerja harian mereka. Ini memudahkan penggabungan keselamatan maklumat ke dalam budaya korporat. Budaya korporat organisasi harus mempengaruhi tingkah laku keselamatan pekerjanya (Thomson et al., 2006).

Walaupun langkah keselamatan teknikal yang paling moden, pekerja (selalunya tanpa disedari) menyokong pelanggaran

keselamatan melalui tingkah laku yang tidak bertanggungjawab, yang berpunca daripada budaya keselamatan maklumat yang lemah (Singh et al., 2014; Tsohou et al., 2015). Dari perspektif sistem sosioteknikal, organisasi hanya boleh selamat jika komponen teknologi dan sosiobudaya mereka berada dalam harmoni. Unsur manusia dalam keselamatan maklumat biasanya dirujuk sebagai " tingkah laku keselamatan maklumat" dan merupakan fokus utama kebanyakan penyelidikan keselamatan tingkah laku. Kesedaran keselamatan maklumat, tingkah laku penjagaan sedar, pematuhan kepada keperluan keselamatan, budayaperlindungan maklumat dan budaya keselamatan siber, serta beberapa model teori, telah dibangunkan dalam domain ini.

Pengetahuan Tingkah Laku Keselamatan Maklumat

Dengan percambahan teknologi komputer, orang ramai boleh menggunakannya dalam beberapa situasi, atau konteks. Ini termasuk tempat kerja, rumah dan lokasi lain dengan komputer atau rangkaian awam. Dalam menetapkan tingkah laku keselamatan maklumat manusia dalam tetapan yang pelbagai mungkin rumit dan berubah-ubah. Individu boleh memilih sama ada dan bagaimana untuk melibatkan diri dalam tingkah laku keselamatan di rumah atau atas talian. Disebabkan oleh sifat subjektif dan sukarela keputusan pengguna yang bekerja dari rumah dan di mana saja diatas talian selain dari pejabat, serta hakikat bahawa persekitaran dan tetapan pengguna ini juga berbeza daripada organisasi, terdapat kemungkinan bahawa tingkah laku pengguna ini akan berbeza daripada yang diperhatikan di tempat kerja. Sebagai contoh, pekerja tidak perlu memasang anti-perisian pengintip kerana pentadbir IT mengendalikannya, manakala pengguna kediaman mesti memasangnya sendiri. Apabila memutuskan sama ada untuk memasang perisian atau tidak, pengguna rumah mungkin mempertimbangkan sama ada komputer itu menimbulkan ancaman atau tidak, sama ada mereka memerlukan perisian itu atau tidak, dan sebarang kriteria lain yang berkaitan. Contoh ini menunjukkan bahawa semasa di waktu pejabat, pekerja mempunyai akses kepada bantuan IT, sebaliknya apabila mereka berada luar waktu pejabat, yang mungkin mempengaruhi pertimbangan dan tindakan mereka berkenaan keselamatan komputer. Ini kerana pengaruh kontekstual. Pekerja boleh merahsiakan kata laluan berkaitan kerja mereka, kerana terdapat dasar keselamatan yang ketat, dan mereka bertanggungjawab terhadap masalah yang dibuat dengan mendedahkan kata laluan berkaitan kerja mereka kepada orang lain. Mungkin tiada undang-undang mengenai kata laluan peribadi mereka. Orang ramai boleh berkongsi kata laluan yang tidak berkaitan dengan kerja dengan keluarga, rakan dan rakan sekerja. Perbezaan ini berdasarkan jenis penggunaan, sama ada untuk kegunaan bekerja atau bukan kerja.

Kebimbangan Keselamatan Berkenaan Kerja Atas Talian

Rangkaian syarikat terdedah kepada pelbagai jenis kelemahan, had dan penjenayah siber. Memandangkan kerja pejabat boleh dipindahkan secara atas talian selain waktu pejabat, pengguna boleh log masuk ke rangkaian syarikat dari rumah atau tempat lain. Pengguna kekangan akhir ini juga akan diambil kira dalam perlindungan rangkaian korporat (Thompson et al., 2017). Tiada penyelidikan yang jelas mengenai pengguna komputer bagi mereka yang bekerja secara atas talian atau dari rumah yang menyerang rangkaian korporat. Selain itu, walaupun Penyedia Rangkaian Keselamatan (*Network Security Provider*) secara amnya berpendapat bahawa meminimumkan kelemahan me- merlukan peningkatan komponen teknologi rangkaian seperti perkakasan, perisian dan rangkaian, budaya, dasar dan proses dalaman yang masih belum dipertimbangkan (White, 2015; White, Ekin & Visinescu; 2017). Adalah dijangkakan bahawa lebih sepa- ruh daripada semua pelanggaran keselamatan akan mengakibatkan akses sistem yang tidak dibenarkan untuk pengguna. Penyelidikan juga mendedahkan bahawa insiden keselamatan maklumat semakin meningkat. Kesan sedemikian boleh dikurangkan jika organisasi memberi lebih tumpuan kepada risiko terhadap pekerja, terutamanya yang berkaitan dengan kerja luar pejabat dan atas talian (Bulgurcu et al., 2010; Guo, Yuan, Archer, & Connelly, 2011; Shropshire et al., 2015; Spears & Barki, 2010). Oleh itu, pembekal keselamatan rangkaian korporat bimbang tentang kelemahan pengguna ketika diluar waktu pejabat, terutamanya pengguna di rumah.

Perbincangan

Teknologi adalah elemen penting dalam kehidupan. Ia telah menjadi begitu meluas sehinggakan semua yang dilakukan, sama ada di tempat kerja atau di rumah, memerlukan interaksi dengan teknologi. Untuk menikmati faedah atau kemudahan menggunakan teknologi tersebut disamping mengekalkan privasi dan keselamatan data seseorang, penggunaan teknologi terpaksa memikul tanggungjawab tambahan iaitu literasi digital. Pada masa lalu, hanya pakar yang boleh menggunakan teknologi, tetapi ini telah berubah secara dramatik dari semasa ke semasa. Sesungguhnya, interaksi dengan teknologi telah menjadi komponen penting dalam kehidupan seharian. Untuk individu menjadi berkesan dan cekap di tempat kerja, tahap kemahiran tertentu diperlukan atau mesti dipelajari.

Organisasi harus melihat literasi digital sebagai proses berterusan yang boleh dilihat dari segi pembangunan peribadi pekerja (bergantung kepada persekitaran kerja mereka) dan kemajuan teknologi. Maklumat atau data adalah salah satu aset organisasi yang paling penting. Oleh itu, pengendalian dan perlindungannya adalah penting. Oleh itu perlunya menumpukan pada perspektif pekerja tentang penggunaan atau penglibatan dengan teknologi. Beberapa kajian telah dijalankan untuk mengkaji cara untuk meningkatkan privasi dan keselamatan maklumat dalam konteks meningkatkan celik digital dalam organisasi, serta halangan yang mereka hadapi apabila menggunakan atau terlibat dengan pelbagai platform teknologi. Di samping itu, untuk menentukan inisiatif yang boleh membantu dalam merapatkan jurang tersebut.

Kajian terdahulu telah menilai literasi digital pengguna maklumat dalam usaha untuk menentukan sama ada tahap literasi digital mereka memberi kesan kepada tingkah laku penggunaan maklumat mereka. Kajian memperincikan tingkah laku penggunaan maklumat sebagai satu set aktiviti diskret, seperti pemilihan dan kekerapan jenis sumber dan jumlah masa yang diperuntukkan dalam menggunakan peralatan dan sumber. Bates dan Maack (2010) menerangkan tingkah laku maklumat sebagai "cara di mana manusia terlibat dengan maklumat, terutamanya cara manusia mencari dan menggunakan maklumat." Ia adalah penting kepada perpustakaan atau mana-mana organisasi yang menyediakan akses kepada maklumat, serta saintis sosial yang ingin memahami

cara individu menggunakan dan memahami maklumat setiap hari.

Walaupun data yang luas ini, tidak ada penyiasatan terhadap perkaitan antara celik digital dan gelagat keselamatan maklumat. Semasa menjalankan kajian literatur ini, Hos EBSCO, LISA, Google Scholar, perpustakaan negara beberapa negara dan pangkalan data lain yang berkaitan telah disemak. Walau bagaimanapun, tiada kajian ditemui yang mengkaji korelasi antara celik digital dan tingkah laku keselamatan maklumat. Kedua-dua topik sentiasa disiasat secara bebas.

Pendekatan organisasi terhadap keselamatan maklumat harus tertumpu kepada tingkah laku pekerja, kerana kejayaan atau kegagalan organisasi bergantung kepada tindak tanduk pekerjanya. Budaya mementingkan keselamatan maklumat akan mengurangkan risiko kepada aset maklumat, terutamanya bahaya salah laku pekerja dan hubungan negatif dengan aset maklumat. Organisasi memerlukan arahan dalam membina atau melaksanakan budaya kesedaran keselamatan maklumat yang sesuai. Mereka mesti pandai menilai dan melaporkan keadaan budaya keselamatan maklumat organisasi. Terdapat banyak kaedah untuk menangani bahaya yang mungkin diberikan oleh tingkah laku pekerja. Walau bagaimanapun, teknik ini tidak menumpukan secara langsung kepada hubungan antara tingkah laku pekerja dan budaya organisasi. Organisasi memerlukan rangka kerja yang komprehensif untuk memupuk budaya mementingkan keselamatan.

Komponen budaya organisasi, tingkah laku organisasi dan keselamatan maklumat perlu dikaji dengan lebih lanjut. Hubungan antara prinsip-prinsip ini perlu di buat melalui pembinaan kerangka bagi menunjukkan bagaimana budaya keselamatan maklumat dipengaruhi dan dipupuk. Budaya keselamatan maklumat berkembang sebagai hasil daripada tingkah laku keselamatan maklumat pekerja, sama seperti budaya organisasi berkembang sebagai hasil daripada tingkah laku pekerja dalam organisasi (Martins dan Eloff, 2002; Hellriegel et al., 1998). Oleh itu, budaya keselamatan maklumat organisasi diasaskan pada interaksi pekerja dengan aset maklumat dan tingkah laku keselamatan yang mereka paparkan dalam rangka kerja budaya organisasi.

Kesimpulan

Literasi digital memainkan peranan dalam cara pekerja berinteraksi dengan platform digital. Intipatinya ialah bagaimana untuk melindungi aset maklumat sambil menggunakan teknologi. Ini boleh dipengaruhi oleh faktor luaran. Pendigitalan sentiasa perlu dan memperkasakan tenaga kerja adalah sangat penting dalam mana-mana organisasi. Melindungi aset maklumat juga penting, dengan mengeluarkan modal kepada pekerja, dengan memberikan set kemahiran yang diperlukan dan memastikan terdapat lebih banyak kesedaran mengenai platform baharu dan teknologi sedia ada. Penyelidikan masa depan akan diperlukan untuk menyiasat dan menyoal siasat cara pekerja berinteraksi dan melihat teknologi. Langkah-langkah yang diperlukan untuk memastikan literasi digital diperkukuh dan privasi dan keselamatan maklumat dipertingkatkan melalui program pembelajaran dan kesedaran.

Adalah penting bagi organisasi untuk mewujudkan rangka kerja yang teguh untuk melindungi aset maklumat mereka. Untuk membantu organisasi mengintegrasikan komponen keselamatan maklumat dengan cara yang akan mempengaruhi tingkah laku pekerja secara positif terhadap perlindungan aset maklumat, rangka kerja budaya keselamatan maklumat dibentangkan. Hasilnya, rangka kerja itu memberi hala tuju untuk memupuk budaya keselamatan maklumat yang menggalakkan tingkah laku keselamatan maklumat yang boleh diterima. Rangka kerja ini terdiri daripada elemen keselamatan maklumat, tingkah laku organisasi dan budaya. Rangka kerja ini boleh digunakan oleh pihak pengurusan sebagai strategi strategik untuk menyediakan kakitangan dengan hala tuju tentang cara mewujudkan budaya keselamatan maklumat. Pada asasnya, ini adalah budaya yang menggalakkan tingkah laku keselamatan maklumat yang sesuai untuk meminimumkan risiko dan yang membantu organisasi mencapai matlamatnya. Ia membentangkan set komprehensif komponen keselamatan maklumat yang mesti dinilai pada setiap peringkat tingkah laku keselamatan maklumat sebagai sebahagian daripada keseluruhan struktur budaya keselamatan maklumat.

Rujukan

Alhogail, A. (2015), “Design and validation of information security culture framework”, Computers in Human Behavior, Vol. 49, pp. 567-575, doi: 10.1016/j.chb.2015.03.054.

Van Niekerk, J.F. and Von Solms, R. (2010), “Information security culture: a management perspective”, Computers and Security, Vol. 29 No. 4, pp. 476-486, doi: 10.1016/j.cose.2009.10.005

PriceWaterhouseCoopers. The Global State of Infor- mation Security® Survey 2018. https://www.pwc.com/ us/en/services/consulting/cybersecurity/library/infor- mation- security-survey.html. Accessed October 2, 2019.

Thomson, K.L., Von Solms, R. and Louw, L. (2006), “Cultivating an organizational information security culture”, Computer Fraud and Security, Vol. 2006 No. 10, pp. 7-11

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. Information and Computer Security, 27(2), 146–164. https://doi.org/10.1108/ICS-12-2016- 0095

Cheng, L., Liu, F. and Yao, D. (2017), “Enterprise data breach: causes, challenges, prevention, and future directions”, Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, Vol. 7 No. 5, p. e1211, doi: 10.1002/widm.1211.

MyCert (2017), "2017 data breaches known so far", available at: www.mycert.org.my/data/ content_files/27/831.pdf (accessed 8 May 2020).

Schlienger T, Teufel S. Tool supportedmanagement ofinformation security culture. In: 20th IFIP international information security conference. Makuhari-Messe, Chiba, Japan; 2005.

Ramachandran, S., Rao, S.V. and Goles, T. (2008), "Information security cultures of four professions: a comparative study", Proceedings ofthe 41stHIInternational Conference on System Sciences.

Malcolmson (2009). What is Security Culture? Does it differ in content from general Organisational Culture? IEEE Cody Technology Park, Farnborough, Hants, 2009.

Alhogail, A. and Mirza, A. (2014b), "Information security culture: A definition and a literature review", Computer Applications and Information Systems, pp. 1-7.

Masrek, M. N. (2018). Assessing information security culture: The case of Malaysia public organization. 1–1. https://doi.org/10.1109/icitacee.2017.8257663

Ng, W. (2012). Can we teach digital natives digital literacy? Computers and Education, 59(3), 1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016

Burkell, J. A., Fortier, A., Di Valentino, L., & Roberts, S. (2015). Enhancing Key Digital Literacy Skills: Information Privacy, Information Security, and Copyright / Intellectual Property. FIMS Publications, 35, 67. Retrieved from https://works.bepress.com/jacquelyn.burkell/2/%0Ahttps://www.researchgate.net/publication/283551425_Enhancing_Key_Digital_Literacy_Skills_Information_Privacy_Information_Security_and_CopyrightIntellectual_Property

Majlis Keselamatan Negara(MKN). (n.d.). Retrieved September 18, 2022, from https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf

About the author Siti Aiysyah Tumin Siti Aiysyah Tumin is a researcher at Khazanah Research Institute, Siti Aiysyah Tumin Siti Aiysyah Tumin is a researcher at Khazanah Research Institute, Tumin, S. A., Siti Aiysyah Tumin is a researcher at Khazanah Research Institute, Posted In: COVID-19 and Southeast Asia, Says:, P., & *, N. (2020, November 23). Covid- 19 and work in Malaysia: How common is working from home? LSE Southeast Asia Blog. Retrieved January 5, 2022, from https://blogs.lse.ac.uk/seac/2020/11/23/covid-19-and-work- in-malaysia-how-common-is-working-from-home/
Economic Planning Unit. (n.d.). Retrieved September 18, 2022, from https://www.epu.gov.my/sites/default/files/2021-02/malaysia-digital-economy- blueprint_.pdf

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. Computers and Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Qjarterly Special Issue Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness1. Source: MIS Quarterly, 34(3), 39.

Singh, N., Gupta, A.M. and Ojha, A. (2014), "Identifying factors of organizational information security management'", Journal of Enterprise Information Management, Vol. 27 No. 5, pp. 644-667.

Tsohou, A., Karyda, M. and Kokolakis, S. (2015), "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs", Computers and Security, Vol. 52, pp. 128-141.

Thompson, N., McGill, T. J., & Wang, X. (2017). "security begins at home": Determinants of Home Computer and mobile device security behavior. Computers & Security, 70, 376–391. https://doi.org/10.1016/j.cose.2017.07.003

White, G. L. (2015). Education and prevention relationships on security incidents for the home computers. Journal Of Computer Information Systems, 55(3), 29-37. Retrieved from http://iacis.org/

White, G., Ekin, T., & Visinescu, L. (2016). Analysis of protective behavior and security incidents for home computers. Journal of Computer Information Systems, 57(4), 353–363. https://doi.org/10.1080/08874417.2016.1232991

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems, 28(2), 203–236. doi:10.2753/MIS0742-1222280208

Shropshire, J., Warkentin, M., & Shaema, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security, 49, 177– 191

Spears, J. & Barki, H. (2010). User Participation in Information Systems Security Risk Management, MIS Quarterly (34:3), pp 503-522

Bates, M. J., & Maack, M. N. (2010). Information Behavior. 3, pp. 2381-2391(3 rd ed.). Los Angeles: CRC Press. [Diakses melalui https://pages.gseis.ucla.edu/faculty/bates/articles/information-behavior.html], 7 Juli 2017

Martins, A. and Eloff, J. (2002), "Assessing Information Security Culture", Information for Security for South-Africa 2nd Annual Conference, pp1–14.

Hellriegel D, Slocum .Jr JW, WoodmanRW. Organizational behavior. Eighth edition. South- Western College Publishing; 1998.