https://doi.org/10.17576/apjitm-2021-1001-08
Asia-Pacific Journal of Information Technology and Multimedia
Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik
Vol. 10 No. 8, June 2021: 86 - 99
e-ISSN: 2289-2192

Received: 26 October 2020
Accepted: 27 May 2021
Published: 1 June 2021

CIVIL SERVANTS AWARENESS GUIDELINE TOWARDS COMPUTER SECURITY POLICY: A CASE STUDY AT THE MANPOWER DEPARTMENT, MINISTRY OF HUMAN RESOURCES

YUSMAWATI MUHD YUSOF
DALBIR SINGH

ABSTRACT

ICT Security Policy includes information security-related policies, guidelines and best practices that are enforced in the Malaysian public sector. These policies are priority areas that contain guidelines for implementing ICT infrastructure in the public sector. However, there is a significant gap between these policies and awareness towards computer security policy among government servants in the public sector. Therefore a study involving government servants in the Manpower Department, Ministry of Human Resources was carried out to identify the critical success factor of these policies. The study was conducted through quantitative and qualitative methods. A survey was conducted to measure the level of awareness among government servants in agencies against computer security policies. Flaw factors in computer security policy implementation were discussed to obtain strategies to ensure the successful implementation of computer security policies in an agency. The significant factors leading to a successful implementation of computer security policy at the governmental agencies were validated by experts. As a result, a guideline has been prepared to be applied as an improvement proposal to increase the awareness of government servants on ICT security policy in the agencies.

Keywords: Security policy; public sector; awareness; guidelines.

GARIS PANDUAN KESEDARAN PENJAWAT AWAM TERHADAP DASAR KESELAMATAN KOMPUTER: KAJIAN KES DI JABATAN TENAGA MANUSIA, KEMENTERIAN SUMBER MANUSIA

ABSTRAK

Dasar Keselamatan ICT (DKICT) adalah dasar, garis panduan dan amalan terbaik yang berkaitan keselamatan komputer yang dikuatkuasakan di sektor awam Malaysia. Dasar ini mempunyai bidang keutamaan yang mengandungi garis panduan dalam melaksanakan infrastuktur ICT di sektor awam. Namun, terdapat jurang yang ketara di antara dasar dan kesedaran terhadap dasar keselamatan komputer ini di kalangan penjawat awam di sektor awam. Sehubungan dengan itu, suatu kajian melibatkan penjawat awam di Jabatan Tenaga Manusia, Kementerian Sumber Manusia telah dilaksanakan untuk mengenal pasti faktor kejayaan kritikal bagi pelaksanaan dasar tersebut. Kajian dilakukan melalui kaedah kuantitatif dan kualitatif. Kaji selidik telah dilaksanakan bagi mengukur tahap kesedaran penjawat awam di agensi terhadap pelaksanaan dan penguatkuasaan dasar keselamatan komputer. Faktor-faktor kelemahan dalam pelaksanaan dasar keselamatan komputer di agensi dibincangkan untuk mendapatkan strategi bagi menentukan kejayaan pelaksanaan keselamatan komputer di agensi. Seterusnya faktor-faktor signifikan yang membawa kepada kejayaan pelaksanaan dasar keselamatan komputer di agensi kerajaan telah disahkan oleh pakar. Hasilnya, satu garis panduan telah disediakan untuk diaplikasikan sebagai cadangan penambahbaikan untuk meningkatkan kesedaran penjawat awam terhadap dasar keselamatan ICT di agensi.

Kata kunci: Dasar keselamatan; sektor awam; kesedaran; garis panduan.

PENGENALAN

Penggunaan komputer dan teknologi dalam sektor awam semakin berkembang selaras dengan hasrat kerajaan untuk meningkatkan kecekapan dan keberkesanan penyampaian perkhidmatan kepada warga Malaysia. Kerajaan dari masa ke semasa mengukuhkan prasarana dan infrastruktur teknologi maklumat dan komunikasi (ICT) di sektor awam untuk melancarkan urusan pentadbiran dan pengurusan. Fungsi pemodenan pentadbiran ini dipertanggungjawabkan kepada sebuah agensi yang dikenali sebagai Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU). Di MAMPU, Bahagian Transformasi Dasar berfungsi untuk merancang dan menetapkan hala tuju strategik makro bagi transformasi pemodenan pengurusan dan dasar keselamatan komputer sektor awam selaras dengan dasar semasa kerajaan (Malaysia, 2015).

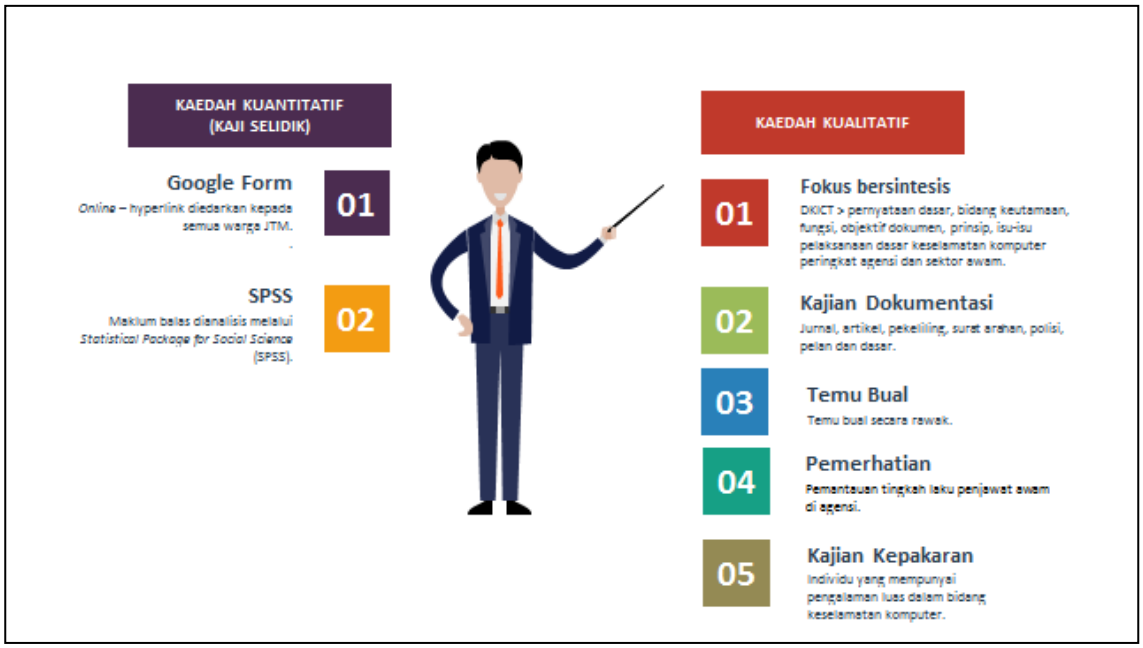
Bagi memenuhi transformasi dan pembudayaan ICT ini, MAMPU juga telah menggariskan Dasar Keselamatan ICT (DKICT) sebagai dasar bagi memastikan keselamatan maklumat dan aset ICT kerajaan terjamin kerahsiaannya, berintegriti dan tidak boleh disangkal (Malaysia, 2015). DKICT ini turut dikuatkuasakan di semua agensi sektor awam. Dasar keselamatan ICT adalah panduan kepada organisasi berkenaan keselamatan ICT (Shamsul Kamal et al., 2012). Penjawat awam sebagai pelaksana dan pengguna akhir kepada infrastruktur ICT yang disediakan perlu mematuhi dasar keselamatan komputer ini.

Namun demikian, pematuhan dan pemakaian dasar keselamatan komputer di kalangan penjawat awam adalah tidak menyeluruh di agensi kerajaan. Terdapat jurang yang ketara di antara dasar dan kesedaran keselamatan komputer di kalangan penjawat awam di mana 60% daripada agensi kerajaan tidak mematuhi sepenuhnya dasar, pekeliling dan garis panduan keselamatan komputer yang dikeluarkan oleh kerajaan (Ilyana et al., 2015). Pekara ini juga telah disahkan melalui soal selidik yang melibatkan penjawat awam di Jabatan Tenaga Manusia, Kementerian Sumber Manusia sebagai kajian kes dan pengesahan pakar.

Sehubungan dengan itu, perluasan kesedaran terhadap dasar keselamatan komputer melalui program kesedaran perlu dilakukan untuk mengelakkan berlakunya kompromi terhadap keselamatan komputer (Hasmanizam et al., 2015). Oleh yang demikian, kajian terhadap keselamatan komputer dari aspek tahap kesedaran penjawat awam di agensi telah dijalankan dan seterusnya mengesyorkan garis panduan yang perlu dibangunkan untuk meningkatkan kesedaran tersebut (Amri & Zawiyah 2018).

KAEDAH KAJIAN

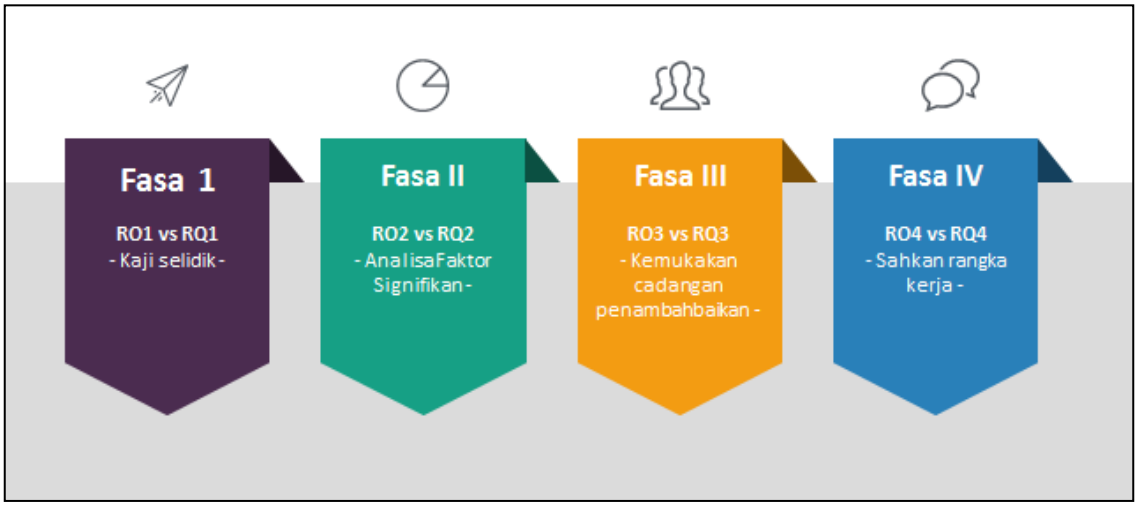
Kajian ini menggunakan metodologi kuantitatif dan kualitatif yang mengambil kira gabungan kelebihan dan kelemahan bagi setiap pendekatan yang diguna pakai (Kothari, 2007). Bagi metodologi kuantitatif, kaji selidik menggunakan instrumen iaitu Employee Security Awareness Survey (Trenton Bond, 2012) telah dilaksanakan di Jabatan Tenaga Manusia (JTM), Kementerian Sumber Manusia (KSM). Ianya dipilih kerana pilihan jawapan pada setiap soalan telah ditetapkan markah risiko. Pilihan jawapan oleh responden menunjukkan tahap kesedaran terhadap keselamatan komputer dalam situasi tertentu. Seterusnya metodologi kualitatif dilaksanakan melalui kaedah kajian kepustakaan dan kajian kepakaran. Pendekatan ini memberikan maklumat yang lebih mendalam melalui pengalaman dan pandangan individu yang terlibat dalam kajian kes ini (Turner, 2010). Ianya menghasilkan keputusan yang tidak menjurus kepada sesuatu perkara berbanding metodologi kuantitatif yang dikawal dan terhad. Rajah 1 menunjukkan metodologi kajian yang digunakan.



RAJAH 1: Metodologi kajian.

FASA KAJIAN

Fasa kajian bertujuan menerangkan aktiviti yang dilakukan untuk mencapai objektif yang disasarkan dengan menggunakan metodologi secara kualitatif berdasarkan fokus bersintesis, kajian dokumentasi, pemerhatian, temu bual dan kajian kepakaran. Fasa yang seterusnya dalam kajian ini akan menerangkan lebih lanjut berkenaan pengumpulan data. Rajah 2 menunjukkan fasa metodologi kajian.



RAJAH 2: Fasa Metolodologi Kajian

FASA I

Dalam fasa ini, kaji selidik dilaksanakan untuk mencapai objektif kajian yang pertama iaitu mengukur tahap kesedaran penjawat awam terhadap keselamatan komputer di agensi. Soalan kaji selidik diedarkan kepada penjawat awam di agensi melalui e-mel yang mengandungi pautan google form. Soalan kaji selidik diadaptasi daripada Employee Security Awareness

Survey (Trenton Bond, 2012). Analisa kajian ini disokong oleh perisian SPSS untuk mendapatkan purata markah risiko.

Maklum balas yang diperolehi daripada responden dikumpul dan dianalisa untuk mendapatkan markah risiko. Untuk mendapatkan markah risiko, sebanyak empat (4) langkah pengiraan dilakukan. Kemudian analisis demografik responden dilakukan sebagai latar belakang kaji selidik. Pengkelasan soalan kaji selidik kepada faktor manusia, teknikal dan pengurusan dilakukan untuk mendapatkan markah risiko bagi setiap faktor dan seterusnya analisa faktor penentu kesedaran keselamatan komputer untuk mengenal pasti faktor yang signifikan terhadap kesedaran keselamatan komputer.

FASA II

Objektif kajian yang kedua iaitu mengkaji faktor kelemahan dan kejayaan pelaksanaan dasar keselamatan komputer pada Fasa II. Objektif ini dicapai melalui kaedah fokus bersentesis, kajian dokumentasi, pemerhatian dan temu bual. Kajian terhadap DKICT KSM dilakukan untuk mendapatkan maklumat dan peraturan yang terkandung di dalamnya. Kajian literatur dijalankan untuk mengenal pasti faktor signifikan kepada pelaksanaan dasar keselamatan komputer di agensi. Hasil daripada kajian di fasa ini, garis panduan kesedaran penjawat awam terhadap dasar keselamatan komputer dihasilkan.

FASA III

Dalam Fasa III, objektif kajian yang ketiga dicapai dengan mengemukakan garis panduan kesedaran penjawat awam terhadap pelaksanaan dasar keselamatan komputer sedia ada. Faktor kelemahan dan kejayaan pelaksanaan dasar keselamatan komputer di agensi menghasilkan garis panduan kesedaran keselamatan komputer. Garis panduan ini dibentangkan kepada dua (2) orang pegawai di KSM dan JTM secara berasingan. Cadangan penambahbaikan diklasifikasikan mengikut faktor. Cadangan yang terkandung dalam pengkelasan faktor ini adalah berdasarkan keperluan bagi meningkatkan kesedaran penjawat awam terhadap dasar keselamatan komputer. Sebanyak lapan (8) langkah di bawah faktor manusia, empat (4) langkah di bawah faktor pengurusan dan tiga (3) langkah dicadangkan di bawah faktor teknikal.

FASA IV

Pada fasa ini, objektif kajian keempat dicapai dengan mengesahkan cadangan garis panduan pelaksanaan keselamatan komputer di kalangan penjawat awam. Cadangan garis panduan di Fasa III dibentangkan dalam kajian kepakaran yang dijadualkan. Borang penilaian disediakan untuk disahkan oleh responden. Persoalan kajian sama ada rangka kerja yang dicadangkan diterima dan ditambah baik oleh pakar yang terlibat dalam kajian dan pandangan pakar terhadap langkah pelaksanaan yang dicadangkan akan dimasukkan dalam hasil akhir kajian.

ANALISIS KAJIAN

Objektif dan persoalan kajian dicapai mengikut fasa demi fasa berdasarkan metodologi kajian yang dinyatakan. Hasil utama kajian ini adalah garis panduan kesedaran penjawat awam terhadap dasar keselamatan komputer yang sedang berkuat kuasa melalui kajian kepakaran.

FASA I

Untuk mengukur tahap kesedaran penjawat awam terhadap keselamatan komputer di agensi, objektif ini dicapai melalui kaji selidik yang dijalankan di agensi. Seramai 70 orang responden telah memberikan maklum balas.

BAHAGIAN 1: PENGIRAAN MARKAH RISIKO

JADUAL 1: Skala pengukuran tahap risiko yang disediakan di dalam instrumen.

Markah risiko	**1**	**2**	**3**	**4**	**5**
Tahap risiko	Sangat rendah	Rendah	Sederhana	Tinggi	Sangat tinggi

Jawapan bagi soalan 6 hingga 29 dalam instrumen telah ditetapkan markah risikonya untuk mengukur tahap risiko.

i. Langkah 1: setiap maklum balas daripada responden bagi soalan 6 hingga 29 dilakukan operasi darab dengan tahap risiko 1 hingga 5 seperti berikut:

<tahap risiko>×<kekerapan maklum balas>=<jumlah nilai risiko>

ii. Langkah 2: Jumlah risiko yang diperolehi daripada soalan 6 hingga 29 ditambah untuk mendapatkan jumlah nilai risiko terkumpul.

Jumlah Nilai Risiko Terkumpul bagi Soalan 6 hingga Soalan 29 adalah 3,789.

iii. Langkah 3: Jumlah nilai risiko terkumpul dibahagi dengan jumlah responden untuk mendapatkan markah risiko.

<jumlah nilai risiko terkumpul>	÷	<jumlah kekerapan maklum balas>	=	Markah risiko
3,789	÷	70	=	54.13

iv. Langkah 4: Markah risiko yang diperolehi daripada pengiraan di atas dibandingkan menggunakan "Jadual Peringkat Risiko" untuk mendapatkan tahap risiko seperti di Jadual 2.

JADUAL 2: Jadual Peringkat Risiko

Peringkat Risiko	**Penerangan**
Sangat Rendah (25 - 39)	Pekerja menyedari akan prinsip-prinsip keselamatan yang baik dan sesuatu ancaman, telah diberi latihan sewajarnya, dan mematuhi semua piawaian dan dasar keselamatan organisasi.
Rendah (40 - 60)	Pekerja telah dilatih berkenaan piawaian dan dasar keselamatan organisasi, mereka sedar akan sesuatu ancaman, tetapi mungkin tidak mengikuti prinsip-prinsip dan kawalan keselamatan yang baik.
Sederhana (61 - 81)	Pekerja menyedari akan sesuatu ancaman dan perlu mengikut prinsip-prinsip dan kawalan keselamatan yang baik, tetapi memerlukan latihan berkenaan piawaian dan dasar keselamatan organisasi. Mereka juga mungkin tidak tahu bagaimana untuk mengenal pasti atau melaporkan sesuatu insiden keselamatan.
Tinggi (82 - 96)	Pekerja tidak menyedari akan sesuatu ancaman atau prinsip-prinsip keselamatan yang baik serta pematuhan terhadap piawaian dan dasar keselamatan organisasi.
Sangat Tingi (97 - 110)	Pekerja tidak menyedari sesuatu ancaman serta mengabaikan polisi dan piawaian keselamatan atau tidak mematuhi peraturan. Mereka melakukan perkara atau amalan yang mudah mendatangkan ancaman serta eksploitasi.

Objektif kajian di Fasa I diperolehi dengan nilai purata markah risiko 54.13. Tahap risiko keselamatan komputer adalah Rendah menunjukkan penjawat awam di agensi adalah pekerja yang

terlatih dari segi piawaian dan dasar keselamatan organisasi, mereka sedar akan sesuatu ancaman, tetapi mungkin tidak mengikuti prinsip-prinsip dan kawalan keselamatan yang baik. Sehubungan dengan itu, garis panduan bagi meningkatkan kesedaran terhadap pelaksanaan penguatkuasaan dasar keselamatan komputer di organisasi perlu diwujudkan. Ini adalah bagi memastikan keselamatan aset ICT di agensi terpelihara daripada ancaman sama ada dari luar atau melalui tingkah laku penjawat awam itu sendiri.

BAHAGIAN 2: ANALISIS DEMOGRAFIK RESPONDEN

Soalan berkaitan jantina, pengalaman dalam perkhidmatan awam, kategori kumpulan perkhidmatan, kelulusan akademik dan tahap penguasaan dalam bidang ICT dianalisis seperti berikut:

1. Sebanyak 57.14% atau 40 orang responden adalah perempuan manakala 42.86% atau 30 orang responden adalah lelaki.
2. Seramai 10 responden atau 14.29% mempunyai pengalaman kurang daripada 5 tahun, 27 orang atau 38.57% responden mempunyai pengalaman antara 6 hingga 10 tahun, seramai 16 orang responden atau 22.86% mempunyai pengalaman antara 11 hingga 15 tahun, seramai enam (6) orang responden atau 8.57% mempunyai pengalaman antara 16 hingga 20 tahun dan 11 orang atau 15.71% orang responden mempunyai pengalaman lebih daripada 20 tahun.
3. pegawai atau 17.14% adalah daripada kumpulan Pengurusan dan Profesional dan seramai enam (6) orang pegawai atau 8.57% orang pegawai daripada kumpulan Pengurusan Atasan memberikan maklum balas.
4. Majoriti responden di agensi iaitu seramai 27 orang atau 38.57% mempunyai kelayakan Diploma/STPM/STP/STAM, seramai 19 orang atau 27.14% berkelulusan SPM/SPMV/Sijil, seramai 12 orang atau 17.14% berkelulusan Ijazah, seramai 11 orang atau 15.71% berkelulusan Sarjana/Master dan satu (1) orang atau 1.43% berkelulusan PhD.
5. Berdasarkan maklum balas responden, tiada responden memilih skala 1 atau 0%, seorang (1) orang memilih skala 2 atau 1.43%, dua (2) orang memilih skala 3 atau 2.86%, lapan (8) orang memilih skala 4 atau 11.43%, 16 orang memilih skala 5 atau 22.86%, 11 orang memilih skala 6 atau 15.71%, 12 orang memilih skala 7 atau 17.14%, 12 orang memilih skala 8 atau 17.14%, 6 orang memilih skala 9 atau 8.57% dan 2 orang memilih skala 10 atau 2.86%.

BAHAGIAN 3: ANALISIS RISIKO TERHADAP SOALAN MENGIKUT KATEGORI FAKTOR. SOALAN 6 HINGGA 29 TELAH DIKATEGORIKAN KEPADA FAKTOR MANUSIA, PENGURUSAN DAN TEKNIKAL.

Soalan 6 hingga 29 telah dikategorikan kepada faktor manusia, pengurusan dan teknikal iaitu Faktor Manusia (16 soalan), Pengurusan (5 soalan) dan Teknikal (3) soalan. Maklum balas yang diterima daripada responden dimasukkan ke dalam SPSS untuk mendapatkan nilai *mean* bagi setiap faktor yang terlibat. Nilai *mean* yang diperoleh akan dibandingkan dengan Jadual 1. Keputusan adalah seperti di Jadual 3.

Faktor yang paling signifikan adalah faktor manusia dengan purata markah risiko paling tinggi iaitu 2.37, manakala faktor teknikal merupakan faktor kedua tertinggi iaitu 2.30 dan faktor pengurusan iaitu 1.87. Faktor manusia dengan skala 2.37 menunjukkan risiko yang paling tinggi dan sekali gus menunjukkan tahap kesedaran yang paling rendah di antara ketiga-tiga faktor yang terlibat.

JADUAL 3: Analisa penentu faktor kesedaran

Faktor	Purata Markah Risiko
Manusia	2.37
Teknikal	2.30
Pengurusan	1.87

FASA II

Faktor-faktor signifikan yang membawa kepada kelemahan pelaksanaan DKICT ini dikaji untuk mengenal pasti cadangan penambahbaikan. Antara kelemahan yang terdapat pada faktor manusia seperti dari aspek salah laku penjawat awam dalam penggunaan infrastruktur ICT yang disediakan, kelemahan pada faktor teknikal dari aspek pelaksanaan sekuriti serta kelemahan faktor pengurusan dari aspek penyampaian DKICT kepada penjawat awam di KSM.

Selain daripada faktor-faktor di atas, peruntukan kewangan dan sokongan pihak pengurusan atasan turut memainkan peranan kepada kejayaan DKICT di agensi. Pembiayaan dan sokongan pihak pengurusan atasan yang berterusan seperti peruntukan kewangan bagi mempromosikan DKICT, penganjuran kursus serta penglibatan pengurusan atasan dalam penguatkuasaan, penubuhan pasukan khas keselamatan komputer dengan sumber tenaga yang mencukupi dan melaksanakan pengkhususan dalam bidang keselamatan komputer adalah pemangkin kepada kejayaan pelaksanaan DKICT.

FASA III

Cadangan penambahbaikan terhadap pelaksanaan kesedaran penjawat awam terhadap garis panduan dasar keselamatan komputer adalah seperti model yang dipaparkan seperti Rajah 3.

RAJAH 3: Model cadangan penambahbaikan DKICT

01. Faktor Manusia - Pembangunan Modal Insan

Pembangunan modal insan adalah elemen yang perlu diberi keutamaan. Bagi mencapai hasrat tersebut, beberapa tindakan perlu diambil bagi meningkatkan kesedaran penjawat awam terhadap pelaksanaan garis panduan keselamatan komputer yang sedang berkuat kuasa.

(a) Program Kesedaran Garis Panduan Keselamatan Komputer

Program kesedaran keselamatan komputer yang berkesan daripada penyampaian bahan atau isi kandungan yang relevan pada masa yang tepat dan cekap adalah sangat penting. Program ini perlu dilaksanakan secara berkala dan wajib dihadiri oleh setiap penjawat awam. Antara aktiviti yang boleh dilakukan adalah seperti berikut:-

i. Video Pendek Dasar Keselamatan Komputer

Paparan secara audio visual lebih berkesan kerana dapat menarik perhatian penjawat awam untuk lebih memahami dan berfikir secara lebih spesifik tentang mesej yang disampaikan. Video berdurasi kurang dari 3 minit yang mempunyai maklumat mengenai polisi keselamatan komputer yang sedang berkuatkuasa dapat memperkukuhkan pemahaman dan mengubah pemikiran penjawat awam terhadap dasar keselamatan komputer.

ii. Poster Dasar Keselamatan Komputer

Poster yang mempunyai pemberitahuan mengenai penguatkuasaan dasar keselamatan komputer kepada semua penjawat awam. Poster ditampal di ruangan papan kenyataan atau di ruangan yang kerap dikunjungi oleh pekerja seperti di kawasan lobi, pantri, bilik cetakan dan sebagainya.

iii. Infografik Dasar Keselamatan Komputer

Kempen pelaksanaan dasar keselamatan komputer yang memaparkan lebih banyak grafik yang menarik berbanding teks. Untuk memaparkan bahan berkenaan dasar keselamatan komputer dan informasi penting yang terkandung di dalamnya. Maklumat yang banyak lebih efektif ditampilkan dalam bentuk grafik.

iv. Kursus

Kursus yang memberi pendedahan dan pengukuhan terhadap Dasar Keselamatan ICT kepada penjawat awam, ancaman keselamatan dalam penggunaan kemudahan ICT yang disediakan oleh agensi. Kursus ini mempunyai peperiksaan atau penilaian. Kehadiran adalah diwajibkan oleh setiap penjawat awam dan dijalankan sebagai program tahunan.

v. Screensavers

Garis panduan DKICT dan kempen keselamatan komputer yang ringkas dijadikan screensavers di komputer yang digunakan oleh penjawat awam di organisasi.

vi. Buletin/Emel/Risalah Dasar Keselamatan Komputer

Maklumat berkenaan dasar keselamatan komputer yang berkuatkuasa didokumentasikan dalam bentuk buletin/emel/risalah untuk tujuan publisiti, promosi, diedar dan dijadikan bahan rujukan seperti kempen Sedar ICT.

(b) Pemantapan Penjawat Awam Terhadap Kesedaran Keselamatan Komputer

Pendedahan kepada penjawat awam yang baharu dilantik ke dalam perkhidmatan awam berkenaan dasar keselamatan komputer yang sedang berkuatkuasa dan kesedaran keselamatan komputer. Dasar keselamatan komputer dijadikan sebagai silibus atau subjek semasa minggu orientasi penjawat awam.

Pendedahan penjawat awam yang masih baru dalam perkhidmatan menerapkan pengukuhan, disiplin, motivasi dan kepatuhan kepada dasar keselamatan komputer di samping dapat mengurangkan risiko terhadap keselamatan komputer itu sendiri.

(c) Pelaksanaan Aku Janji dan Ikrar

Pihak pengurusan perlu mewajibkan penjawat awam untuk menandatangani surat aku janji sebagai keakuran dan pematuhan kepada dasar keselamatan komputer yang sedang berkuatkuasa. Kaedah ini dapat memupuk etika dalam penggunaan infrastruktur ICT di agensi. Kegagalan penjawat awam mematuhi surat aku janji ini boleh dikenakan tindakan tatatertib. Ianya boleh mengatasi masalah kebocoran maklumat atau sebarang risiko terhadap keselamatan komputer di agensi.

02. Faktor Pengurusan – Tadbir Urus

Untuk menyokong usaha ini, struktur tadbir urus perlu diperkemaskan dengan mewujudkan jawatan, fungsi dan akauntabiliti yang lebih kukuh dalam mengurus, memastikan keselamatan dan memanfaatkan aset kerajaan.

(a) Mewujudkan pasukan kesedaran keselamatan komputer

Pasukan ini bertindak untuk merancang perancangan strategik, program kesedaran, kajian pengurusan, pengurusan dasar dan prosedur keselamatan komputer. Pengkhususan tanggungjawab dapat memantapkan pelaksanaan dasar keselamatan komputer di agensi. Bilangan dan keahlian bagi pasukan keselamatan ini adalah bergantung kepada keperluan sesuatu organisasi dan tingkah laku sosialnya (budaya) dan perlu diketuai oleh Pegawai Teknologi Maklumat Gred F44 atau F48.

(b) Menetapkan tahap kesedaran keselamatan berasaskan bidang tugas

Penetapan tahap kesedaran keselamatan berdasarkan bidang tugas membolehkan agensi merancang latihan yang sesuai kepada penjawat awam mengikut tahap tanggungjawab dan peranan di agensi.

Penetapan tahap kesedaran keselamatan berdasarkan bidang tugas membolehkan agensi merancang latihan yang sesuai kepada personel mengikut tahap tanggungjawab dan peranan di agensi. Setiap personel perlu menghadiri program kesedaran keselamatan sebelum mengakses sistem dan menghadiri program tersebut secara berkala setiap tahun. Lima (5) peringkat jawatan tertentu perlu menjalani latihan kesedaran iaitu:-

i. Semua pengguna – Asas kepada dasar keselamatan komputer.
ii. Pegawai, Eksekutif – Asas kepada dasar keselamatan komputer dan pengurusan keselamatan aplikasi.
iii. Ketua Penolong Pengarah, Pengurus – Asas kepada dasar keselamatan komputer, kursus peringkat pelaksanaan dan pengurusan keselamatan, kursus untuk membangunkan pelan tindakan dan pengurusan keselamatan komputer, pengurusan keselamatan aplikasi, pengurusan kitaran hayat sistem/aplikasi dan pengurusan risiko dan perancangan luar jangka.

iv. Ketua Jabatan, CIO, Juruaudit – Asas kepada dasar keselamatan komputer, kursus peringkat pelaksanaan dan pengurusan keselamatan yang lebih luas, kursus untuk membangunkan pelan tindakan dan pengurusan keselamatan komputer, pengurusan keselamatan aplikasi, pengurusan kitaran hayat sistem/ aplikasi, pengurusan risiko dan perancangan luar jangka dan kursus analisis keperluan keselamatan komputer.

v. Bahagian Pengurusan Maklumat dan Pegawai Teknologi Maklumat – Asas kepada dasar keselamatan komputer, kursus peringkat pelaksanaan dan pengurusan keselamatan, kursus untuk membangunkan pelan tindakan dan pengurusan keselamatan komputer, pengurusan keselamatan aplikasi, pengurusan kitaran hayat sistem/aplikasi, pengurusan risiko dan perancangan luar jangka dan kursus analisis keperluan keselamatan komputer.

(c) Arahan Dalaman

Pekeliling dalaman yang mengandungi arahan dari pihak yang berkuasa seperti Ketua Setiausaha Kementerian, Timbalan Ketua Setiausaha (Operasi), Setiausaha Bahagian Pengurusan Maklumat atau Ketua Jabatan berkenaan pematuhan dasar keselamatan komputer. Pematuhan dasar keselamatan komputer perlu diedarkan kepada penjawat awam sebagai perkara yang perlu dipraktikkan secara serius dan tiada kompromi. Arahan yang dikeluarkan oleh pegawai pengurusan tertinggi kementerian akan lebih diberi perhatian oleh penjawat awam di agensi.

Penjawat awam perlu diingatkan bahawa setiap infrastruktur ICT yang disediakan digunakan dengan tanggungjawab, cekap, beretika dan mereka adalah tertakluk kepada undang-undang dan peraturan yang sedang berkuat kuasa. Sebarang percubaan untuk menggodam komputer atau perkakasan milik kerajaan dianggap sebagai perbuatan salah laku dan akan dikenakan tindakan disiplin.

Penjawat awam juga diingatkan untuk melaporkan sebarang kegagalan pada perkakasan dan perisian dengan kadar segera, melaporkan penyalahgunaan, apa-apa kerosakan dengan dokumen, tidak memasang perisian yang tidak berlesen dan sebagainya.

(d) Pemantauan Prestasi Pekerja

Menjadikan tahap kesedaran komputer sebagai sebahagian daripada proses kajian semula kepada setiap personel untuk mengenalpasti latihan dan kursus yang diperlukan. Penilaian terhadap tahap pematuhan boleh dilakukan melalui soalan kaji selidik yang diedarkan kepada penjawat awam. Analisis keperluan boleh dirancang melalui maklum balas kaji selidik yang dikemukakan oleh penjawat awam yang terlibat.

03. Faktor Teknikal

Faktor teknikal adalah perkara yang tidak boleh diabaikan. Dalam usaha untuk meningkatkan kesedaran penjawat awam terhadap penguatkuasaan dasar keselamatan komputer sedia ada, tindakan yang perlu diambil adalah sepert berikut:-

(a) Prosedur Operasi Standard

Melaksanakan prosedur operasi standard (S.O.P) di setiap ruang kerja, perkakasan terutamanya komputer penjawat awam untuk memberi peringatan pematuhan kepada keselamatan komputer dan dasar keselamatan yang sedang berkuat kuasa. S.O.P ini ditampal pada setiap mesin yang dikendalikan oleh personel.

(b) *Handbook* Dasar Keselamatan Komputer

Dokumen DKICT diringkaskan kepada buku panduan atau *handbook* dasar keselamatan komputer yang padat dan mudah untuk digunakan dan lebih praktikal. Buku panduan ini wajib diedarkan kepada setiap penjawat awam di agensi. Melalui kaedah ini, penjawat awam boleh mengakses maklumat berkenaan dasar keselamatan komputer pada bila-bila masa. Dengan itu juga, tiada penafian boleh dilakukan oleh pegawai berkenaan pelaksanaan dasar keselamatan komputer di agensi.

(c) Penetapan *Interactive Logon* dan *Screensavers*

Makluman melalui *interactive logon* iaitu *welcome message* sebelum pengguna menggunakan komputer dan *screensavers* untuk memberi peringatan kepada personel bahawa mereka adalah terikat dengan dasar keselamatan komputer yang sedang berkuat kuasa. Ia boleh dipraktikkan sebagai salah satu cara penguatkuasaan. Arahan dan maklumat ringkas yang bersesuaian berkenaan dasar keselamatan yang dipaparkan secara individu di stesen kerja masing-masing akan meningkatkan kesedaran penjawat awam terhadap pelaksanaan dasar keselamatan komputer yang sedang berkuatkuasa. Agensi digalakkan untuk menggunakan *screensavers* untuk memberi peringatan kepada pekerja untuk log keluar apabila meninggalkan stesen kerja atau untuk memaparkan maklumat keselamatan komputer yang penting.

Cadangan penambahbaikan di Fasa III adalah hasil daripada penemuan dalam fasa II iaitu faktor kejayaan dan kelemahan pelaksanaan dasar keselamatan komputer di agensi. Ia menunjukkan bahawa kesedaran penjawat awam yang rendah perlu di atasi melalui tiga (3) faktor signifikan iaitu faktor manusia, faktor teknikal dan faktor pengurusan.

FASA IV

Dalam fasa ini objektif kajian yang keempat dicapai iaitu mengesahkan garis panduan yang dicadangkan. Responden adalah Setiausaha Bahagian Pengurusan Maklumat dan Ketua Pegawai Maklumat di peringkat Jabatan. Selain daripada itu, responden ini dipilih berdasarkan pengalaman kerja dan penglibatan mereka dalam bidang keselamatan komputer.

Jadual 4 menunjukkan ulasan responden terhadap garis panduan yang dicadangkan bagi meningkatkan kesedaran penjawat awam terhadap pelaksanaan dasar keselamatan komputer. Berdasarkan pembentangan tersebut, responden memberikan maklum balas yang positif dan cadangan garis panduan tersebut disahkan dengan penambahbaikan seperti dinyatakan dalam Jadual 4.

JADUAL 4: Ulasan responden terhadap cadangan penyelidik

Cadangan Oleh Penyelidik	
Ulasan CIO JTM	**Ulasan SUB BPM**
Faktor Manusia – Pembangunan Modal Insan	
▪ Video diselaraskan di peringkat Kementerian. ▪ Peringatan perlu dilakukan secara langsung kepada individu. ▪ Infografik dan poster digabungkan. ▪ Edaran maklumat dalam bentuk digital untuk kurangkan kos dan meluaskan edaran. ▪ Pemantauan prestasi dicadangkan dilakukan melalui *usage/ network monitoring tools* untuk melihat kelakuan penjawat awam di internet.	▪ Pendedahan dasar keselamatan komputer kepada penjawat awam lantikan baharu diselaraskan di peringkat Agensi Pusat. ▪ Aku janji diselaraskan di peringkat agensi Pusat.

Faktor Pengurusan – Tadbir Urus	
▪ Nama pasukan dicadangkan Pasukan Khas Keselamatan Siber, diwujudkan di peringkat Kementerian.	▪ Kursus tahap kesedaran keselamatan berdasarkan bidang tugas diwajibkan kepada semua kumpulan perkhidmatan. Dijadikan syarat kelayakan kenaikan pangkat dan diselaraskan di Agensi Pusat.
Faktor Teknikal	
▪ Pendekatan *Safe Operating Procedure* dan *Standard Operating Procedure* diterapkan bersama.	▪ Tiada komen dan diterima.

Jadual 5 menunjukkan lain-lain cadangan dan rumusan responden terhadap cadangan penyelidik dalam meningkatkan kesedaran penjawat awam terhadap pelaksanaan dasar keselamatan komputer.

JADUAL 5: Lain-lain cadangan dan rumusan responden

Cadangan Oleh Responden	
Ulasan CIO JTM	**Ulasan SUB BPM**
▪ Paparan *pop-up message* di laman web Kementerian/Jabatan bagi memaklumkan makluman terkini berkenaan keselamatan komputer. ▪ Salah laku penjawat awam yang bertentangan dengan DKICT disenaraikan. ▪ Risiko akibat salah laku dan bentuk ancaman disenaraikan.	▪ Apakah bentuk hukuman atau tindakan tatatertib yang perlu dikenakan kepada penjawat awam yang melakukan perbuatan yang menyalahi dasar keselamatan komputer yang sedang berkuatkuasa.
Rumusan Oleh Responden	
▪ Responden yakin langkah-langkah yang dicadangkan oleh penyelidik dapat dilaksanakan dengan jaya dan efektif.	▪ Responden bersetuju dengan langkah-langkah yang dicadangkan oleh penyelidik. Langkah-langkah yang dicadangkan perlu diangkat ke peringkat agensi pusat bagi memperkukuhkan pelaksanaan dasar keselamatan komputer yang sedang berkuatkuasa.

Dalam fasa ini, cadangan yang dikemukakan oleh penyelidik untuk Faktor Manusia – Pembangunan Modal Insan, Faktor Pengurusan – Tadbir Urus dan Faktor Teknikal diterima dengan cadangan penambahbaikan dan pengukuhan daripada kajian kepakaran yang dilakukan. Strategi ini akan memacu kepada perubahan dalam meningkatkan kesedaran penjawat awam terhadap dasar keselamatan komputer di agensi.

Sebagai perbincangan berdasarkan hasil kajian, matlamat, objektif, dasar dan strategi pembangunan negara harus selari dengan dasar keselamatan komputer agar boleh memberikan kesan yang signifikan kepada negara, (Nepal, 2015; Federated States of Micronesia, 2010). Pelaksanaan dasar keselamatan komputer memerlukan usaha bersepadu daripada semua pihak yang terlibat terutamanya mereka yang dikenalpasti dalam dasar (Republic of Malawi, 2013). Selain daripada itu, pelaksanaan dasar keselamatan negara juga boleh dipengaruhi oleh tahap literasi dan kesedaran penjawat awam yang rendah terhadap dasar tersebut, selain penggantungan kepada sumber luar dan agihan peruntukan berdasarkan keutamaan. Menurut UK Government ICT Strategy (United Kingdom, 2011), kesinambungan daripada aspek kepimpinan dan akauntabiliti adalah faktor kritikal bagi kejayaan sesuatu projek ICT. Peningkatan dalam penyeragaman pelaksanaan dasar juga seterusnya dapat mewujudkan suatu platfom kepada kerajaan untuk memberikan perkhidmatan yang terbaik kepada rakyat. Selain daripada itu, kajian lain yang berkaitan kesedaran keselamatan komputer dikalangan pengguna juga memberi

penekanan kepada faktor-faktor sepunya, terutama yang berkaitan Modal Insan (Zakiah & Dalbir, 2018). Ini juga diselari dalam United Nations E-Government Survey yang mengkaji amalan terbaik di Denmark, Korea and Estonia (United Nations, 2020). Secara tidak langsung, usaha membangun garis panduan berdasarkan dasar kesedaran keselamatan komputer harus memberi fokus kepada aspek modal insan selain daripada pengurusan dan teknikal.

KESIMPULAN

Kesedaran penjawat awam terhadap pelaksanaan dasar keselamatan komputer adalah perkara yang perlu diambil perhatian. Ianya memerlukan perhatian dan sokongan daripada semua pihak untuk menyelaras pelaksanaannya. Garis panduan yang dicadangkan adalah hasil daripada kajian penyelidik bagi menangani isu kelemahan berkaitan kesedaran penjawat awam terhadap dasar keselamatan komputer di agensi. Ia berpotensi dijadikan *check and balance* oleh responden dalam melaksanakan dasar keselamatan komputer di agensi negeri dan agensi pusat. Kajian ini membangunkan garis panduan untuk meningkatkan kesedaran penjawat awam terhadap pelaksanaan dasar keselamatan komputer sedia ada. Garis panduan ini adalah untuk dilaksanakan di agensi khususnya dan sektor awam umumnya. Untuk membangunkan garis panduan ini, keempat-empat objektif kajian dan persoalan kajian telah dicapai. Penyelidikan terhadap dasar keselamatan dan strategi pelaksanaannya adalah suatu proses pembelajaran yang baik, menggalakkan aktiviti penyelidikan dalam teknologi maklumat dan komunikasi, mengenalpasti pihak berkepentingan dan perluasan pendidikan keselamatan. Cadangan yang terkandung dalam kajian ini adalah relevan dengan situasi semasa berkaitan keselamatan komputer di kalangan penjawat awam atau sebagai asas kepada pembangunan garis panduan yang lebih baik. Diharap kajian ini juga boleh memangkin penyelidikan lanjut pada masa hadapan untuk agensi kerajaan yang lain (Hart et al., 2020).

RUJUKAN

Amri Jamil & Zawiyah M. Yusof. 2018. *Information Security Governance Framework of Malaysia Public Sector*. Asia-Pacific Journal of Information Technology and Multimedia (APJITM), 7(2):85-98.

Republic of Malawi. 2013. An ICT-led Malawi. National ICT Policy.

C. R. Kothari. 2007. *Research Methodology Methods and Techniques (Second Revised Edition).* New Delhi : New Age International Publishers.

Federated States of Micronesia. 2010. Development of the Federated States of Micronesia National ICT. Policy.

Hart, S., Margheri, A., Paci, F. & Sassone, V. 2020. *Riskio: A Serious Game for Cyber Security Awareness and Education*. Computers & Security, Vol. 95:101827

Hasmanizam Abdul Majid, Mazlina Abdul Majid, Mohd Izham Ibrahim, Wan Nurul Safawati Wan Manan & Muhammed Ramiza Ramli. 2015. *Investigation of Security Awareness on e-Learning System Among Lecturers and Students in Higher Education Institution*. Universiti Malaysia Pahang.

United Kingdom. 2011. Government ICT Strategy. Cabinet Office.

Malaysia. 2015. Laporan Tahunan MAMPU Tahun 2015. MAMPU.

Nepal. 2015. National Information and Communication Technology Policy. Ministry of Information and Communication. Government of Nepal.

Nur Ilyana Ismarau Tajuddin & Zawiyah M. Yusof. 2015. *Behaviour Compliance Model Of Internet Use Among Employees In Klang Valley*. Universiti Kebangsaan Malaysia.

Shamsul Kamal Wan Fakeh, Mohd Nabil Zulhemay, Mohd Sazili Shahibi, Juwahir Ali & Muhammad Khairulnizam Zaini. 2012. *Information security awareness amongst academic librarians*. Universiti Teknologi Mara.

Turner D.W. 2010. *Qualitative Interview Design: A Practical Guide for Novice Investigators.* The Qualitative Report Volume 15. Nova Southeastern University.

Trenton Bond. 2012. Employee Security Awareness Survey. https://devlegalsimpli.blob.core.windows.net/pdfseoforms/pdf-20180219t134432z-001/pdf/employee-security-awareness-survey.pdf?sv=2018-03-28&si=readpolicy&sr=c&sig=MXHnWmn0sXNXztiU%2Bugk2d7DV7KBCOuXF3oBMx0EeEw%3D [Disember 15, 2020]

United Nations. 2020. United Nations E-Government Survey.

Zakiah Saizan, Dalbir Singh. 2018. *Cyber Security Awareness among Social Media Users: Case Study in German-Malaysian Institute (GMI)*. Asia-Pacific Journal of Information Technology and Multimedia (APJITM), 7(2-2):111-127.

Yusmawati Muhd Yusof

Dalbir Singh

Pusat Kajian Teknologi & Pengurusan Perisian (SOFTAM),
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia.
yusmawati_myusof@yahoo.com, dalbir@ukm.edu.my