Model Tahap Kesedaran dan Kepatuhan Terhadap Dasar Keselamatan Teknologi Maklumat dan Komunikasi Polis Diraja Malaysia (PDRM)

Farouk bin Jani Basha
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
farouk82@gmail.com

Ibrahim bin Mohamed
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
ibrahim@ukm.edu.my

ABSTRAK

Tidak dinafikan penggunaan teknologi maklumat dan komunikasi (TMK) telah meningkatkan produktiviti dan keberkesanan sesebuah organisasi. Bagaimanapun, isu keselamatan maklumat perlu dititikberat bagi memasti kerahsiaan, integriti dan kebolehsediaan maklumat adalah selamat terutamanya di sektor keselamatan dalam negara. Kurangnya kesedaran terhadap keselamatan maklumat boleh menyebab pelanggaran keselamatan maklumat walaupun organisasi telah melaksana kawalan keselamatan yang kuat. Justeru, kesedaran terhadap amalan keselamatan TMK adalah penting bagi mengelak berlaku sebarang kebocoran maklumat dan tindakan yang perlu diambil sekiranya berlaku insiden keselamatan. Kajian ini bertujuan mengenal pasti tahap kesedaran dan kepatuhan keselamatan TMK yang melibatkan warga Polis Diraja Malaysia (PDRM) Kontinjen Melaka sebagai kajian kes. Bagi mengukurkan tahap kesedaran TMK responden, kaedah model kesedaran digunakan untuk mengukur pengetahuan, sikap dan tingkah laku pekerja. Pendekatan kajian adalah gabungan kaedah kualitatif melalui temu bual bagi penentusahan model bersama pakar dan kuantitatif bagi mengukurkan tahap kesedaran TMK responden dan membentuk model kajian ini melalui kaji selidik. Hasil dapatan mendapati, indeks kebolehpercayaan setiap komponen soalan kaji selidik adalah baik dan skor min menunjukkan tahap kesedaran dan kepatuhan responden terhadap DKICT adalah di tahap yang tinggi. Menerusi ujian analisis faktor, komponen dikategorikan sebagai formaliti dan simpanan berdasarkan nilai hasil dapatan pusingan *varimax*. Hasil keseluruhan komponen formaliti dan simpanan dijadikan model akhir Tahap Kesedaran Keselamatan TMK dalam kalangan warga PDRM Kontinjen Melaka.

Kata kunci—Teknologi Maklumat dan Komunikasi (TMK); keselamatan maklumat; tahap kesedaran

1. PENGENALAN

Penggunaan Teknologi Maklumat dan Komunikasi (TMK) kini menjadi tulang belakang dan kejayaan kepada sesebuah organisasi. Oleh itu, keselamatan teknologi maklumat perlu menjadi keutamaan dan cabaran di dalam sesebuah organisasi [1] bagi mengekal aspek

keselamatan maklumat iaitu kerahsiaan, ketersediaan dan integriti [2]. Keselamatan maklumat perlu diakui sebagai isu kritikal yang boleh mempengaruhi prestasi organisasi [3]. Malahan, kebolehan untuk mengurus keselamatan maklumat juga boleh menjamin kesinambungan perkhidmatan organisasi. Di dalam institusi kerajaan, keselamatan maklumat adalah lebih penting kerana melibatkan maklumat kerahsiaan, keselamatan dan pertahanan negara.

Jabatan Perdana Menteri menerusi Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU) telah mengeluarkan Dasar Keselamatan ICT (DKICT) yang mengandungi peraturan, tanggungjawab dan peranan penjawat awam dalam melindungi aset TMK organisasi di bawah institusi kerajaan [4]. Dengan adanya DKICT ini, ia menjamin kesinambungan perkhidmatan sesebuah institusi kerajaan dengan mengurangkan insiden keselamatan TMK [4]. DKICT ini juga dijadikan sebagai penanda aras kepada semua institusi kerajaan untuk mematuhi standard piawaian yang dikeluarkan oleh MAMPU.

Dasar tersebut perlu dikongsi, difahami dan dipatuhi menerusi kaedah latihan atau program kesedaran. Menurut [5], penyampaian kesedaran adalah bertujuan memberi tumpuan kepada keselamatan, membolehkan individu mengenal pasti dan prihatin terhadap insiden keselamatan teknologi maklumat serta bertindak balas dengan sewajarnya. Sehingga Mei 2019, sebanyak 3,743 insiden keselamatan maklumat telah dilaporkan kepada *Malaysia Computer Emergency Response Team* (MyCERT) [6]. Oleh itu, insiden keselamatan maklumat perlu diminimumkan dan organisasi perlu melindungi maklumat dan aset TMK terutamanya di organisasi yang berisiko tinggi seperti Polis Diraja Malaysia (PDRM).

Apabila melibatkan organisasi keselamatan seperti polis, kesannya boleh merbahaya kepada keselamatan awam, privasi, integriti bahan bukti dan proses penghakiman [7]. Tambahan pula, maklumat seperti penyiasatan, penahanan dan penguatkuasaan turut dijadikan sebagai sasaran utama ancaman siber. Maklumat laporan daripada PDRM, adalah penting dalam melaksana sesuatu penyiasatan terutama laporan elektronik kerana ia berperanan utama dalam prosiding perundangan [8]. Malah, maklumat yang dikompromi dalam laporan polis boleh menghalang siasatan, pendakwaan dan adjudikasi jenayah. Maklumat tersebut amat penting bagi membolehkan hakim dan para juri membuat keputusan kehakiman. Malah penyerang siber juga menyasar kakitangan polis sebagai sasaran baru. Ini terbukti apabila sekumpulan penyerang siber telah menggodam beberapa laman sesawang FBI dan berjaya

mengambil sekurang-kurangnya satu juta data yang mengandungi maklumat peribadi ejen persekutuan dan pegawai penguatkuasaan undang-undang Amerika Syarikat [9].

Oleh itu adalah penting untuk mempersiap dan melatih setiap kakitangan di dalam organisasi terhadap serangan siber. Maklumat penting organisasi perlu dijaga sepenuhnya dan ia harus bermula daripada staf di dalam organisasi. Jika sumber dalaman tidak mencukupi, perkhidmatan profesional luar mungkin diperlu untuk mengurus aspek tindak balas insiden keselamatan maklumat.

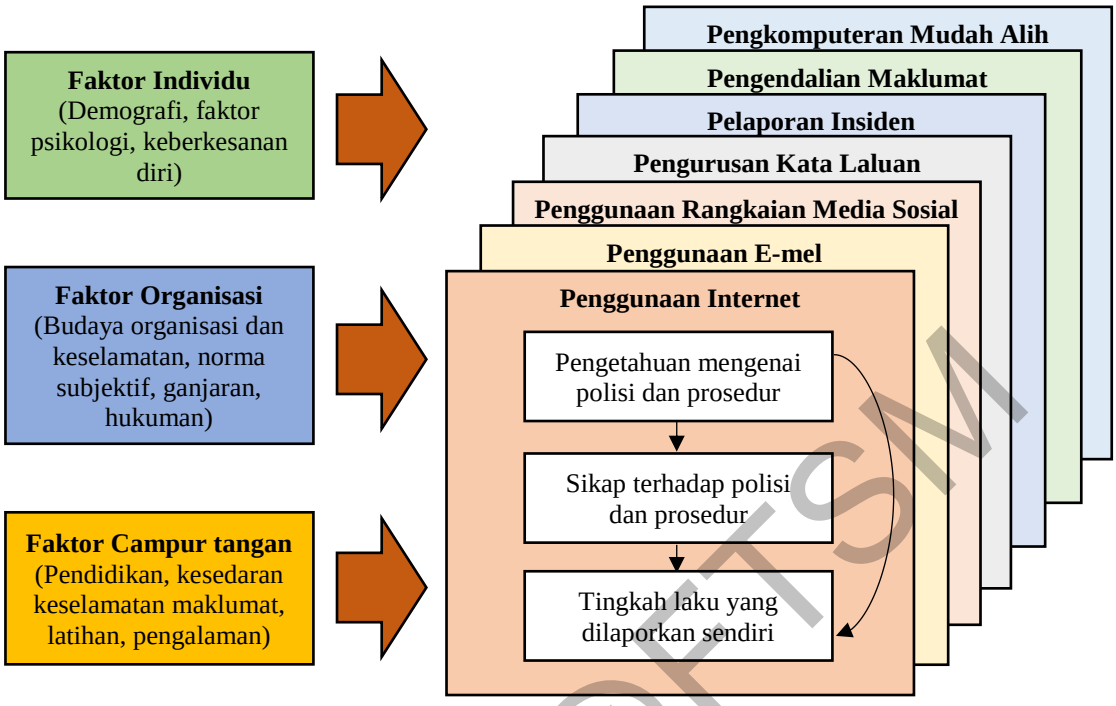
2. KAJIAN BERKAITAN

Kerajaan dan organisasi komersial di seluruh dunia menggunakan TMK secara meluas, dan berfungsi sebagai modul utama dalam perniagaan organisasi dan kestabilan fungsi. Oleh yang demikian, untuk mengatasi sikap tidak berhati-hati ini, dan memasti kejayaan perniagaan organisasi, budaya keselamatan maklumat perlu diwujud [10]. Penerapan langkah-langkah keselamatan teknikal dan polisi keselamatan perlu dipatuhi oleh setiap pengguna. Namun, masih ramai pengguna yang tidak mematuhi dasar yang telah digariskan atau mengamal tingkah laku yang ditetap [11]. Antara sebab mengapa pengguna tidak mematuhi dasar yang ditetapkan adalah kerana tidak menyedari risiko yang bakal dihadapi oleh mereka.

Pemahaman mengenai model dan kerangka kerja kesedaran sedia ada adalah penting untuk membina model kesedaran keselamatan maklumat. Kajian semula kerangka kerja sedia ada dan langkah kesedaran keselamatan penting untuk mengembang model konsep baharu. Hasil penelitian terhadap model sedia ada ini penting dan menjadi nilai tambah dalam membangun model awal kajian.

A. Model *Human Aspect Of Information Security Questionnaire* (HAIS-Q)

[12] mengenal pasti tujuh (7) bidang fokus iaitu, (i) penggunaan Internet; (ii) penggunaan e-mel; (iii) penggunaan rangkaian media sosial; (iv) pengurusan kata laluan; (v) pelaporan insiden; (vi) pengendalian maklumat; dan (vii) pengkomputeran mudah alih seperti di Rajah 1.



Rajah 1: Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) [12].

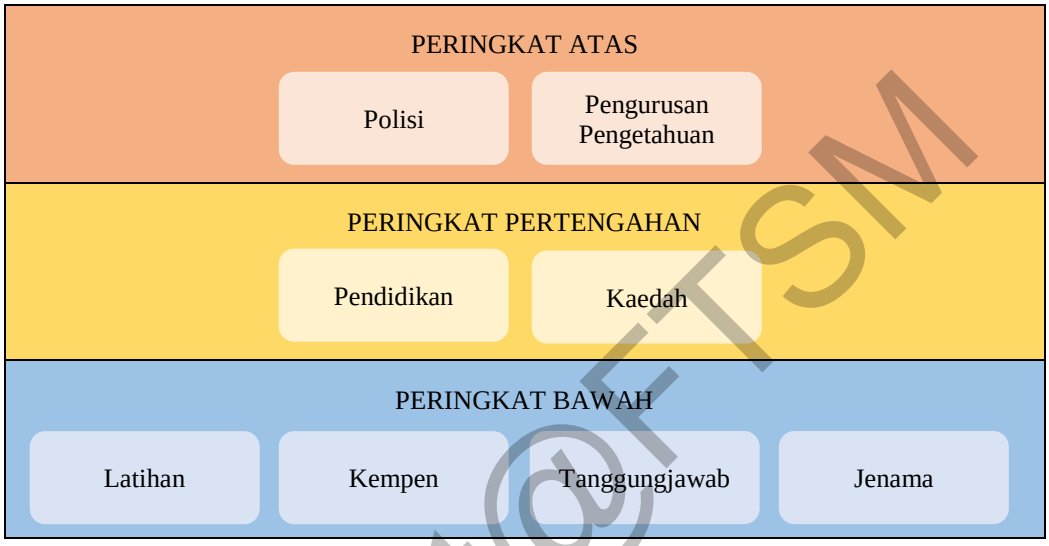
B. Model *Information Security Awareness Identification* (ISAIM)

Model *Information Security Awareness Identification* (ISAIM) yang dibangunkan oleh [13] mempunyai enam (6) elemen utama yang iaitu, (i) penggunaan yang berkesan; (ii) kesedaran organisasi; (iii) kesedaran ancaman; (iv) kesedaran perlindungan; (v) kesedaran kandungan; dan (vi) amalan keselamatan, seperti di Rajah 2.

Rajah 2: Model *Information Security Awareness Identification* (ISAIM) [13].

C. Model Kesedaran Keselamatan Maklumat

Model Kesedaran Keselamatan Maklumat [5] diklasifikasikan kepada tiga (3) peringkat iaitu peringkat atas, peringkat pertengahan dan peringkat bawah seperti di Rajah 3.



Rajah 3: Model Kesedaran Keselamatan Maklumat [5].

D. Standard Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO 27001:2013

Pemakaian standard MS ISO/IEC 27001:2013 Pengurusan Sistem Keselamatan Maklumat (*Information Security Management System*, ISMS) seperti di Rajah 4 pula adalah pelengkap kepada sistem pengurusan kualiti di mana piawaian ini menyediakan spesifikasi dan kawalan-kawalan bagi melindungi keselamatan aset maklumat dan seterusnya meningkatkan integriti dan keyakinan pelanggan kepada agensi berkenaan. Melalui pengauditan ke atas aset TMK, tindakan pembetulan dan penambahbaikan dapat diambil ke atas sebarang kelemahan, ketidakpatuhan atau kekurangan kepada sistem pengurusan keselamatan TMK sedia ada demi memantapkan perlindungan kepada prinsip-prinsip kerahsiaan, integriti dan ketersediaan.

Rajah 4: Model Standard Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO 27001:2013.

2.1 CADANGAN MODEL AWAL

Berdasarkan kajian kesusasteraan yang dijalankan terhadap kajian lampau dan model sedia ada, didapati aspek kesedaran keselamatan maklumat adalah penting dalam mengukur tahap kesedaran organisasi dalam memastikan keselamatan perkhidmatan TMK adalah terjamin selamat. Pemilihan komponen adalah berdasarkan norma harian pengguna terhadap penggunaan TMK iaitu kata laluan, e-mel, Internet, taklimat/latihan, dasar/polisi dan insiden keselamatan. Komponen tersebut juga telah tersedia ada di dalam dokumen DKICT PDRM.

Oleh yang demikian, pembangunan model awal dalam kajian ini adalah gabungan daripada beberapa komponen kajian sedia ada dan enam (6) domain telah dipilih sebagai komponen untuk pembangunan model awal adalah seperti di Jadual 1.

JADUAL 1: PENEMUAN ENAM (6) KOMPONEN SEDIA ADA DARI KAJIAN LEPAS

Komponen	Model
Pengurusan kata laluan	Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) [12]. Kajian tertumpu kepada tingkah laku yang dikenali sebagai "Kelakuan Neutral (tidak sengaja) yang dikaitkan dengan kesalahan manusia dan pengurusan kata laluan adalah contoh yang diberikan oleh [14].
Penggunaan e-mel	Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) [12]. Kajian tertumpu kepada tingkah laku yang dikenali sebagai "Kelakuan Neutral (tidak sengaja) yang dikaitkan dengan kesalahan manusia dan penggunaan e-mel adalah contoh yang diberikan oleh [14].

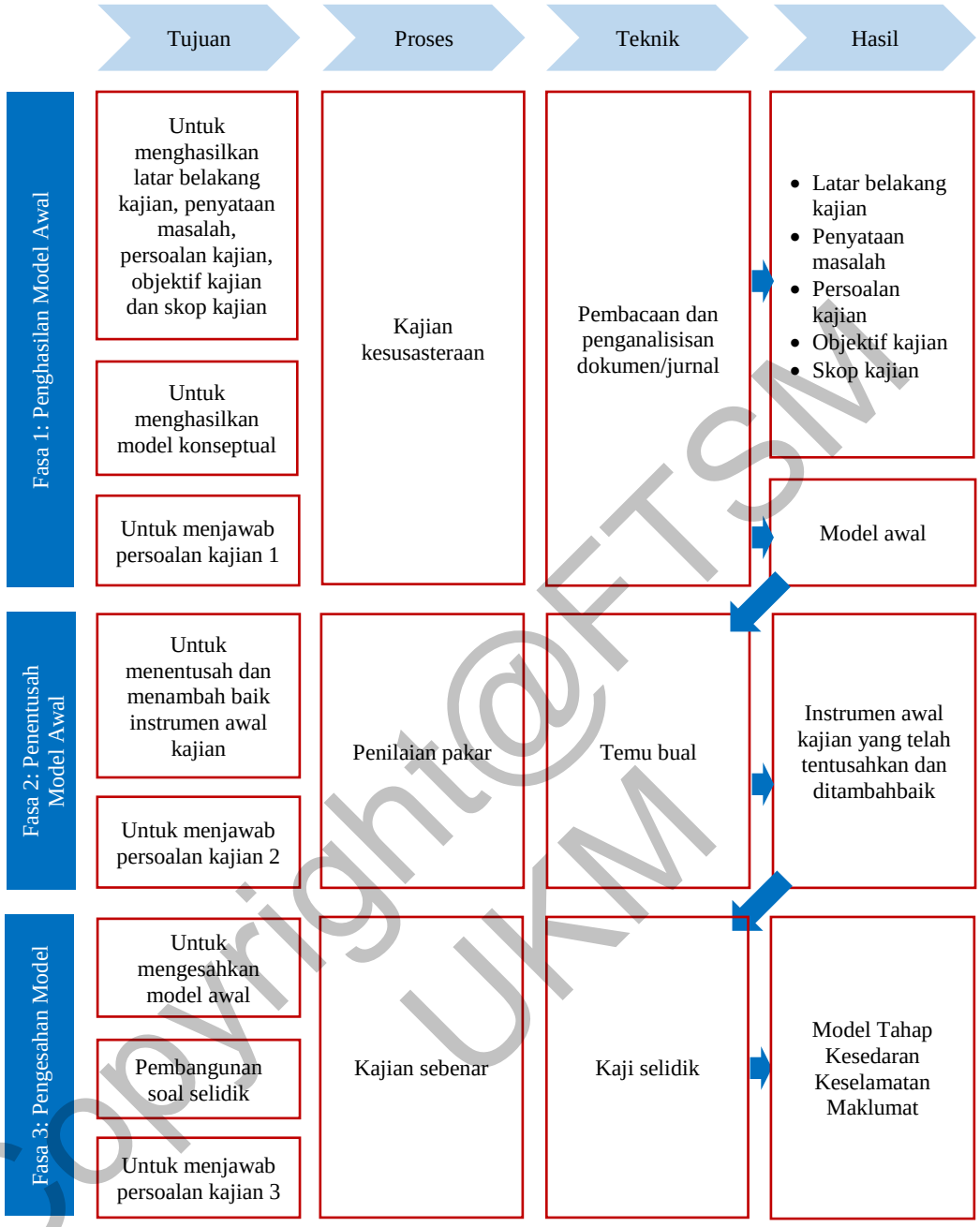
...bersambung

...sambungan

Penggunaan Internet	Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) [12] Kajian tertumpu kepada tingkah laku yang dikenali sebagai "Kelakuan Neutral (tidak sengaja) yang dikaitkan dengan kesalahan manusia dan penggunaan Internet adalah contoh yang diberikan oleh [14].
Dasar/polisi	• Dasar atau polisi keselamatan maklumat kepada bagi melindungi maklumat organisasi menerusi Model Kesedaran Keselamatan Maklumat [5]. • Dasar atau polisi untuk menguruskan data sensitif organisasi secara sistematik serta meminimumkan risiko dan memastikan kesinambungan perniagaan menerusi Model Standard Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO 27001:2013.
Taklimat/latihan	• Taklimat atau latihan keselamatan maklumat kepada bagi melindungi maklumat organisasi menerusi Model Kesedaran Keselamatan Maklumat [5]. • Amalan keselamatan bagi mengenal pasti latihan yang diperlukan menerusi Model *Information Security Awareness Identification* (ISAIM) [13].
Insiden keselamatan	• Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) [12]. Kajian tertumpu kepada tingkah laku yang dikenali sebagai "Kelakuan Neutral (tidak sengaja) yang dikaitkan dengan kesalahan manusia dan pengendalian maklumat adalah contoh yang diberikan oleh [12]. • Kesedaran ancaman bagi mengenal pasti pengetahuan polisi keselamatan dan mekanisme pelaporan insiden keselamatan menerusi Model *Information Security Awareness Identification* (ISAIM) [13]. • Pendekatan yang konsisten dan berkesan untuk pengurusan insiden keselamatan maklumat, termasuk komunikasi mengenai kejadian dan kelemahan keselamatan menerusi Model Standard Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO 27001:2013.

3. PENDEKATAN KAJIAN

Dalam kajian ini, metodologi yang digunakan adalah gabungan kaedah kuantitatif iaitu penggunaan kaji selidik, dan kaedah kualitatif iaitu secara temu bual. Pendekatan kajian melibatkan tiga (3) fasa utama iaitu (i) penghasilan model awal; (ii) penentusah model awal; dan (iii) pengesahan model. Setiap fasa mempunyai beberapa aktiviti yang dirancang mengikut keutamaan berdasarkan kesesuaian organisasi yang dikaji. Gambaran pendekatan kajian adalah seperti di dalam Rajah 5.



Rajah 5: Pendekatan kajian.

3.1 FASA 1: PENGHASILAN MODEL AWAL

A Mengenal Pasti Permasalahan Kajian

Analisis ini tersebut bertujuan untuk mendapatkan latar belakang kajian, penyataan masalah, persoalan kajian, objektif kajian dan skop kajian serta untuk menghasilkan model

awal. Rumusan komponen penting yang telah dikenal pasti menerusi kajian kesusasteraan yang dijalankan adalah seperti di Jadual 2.

JADUAL 2: MENGENAL PASTI PERMASALAHAN KAJIAN

Proses	Teknik	Hasil
Mengenal pasti permasalahan kajian	• Pembacaan dan penganalisisan terhadap kajian kesusasteraan • Jurnal, artikel, buku, garis panduan dan dokumen	• Latar belakang kajian • Penyataan masalah • Persoalan kajian • Objektif kajian • Skop kajian

B Merangka Model Awal

Dalam merangka penghasilan model konseptual, kajian kesusasteraan telah dilakukan yang merangkumi aktiviti pembacaan jurnal, buku dan artikel yang berkaitan dengan model kesedaran. Kajian kesusasteraan dapat meningkatkan pemahaman tentang bidang kajian dan aspek-aspek yang berkaitan dengan penyelidikan dapat diterokai. Menerusi kajian kesusasteraan juga, ianya dapat membantu memahami dan mengenal pasti jurang pengetahuan yang hasilkan dari kajian terdahulu dalam bidang yang dikaji. Proses yang terlibat dalam merangka model konseptual kajian adalah seperti di Rajah 3.

JADUAL 3: MERANGKA MODEL AWAL.

Proses	Teknik	Hasil
Merangka model awal	• Pembacaan dan penganalisisan terhadap kajian kesusasteraan berkenaan tahap kesedaran keselamatan TMK • Jurnal, artikel, buku dan garis panduan DKICT	• Model awal kajian

Setiap model kesedaran yang dikaji mempunyai kekuatannya tersendiri. Namun begitu, bagi tujuan kajian ini dijalankan, beberapa komponen utama diadaptasi daripada setiap model tersebut untuk dijadikan model kesedaran yang baharu. Pemilihan komponen ini adalah berdasarkan ciri-ciri yang terdapat di dalam dokumen DKICT. Pemilihan komponen daripada setiap model yang terlibat adalah seperti di Jadual 4.

JADUAL 4: PEMILIHAN KOMPONEN SETIAP MODEL

Bil.	Model	Komponen
1.	*Human Aspect of Information Security Questionnaire* (HAIS-Q)	• Pengurusan kata laluan • Penggunaan e-mel • Penggunaan Internet • Insiden keselamatan
2.	*Information Security Awareness Identification Model* (ISAIM)	• Taklimat/latihan • Insiden keselamatan
3.	*Conceptual Model for Information Security Awareness*	• Dasar/polisi • Taklimat/latihan
4.	*Model Standard Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO 27001:2013*	• Dasar/polisi • Insiden keselamatan

3.2 FASA 2: PENENTUSAH MODEL AWAL

Bagi menentusah model awal dan memudahkan analisis dibuat, temu bual bersama pakar diadakan bagi mendapatkan penjelasan yang lebih terperinci instrumen yang dicadangkan dan hasil daripada kaji selidik yang diterima. Kaedah temu bual ini amat berkesan untuk mendapatkan penjelasan dan perincian sesuatu kajian dengan lebih cepat dan tepat. Rumusan proses kerja di fasa ketiga yang dijalankan adalah seperti di Jadual 5.

JADUAL 5: PENGESAHAN MODEL AWAL

Proses	Teknik	Hasil
Penentusah model awal	• Temu bual bersama pakar di organisasi kajian	• Model awal kajian ditambahbaik dan disahkan

Sebelum soalan kaji selidik dibangunkan sepenuhnya, komponen soalan kaji selidik dipilih berdasarkan ciri-ciri yang terdapat di dalam dokumen DKICT. Komponen tersebut kemudiannya dinilai dan dikomen oleh pakar di organisasi yang dikaji menerusi kaedah temu bual. Kaedah temu bual ini digunakan agar penentuan komponen dapat ditentukan dan diselaraskan dengan lebih cepat dan berkesan untuk dilaksanakan ke atas responden. Setelah soalan kaji selidik dibangunkan, soalan-soalan tersebut kemudiannya dinilai semula dan dikomen oleh pakar bagi mendapatkan soalan yang terbaik berkaitan kajian ini dan untuk memudahkan pemahaman responden untuk menjawab soalan kaji selidik ini dengan mudah. Apabila responden menjawab kesemua soalan kaji selidik yang dihantar, jawapan soalan tersebut dikumpul dan dianalisis.

Bagi melancarkan perjalanan kajian ini, semua soalan kaji selidik disemak dan dipersetujui oleh pakar di Bahagian Telekomunikasi dan Sistem Maklumat (TSM), Ibu Pejabat

Polis Kontinjen Melaka. Pakar tersebut merupakan daripada kumpulan Pengurusan dan Profesional yang telah berkhidmat di organisasi selama 18 tahun. Beliau juga memegang jawatan sebagai Pegawai Turus TSM di Ibu Pejabat Polis Kontinjen Melaka dan terlibat secara langsung dalam pengoperasian TMK dan pelaksanaan dasar serta polisi organisasi termasuklah DKICT dan ISMS.

Bagi memudahkan soalan kaji selidik disampaikan kepada responden, dua kaedah digunakan, iaitu dengan menggunakan kertas (secara manual) dan menggunakan platform *Google Forms* (secara digital). Pengujian terhadap *Google Forms* juga dibuat terlebih dahulu untuk mengelak daripada kegagalan capaian dan kesilapan pada soalan.

3.3 FASA 3: PENGESAHAN MODEL

Fasa yang terakhir ini adalah untuk mengesahkan model awal yang dibangunkan di fasa pertama. Menerusi kajian sebenar yang dijalankan dan hasil kajian melalui kaedah kaji selidik, maka model kajian iaitu Model Tahap Kesedaran Keselamatan Maklumat dapat dihasilkan. Menerusi kajian yang dijalankan juga dapat menjawab objektif dan persoalan kajian. Analisis pengesahan model ini akan dibincangkan lanjut di bab seterusnya. Proses yang terlibat dalam mengesahkan model kajian adalah seperti di Rajah 6.

JADUAL 6: PENGESAHAN MODEL KAJIAN

Proses	Teknik	Hasil
Mengesahkan model awal	• Kajian sebenar dan analisis menerusi kaji selidik	• Model kajian

3.4 ANALISIS DATA

Analisis data merupakan aktiviti yang penting dan tidak boleh diabaikan dalam proses kajian. Menurut [15], analisis data adalah satu proses penelitian yang dilakukan setelah semua data yang diperlukan telah diperolehi dengan lengkap. Oleh itu, pemilihan instrumen analisis perlu diberi perhatian kerana penentuan arah kesimpulan kajian bergantung kepada analisis yang dijalankan. Kesilapan dalam memilih instrumen analisis boleh mengganggu pemprosesan data dan seterusnya menjejaskan keputusan dan kesimpulan terhadap kajian yang dilaksanakan. Pada keseluruhannya, analisis data bagi kajian ini dikendalikan secara statistik deskriptif.

A. Ujian Kebolehpercayaan

Pekali *Cronbach Alpha* digunakan untuk mengukur kebolehpercayaan, atau konsistensi dalaman. "Kebolehpercayaan" adalah sejauh mana ujian itu mengukur sesuatu konstruk. Kebolehpercayaan yang tinggi memberi maksud item-item di dalam kaji selidik tersebut benar-benar mengukur kepuasan responden, manakala kebolehpercayaan yang rendah memberi maksud ia mengukur sesuatu yang lain daripada kepuasan responden. Oleh yang demikian, analisis *Cronbach Alpha* dijalankan untuk melihat adakah soalan kaji selidik yang diukur melalui skala *likert* itu boleh dipercayai.

B. Ujian Skor Min

Analisis deskriptif digunakan untuk mendapatkan min dan sisihan piawai untuk memenuhi objektif yang ditentukan. Menurut [16], konsep min statistik mempunyai tahap penerapan yang sangat luas dalam statistik untuk sejumlah jenis eksperimen yang berbeza. Tambahnya lagi, min memberikan maklumat penting mengenai set data yang ada dan sebagai satu nombor dapat memberikan banyak pandangan tentang eksperimen dan sifat data. Menurut kajian daripada [17], min atau purata adalah statistik yang paling umum digunakan untuk mengukur pusat kumpulan data berangka dan jumlah semua nilai dalam kumpulan data dibahagi dengan jumlah nilai dalam kumpulan data.

C. Analisis Faktor

Analisis faktor yang bertujuan untuk melihat kesahan item dan pemuatan item mengikut dimensi-dimensi yang dibentuk di dalam konstruk borang soal selidik. Ini adalah bertujuan untuk meningkatkan lagi kesahan kandungan konstruk dan item-item selepas pra uji dilakukan terhadap instrumen kajian. Kajian daripada [18] menyatakan bahawa, analisis faktor adalah bertujuan untuk mengurangkan dan merumuskan data yang melibatkan item yang berulang digabungkan dan item yang tidak berkaitan digugurkan. Menurut [19] pula, analisis faktor merupakan prosedur yang lazim digunakan oleh penyelidik bagi mengenal pasti, mengurangkan dan menyusun sebilangan besar item soal selidik dalam konstruk- konstruk tertentu.

Kajian ini menggunakan analisis faktor pada pemboleh ubah tidak bersandar dengan memilih kaedah putaran *varimax*. Kaedah putaran *varimax* digunakan bagi memfokuskan analisis untuk mempermudahkan lajur pada faktor matriks. Selain itu, kaedah putaran *varimax* dilakukan kerana dapat mengurangkan jumlah pemboleh ubah yang kompleks dan dapat meningkatkan hasil jangkaan.

4. HASIL PENGUJIAN

Soalan kaji selidik diagih secara serentak kepada kumpulan yang telah disasar iaitu (i) pengguna biasa (yang tidak melibatkan penggunaan sistem); (ii) pengguna sistem; dan (iii) pentadbir sistem; yang melibatkan seramai 70 orang responden di Bahagian TSM, PDRM Kontinjen Melaka. Sejumlah 70 soalan kaji selidik telah diedarkan, namun 59 orang responden sahaja yang memberi maklum balas. Tempoh menjawab soalan kaji selidik adalah selama tiga belas (13) hari iaitu 3 hingga 15 Februari 2020. Tempoh ini adalah sesuai bagi memudah responden menjawab soalan dengan tenang, tidak terburu-buru dan seterusnya memberi jawapan yang tepat. Ringkasan maklumat pengumpulan data adalah seperi di Jadual 7.

JADUAL 7: MAKLUMAT PENGUMPULAN DATA

Tarikh	3 - 15 Februari 2020 (13 hari)
Tajuk	Kaji Selidik Tahap Kesedaran dan Kepatuhan Dasar Keselamatan ICT (DKICT)
Entiti terlibat	Bahagian Telekomunikasi dan Sistem Maklumat Jabatan Sumber Strategik dan Teknologi
Kumpulan sasaran	• Pengguna biasa (tidak melibatkan sistem) • Pengguna sistem • Pentadbir sistem
Bilangan responden	• 59 daripada 70 responden
Kaedah agihan	• Menggunakan kertas • Dalam talian

4.1 PENGESAHAN MODEL

Pengesahan model daripada pakar menjadikan enam (6) komponen terlibat iaitu (i) pengurusan kata laluan; (ii) penggunaan e-mel; (iii) penggunaan Internet; (iv) dasar/polisi; (v) taklimat/latihan; dan (vi) insiden keselamatan seperti di Rajah 6.

Rajah 6: Gabungan enam (6) komponen daripada model sedia ada dari kajian lepas.

4.2 UJIAN KEBOLEHPERCAYAAN

Nilai *Alpha Cronbach* dicari untuk menentukan kebolehpercayaan item soal selidik. Menurut [18] ukuran kebolehpercayaan adalah dari kosong hingga satu dan nilai di antara 0.60 hingga 0.70 dianggap had penerimaan paling minimum. Pemboleh ubah konsisten apabila tahap kebolehpercayaan tidak berubah-ubah apabila digunakan berulang kali dalam kajian yang berlainan.

Nilai kebolehpercayaan bagi instrumen kaji selidik adalah merujuk kepada nilai kebolehpercayaan serta pengasingan item. Nilai kebolehpercayaan yang diperolehi daripada nilai *Alpha Cronbach* adalah di antara 0.724 - 0.842 seperti dalam Jadual 8. Nilai ini menunjukkan indeks kebolehpercayaan item adalah baik, boleh diterima dan memenuhi ciri dikehendaki.

JADUAL 8: NILAI KEBOLEHPERCAYAAN *ALPHA CRONBACH*

Komponen	**Bilangan Item**	**Nilai *Alpha Cronbach***
Teknologi	9	.727
Dasar/Polisi	3	.724
Taklimat/Latihan	3	.842
Insiden Keselamatan	3	.767

4.3 ANALISIS MIN

Secara keseluruhannya, skor min bagi keseluruhan kaji selidik adalah di antara 5.64 – 6.90. Berdasarkan tafsiran skor min yang ditetapkan oleh [20] nilai-nilai tersebut menunjukkan tahap yang tinggi. Skor ini juga menunjukkan bahawa tahap kesedaran dan kepatuhan responden terhadap DKICT berada di tahap yang tinggi.

JADUAL 9: SKOR MIN DAN TAHAP KESEDARAN RESPONDEN

No Soalan	Soalan	Min	Tahap Kesedaran
S7	Penggunaan kata laluan yang berbeza	6.37	Tinggi
S8	Penggunaan kata laluan yang mengandungi huruf, nombor dan simbol	6.14	Tinggi
S9	Kata laluan perlu diingati dan disimpan di tempat yang selamat	6.53	Tinggi
S10	Penggunaan e-mel rasmi untuk kegunaan peribadi	6.80	Tinggi
S11	Penggunaan e-mel peribadi untuk kegunaan rasmi pejabat	6.85	Tinggi
S12	Pautan (*link*) di dalam e-mel yang mencurigakan	6.90	Tinggi
S13	Memuat turun (*download*) perisian dari Internet	6.51	Tinggi
S14	Memuat turun (*download*) atau memuat naik (*upload*) video atau lagu dari Internet	6.37	Tinggi
S15	Memuat turun (download) atau memuat naik (*upload*) bahan lucah	6.95	Tinggi
S16	Dasar Keselamatan ICT (DKICT) membantu memahami peranan dan tanggungjawab penggunaan ICT	6.03	Tinggi
S17	DKICT sedia ada adalah mudah difahami dan dipatuhi	5.64	Tinggi
S18	Surat pematuhan DKICT	6.63	Tinggi
S19	Taklimat/latihan DKICT	6.63	Tinggi
S20	Hebahan poster atau risalah DKICT secara berkala	6.66	Tinggi
S21	Taklimat/latihan DKICT secara berkala	6.69	Tinggi
S22	Hebahan e-mel yang mencurigakan	6.71	Tinggi
S23	Dokumen atau fail yang mencurigakan	6.83	Tinggi
S24	E-mel yang berunsurkan ugutan (*ransomware*)	6.88	Tinggi

(n=59)

4.4 UJIAN ANALISIS FAKTOR

Ujian analisis faktor kajian ini dijalankan dengan menggunakan analisis komponen prinsipal. Data tersebut kemudiannya diputar dengan mengguna pusingan *varimax* dan hasilnya adalah seperti di dalam Jadual 10. Hasil pusingan *varimax* menunjukkan, nilai item menjadi lebih tinggi dan hampir dekat di antara satu sama lain. Ini membukti bahawa hubungan korelasi di antara item dengan faktor yang terbentuk dan ini merupakan kunci untuk memahami sifat faktor-faktor tersebut. Berdasarkan bukti ini, putaran *varimax* dapat digunakan untuk menghasilkan tafsiran data yang baik.

JADUAL 10: MATRIKS KOMPONEN BAGI ANALISIS FAKTOR

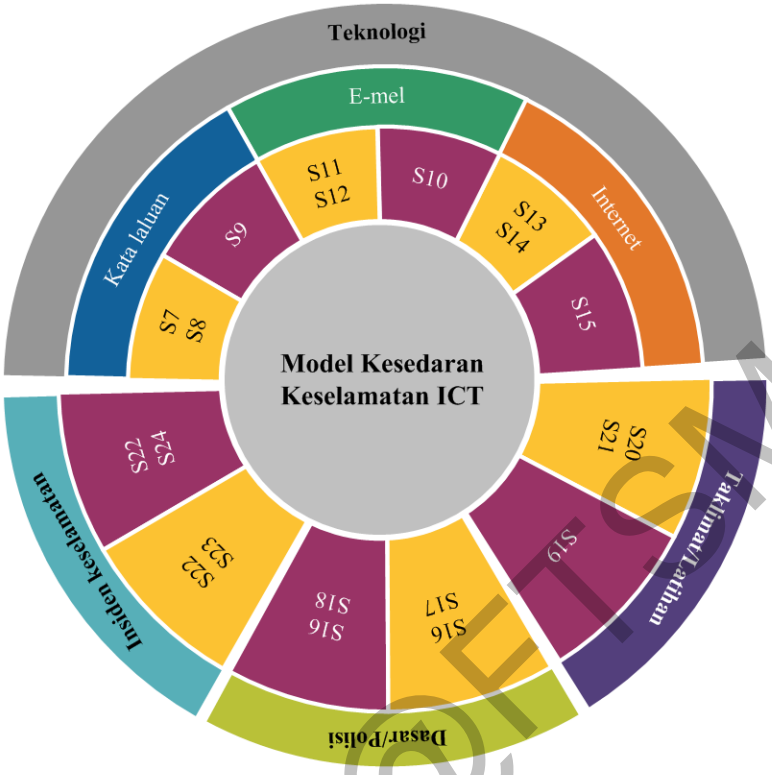
No Soalan	Soalan	Komponen	
		1	2
S7	Penggunaan kata laluan yang berbeza	.884	
S8	Penggunaan kata laluan yang mengandungi huruf, nombor dan simbol	.827	
S9	Kata laluan perlu diingati dan disimpan di tempat yang selamat		.980
S10	Penggunaan e-mel rasmi untuk kegunaan peribadi		.957
S11	Penggunaan e-mel peribadi untuk kegunaan rasmi pejabat	.699	
S12	Pautan (*link*) di dalam e-mel yang mencurigakan	.891	
S13	Memuat turun (*download*) perisian dari Internet	.906	
S14	Memuat turun (*download*) atau memuat naik (*upload*) video atau lagu dari Internet	.887	
S15	Memuat turun (download) atau memuat naik (*upload*) bahan lucah		.995
S16	Dasar Keselamatan ICT (DKICT) membantu memahami peranan dan tanggungjawab penggunaan ICT	.735	.507
S17	DKICT sedia ada adalah mudah difahami dan dipatuhi	.946	
S18	Surat pematuhan DKICT		.964
S19	Taklimat/latihan DKICT		.959
S20	Hebahan poster atau risalah DKICT secara berkala	.949	
S21	Taklimat/latihan DKICT secara berkala	.904	
S22	Hebahan e-mel yang mencurigakan	.685	.571
S23	Dokumen atau fail yang mencurigakan	.948	
S24	E-mel yang berunsurkan ugutan (*ransomware*)		.955

Kaedah pengekstrakan: Analisis komponen prinsipal

4.5 MODEL AKHIR KAJIAN

Berdasarkan penentusahan dan pengesahan yang dibuat oleh pakar, model akhir kajian adalah seperti di Rajah 8. Daripada hasil putaran *varimax*, setiap komponen dibahagikan kepada dua (2) kategori iaitu formaliti dan simpanan. Bagi komponen pengurusan kata laluan, S7 dan S8 diletakkan di kategori formaliti, dan S9 adalah simpanan. Untuk komponen penggunaan e-mel pula, S11 dan S12 diletakkan di kategori formaliti, dan S10 adalah simpanan. Manakala komponen penggunaan Internet pula, S13 dan S14 diletakkan di kategori formaliti, dan S15 adalah simpanan. Ketiga-tiga komponen disatukan menjadi kategori "Teknologi" seperti mana yang telah dipersetujui oleh pakar.

Bagi komponen dasar/polisi, S16 dan S17 diletakkan di kategori formaliti, dan S16 dan S18 adalah simpanan. Untuk komponen taklimat/latihan pula, S19 diletakkan di kategori formaliti, dan S20 dan S21 adalah simpanan. Manakala komponen insiden keselamatan pula, S22 dan S23 diletakkan di kategori formaliti, dan S22 dan S24 adalah simpanan. Jadual 11 menunjukkan keseluruhan komponen model akhir yang dipecahkan mengikut kategori.



Rajah 8: Model akhir kajian.

JADUAL 11: KOMPONEN MODEL AKHIR MENGIKUT KATEGORI

Teknologi	Kata laluan	S7	Penggunaan kata laluan yang berbeza
		S8	Penggunaan kata laluan yang mengandungi huruf, nombor dan simbol
		S9	Kata laluan perlu diingati dan disimpan di tempat yang selamat
	E-mel	S10	Penggunaan e-mel rasmi untuk kegunaan peribadi
		S11	Penggunaan e-mel peribadi untuk kegunaan rasmi pejabat
		S12	Pautan (*link*) di dalam e-mel yang mencurigakan
	Internet	S13	Memuat turun (*download*) perisian dari Internet
		S14	Memuat turun (*download*) atau memuat naik (*upload*) video atau lagu dari Internet
		S15	Memuat turun (download) atau memuat naik (*upload*) bahan lucah
Dasar/ polisi		S16	Dasar Keselamatan ICT (DKICT) membantu memahami peranan dan tanggungjawab penggunaan ICT
		S17	DKICT sedia ada adalah mudah difahami dan dipatuhi
		S16	Dasar Keselamatan ICT (DKICT) membantu memahami peranan dan tanggungjawab penggunaan ICT
		S18	Surat pematuhan DKICT
Taklimat / latihan		S19	Taklimat/latihan DKICT
		S20	Hebahan poster atau risalah DKICT secara berkala
		S21	Taklimat/latihan DKICT secara berkala
Insiden keselamatan		S22	Hebahan e-mel yang mencurigakan
		S23	Dokumen atau fail yang mencurigakan
		S22	Hebahan e-mel yang mencurigakan
		S24	E-mel yang berunsurkan ugutan (*ransomware*)

5. KESIMPULAN

5.1 PENCAPAIAN OBJEKTIF

Secara keseluruhannya, kajian ini berjaya memenuhi tiga (3) objektif kajian yang dinyatakan di dalam Bab I iaitu (i) mereka bentuk Model Tahap Kesedaran Keselamatan TMK di kalangan staf PDRM Kontinjen Melaka; (ii) mengesahkan model yang dibangunkan; dan (iii) mengkaji tahap kesedaran dan kepatuhan DKICT di kalangan staf PDRM Kontinjen Melaka.

A Mereka Bentuk Model Tahap Kesedaran Keselamatan TMK Dalam Kalangan Warga PDRM Kontinjen Melaka

Objektif pertama adalah untuk mereka bentuk Model Tahap Kesedaran Keselamatan ICT di kalangan staf PDRM Kontinjen Melaka. Pembangunan model dalam kajian ini adalah bermula dengan melakukan kajian kesusasteraan terhadap model kesediaan yang lepas yang berkaitan dengan kesedaran maklumat. Hasil kajian kesusasteraan telah menghasilkan model awal kajian. Model awal kajian ini terdiri daripada enam (6) komponen, iaitu pengurusan kata laluan, penggunaan e-mel, penggunaan Internet, dasar/polisi, taklimat/latihan dan insiden keselamatan. Seterusnya, model awal kajian ini diteliti dan disahkan oleh pakar yang berpengalaman dalam bidang pengurusan keselamatan maklumat. Cadangan dan idea pakar diteliti dan dianalisis bagi menghasilkan model yang disahkan oleh pakar. Komponen-komponen ini kemudiannya dijadikan ke dalam bentuk soalan kaji selidik. Soalan kaji selidik tersebut seterusnya disahkan oleh pakar sebelum dibuat edaran kepada responden untuk menjawab.

B Menentusah Tahap Kesedaran dan Kepatuhan Warga PDRM Kontinjen Melaka Terhadap DKICT

Objektif kajian yang kedua ialah mengkaji tahap kesedaran dan kepatuhan DKICT di kalangan staf PDRM Kontinjen Melaka. Menerusi kaji selidik yang dijalankan, didapati bahawa tahap kesedaran dan kepatuhan DKICT dalam kalangan warga PDRM Kontinjen Melaka adalah berada di tahap yang tinggi. Setiap soalan di dalam kaji selidik tersebut mencatatkan peratusan yang tinggi terhadap semua komponen yang terlibat. Ini juga dibuktikan

melalui analisis data yang dibuat menerusi analisis min yang menunjukkan nilai min yang tinggi untuk kesemua komponen.

C Mengesahkan Model Yang Dibangunkan

Objektif yang ketiga ialah mengesahkan model yang dibangunkan. Beberapa analisis diadakan ke atas data yang diterima daripada responden menerusi kaji selidik yang dijalankan. Melalui ujian kebolehpercayaan, nilai Alpha Cronbach adalah di antara 0.724 – 0.842 dan menunjukkan indeks kebolehpercayaan item adalah baik, boleh diterima dan memenuhi ciri dikehendaki. Menerusi ujian analisis faktor, data-data diputarkan menggunakan pusingan varimax dan menghasilkan nilai yang lebih tinggi dan hampir dekat di antara satu sama lain. Ini membuktikan bahawa hubungan korelasi antara item dengan faktor yang terbentuk dan ini merupakan kunci untuk memahami sifat faktor-faktor tersebut. Berdasarkan bukti ini, putaran varimax dapat digunakan untuk menghasilkan tafsiran data yang baik dan wajar dipertimbangkan untuk dijadikan komponen di dalam model kesedaran. Melalui analisis ujian inter-korelasi Pearson, ada beberapa komponen yang hubungannya adalah lemah. Namun begitu, hubungan antara komponen tersebut adalah positif. Keputusan nilai signifikan juga menunjukkan terdapat hubungan yang tidak signifikan, namun begitu hubungan tersebut adalah positif. Berdasarkan ujian statistik yang telah dilaksanakan dan hasil analisis faktor, maka model akhir dapat dibentuk.

5.2 SUMBANGAN KAJIAN

Berdasarkan kajian yang telah dijalankan, terdapat tiga (3) sumbangan utama yang telah diberikan dalam kajian ini. Sumbangan tersebut adalah seperti berikut:

a. Membangunkan Model Tahap Kesedaran Keselamatan TMK untuk digunakan pada staf PDRM Kontinjen Melaka. Dengan adanya model ini, pihak pengurusan atasan organisasi boleh membuat latihan dan kempen kesedaran keselamatan TMK secara berkala.

b. Sebagai panduan kepada pihak pengurusan atasan organisasi untuk menilai tahap kesedaran staf terhadap keselamatan maklumat siber. Hasil kajian dapat memudahkan pihak pengurusan atasan untuk merangka strategi bagi mengatasi masalah yang dihadapi oleh staf terhadap keselamatan maklumat siber dan pematuhan DKICT.

c. Meningkatkan kesedaran terhadap keselamatan siber dan DKICT organisasi yang perlu dipatuhi oleh setiap staf. Latihan dan kempen kesedaran keselamatan TMK secara berkala mampu meningkat kesedaran staf terhadap keselamatan siber dari semasa ke semasa.

5.3 CADANGAN KAJIAN MASA HADAPAN

Kajian ini berjaya menghasilkan satu model untuk menentukan tahap kesedaran TMK yang terdiri daripada enam (6) komponen, iaitu pengurusan kata laluan, penggunaan e-mel, penggunaan Internet, dasar/polisi, taklimat/latihan dan insiden keselamatan. Walau bagaimanapun, terdapat banyak aspek yang belum diterokai. Oleh itu, beberapa cadangan kajian disyorkan untuk dibuat pada masa hadapan seperti berikut:

a. Kajian ini boleh diperluaskan ke kontinjen PDRM yang lain. Data dan maklumat yang diperolehi boleh dibuat perbandingan serta dapat melihat keberkesanan model tersebut.

b. Menambah komponen model yang berkaitan dengan DKICT seperti keselamatan rangkaian, kawalan capaian, pengurusan aset dan *bring your own device* (BYOD).

c. Menambah jumlah bilangan populasi bagi menggambarkan kajian secara menyeluruh.

RUJUKAN

[1] Haeussinger, F. J. & Kranz, J. J. 2013. Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. *Thirty Fourth International Conference on Information Systems* 1–16.

[2] Hina, S. & Dominic, D. D. 2016. Information Security Policies: Investigation of Compliance in Investigation Information Policies : of Compliance. *3rd International Conference on Computer and Information Sciences (ICCOINS)* 1–6.

[3] Wahyudiwan, D. D. H., Sucahyo, Y. G. & Gandhi, A. 2017. Information Security Awareness Level Measurement for Employee: Case Study at Ministry of Research, Technology, and Higher Education. *International Conference on Science in Information Technology* 654–658.

[4] MAMPU. 2010a. *Dasar Keselamatan ICT Unit Pemodenan T adbiran dan Perancangan Pengurusan Malaysia (MAMPU) Jabatan Perdana Menteri*. *MAMPU*. Retrieved from https://www.mampu.gov.my/ms/warga-mampu/dasar- keselamatan-ict.

[5] Bharathi, S. & Suguna, J. 2014. A Conceptual Model To Understand Information Security A wareness. *International Journal of Engineering Research & Technology* 3(8).

[6] CyberSecurity Malaysia. 2019. Incident Statistics: Reported Incidents based on General Incident Classification Statistics 2019. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=963fc7d8-b979-48f3-a413-ba7c24561911 [15 June 2019].

[7] Findlay, V. 2016. No Cyber Threats Against Police. *National Police Foundation*. https://www.policefoundation.org/cyber-threats-a-glocal-problem-for-law-enforcement/ [28 June 2019].

[8] Vredeveldt, A., Kesteloo, L. & Koppen, P. J. van. 2018. Writing Alone or Together: Police Officers' Collaborative Reports of an Incident. *Criminal Justice and Behavior* 45(7): 1071–1092. doi:10.1177/0093854818771721.

[9] Whittaker, Z. 2019. Hackers Publish Personal Data on Thousands of US Police Officers and Federal Agents. *TechCrunch*. https://techcrunch.com/2019/04/12/police-data- hack/ [28 June 2019].

[10] Chen, Y., Ramamurthy, K. (Ram) & Wen, K.-W. 2015. Impacts of Comprehensive Information Security Programs on Information Security Culture. *The Journal of Computer Information Systems* 55(3): 11.

[11] Humaidi, N. & Vimala Balakrishnan. 2013. Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security. *Journal of Health & Medical Informatics* 04(02): 2–9. doi:10.4172/2157-7420.1000123.

[12] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. 2014. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security* 42. doi:10.1016/j.cose.2013.12.003.

[13] Ramalingam, R., Lakshminarayanan, R. & Khan, S. 2014. *Information Security Awareness at Oman Educational Institutions: An Academic Perspective*.

[14] Pattinson, M. R. and Anderson, G. (2007) 'How Well Are Information Risks Being Communicated to Your Computer End-users?', *Information Management and Computer Security*, 15(5), pp. 362–371. doi: 10.1108/09685220710831107.

[15] Muhson, A. 2006. Teknik Analisis Kuantitatif. Retrieved from http://staffnew.uny.ac.id/upload/132232818/lainlain/Ali+Muhson+(2006)+Analisis+Kuantitatif.pdf.

[16] Siddharth Kalla (2009) *Statistical Mean, Explorable.com*.

[17] Rumsey, D. J. (2009) 'Why Mean and Median Are Both Important in Statistical Data', in *Statistics II for Dummies*. 1st Edition. For Dummies. Available at: https://www.dummies.com/education/math/statistics/why-mean-and-median-are-both-important-in-statistical-data/.

[18] Joseph F. Hair, J., Black, W. C., Babin, B. J. & Anderson, R. E. 2010. Multivariate Data Analysis. *Pearson*, hlm. Seventh Ed. Pearson. doi:10.1016/j.foodchem.2017.03.133.

[19] Costello, A. B. & Osborne, J. W. 2005. Best Practices in Exploratory Factor Analysis: Four Recommendations for Getting the Most From Your Analysis. *Practical Assessment, Research and Evaluation* 10(7).

[20] Landell, K. 1997. Management by Menu. London: John Wiley & Sons, Inc.