Model Kesedaran Keselamatan Maklumat Peranti Mudah Alih Dalam Kalangan Pekerja Syarikat Swasta

Mohd Hanis Bin Jenalis
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
hanisjenalis@gmail.com

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

ABSTRAK

Peningkatan penggunaan peranti mudah alih seperti telefon pintar dan komputer riba di tempat kerja mengundang kebimbangan terhadap keselamatan maklumat. Perkara utama yang menjadi kebimbangan adalah tahap keselamatan maklumat yang terdiri daripada data peribadi, kata laluan dan maklumat sensitif yang terdapat dalam kedua-dua peranti. Oleh itu, satu kajian terhadap tahap kesedaran keselamatan maklumat peranti mudah alih diperlukan untuk mengenal pasti faktor yang mempengaruhi tahap kesedaran keselamatan maklumat pekerja swasta. Kajian lampau hanya memfokus kepada faktor asas dan fokus tertentu yang mempengaruhi tahap kesedaran keselamatan maklumat khususnya untuk organisasi kerajaan. Tujuan kajian ini adalah untuk membangunkan model kesedaran yang dapat menilai tahap kesedaran keselamatan maklumat dalam penggunaan peranti mudah alih dalam kalangan pekerja syarikat swasta. Model yang dipilih terdiri daripada Model *Knowledge-Attitude-Behavior (KAB)* dan model kesedaran keselamatan maklumat, Model *Human Aspect of Information Security Questionnaire (HAIS-Q)*. Kajian ini menggunakan analisis kualitatif (temubual) dan kuantitatif (kaji selidik) dan model yang dibangunkan terdiri daripada 6 komponen faktor iaitu pengetahuan, tingkah laku, sikap, sokongan pihak pengurusan, latihan dan pendidikan dan polisi/dasar keselamatan maklumat. Kajian kes telah dilaksanakan di syarikat swasta berasaskan IT iaitu BIT Group Sdn Bhd yang terdiri daripada 7 anak syarikat. Borang soal selidik telah dihantar menggunakan emel dan seramai 75 responden telah memberikan maklumbalas. Analisis soal selidik menggunakan ujian kebolehpercayaan, ujian skor min, analisis faktor dan analisis korelasi Pearson. Hasil kajian mendapati indeks kebolehpercayaan setiap komponen soalan kaji selidik adalah baik dengan nilai *Cronbach Alpha* di antara 0.700 hingga 0.889. Menerusi ujian skor min, nilai yang diperoleh untuk setiap komponen adalah di antara 3.48 hingga 6.79. Hasil analisis faktor pula memberikan 8 komponen pemboleh ubah iaitu Pengurusan Kata Laluan (PM), Penggunaan Internet (IU), Penggunaan Emel (EU), Pengendalian Maklumat (IH), Penggunaan Rangkaian Media Sosial (SMU), Polisi Syarikat (CP), Taklimat Keselamatan Maklumat (ISB) dan Latihan Kesedaran Keselamatan Maklumat (ISAT). Analisis korelasi *Pearson* pula menunjukkan hubungan yang sederhana dan kuat serta signifikan antara semua faktor. Model ini diharap dapat membantu pihak syarikat dan para pekerja swasta untuk lebih peka dan mengambil langkah keselamatan maklumat bagi melindungi maklumat peribadi pada peranti mudah alih yang berisiko tinggi seperti telefon pintar dan komputer riba.

Kata kunci—tahap kesedaran; keselamatan maklumat; peranti mudah alih; syarikat swasta

1. PENGENALAN

Penggunaan peranti mudah alih seperti telefon pintar, komputer riba dan tablet amat popular digunakan di tempat kerja kerana fleksibiliti dan ia bersifat peribadi. Ramai pekerja terutama di syarikat swasta menggunakan peranti mudah alih peribadi. Peningkatan penggunaan peranti mudah alih di tempat kerja mengundang kebimbangan terhadap keselamatan maklumat. Perkara utama yang menjadi kebimbangan adalah tahap keselamatan maklumat yang terdiri daripada data peribadi, kata laluan dan maklumat sensitif yang terdapat dalam peranti mudah alih.

Sekiranya tahap kesedaran keselamatan maklumat berkaitan dengan peranti mudah alih ditingkatkan, ia akan menjadi antara faktor penyumbang kepada kejayaan sesebuah organisasi. Oleh itu, keselamatan teknologi maklumat perlu menjadi keutamaan dan merupakan cabaran dalam sesebuah organisasi [1] bagi mengekal aspek keselamatan maklumat iaitu kerahsiaan, ketersediaan dan integriti [2] perlu dijaga.

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 swasta, keselamatan maklumat adalah lebih penting kerana melibatkan maklumat kerahsiaan, keselamatan dan perlindungan data. Pendekatan proaktif harus diambil oleh organisasi demi melindungi keselamatan maklumat dalam persekitaran semasa [4]. Langkah proaktif ini wajar bermula dari peringkat kumpulan pengurusan tertinggi, diikuti dengan kumpulan pengurusan profesional dan kumpulan pelaksana dengan menguatkuasakan dan mematuhi dasar keselamatan maklumat organisasi [5].

Teknologi maklumat semakin berkembang dari hari ke hari. Pelbagai jenis peranti mudah alih digunakan untuk berkomunikasi melalui internet. Peranti mudah alih ini juga dipanggil gajet peribadi. Gajet peribadi atau lebih dikenali sebagai *Bring Your Own Device* (*BYOD*) merupakan situasi apabila pekerja di sebuah organisasi diberi kebenaran menggunakan gajet dan aplikasi milik sendiri. Gajet peribadi seperti komputer riba, peranti storan mudah alih, telefon pintar dan tablet adalah contoh gajet peribadi yang dibenarkan dibawa ke organisasi. Gajet seperti telefon pintar dan komputer riba mudah dibawa ke mana-mana dan penggunaannya sangat membantu mereka. Segala maklumat boleh didapati di dalam gajet peribadi masing-masing [6]. Lagipun harga pasaran untuk memiliki gajet peribadi terutamanya telefon pintar tidaklah terlalu tinggi yang mana ia mampu dimiliki oleh semua golongan.

Reka bentuk telefon pintar kecil dan ringan menyebabkan semua kategori umur suka menggunakannya terutama jika terdapat kemudahan internet [7]. Kebanyakan telefon pintar dan komputer riba mempunyai kemudahan *built-in WiFi* yang membolehkan pengguna untuk membuat sambungan internet sama ada melalui internet hotspot peribadi mahupun yang terbuka *(open Wireless Fidelity (WiFi)).* Pengguna tidak sedar bahaya mengguna *open WiFi* untuk mengakses internet [6].

Penggunaan peranti mudah alih seperti telefon pintar dan komputer riba dalam kalangan pekerja semakin meningkat dari tahun ke tahun. Peratusan capaian telefon pintar kekal pada 98.2% pada 2019. Manakala peratusan capaian isi rumah kepada komputer menurun kepada 71.3% pada 2019 berbanding 71.7% pada 2018 [8].

Bagi mengukur tahap kesedaran keselamatan maklumat, kaedah model kesedaran digunakan. Dengan menggunakan kaedah model kesedaran, ia dapat digunakan untuk mengukur pengetahuan, sikap dan tingkah laku pekerja untuk memberikan penanda aras kepada pengurusan organisasi, yang kemudian dapat digunakan untuk menilai keberkesanan strategi pengendalian tahap kesedaran keselamatan maklumat yang berbeza, atau untuk mengesan tahap keselamatan maklumat untuk jangka panjang organisasi [9]. Selain itu, kaedah model kesedaran juga digunakan untuk mengkaji hubungan antara pengetahuan mengenai polisi dan prosedur, sikap terhadap polisi dan prosedur dan tingkah laku ketika menggunakan peranti di organisasi [9].

Oleh itu, satu kajian perlu dilakukan bagi mengukur tahap kesedaran keselamatan maklumat dalam penggunaan peranti mudah alih mereka sama ada telefon pintar atau komputer riba, dan seterusnya mengkaji faktor-faktor lain yang mempengaruhi tahap kesedaran keselamatan maklumat mereka.

Kajian ini menggunakan gabungan beberapa model konseptual yang sedia ada iaitu:

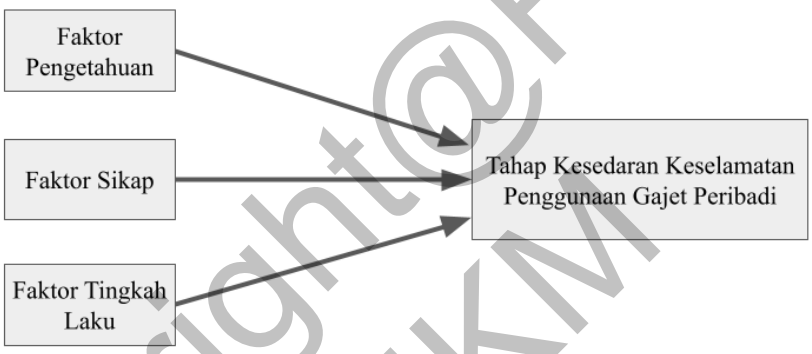
1) Model *Knowledge-Attitude-Behavior* (KAB) [10]
2) Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) [9]
3) Model *Information Security Awareness Identification* (ISAIM) [11]
4) Model Kesedaran Keselamatan Maklumat [12]

Beberapa komponen atau faktor daripada setiap model diadaptasi dan dipilih untuk dijadikan model baharu untuk diguna pakai bagi mengkaji tahap kesedaran keselamatan maklumat peranti mudah alih dalam kalangan pekerja syarikat swasta.

2. KAJIAN BERKAITAN

A. Model Knowledge-Attitude-Behavior (KAB)

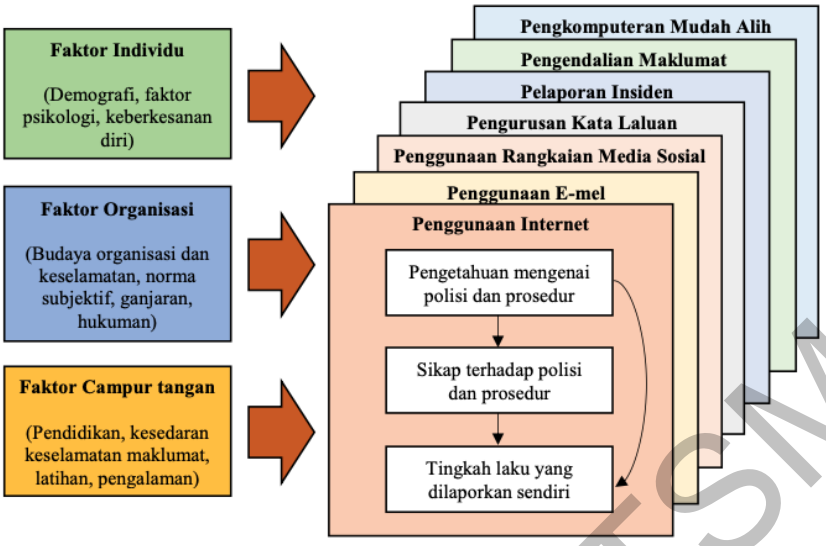
Model KAB (*Knowledge-Attitude-Behavior*) oleh [10] ini merujuk kepada teori psikologi sosial yang mencadangkan tiga komponen yang terlibat adalah i) kognitif, ii) kesan dan iii) tingkah laku. Komponen tersebut digunakan untuk membangunkan tiga faktor utama yang berkaitan dengan manusia dalam keselamatan maklumat yang terdiri daripada (i) pengetahuan (apa yang seseorang tahu), (ii) sikap (apa yang seseorang rasa mengenai sesuatu topik) dan iii) tingkah laku (apa yang seseorang buat). Kerangka kajian ini digunakan untuk mengenal pasti sejauh mana faktor pengetahuan, sikap dan tingkah laku dapat membantu dalam kesedaran keselamatan penggunaan gajet peribadi di tempat kerja. Rajah 1 menunjukkan kerangka kajian atau model konseptual yang telah diubahsuai daripada Model KAB (*Knowledge-Attitude-Behavior*) oleh [10].



RAJAH 1: KERANGKA KAJIAN YANG DIUBAHSUAI DARIPADA MODEL KRUGER DAN KEARNEY [10]

B. Model Human Aspect of Information Security Questionnaire (HAIS-Q)

[9] mengenal pasti tujuh (7) bidang fokus iaitu, (i) penggunaan Internet; (ii) penggunaan emel; (iii) penggunaan rangkaian media sosial; (iv) pengurusan kata laluan; (v) pelaporan insiden; (vi) pengendalian maklumat; dan (vii) pengkomputeran mudah alih seperti di Rajah 2.



RAJAH 2: MODEL HUMAN ASPECT OF INFORMATION SECURITY QUESTIONNAIRE (HAIS-Q) [9]

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

Model *Information Security Awareness Identification* (ISAIM) yang dibangunkan oleh [11] 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 3.

RAJAH 3: MODEL INFORMATION SECURITY AWARENESS IDENTIFICATION (ISAIM) [11]

D. *Model Kesedaran Keselamatan Maklumat*

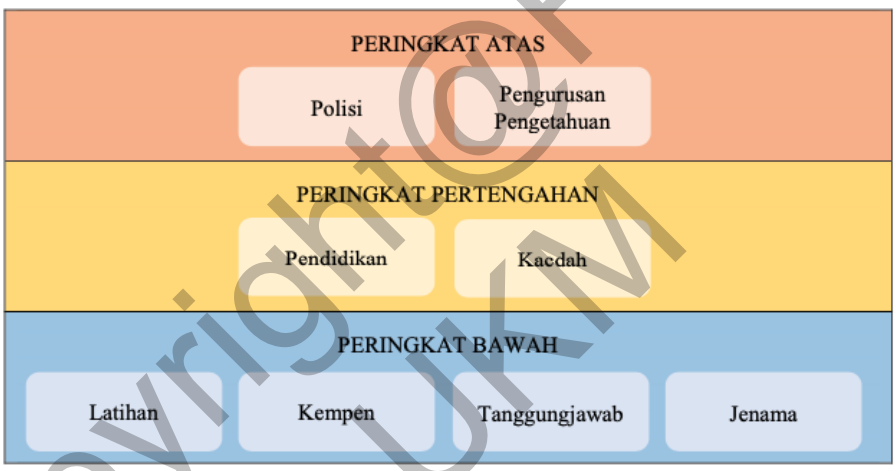
Berdasarkan kajian daripada [12], kesedaran keselamatan adalah sebahagian daripada keselamatan maklumat organisasi. Keselamatan maklumat setiap organisasi adalah bergantung kepada faktor dalaman dan luaran. Melalui penyelesaian kesedaran yang tepat, maklumat organisasi dapat dipelihara dari ancaman dalam dan luar. Selain itu, polisi keselamatan maklumat tertumpu kepada

pengurusan maklumat dan latihan kepada kakitangan. Polisi keselamatan maklumat harus diperkenalkan dari peringkat atasan hingga bawahan bagi memenuhi syarat dan harus dikaji dari semasa ke semasa. Oleh kerana kurangnya kesedaran tentang keselamatan maklumat dalam kalangan pekerja dalam organisasi, polisi sering dikaji dan ditambah baik untuk melindungi maklumat dari sebarang kebocoran atau kecurian data. Model Kesedaran Keselamatan Maklumat [12] diklasifikasikan kepada tiga (3) peringkat iaitu peringkat atas, peringkat pertengahan dan peringkat bawah seperti di Rajah 4.

RAJAH 4: MODEL KESEDARAN KESELAMATAN MAKLUMAT [12]

E. Kajian Lampau

1) Model Knowledge-Attitude-Behavior (KAB) Sebagai Faktor Kesedaran Keselamatan Penggunaan Gajet Peribadi

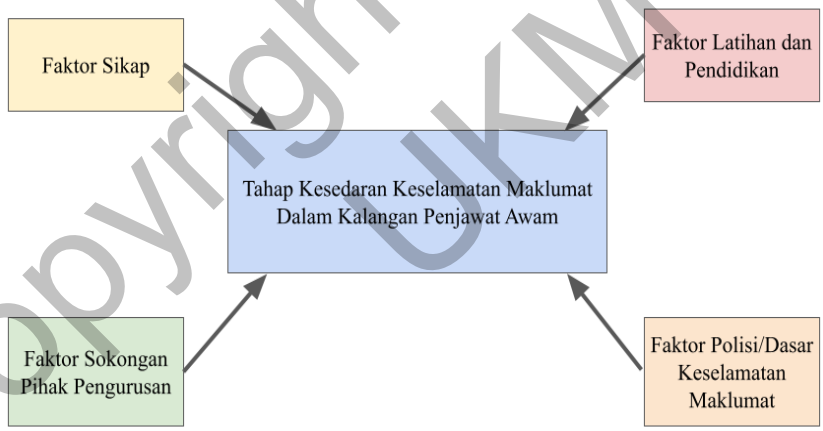


Theory of Planned Behavior (TBA) adalah lanjutan daripada *Theory of Reasoned Action* (TRA) iaitu tingkah laku manusia didorong oleh niat individu yang mana niat dipengaruhi oleh sikap seseorang [13] Menurut [14], apabila TBA dan TRA digabungkan, ianya lebih cenderung untuk mencadangkan kesedaran keselamatan dipengaruhi oleh pengetahuan serta sikap pengguna terhadap keselamatan maklumat dan tingkah laku mereka. Niat pekerja yang positif dipengaruhi oleh kepercayaan normatif dan keberkesanan diri untuk mematuhi dasar-dasar keselamatan. Walaupun penggunaan gajet peribadi memberi impak positif di sesebuah organisasi, namun setiap organisasi perlu melihat impak di sebaliknya kepada sesebuah organisasi. Kecuaian staf yang membawa gajet peribadi dan menggunakan rangkaian organisasi secara tidak langsung boleh memberi kesan kepada organisasi. Kajian oleh [15]; [16], mendapati responden yang mempunyai pengetahuan (*Knowledge*) mengenai keselamatan, lebih menyedari kewujudan perisian hasad (*malware*) di dalam telefon pintar mereka. Menurut [17], sikap (*Attitude*) dipengaruhi oleh beberapa faktor seperti pengalaman

peribadi, kebudayaan, pengaruh orang lain yang dianggap penting, media massa serta faktor emosi dalaman seseorang individu. Selain itu, tingkah laku (*Behavior*) seseorang merupakan suatu perkara yang harus diberi perhatian. Walaupun segelintir pengguna tahu tindakan mereka boleh memberi implikasi kepada diri sendiri mahupun organisasi, mereka memilih jalan mudah untuk membuat sesuatu kerja [18].

2) Model Tahap Kesedaran Keselamatan Dalam Kalangan Penjawat Awam

Kesedaran keselamatan maklumat merangkumi tahap kefahaman para pekerja terhadap ancaman keselamatan maklumat yang boleh mempengaruhi proses organisasi dan juga pemahaman mereka terhadap kepentingan mematuhi tingkah laku keselamatan maklumat untuk mencegah ancaman keselamatan maklumat [19]. Terdapat empat (4) faktor utama yang mempengaruhi tahap kesedaran keselamatan seseorang terutamanya dalam kalangan penjawat awam antara ialah i) faktor sikap, ii) faktor sokongan pihak pengurusan, iii) faktor latihan dan pendidikan dan iv) faktor polisi atau dasar keselamatan maklumat [20]. Rajah 5 menunjukkan secara ringkas bagaimana faktor-faktor ini mempengaruhi tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam.



RAJAH 5: RINGKASAN KEPADA FAKTOR-FAKTOR YANG MEMPENGARUHI MODEL TAHAP KESEDARAN KESELAMATAN MAKLUMAT DALAM KALANGAN PENJAWAT AWAM [20]

3) Model Tahap Keselamatan Maklumat Dalam Kalangan Pekerja Di Pusat Analisis Dan Perkhidmatan Maklumat Suruhanjaya Kehakiman Republik Indonesia

Kajian ini bertujuan untuk mengukur kesedaran pekerja mengenai keselamatan maklumat di Pusat Analisis dan Perkhidmatan Maklumat (*Palinfo*) di Suruhanjaya Kehakiman Republik Indonesia, yang juga merangkumi Jabatan Data / IT. Kajian ini telah dijalankan melalui sesi temu bual dengan tiga pakar dan soal selidik kesedaran keselamatan maklumat kepada semua kakitangan *Palinfo*, berjumlah 25 orang. Hasil soal selidik dinilai menggunakan Model *Human Aspects of Information Security Questionnaire* (HAIS-Q) dan kaedah *Analytic Hierarchy Process* (AHP). Hasil kajian menunjukkan bahawa tahap kesedaran keselamatan maklumat di *Palinfo* dan Jabatan Data / IT adalah pada tahap sederhana; namun terdapat satu fokus tumpuan yang menunjukkan tahap yang baik. di Jabatan Data / IT, beberapa bahagian menunjukkan tahap yang baik. Berdasarkan keputusan kajian ini, [21] mencadangkan bagi mengekalkan keselamatan maklumat, mereka menggunakan tujuh (7) bidang fokus, sepuluh (10) pendekatan teknologi maklumat dan latihan yang dijalankan dalam pelbagai cara.

Oleh itu, kajian lebih lanjut diperlukan untuk mengukur tahap kesedaran keselamatan maklumat untuk mengenal pasti bidang keselamatan maklumat yang masih perlu ditingkatkan untuk mengembangkan strategi atau kaedah kesedaran keselamatan maklumat yang lebih sesuai. Pelbagai kerangka kajian yang telah digunakan untuk mengukur tahap kesedaran keselamatan maklumat. Menurut [21], dalam kajian ini mereka memilih Model *Knowledge Attitude Behavior* (KAB) yang dihasilkan oleh [10] dan juga digabungkan dengan *Analytic Hierarchy Process* (AHP). Model KAB sering digunakan sebagai salah satu model yang sesuai digunakan untuk mengukur tahap kesedaran keselamatan maklumat [22].

F. Cadangan Model Awal

Cadangan model awal bagi kajian ini adalah berdasarkan kepada pemilihan komponen yang mempengaruhi kesedaran keselamatan maklumat dalam penggunaan peranti mudah alih seperti faktor pengetahuan, faktor sikap, faktor tingkah laku, faktor sokongan pihak pengurusan, faktor latihan dan pendidikan dan faktor polisi/dasar keselamatan maklumat. Gabungan daripada beberapa komponen kajian sedia ada dan enam (6) faktor telah dipilih sebagai komponen untuk pembangunan model awal seperti Jadual 1.

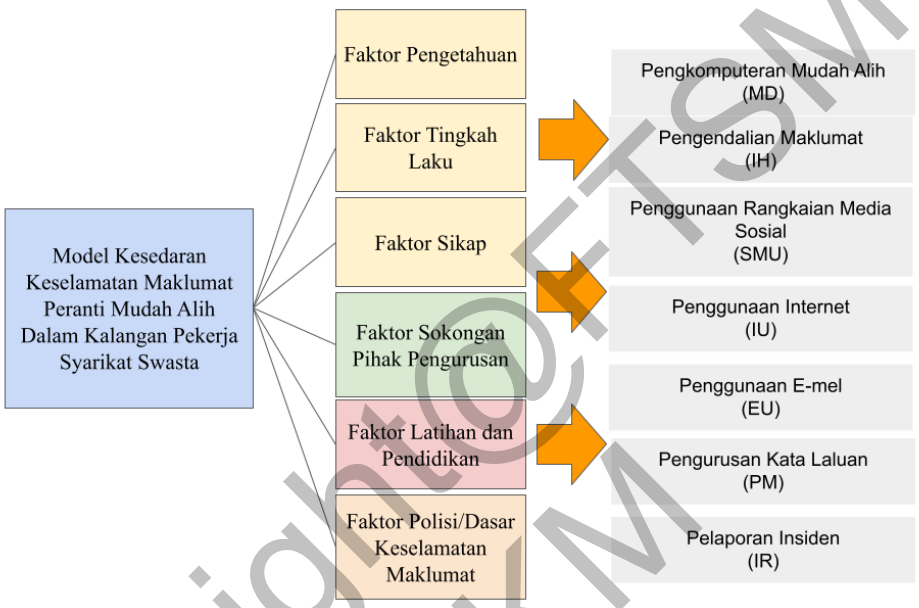
JADUAL 1: ENAM (6) FAKTOR YANG DIPILIH DALAM PEMBANGUNAN MODEL AWAL

Komponen (Faktor Kesedaran)	**Rumusan Kajian / Model**
Faktor Pengetahuan	Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi kekurangan pengetahuan. ● Pengetahuan adalah tahap kecekapan dan kecerdasan dan jumlah ilmu

	yang dimiliki oleh manusia dalam konteks organisasi. Pengetahuan telah diiktiraf sebagai salah satu faktor untuk pengeluaran [23]. ● Kajian oleh [15]; [16], mendapati responden yang mempunyai pengetahuan mengenai keselamatan, lebih menyedari kewujudan perisian hasad (*malware*) di dalam telefon pintar mereka. Selain daripada itu, kajian yang dijalankan oleh [16] mendapati responden melakukan penyulitan (*encryption*) ke atas data mereka.
Faktor Tingkah Laku	Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi tindakan dan tingkah laku. ● 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 [24]. ● Kajian menunjukkan segelintir pengguna tahu tindakan mereka boleh memberi implikasi kepada diri sendiri mahupun organisasi, mereka memilih jalan mudah untuk membuat sesuatu kerja [18].
Faktor Sikap	Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi faktor dalaman seseorang terhadap isu berkaitan keselamatan maklumat. ● Sikap adalah perasaan umum atau pendapat seseorang mengenai sesuatu [25], Ia adalah pengawal tingkah laku sebenar seseorang secara sedar atau tidak secara sedar. ● Sikap dipengaruhi oleh beberapa faktor seperti pengalaman peribadi, kebudayaan, pengaruh orang lain yang dianggap penting, media massa serta faktor emosi dalaman seseorang individu [26]. ● Sikap mengabaikan mesej memberi kebenaran (*need access to)* semasa memuat turun atau memasang aplikasi secara tidak langsung membuka ruang kepada penjenayah siber untuk mengancam gajet peribadi untuk mendapatkan data peribadi pengguna mahupun data organisasi [17].
Faktor Sokongan Pihak Pengurusan	Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi isu kepimpinan pihak pengurusan. ● Sokongan pihak pengurusan merujuk kepada komitmen daripada pihak pengurusan di dalam organisasi seperti yang dilihat oleh pekerja [27]. ● Sokongan penuh daripada pihak pengurusan di dalam mana-mana organisasi adalah penting kerana ia dapat memastikan keberkesanan sistem keselamatan maklumat dan boleh menghasilkan persekitaran yang selamat untuk pengendalian maklumat [28];[26];[29].
Faktor Latihan dan Pendidikan	Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi kekurangan latihan dan pendidikan. ● Kesedaran keselamatan maklumat boleh dicapai melalui latihan keselamatan pekerja kerana latihan adalah salah satu cara untuk menyampaikan maklumat keselamatan siber organisasi [30]. ● Latihan keselamatan maklumat juga dapat meningkatkan kemahiran pekerja untuk menggunakan sistem keselamatan dengan betul yang dapat mencegah ancaman keselamatan [31]; [32]. bersambung...
...sambungan Faktor Polisi/Dasar Keselamatan Maklumat	Kajian terhadap kesilapan manusia yang sering berlaku terhadap pelanggaran keselamatan maklumat menerusi penguatkuasaan dan pematuhan polisi dan dasar keselamatan maklumat. ● Polisi atau dasar keselamatan maklumat kepada bagi melindungi maklumat organisasi menerusi Model Kesedaran Keselamatan Maklumat [12]. ● Kajian semasa menunjukkan bahawa polisi atau dasar keselamatan

maklumat yang didokumentasi dengan baik dengan penerangan yang jelas dapat meningkatkan kesedaran pengguna tentang keselamatan maklumat [33].

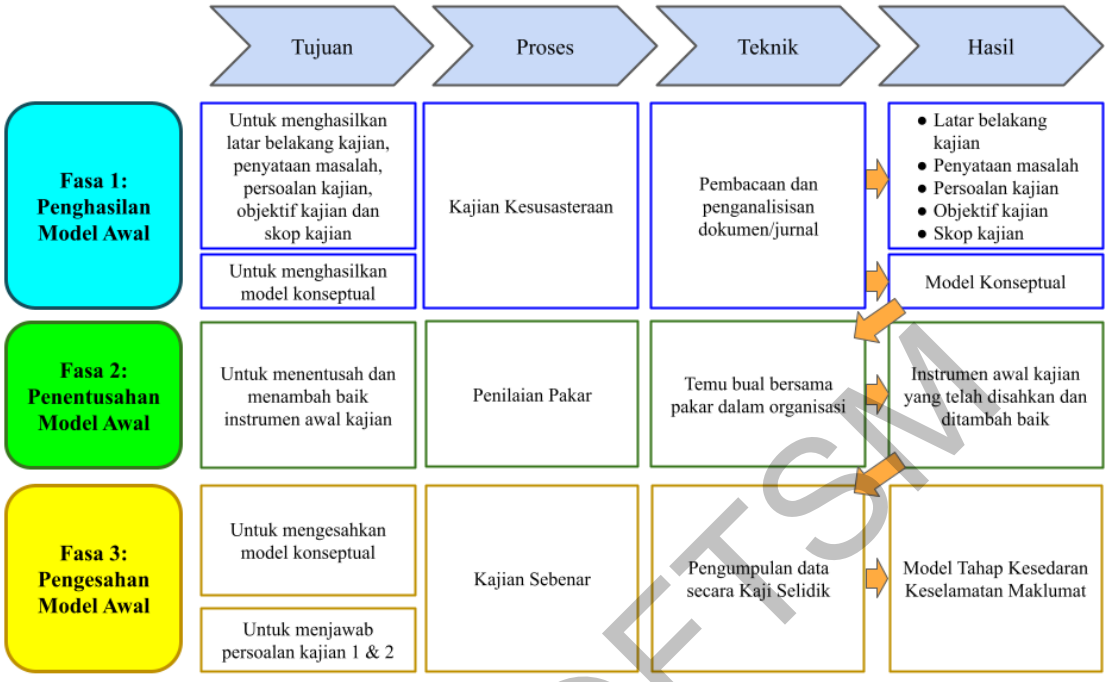
Enam (6) faktor dan tujuh (7) sub-bidang sedia ada yang mempengaruhi tahap kesedaran keselamatan maklumat berdasarkan kajian lampau digabungkan. Rumusan pemilihan komponen yang dipilih daripada kajian sedia ada adalah seperti Rajah 6.



RAJAH 6: MODEL AWAL HASIL GABUNGAN ENAM (6) FAKTOR DAN TUJUH (7) SUB-BIDANG SEDIA ADA YANG DIADAPTASI DARI MODEL KNOWLEDGE-ATTITUDE-BEHAVIOR (KAB) (JACEY MARIADASS ET AL. 2017), MODEL TAHAP KESEDARAN KESELAMATAN MAKLUMAT DALAM KALANGAN PENJAWAT AWAM (MOHD RAFIZAM MOHAMED ET AL. 2018) DAN MODEL HUMAN ASPECT OF INFORMATION SECURITY QUESTIONNAIRE (HAIS-Q) (MAINAR SWARI MAHARDIKA ET. AL 2020).

3. PENDEKATAN KAJIAN

Kajian ini dilaksanakan secara kaedah persampelan dengan melibatkan responden yang terdiri daripada para pekerja di syarikat swasta. Pendekatan kajian dilaksanakan merupakan gabungan kaedah kualitatif dan kuantitatif. Pendekatan kajian terbahagi kepada tiga (3) fasa iaitu penghasilan model awal, penentusahan model awal dan pengesahan model awal. Setiap fasa mempunyai beberapa aktiviti yang dirancang mengikut keutamaan berdasarkan kesesuaian organisasi yang dikaji. Gambaran pendekatan kajian adalah seperti di dalam Rajah 7.



RAJAH 7: PENDEKATAN KAJIAN

A. Penghasilan Model Awal

1) Mengenal Pasti Permasalahan Kajian

Permulaan kajian dimulakan dengan melaksanakan kajian susastera untuk mendapatkan maklumat berkaitan kajian. Proses mendapatkan maklumat tertumpu pada pembacaan, rujukan dan analisis daripada jurnal, buku, artikel, garis panduan dan dokumen berkaitan dengan kajian.

Analisis tersebut bertujuan untuk mendapatkan latar belakang kajian, penyataan masalah, persoalan kajian, objektif kajian dan skop kajian serta untuk menghasilkan model konseptual. 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, tesis, buku, model berkaitan, garis panduan, laman web rasmi dan dokumen	• Latar belakang kajian • Penyataan masalah • Persoalan kajian • Objektif kajian • Skop kajian

2) Merangka Model Awal

Proses yang terlibat dalam merangka model konseptual kajian adalah seperti di Jadual 3.

JADUAL 3: MERANGKA MODEL AWAL

Proses	Teknik	Hasil
Merangka model konseptual	● Pembacaan dan penganalisisan terhadap kajian kesusasteraan berkenaan tahap kesedaran keselamatan maklumat ● Jurnal, artikel, tesis, buku, model sedia ada, garis panduan, laman web rasmi dan dokumen berkaitan tahap kesedaran keselamatan maklumat	● Model konseptual kajian

Jadual 3 juga menerangkan bagaimana proses merangka model awal kajian dibuat. Selain itu, untuk merangka model awal kajian, kajian kesusasteraan terhadap asas teori kerangka kerja lampau berkaitan sistem keselamatan maklumat turut dilakukan. Hasil kajian kesusasteraan berkenaan kajian kesedaran keselamatan maklumat sedia ada ini telah berjaya menghasilkan model awal kajian yang menggabungkan dua (2) model utama dan huraian sub-bidang menerusi model seterusnya sebagaimana diterangkan dengan terperinci.

Pembangunan model konseptual dibangunkan dengan mengenal pasti model kesedaran yang sedia ada iaitu model daripada (i) Model *Knowledge-Attitude-Behavior* (KAB) [10] (ii) Model Tahap Kesedaran Keselamatan Maklumat Dalam Kalangan Penjawat Awam [20]; dan (iii) *Human Aspect of Information Security Questionnaire* (HAIS-Q) [9].

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 daripada setiap model yang terlibat adalah seperti di Jadual 4.

JADUAL 4: PEMILIHAN KOMPONEN SETIAP MODEL

Bil	Model	Komponen
1	Model *Knowledge-Attitude-Behavior*	● Faktor Pengetahuan

	(KAB)	• Faktor Sikap • Faktor Tingkah Laku
2	Model Tahap Kesedaran Keselamatan Maklumat Dalam Kalangan Penjawat Awam	• Faktor Sikap • Faktor Sokongan Pihak Pengurusan • Faktor Latihan dan Pendidikan • Faktor Polisi/Dasar Keselamatan Maklumat
3	*Human Aspect of Information Security Questionnaire* (HAIS-Q)	• Pengkomputeran Mudah Alih (MD) • Pengendalian Maklumat (IH) • Penggunaan Rangkaian Media Sosial (SMU) • Penggunaan Internet (IU) • Penggunaan Email (EU) • Pengurusan Kata Laluan (PM) • Pelaporan Insiden (IR)

Berdasarkan komponen yang dipilih, setiap komponen memainkan peranan yang penting dalam kajian ini. Ringkasan komponen yang terlibat adalah seperti di Jadual 5:

JADUAL 5: RINGKASAN KOMPONEN YANG DIPILIH.

Bil	Komponen	Penerangan
1	Faktor Pengetahuan	Bagi mengukur tahap pengetahuan sedia ada mengenai keselamatan maklumat, ancaman siber dan langkah-langkah keselamatan maklumat.
2	Faktor Tingkah Laku	Bagi mengukur tahap kepantasan, ketepatan dan kesediaan seseorang dalam melakukan tindakan berkaitan keselamatan maklumat.
3	Faktor Sikap	Bagi mengukur tahap kepekaan seseorang terhadap kesedaran keselamatan maklumat dari segi pengalaman peribadi, pengaruh dari orang lain dan pengaruh media massa.
4	Faktor Sokongan Pihak Pengurusan	Bagi mengukur tahap kepimpinan pihak pengurusan terhadap keselamatan maklumat dari segi sokongan, galakkan dan pelaksanaan pematuhan.
5	Faktor Latihan dan Pendidikan	Bagi mengukur tahap kesediaan dan kewajaran mengadakan sesi latihan kesedaran keselamatan maklumat dan kaedah pendidikan berterusan kepada semua pekerja.
6	Faktor Polisi/Dasar Keselamatan Maklumat	Bagi mengukur tahap penyediaan polisi dan dasar keselamatan maklumat oleh pihak pengurusan tertinggi kepada seluruh syarikat.
		bersambung...
	...sambungan	
7	Pengkomputeran Mudah Alih (MD)	Soal selidik akan berkisar tentang perkara berikut: • Memeriksa emel kerja melalui rangkaian percuma. • Memasukkan peranti USB.

		● Membiarkan bahan sensitif tidak dilindungi.
8	Pengendalian Maklumat (IH)	Soal selidik akan berkisar tentang perkara berikut: ● Melindungi peranti peribadi elektronik secara fizikal. ● Menghantar maklumat sensitif melalui rangkaian mudah alih. ● Membuang dokumen sensitif.
9	Penggunaan Rangkaian Media Sosial (SMU)	Soal selidik akan berkisar tentang perkara berikut: ● Jumlah masa kerja yang dihabiskan di rangkaian media sosial. ● Akibat daripada rangkaian media sosial. ● Memuat naik mengenai kerja di rangkaian media sosial.
10	Penggunaan Internet (IU)	Soal selidik akan berkisar tentang perkara berikut: ● Memasang perisian yang tidak dibenarkan. ● Melayari laman sesawang yang meragukan. ● Penggunaan Internet yang tidak sesuai.
11	Penggunaan Email (EU)	Soal selidik akan berkisar tentang perkara berikut: ● Memajukan (*forwarding*) emel. ● Membuka lampiran emel. ● Membuka pautan dalam emel.
12	Pengurusan Kata Laluan (PM)	Soal selidik akan berkisar tentang perkara berikut: ● Mengunci komputer. ● Perkongsian kata laluan. ● Memilih kata laluan yang baik.
13	Pelaporan Insiden (IR)	Soal selidik akan berkisar tentang perkara berikut: ● Melaporkan individu yang mencurigakan. ● Melaporkan tingkah laku buruk oleh rakan sekerja. ● Melaporkan semua insiden keselamatan.

B. Penentusahan Model Awal

Kaedah kajian adalah secara kualitatif melalui temubual untuk mendapatkan penentusahan terhadap model awal yang dibina. Dalam ini, penentusahan model awal dilaksanakan oleh dua (2) pakar dalam bidang sumber manusia dan transformasi dan pengurusan projek keselamatan siber. Model awal tersebut akan dipersetujui dan soalan kaji selidik akan diperbaiki mengikut cadangan penambahbaikan pakar dan seterusnya terhasil soalan kaji selidik yang telah ditambah baik. 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 6.

JADUAL 6: RINGKASAN KOMPONEN YANG DIPILIH.

Proses	**Teknik**	**Hasil**

Penentusahan model awal	● Temu bual bersama 2 orang pakar di dalam organisasi kajian	● Model awal kajian ditambah baik dan ditentusah

Sebelum soalan kaji selidik dibangunkan sepenuhnya, komponen soalan kaji selidik dipilih berdasarkan ciri-ciri yang terdapat di dalam Jadual 5. Komponen tersebut kemudiannya ditentusah dan dikomen oleh pakar di organisasi yang dikaji menerusi kaedah temu bual. 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.

Setelah soalan kaji selidik dikomen, diubahsuai, dipersetujui dan disahkan oleh pakar, akhirnya soalan kaji selidik dapat dibangunkan. Bagi memudahkan soalan kaji selidik disampaikan kepada responden, satu (1) kaedah digunakan, iaitu dengan menggunakan platform *Google Forms* (secara digital). Kaji selidik ini dijalankan secara digital kerana ketika kajian soal selidik ini dilakukan, semua pekerja bekerja dari rumah (*Work From Home, WFH*). Pengujian terhadap *Google Forms* juga dibuat terlebih dahulu untuk mengelak daripada kegagalan capaian dan kesilapan pada soalan. Soalan di *Google Forms* boleh dicapai di alamat [https://bit.ly/KajiSelidikKesedaranKeselamatanMaklumat]

C. Pengesahan Model Awal

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 Kesedaran Keselamatan Maklumat Peranti Mudah Alih Dalam Kalangan Pekerja Syarikat Swasta dapat dihasilkan. Menerusi kajian yang dijalankan juga dapat menjawab objektif dan persoalan kajian. Proses yang terlibat dalam mengesahkan model kajian adalah seperti di Jadual 7.

JADUAL 7: PENGESAHAN MODEL AWAL

Proses	**Teknik**	**Hasil**
Pengesahan model awal	● Kajian sebenar dan analisis menerusi kaji selidik	● Model kajian

3.1 ANALISIS DATA

Analisis data merupakan aktiviti yang penting dan amat diperlukan dalam proses kajian. Menurut [34], 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. Kesalahan 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. Menurut Dewan Bahasa dan Pustaka, statistik deskriptif menunjukkan darjah perkaitan atau perhubungan yang wujud antara dua pemboleh ubah kategori.

A. Ujian Kebolehpercayaan

Pekali *Cronbach Alpha* digunakan untuk mengukur kebolehpercayaan, atau konsistensi dalaman. Kebolehpercayaan membawa maksud 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* (1 hingga 7) itu boleh dipercayai atau tidak. Nilai *Cronbach Alpha* dicari untuk menentukan kebolehpercayaan item soal selidik. Menurut [35], 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.

B. Kekerapan dan Ujian Skor Min

Analisis deskriptif digunakan untuk mendapatkan kekerapan, min dan sisihan piawai untuk memenuhi keperluan objektif yang ditentukan. Menurut [36], konsep min statistik mempunyai tahap penerapan yang sangat luas dalam statistik untuk sejumlah jenis eksperimen yang berbeza. Tambahnya lagi, kekerapan dan min memberikan maklumat penting mengenai set data yang ada dan sebagai satu nombor dapat memberikan banyak pandangan tentang eksperimen dan sifat data tersebut. Menurut kajian daripada [37], min atau purata adalah statistik 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 pula digunakan 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 [35] menyatakan bahawa, analisis faktor adalah bertujuan untuk mengurangkan dan merumuskan data yang melibatkan item yang berulang digabungkan dan item yang tidak berkaitan digugurkan. Menurut [38] 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. Penyederhanaan dimaksimumkan apabila hanya terdapat nilai 0 dan 1 dalam lajur. Dalam kaedah ini terdapat kecenderungan untuk menghasilkan beberapa nilai pemuatan faktor tinggi (dekat dengan -1 atau +1) dan beberapa nilai pemuatan faktor mendekati 0 di setiap lajur matriks. Logik penafsiran lebih mudah apabila korelasi antara faktor dan pemboleh ubah adalah +1 atau -1 kerana menunjukkan perkaitan sempurna yang positif atau negatif. Selain itu, kaedah putaran *varimax* dilakukan kerana dapat mengurangkan jumlah pemboleh ubah yang kompleks dan dapat meningkatkan hasil jangkaan.

D. Ujian Korelasi

Menurut [39], korelasi merupakan kaedah statistik yang menentukan hubungan dan menunjukkan kekuatan antara pemboleh ubah bagi tujuan untuk mencari nilai statistik yang menyatakan hubungan di antara pemboleh ubah. Manakala menurut [40] pula, korelasi adalah kajian mengenai hubungan linear di antara dua pemboleh ubah dan ukuran untuk menentukan darjah perkaitan ialah pekali korelasi. Pekali korelasi yang kerap digunakan oleh penyelidik ialah pekali *Pearson* iaitu untuk menentukan hubungan antara dua pemboleh ubah aras selang dan nisbah.

Menerusi kajian oleh [41], korelasi *Pearson* digunakan untuk mengukur dan menilai hubungan antara dua atau lebih pemboleh ubah selanjar dan linear. Tambahannya lagi, nilai pekali korelasi ini antara -1 hingga +1 menunjukkan tiga kemungkinan hubungan, iaitu hubungan positif (+), hubungan negatif (-) atau tiada hubungan ($r=0$); dan tanda (+) atau (-) masing-masing

menjelaskan arah hubungan yang positif atau negatif, manakala nilai mutlaknya pula menjelaskan kekuatan hubungan.

4. HASIL PENGUJIAN

A. Hasil Penentusahan Model Awal

Penghasilan model awal kajian dihasilkan berdasarkan kepada kajian kesusasteraan yang dijalankan terhadap kajian lampau dan model sedia ada. Enam (6) komponen utama telah dipilih sebagai domain untuk pembangunan model awal hasil daripada gabungan komponen utama daripada model sedia ada. Enam (6) komponen tersebut merupakan faktor yang mempengaruhi tahap kesedaran keselamatan maklumat dalam penggunaan peranti mudah alih dalam kalangan pekerja swasta seperti (i) faktor pengetahuan; (ii) faktor tingkah laku; (iii) faktor sikap; (iv) faktor sokongan pihak pengurusan; (v) faktor latihan dan pendidikan; dan (vi) faktor polisi/dasar keselamatan maklumat.

Bagi menentusah model awal kajian, enam (6) komponen yang telah dikenal pasti pada fasa penghasilan model awal diperincikan dalam bentuk soalan kaji selidik. Pengesahan tersebut dibuat secara temu bual dan penilaian bersama pakar yang telah dikenal pasti. Daripada soalan kaji selidik yang dicadangkan, pakar berpendapat komponen yang terlibat sudah mencukupi dan menepati keperluan Bahagian Sumber Manusia tetapi memerlukan penambahbaikan dari segi bentuk soalan yang ditanya dan kaedah ia ditanya.

Pakar juga bersetuju untuk menggunapakai model kesedaran yang sedia ada yang dibincangkan dalam kajian kesusasteraan (i) Model *Knowledge-Attitude-Behavior* (KAB) [10] (ii) Model Tahap Kesedaran Keselamatan Maklumat Dalam Kalangan Penjawat Awam [20]; dan (iii) *Human Aspect of Information Security Questionnaire* (HAIS-Q) [9].

B. Hasil Pengesahan Model Awal

Dapatan sesi penentusahan dari pakar daripada kedua-dua syarikat swasta dikumpul dan dianalisis. Oleh kerana faktor kekangan masa oleh pakar dan kekangan untuk berjumpa di pejabat, proses pengesahan ini dijalankan secara atas talian, iaitu menggunakan kemudahan aplikasi *Zoom, Google Docs & Google Form*. Keputusannya, kedua-dua pakar bersetuju dengan model awal yang dibangunkan dengan penambahbaikan yang perlu dilakukan sedikit pada soalan kaji selidik.

Soalan kaji selidik diagih secara serentak dan secara atas talian kepada pihak Sumber Manusia. Pihak Sumber Manusia kemudiannya menghantar soalan kaji selidik melalui emel kepada

semua staf di BIT Group Sdn Bhd dan tujuh (7) anak syarikat di bawahnya. Kumpulan sasaran pula terdiri daripada (i) pengguna biasa (yang tidak melibatkan penggunaan sistem secara langsung); (ii) pengguna sistem; dan (iii) pentadbir sistem. Manakala kedudukan di dalam organisasi pula dipilih dalam kalangan kumpulan Pengurusan dan Profesional, kumpulan Pelaksana dan kumpulan Sokongan sama ada pekerja Latihan Industri, *Contract For Services* (CFS), *Contract Of Services* (COS) dan Tetap (*Permanent*) yang melibatkan seramai 176 orang responden dalam kalangan pekerja swasta yang bernaung di bawah BIT Group dari seluruh Malaysia.

Borang kaji selidik telah dihantar melalui emel oleh Bahagian Sumber Manusia kepada 176 responden, namun 75 orang responden sahaja yang memberi maklum balas dan respon. Tempoh menjawab soalan kaji selidik adalah selama tiga (3) hari sahaja iaitu 11 hingga 13 Ogos 2021. Tempoh ini adalah sesuai bagi memudah responden menjawab soalan dengan tenang, tidak terburu-buru dan seterusnya memberi jawapan yang tepat.

C. Analisis Ujian Kebolehpercayaan

Nilai *Cronbach Alpha* dicari untuk menentukan kebolehpercayaan setiap item dalam soalan kaji selidik. Menurut [42], 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. Analisis ujian kebolehpercayaan dilakukan ke atas instrumen soalan kaji selidik dengan menggunakan perisian SPSS. Menurut [43], nilai *Cronbach's Coefficient Alpha* boleh mengukur tahap kebolehpercayaan items untuk menguji kesahihan soalan kaji selidik yang dibangunkan. Seramai sebelas (11) orang responden yang menjawab soalan kaji selidik ini sebagai kajian rintis dan untuk menilai kebolehpercayaan. Nilai kebolehpercayaan yang diperolehi daripada nilai *Cronbach Alpha* adalah di antara 0.700 hingga 0.889 seperti dalam Jadual 8. Nilai ini menunjukkan indeks kebolehpercayaan item adalah baik dan boleh diterima serta memenuhi ciri-ciri yang dikehendaki.

JADUAL 8: KEPUTUSAN UJIAN CRONBACH ALPHA PADA INSTRUMEN KAJIAN

Komponen	**Bilangan item yang diuji**	**Nilai *Cronbach Alpha***
Bahagian A : Faktor Pengetahuan	2	.889

Bahagian B : Faktor Tingkah Laku	7	.716
Bahagian C : Faktor Sikap	4	.700
Bahagian D : Faktor Sokongan Pihak Pengurusan	5	.811
Bahagian E : Faktor Latihan dan Pendidikan	4	.730
Bahagian F : Faktor Polisi/Dasar Keselamatan Maklumat	3	.808

D. Analisis Kekerapan dan Ujian Skor Min

Dalam kajian ini, tahap kesedaran keselamatan maklumat di antara penggunaan peranti mudah alih dalam kalangan pekerja swasta dinilai berdasarkan bilangan kekerapan dan analisis skor min mengikut faktor-faktor yang dikenal pasti pada model awal. Beberapa soalan dalam kaji selidik ini menggunakan Skala nominal (soalan berbentuk fakta dan pilihan) yang boleh diukur dengan mengkaji bilangan kekerapan dan Skala Pengukuran Likert bagi mengukur skor min. Nilai Skala Pengukuran Likert akan di kategori kepada tiga (3) iaitu rendah, sederhana dan tinggi untuk menentukan tahap kesedaran keselamatan maklumat. Skor min yang ditafsir sebagaimana yang dicadangkan oleh [44] adalah item yang dianalisis berada pada julat 1.00 hingga 3.26, ini menunjukkan tahap kesedaran keselamatan maklumat dalam kalangan pekerja berada pada tahap yang rendah. Keputusan sederhana pula merangkumi skor min antara 3.27 hingga 5.14. Manakala skor min 5.15 hingga 7.00 pula menunjukkan tahap kesedaran keselamatan maklumat dalam kalangan pekerja yang tinggi. Jadual 9 menunjukkan keseluruhan skor min dan tahap kesedaran responden untuk setiap hasil soalan kaji selidik yang dinilai.

JADUAL 9: KESELURUHAN SKOR MIN DAN TAHAP KESEDARAN RESPONDEN UNTUK SETIAP HASIL SOALAN KALI SELIDIK YANG DINILAI

Domain (Faktor Kesedaran)	Kod Item	Min (μ)	Tahap Kesedaran
Faktor Pengetahuan	A5	6.56	Tinggi
	A6	6.55	Tinggi
Faktor Tingkah Laku	B1	3.95	Sederhana
	B2	6.23	Tinggi
	B3	4.85	Sederhana
	B4	4.05	Sederhana
	B5	6.57	Tinggi
	B6	6.52	Tinggi
	B7	6.29	Tinggi
Faktor Sikap	C1	5.51	Tinggi
	C4	6.60	Tinggi
	C5	4.36	Sederhana
	C6	6.79	Tinggi
Faktor Sokongan Pihak Pengurusan	D1	6.56	Tinggi
	D2	6.77	Tinggi
	D3	6.36	Tinggi
	D4	3.48	Sederhana
Faktor Latihan dan Pendidikan	E1	3.60	Sederhana

	E4	5.60	Tinggi
Faktor Polisi/Dasar Keselamatan Maklumat	F3	6.21	Tinggi

(n=75)

E. Analisis Ujian Analisis Faktor

Analisis faktor adalah sebuah teknik yang digunakan untuk mencari faktor-faktor yang mampu menjelaskan hubungan atau korelasi antara pelbagai indikator tidak bersandar yang diperhatikan. Menurut [45], analisis faktor adalah alat analisis statistik yang digunakan untuk mengurangkan faktor-faktor yang mempengaruhi pemboleh ubah kepada beberapa set indikator, tanpa kehilangan maklumat yang signifikan.

Secara umum, proses analisis faktor adalah memilih pemboleh ubah yang patut dimasukkan dalam analisis faktor. Oleh kerana analisis faktor mengumpulkan nombor pemboleh ubah, maka ianya perlu menjadi korelasi (hubungan) yang cukup kuat di antara pemboleh ubah, sehingga wujudnya kumpulan tertentu. Setelah sejumlah pemboleh ubah dipilih, ianya diekstrak menjadi satu atau beberapa kumpulan pemboleh ubah. Kaedah yang sering digunakan bagi analisis faktor adalah *Principal Component Analysis (PCA)*. Jadual 10 menunjukkan keseluruhan komponen bagi setiap faktor menggunakan kaedah PCA.

JADUAL 10: KESELURUHAN KOMPONEN BAGI SETIAP FAKTOR MENGGUNAKAN KAEDAH PCA.

Domain	Komponen	Kod Item
Faktor Pengetahuan	Pengurusan Kata Laluan (PM)	A5, A6
Faktor Tingkah Laku	Penggunaan Internet (IU)	B1, B2, B7
	Pengendalian Maklumat (IH)	B3, B4
	Penggunaan Emel (EU)	B5, B6
Faktor Sikap	Pengurusan Kata Laluan (PM)	C1, C4
	Penggunaan Rangkaian Media Sosial (SMU)	C5, C6
Faktor Sokongan Pihak Pengurusan	Polisi Syarikat (CP)	D1, D2, D3
	Taklimat Keselamatan Maklumat (ISB)	D4, D5
Faktor Latihan dan Pendidikan	Latihan Kesedaran Keselamatan Maklumat (ISAT)	E1, E2, E3
	Taklimat Keselamatan Maklumat (ISB)	E4
Faktor Polisi/Dasar Keselamatan Maklumat	Polisi Syarikat (CP)	F1, F2, F3

F. Analisis Ujian Korelasi

Analisis korelasi *Pearson* digunakan untuk menguji dan menerangkan arah serta kekuatan hubungan antara enam (6) faktor iaitu pengetahuan, tingkah laku, sikap, sokongan pihak pengurusan, latihan dan pendidikan dan polisi/dasar keselamatan maklumat dengan lapan (8) pemboleh ubah iaitu Pengurusan Kata Laluan (PM), Penggunaan Internet (IU), Penggunaan Emel (EU),

Pengendalian Maklumat (IH), Penggunaan Rangkaian Media Sosial (SMU), Polisi Syarikat (CP), Taklimat Keselamatan Maklumat (ISB) dan Latihan Kesedaran Keselamatan Maklumat (ISAT).

Seterusnya adalah mengadakan ujian korelasi untuk menguji berapa kuat dan berapa signifikan hubungan faktor-faktor yang ada antara satu sama lain. Ujian analisis korelasi *Pearson* digunakan agar dapat memberikan sedikit petunjuk tentang pentingnya pemboleh ubah kepada faktor-faktor sedia ada. Bagaimanapun, kesemua item tersebut adalah wajar dipertimbangkan untuk dijadikan sebahagian komponen di dalam model kesedaran berdasarkan hasil analisis daripada putaran *varimax* dan analisis korelasi *Pearson.*

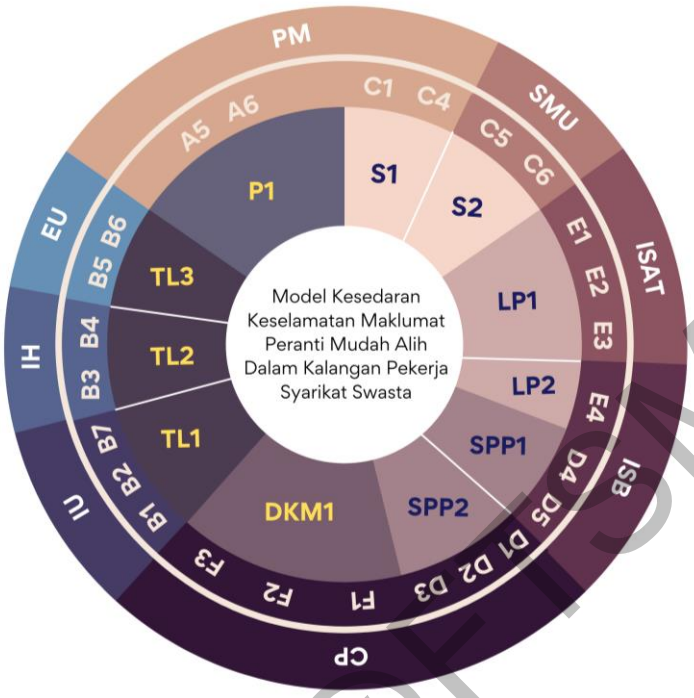
G. Model Akhir

Berdasarkan penentusahan dan pengesahan yang dibuat oleh pakar, model akhir kajian adalah sama dengan model awal kajian dengan sedikit penambahbaikan seperti dalam Rajah 8. Daripada ujian analisis faktor dan hasil putaran *varimax*, setiap komponen dibahagikan kepada satu (1) hingga tiga (3) kategori mengikut konteks soalan bagi setiap item. Bagi komponen faktor pengetahuan, A5 dan A6 diletakkan dalam kategori Pengurusan Kata Laluan (PM), manakala item C1 dan C4 dalam faktor sikap juga diletakkan dalam kategori yang sama. Untuk item C5 dan C6 dalam faktor sikap pula diletakkan dalam kategori Penggunaan Rangkaian Media Sosial (SMU).

Bagi komponen faktor tingkah laku, B1, B2 dan B7 diletakkan dalam kategori Penggunaan Internet (IU), B3 dan B4 diletakkan dalam kategori Pengendalian Maklumat (IH) dan B5 dan B6 pula diletakkan dalam kategori Pengurusan Emel (EU).

Bagi komponen faktor sokongan pihak pengurusan, D1, D2 dan D3 diletakkan dalam kategori Polisi Syarikat (CP), manakala item F1, F2 dan F3 dalam faktor polisi/dasar keselamatan maklumat juga diletakkan dalam kategori yang sama.

Akhir sekali, komponen faktor latihan dan pendidikan, E1, E2 dan E3 diletakkan dalam kategori Latihan Kesedaran Keselamatan Maklumat (ISAT), manakala E4 diletakkan dalam kategori Taklimat Keselamatan Maklumat (ISB) bersama-sama D4 dan D5 dalam faktor sokongan pihak pengurusan. Penambahbaikan di dalam model akhir dibuat daripada kategori Pengkomputeran Mudah Alih (MD) dan Pelaporan Insiden (IR) ditukarkan kepada Latihan Kesedaran Keselamatan Maklumat (ISAT), Taklimat Keselamatan Maklumat (ISB) dan Polisi Syarikat (CP). Rajah 8 menunjukkan keseluruhan komponen model akhir yang dipecahkan mengikut kategori berdasarkan ujian analisis faktor dan hasil putaran *varimax*.



RAJAH 8: MODEL AKHIR KAJIAN

Jadual 11 menunjukkan keseluruhan item-item dalam setiap faktor dalam komponen model akhir kajian beserta dengan kategori bagi setiap item yang diterangkan secara terperinci berdasarkan Rajah 8.

JADUAL 11: KOMPONEN MODEL AKHIR MENGIKUT KATEGORI.

P1 Faktor Pengetahuan Terhadap Kata Laluan	**Pengurusan Kata Laluan (PM)**	**A5**	Kata laluan pada telefon pintar.
		A6	Kata laluan pada komputer riba.
S1 Faktor Sikap Terhadap Kata Laluan		**C1**	Kata laluan yang berbeza bagi setiap sistem
		C4	Kata laluan mengandungi huruf besar, huruf kecil, nombor & simbol (kompleks).
S2 Faktor Sikap Terhadap Rangkaian Media Sosial	**Penggunaan Rangkaian Media Sosial (SMU)**	**C5**	Melayari media sosial untuk tujuan peribadi di tempat kerja dalam tempoh waktu bekerja.
		C6	Berkongsi maklumat rasmi atau sulit tentang syarikat di media sosial.
LP1 Faktor Latihan Kesedaran dan Pendidikan Keselamatan Maklumat	**Latihan Kesedaran Keselamatan Maklumat (ISAT)**	**E1**	Pihak syarikat menjalankan sesi latihan kesedaran keselamatan maklumat kepada semua staf.
			bersambung...
...sambungan **LP1**	**Latihan**	**E2**	Memahami dan mempraktikkan apa yang dipelajari tentang

Faktor Latihan Kesedaran dan Pendidikan Keselamatan Maklumat	**Kesedaran Keselamatan Maklumat (ISAT)**		keselamatan maklumat.
		E3	Melihat risalah atau poster keselamatan maklumat di tempat kerja.
LP2 Faktor Taklimat Keselamatan	**Taklimat Keselamatan Maklumat (ISB)**	**E4**	Taklimat keselamatan maklumat perlu dilaksanakan secara berkala.
SPP1 Faktor Sokongan Pihak Pengurusan Terhadap Taklimat Keselamatan		**D4**	Pihak pengurusan membuat sesi taklimat keselamatan maklumat kepada semua staf.
		D5	Menandatangani surat pematuhan taklimat keselamatan maklumat tersebut.
SPP2 Faktor Sokongan Pihak Pengurusan Terhadap Polisi Syarikat	**Polisi Syarikat (CP)**	**D1**	Pihak pengurusan membenarkan bawa peranti peribadi ke pejabat
		D2	Pihak pengurusan menyediakan emel khas syarikat untuk tujuan kerja.
		D3	Pihak pengurusan menyarankan penukaran kata laluan pada emel pejabat dan peranti peribadi anda setiap 3-6 bulan.
DKM1 Faktor Dasar Keselamatan Maklumat Syarikat		**F1**	Tahu kewujudan Dasar Keselamatan ICT di syarikat.
		F2	Baca Dasar Keselamatan ICT di syarikat.
		F3	Pihak syarikat mengeluarkan satu dokumen berkaitan Dasar Keselamatan ICT di syarikat.
TL1 Faktor Tingkah Laku Terhadap Penggunaan Internet	**Penggunaan Internet (IU)**	**B1**	Menggunakan WiFi Awam (*Public WiFi*).
		B2	Menghantar emel/memuat turun dokumen pejabat menggunakan sambungan WiFi yang selamat (*Secured WiFi*)
		B7	Menerima emel yang mencurigakan dan mengklik pada URL (*link*) di dalam kandungan emel tersebut.
TL2 Faktor Tingkah Laku Terhadap Pengendalian Maklumat	**Pengendalian Maklumat (IH)**	**B3**	Memuat turun (*download*) perisian dari Internet tanpa pengetahuan dan kebenaran daripada syarikat anda.
		B4	Memuat turun (*download*) perisian dari Internet tanpa pengetahuan dan kebenaran daripada syarikat anda.
TL3 Faktor Tingkah Laku Terhadap Penggunaan Emel	**Penggunaan Emel (EU)**	**B5**	Menggunakan akaun emel pejabat untuk kegunaan peribadi.
		B6	Memuat turun (*download*) dokumen/fail yang dihantar oleh penerima yang tidak dikenali.

5. KESIMPULAN

A. Rumusan dan penemuan

Kajian yang dijalankan telah berjaya menjawab persoalan kajian yang telah digariskan seterusnya membolehkan objektif kajian dipenuhi.

1) Objektif pertama kajian adalah untuk mengenal pasti tahap kesedaran dalam kalangan pekerja swasta terhadap keselamatan maklumat terutamanya dalam penggunaan peranti mudah alih di tempat kerja melalui kajian lampau yang berkaitan berjaya mengenal pasti faktor yang mempengaruhi tahap kesedaran keselamatan maklumat. Hasil kajian kesusasteraan telah menghasilkan model awal kajian. Model awal kajian ini terdiri daripada lima (5) komponen iaitu faktor pengetahuan, faktor tingkah laku, faktor sikap, faktor sokongan pihak pengurusan, dan faktor persekitaran. Faktor persekitaran telah ditukarkan ke faktor latihan dan pendidikan dan faktor polisi/dasar keselamatan maklumat. Komponen-komponen ini kemudiannya dijadikan ke dalam bentuk soalan kaji selidik. Soalan kaji selidik tersebut seterusnya ditentusahkan oleh dua (2) orang pakar yang berpengalaman dalam bidang pengurusan keselamatan maklumat dan sumber manusia sebelum dibuat edaran kepada responden untuk menjawab. Cadangan dan idea pakar diteliti dan dianalisis bagi menghasilkan model yang disahkan oleh pakar. Berdasarkan komponen faktor utama ditemukan lapan (8) pemboleh ubah daripada tujuh (7) pemboleh ubah yang dikenalpasti mempengaruhi tahap kesedaran keselamatan pekerja swasta iaitu Pengurusan Kata Laluan (PM), Penggunaan Internet (IU), Penggunaan Emel (EU), Pengendalian Maklumat (IH), Penggunaan Rangkaian Media Sosial (SMU), Polisi Syarikat (CP), Taklimat Keselamatan Maklumat (ISB) dan Latihan Kesedaran Keselamatan Maklumat (ISAT).

2) Objektif kedua kajian adalah mengenal pasti faktor dominan yang mempengaruhi tahap kesedaran keselamatan maklumat di tempat kerja melalui penentusahan model awal oleh pakar dan kajian lampau. Faktor dominan adalah faktor sokongan pihak pengurusan dan faktor yang perlu diberi perhatian adalah faktor sikap dan tingkah laku berdasarkan analisis korelasi *Pearson*. Pembangunan model dalam kajian ini bermula dengan melakukan kajian kesusasteraan terhadap model faktor yang sedia ada dan digabungkan dengan pemboleh ubah daripada HAIS-Q. Hasil temubual bersama dua (2) orang pakar telah membuahkan cadangan serta idea, lalu diteliti dan dianalisis bagi menghasilkan model yang ditentusahkan dan disahkan oleh pakar. Kemudian, menerusi kaji selidik yang dijalankan, didapati bahawa tahap kesedaran keselamatan maklumat dalam kalangan pekerja syarikat swasta (BIT Group of Companies) dalam penggunaan peranti mudah alih adalah berada di tahap yang sederhana dan tinggi. Setiap soalan di dalam kaji selidik tersebut mencatatkan peratusan yang sederhana dan tinggi terhadap semua komponen yang terlibat. Ini juga dibuktikan melalui analisis data yang dibuat menerusi analisis skor min yang menunjukkan nilai min yang tinggi untuk komponen faktor pengetahuan dan faktor polisi/dasar keselamatan

maklumat dan nilai min yang sederhana dan tinggi untuk komponen faktor tingkah laku, sikap, sokongan pihak pengurusan dan latihan dan pendidikan.

3) Objektif ketiga kajian adalah membina model tahap kesedaran keselamatan maklumat peranti mudah alih dan mengesahkan model dengan mendapat penentusahan daripada pakar terhadap model yang dibangunkan serta menjalankan kaji selidik. Proses penilaian dilakukan menggunakan borang soal selidik secara atas talian menggunakan *Google Form*. Melalui ujian kebolehpercayaan, nilai *Cronbach Alpha* adalah di antara 0.700 hingga 0.889 dan menunjukkan indeks kebolehpercayaan item adalah baik, boleh diterima dan memenuhi ciri dikehendaki. Menerusi ujian analisis faktor, data dianalisis menggunakan analisis komponen prinsipal (*Principal Component Analysis*) dan data kemudiannya diputar dengan menggunakan putaran *varimax*. Nilai yang dihasilkan menjadi lebih tinggi dan positif di antara satu sama lain. Ini membuktikan bahawa hubungan korelasi di antara item dengan faktor yang terbentuk dan merupakan kunci untuk memahami sifat faktor-faktor tersebut. Komponen kemudiannya dikategorikan kepada lapan (8) pemboleh ubah berdasarkan nilai hasil dapatan hasil putaran *varimax*. Berdasarkan bukti ini, putaran *varimax* dapat digunakan untuk menghasilkan tafsiran data yang baik dan wajar dipertimbangkan untuk dijadikan komponen di dalam model kesedaran. Ujian analisis korelasi *Pearson* digunakan agar dapat memberikan sedikit petunjuk tentang pentingnya pemboleh ubah kepada faktor-faktor sedia ada. Hasil analisis mendapati secara keseluruhan responden bersetuju dan menerima model yang dicadangkan dan sememangnya terbukti merangkumi semua aspek yang dibincangkan jika dilihat dari hasil analisis deskriptif dan analisis faktor serta model akhir yang dikemukakan.

B. Sumbangan

Kajian ini telah berjaya menghasilkan enam (6) sumbangan utama iaitu :

1) Membangunkan Model Tahap Kesedaran Keselamatan Maklumat Peranti Mudah Alih untuk digunakan oleh syarikat swasta seperti BIT Group of Companies. Dengan adanya model ini, pihak pengurusan syarikat boleh membuat latihan dan kempen kesedaran keselamatan maklumat secara berkala.
2) Membangunkan soalan kaji selidik berdasarkan kajian lepas dan model sedia ada dalam bahasa yang lebih mudah difahami dan bersesuaian.
3) Mempertingkatkan tahap kesedaran keselamatan maklumat dalam kalangan pekerja terutama dalam penggunaan peranti mudah alih dan mengenal pasti jurang yang harus ditambah baik.

4) Meningkatkan kesedaran terhadap keselamatan siber dan polisi syarikat yang perlu dipatuhi oleh setiap pekerja. Latihan dan kempen kesedaran keselamatan maklumat secara berkala mampu meningkatkan kesedaran pekerja terhadap keselamatan siber dari masa ke masa.
5) Sebagai garis panduan kepada pihak pengurusan syarikat swasta dalam menyediakan dan menyedarkan pekerja mereka tentang keselamatan maklumat di tempat kerja bagi memastikan tempat kerja selamat dan terjamin dari sebarang ancaman siber.
6) Sebagai rujukan kepada pihak pengurusan syarikat swasta untuk merangka dan merancang pelan tindakan seterusnya dalam memberi kesedaran keselamatan maklumat kepada pekerja

C. Cadangan dan Kajian Masa Depan

Kajian ini berjaya menghasilkan satu model untuk menentukan tahap kesedaran keselamatan maklumat yang terdiri daripada enam (6) komponen, iaitu faktor pengetahuan, faktor tingkah laku, faktor sikap, faktor sokongan pihak pengurusan, faktor latihan dan pendidikan dan faktor polisi/dasar keselamatan maklumat. Walau bagaimanapun, terdapat banyak aspek yang belum diterokai. Oleh itu, beberapa cadangan kajian disyorkan untuk dibuat pada masa hadapan seperti berikut:

1) Kajian ini boleh diperluaskan ke syarikat swasta yang lain yang mungkin tidak mempunyai latar belakang IT. Data dan maklumat yang diperolehi boleh dibuat perbandingan serta dapat melihat keberkesanan model tersebut.
2) Menambah komponen model yang berkaitan dengan keselamatan maklumat seperti keselamatan rangkaian, pelaporan insiden keselamatan dan pengkomputeran mudah alih.
3) Menambah jumlah bilangan responden 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] AlKalbani, A., Deng, H., Kam, B. & Zhang, X. 2017. *Information Security Compliance in Organizations: An Institutional Perspective*. Data and Information Management, hlm. Vol. 1, 104–114. De Gruyter Poland.

[5] Lee, C., Lee, C. C. & Kim, S. 2016. *Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity*. Computers & Security, hlm. Vol. 59, 60–70. Elsevier Ltd. doi:10.1016/j.cose.2016.02.004.

[6] Lazau, A. & George, W. 2011. *Perceived Risk and Sensitive Data on Mobile Devices*. Cyber forensics 183-196.

[7] Uffen, J., Kaemmerer, N. & Breitner, M.H. 2013. *Personality Traits and Cognitive Determinants – An Empirical Investigation of the Use of Smartphone Security Measures*. Journal of Information Security 4: 203-212.

[8] Anon. 2020. Capaian internet di Malaysia meningkat 90% (Petikan daripada Ketua Perangkaan, Dr Mohd Uzir Mahidin) . Free Malaysia Today, 10 April.

[9] 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.

[10] Kruger, H. A., & Kearney, W. D. 2006. *A Prototype for Assessing Information Security Awareness*. Computers & Security 25(4): 289-296.

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

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

[13] Ajzen, I., & Fishbein, M. 1980. *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice-Hall.

[14] Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness* 34(3): 523–548.

[15] Mylonas A., Kastania A. & Gritzalis D. 2012. *Delegate the Smartphone User? Security Awareness in Smartphone Platforms*. Computers & Security 1-36.

[16] Ophoff, J. & Robinson, M. 2014. *Exploring End-User Smartphone Security Awareness within a South African Context*. Information Security for South Africa 95-101.

[17] Benenson, Z., Peter, O.K., & Krupp, M. 2012. *Attitudes to IT Security when Using a Smartphone*. Proceedings of the FedCSIS, hlm. 1179-1183.

[18] Sari, P.K. & Candiwan. 2014. *Measuring Information Security Awareness of Indonesian Smartphone Users*. TELKOMNIKA 12(2): 493-500.

[19] Ahlan, A R., Arshad, Y. & Lubis, M. 2011. *Implication of human attitude factors toward information security: awareness in Malaysia Public University*. Retrieved from http://irep.iium.edu.my/4119/1/P0533_IAM2011.pdf

[20] Mohd Rafizam Mohamed, Ibrahim Mohamed & Hasimi Sallehuddin. 2018. *Model Tahap Kesedaran Keselamatan Maklumat Dalam Kalangan Penjawat Awam*. UKM.

[21] Mainar Swari Mahardika, Achmad Nizar Hidayanto, Putu Agya Paramartha, Louis Dwysevrey Ompusunggu Rahmatul Mahdalina, Farid Affan. 2020. *Measurement of Employee Awareness Levels for Information Security at the Center of Analysis and Information Services Judicial*

Commission Republic of Indonesia. Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 3, 501-509.

[22] E.A. Puspitaningrum, F.T. Devani, V.Q. Putri, A.N. Hidayanto. 2018. *"Measurement of Employee Information Security Awareness: Case Study At The Directorate General of Resources Management and Postal and Information Technology Equipment Ministry of Communications and Information Technology"* in 2018 Third International Conference on Informatics and Computing (ICIC), Palembang, Indonesia. https://doi.org/10.1109/IAC.2018.8780571

[23] Susanto, H., Almunawar, M. N. & Tuan, Y. C. 2012. *A Novel Method on ISO 27001 Reviews: ISMS Compliance Readiness Level Measurement. Computer Science Journa*l 2(1): 1–12. Retrieved from http://arxiv.org/abs/1203.6622.

[24] Pattinson MR, & Anderson G. 2007. *How well are information risks being communicated to your computer end-users? Info Management Computer Security*, 15(5) .362-371.

[25] Oladosu, K. 2012. *Basic Technology Teachers' Awareness and Attitude Towards the Use Of Information and Communication Technology For Sustainable Development in Lagos State Education Districts*: I, IV and VI 3(13), 46 - 51.

[26] Hu, Q.,Dinev, T., Hart, P. & Cooke. D. 2012. *Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*. Decision Sciences, 43(4), 615-660. doi:10.1111/j.1540-5915.2012.00361.x

[27] Al-Sahily, Ann, Jannet, W., Sures, R. 2003. *Effectiveness of Information Systems Security in IT Organizations in Malaysia*. The 9th Asia-Pacific Conference, 716-720.

[28] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. & Herawan, T. 2015. *Information Security Conscious Care Behaviour Formation in Organizations*. Computers and Security 53: 65–78. doi:10.1016/j.cose.2015.05.012

[29] Brady, J. W. 2011. *Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers*. Proceeding of the Annual Hawaii International Conference on System Sciences, 1-10.

[30] Siponen, M., Adam Mahmood, M. & Pahnila, S. 2014. *Employees' Adherence to Information Security policies: An Exploratory Field Study*. Information and Management 51(2): 217–224. doi:10.1016/j.im.2013.08.006

[31] Beas, M. I. & Salanova, M. 2006. *Self-efficacy beliefs, computer training and psychological well-being among information and communication technology workers*. Computers in Human Behavior, 28(6), 1043-1058.

[32] Torkzadeh, G. & Van Dyke, T. P. 2002. *Effects of training on Internet self-efficacy and computer user attitudes*. Computers in Human Behavior, 18(5), 479-494.

[33] Al-Omari, A.,Deokar, A., El-Gayar, O., Walters, J. & Aleassa, H. 2013. *Information security policy compliance: An empirical study of ethical ideology*. Proceedings of the Annual Hawaii International Conference on System Science, 3018-3027.

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

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

[36] Siddharth Kalla. 2009. *Statistical Treatment Of Data*. Retrieved Jul 29, 2021 from Explorable.com: https://explorable.com/statistical-treatment-of-data

[37] Deborah J. Rumsey. 2009. *Journal of Statistics Education Volume 17*, Number 3 (2009), jse.amstat.org/v17n3/rumsey.html

[38] 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).

[39] Syazwani. 2017. *Cerita 4: Perbezaan Antara Korelasi dan Regresi*. http://syazwanispss.blogspot.com/2017/02/cerita-4-perbezaan-antara-korelasi- dan.html [13 Jun 2020].

[40] Hussin, F. 2011. *Economy and Research Methodology: Korelasi dan Regresi*. http://fauzihussin5252.blogspot.com/2011/12/korelasi-dan-regresi.html

[41] Chong, O. S., Mahamod, Z. & Hamidah Yamat. 2013. *Faktor Jantina, Kaum, Aliran Kelas dan Hubungannya dengan Kecerdasan Emosi Murid dalam Mempelajari Bahasa Melayu. Malay Language Education Journal* – MyLEJ 3(Mei): 12–23.

[42] George, D., & Mallery, P. (2003). *SPSS for Windows step by step: a simple guide and reference (4th edn.)*. Boston: Allyn & Bacon

[43] Taber, K. S. 2018. *The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education*. Research in Science Education 48(6): 1273–1296. doi:10.1007/s11165-016-9602-2

[44] Landell, K.. 1997. Management by menu, London: Wiley and Sons Inc.

[45] Kass, A. Richard & Howard E.A. Tinsley (2018). *Factor Analysis. Journal of Leisure Research*. Volume 11, 1979 - Issue 2. doi.org/10.1080/00222216.1979.11969385