MODEL KESEDARAN KESELAMATAN MAKLUMAT PERANTI MUDAH ALIH DALAM KALANGAN PEKERJA SYARIKAT SWASTA

MOHD HANIS BIN JENALIS

UNIVERSITI KEBANGSAAN MALAYSIA

MODEL KESEDARAN KESELAMATAN MAKLUMAT PERANTI MUDAH ALIH DALAM KALANGAN PEKERJA SYARIKAT SWASTA

MOHD HANIS BIN JENALIS

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT MEMPEROLEHI
IJAZAH SARJANA KESELAMATAN SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2021

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

12 OKTOBER 2021

MOHD HANIS BIN JENALIS
GP06066

PENGHARGAAN

Alhamdulillah, setinggi-tinggi kesyukuran dipanjatkan ke hadrat Allah S.W.T kerana dengan limpah kurnia, rahmat dan inayahNya, akhirnya saya berjaya menyelesaikan kajian ini dalam tempoh masa yang ditetapkan.

Sekalung budi dan ucapan penghargaan serta terima kasih yang tidak terhingga kepada YBrs. Ts. Dr. Ibrahim Mohamed selaku penyelia yang tidak putus memberi tunjuk ajar, teguran, nasihat, motivasi dan bimbingan serta kesabaran dalam memberi panduan sepanjang saya melaksana kajian ini. Tanpa sokongan dan dan dorongan dari beliau tentunya sukar untuk saya menyempurnakan kajian ini.

Terima kasih ditujukan kepada semua pensyarah dan warga Fakulti Teknologi dan Sains Maklumat (FTSM) yang telah banyak memberi tunjuk ajar serta berkongsi pengetahuan sepanjang tempoh pengajian saya di Universiti Kebangsaan Malaysia (UKM). Ucapan terima kasih juga kepada semua tenaga pengajar dari CyberSecurity Malaysia (CSM) yang terlibat dalam memberi ilmu dan berkongsi pengalaman yang cukup bermanfaat.

Ucapan terima kasih tidak terhingga untuk ahli keluarga tercinta iaitu Puan Hjh. Zabariah Md Yusoff (Ibu), Tuan Hj. Jenalis Abd Kahar (Ayah) dan adik beradik yang lain iaitu Muhammad Hafiz Jenalis, Siti Hazirah Jenalis, Muhammad Hazwan Jenalis, Siti Hajar Jenalis dan Muhammad Haziq Jenalis yang sentiasa memberi dorongan, semangat dan doa untuk terus berjaya dalam pelajaran dan kerjaya.

Terima kasih juga diucapkan kepada tenaga kerja dan pakar daripada syarikat BIT Group Sdn Bhd, Tuan Mohd Faizal Ariffin selaku Pengurus Besar (GM) Bahagian Sumber Manusia dan Servis Korporat (Transformasi) dan juga pakar daripada NexQuadrant Sdn Bhd (BIT Group Managed Services), Tuan Ibrahim Inzuddin Hussian selaku Ketua Pegawai Operasi (COO) yang sudi meluangkan masa untuk sesi temubual dan sesi penilaian model kajian serta soalan kaji selidik. Terima kasih kerana sudi membantu saya menyempurnakan tesis ini dengan membantu mengedarkan borang kaji selidik kepada semua responden dari tujuh (7) anak syarikat dari seluruh Malaysia.

Begitu juga ucapan terima kasih kepada rakan-rakan seperjuangan iaitu Puan Nur Ilyani Ahmad, Tuan Ahmad Syukri Abdullah, Tuan Farouk Jani Basha dan Tuan Wan Yuswani Wan Jusoh serta rakan-rakan lain yang banyak memberi dorongan, sokongan, idea dan semangat semasa menjayakan tesis ini. Kepada rakan-rakan seperjuangan yang sentiasa memberikan sokongan dan dorongan serta bantuan yang tidak berbelah bagi, jasa bakti kalian amat besar ertinya kepada saya.

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.

MOBILE DEVICES INFORMATION SECURITY AWARENESS MODEL AMONG PRIVATE COMPANY EMPLOYEES

ABSTRACT

The increasing usage of mobile devices in the office, such as smartphones and laptops, raises concerns about data security. One of the biggest concerns is the level of information security which includes personal data, passwords and sensitive information stored in mobile devices. Therefore, there is an urgent need to study the level of information security awareness on mobile devices to determine factors that influence the level of information security awareness of private employees. Previous studies were focused at the fundamental elements and narrowed in the factors that determine the level of information security awareness in government organization. The purpose of this study is to develop an awareness model that can assess the level of information security awareness in the use of mobile devices among employees of private companies. The chosen model was the Knowledge-Attitude-Behavior (KAB) Model and information security awareness models, the Human Aspect Model of Information Security Questionnaire (HAIS-Q). The study used both qualitative (interview) and quantitative (surveys) analysis and the model consists of 6 components of factors namely knowledge, behavior, attitude, management support, training and education and information security policy. The case study was conducted in an IT-based private company, BIT Group Sdn Bhd, which consists of 7 subsidiaries. Questionnaires were distributed into a total of 75 respondents. Among the tests and analysis used in the questionnaires were reliability test, mean score test, factor analysis and Pearson correlation analysis. The reliability index of each component is found to be good with a Cronbach Alpha value between 0.700 to 0.889. Using the mean score test, the value obtained for each component is between 3.48 to 6.79. On the other hand, the results of the factor analysis provide 8 components of variables, namely Password Management (PM), Internet Usage (IU), Email Usage (EU), Information Handling (IH), Social Media Usage (SMU), Company Policy (CP), Information Security Briefing (ISB) and Information Security Awareness Training (ISAT). The results of Pearson correlation analysis showed a moderate, and strong relationship as well as the significance between all factors. This model is expected to help private enterprises i.e companies and employees to be more sensitive and take information security measures to protect personal information on high-risk mobile devices such as smartphones and laptops.

KANDUNGAN

Halaman

SENARAI JADUAL

SENARAI ILUSTRASI

SENARAI SINGKATAN

AHP	*Analytic Hierarchy Process*
BYOD	*Bring Your Own Device*
CFS	*Contract For Services*
COS	*Contract Of Services*
CP	*Company Policy*
EU	*Email Use*
HAIS-Q	*Human Aspect of Information Security Questionnaire*
ICT	*Information and Communications Technology*
IH	*Information Handling*
IR	*Incident Reporting*
ISAIM	*Information Security Awareness Identification Model*
ISAT	*Information Security Awareness Training*
ISB	*Information Security Briefing*
ISO	*International Organization for Standardization*
IT	*Information Technology*
IU	*Internet Use*
KAB	*Knowledge-Attitude-Behavior*
MAMPU	*Malaysian Administrative Modernisation and Management Planning Unit*
MD	*Mobile Devices*
MITM	*Man-In-The-Middle*
MyCERT	*Malaysia Computer Emergency Response Team*
PCA	*Principal Component Analysis*
PM	*Password Management*

PPN	Pelan Pemulihan Negara
SPSS	*Statistical Package for Social Science*
SMU	*Social Media Use*
TBA	*Theory of Planned Behavior*
TRA	*Theory of Reasoned Action*
UKM	Universiti Kebangsaan Malaysia
WFH	*Work From Home*
WiFi	*Wireless Fidelity*

BAB I

PENDAHULUAN

1.1 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 (Haeussinger & Kranz 2013) bagi mengekal aspek keselamatan maklumat iaitu kerahsiaan, ketersediaan dan integriti (Hina & Dominic 2018) perlu dijaga.

Keselamatan maklumat perlu diakui sebagai isu kritikal yang boleh mempengaruhi prestasi organisasi (Wahyudiwan et al. 2017). 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 (AlKalbani et al. 2017). 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 (Lee et al. 2016).

Dasar tersebut perlu dikongsi, difahami dan dipatuhi menerusi kaedah latihan atau program kesedaran. Menurut Bharathi & Suguna (2014), penyampaian kesedaran adalah bertujuan memberi tumpuan kepada keselamatan, membolehkan individu mengenal pasti dan prihatin terhadap insiden keselamatan teknologi maklumat serta bertindak balas dengan sewajarnya.

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 (Lazau & George 2011). 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 (Uffen et al. 2013). 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 (Lazau & George 2011).

Gajet peribadi pengguna boleh diintip oleh individu yang mempunyai kepakaran dalam bidang penggodaman. Pengintipan berlaku apabila penjenayah siber mampu memintas komunikasi antara gajet peribadi dan open *WiFi*. Pendekatan ini dikenali sebagai serangan orang tengah, serangan *Man-In-The-Middle* (MITM). Sambungan percuma selalu menjadi sasaran penjenayah siber mencuri data peribadi pengguna mahupun organisasi tanpa pengguna sedari sehingga mampu mengawal

gajet peribadi pengguna sepenuhnya (Ophoff & Robinson 2014). Ini secara tidak langsung dapat mendedahkan segala aktiviti yang dibuat oleh pengguna yang menggunakan gajet peribadi mereka. Ada juga pengguna yang menyimpan maklumat sulit mereka dan organisasi dalam gajet peribadi tanpa melakukan penyulitan data (Lazau & George 2011; Mylonas et at. 2012). Sekiranya pengguna merupakan orang penting sesebuah organisasi, sudah semestinya mereka menjadi sasaran penjenayah siber. Walaupun pengguna tidak ada sebarang niat untuk mendedahkan maklumat sulit organisasi, namun tanpa disedari maklumat sulit sudah berada di tangan orang yang mempunyai niat jahat terhadap organisasi.

Kebanyakan peranti mudah alih mempunyai kemudahan untuk menyambung secara automatik apabila berada di kawasan yang terdapat *WiFi* percuma. Terdapat segelintir pengguna tidak sedar bahawa kemudahan penyambungan secara automatik boleh menyebabkan peranti mudah alih mereka terdedah kepada ancaman.

Oleh kerana kebanyakan organisasi menyediakan kemudahan *WiFi* percuma untuk kegunaan pekerja, maka pekerja yang menggunakan *WiFi* percuma di luar organisasi perlulah berhati-hati semasa menggunakan peranti mudah alih di dalam organisasi. Namun, ramai dalam kalangan pekerja tidak sedar bahawa penggunaan *WiFi* di luar organisasi boleh menyebabkan peranti mudah alih mereka kemungkinan besar diancam oleh penjenayah siber ataupun dimasuki virus. Apabila peranti tersebut disambung ke rangkaian organisasi, maka penyebaran virus boleh berlaku dan memberi implikasi kepada organisasi. Situasi ini terjadi disebabkan tidak ada kesedaran dalam kalangan pengguna gajet peribadi di tempat kerja (Sari & Candiwan 2014).

Malaysia merupakan antara negara mencatatkan jumlah penduduk memiliki telefon pintar tertinggi dengan menduduki tempat ke-9 di dunia (Spring 2015 Global Attitudes Survey). Berdasarkan kajian firma Pew Research Center, Malaysia merupakan antara negara tertinggi pemilikan gajet dengan mencatatkan kadar penembusan mencapai 65 peratus. Korea Selatan menduduki tangga pertama dengan kadar 88 peratus diikuti Australia (77 peratus), Israel (74 peratus), Amerika Syarikat (72 peratus), Sepanyol di kedudukan kelima dengan 71 peratus. Sementara itu, pada

kedudukan keenam adalah Britain (68 peratus) diikuti Kanada (67 peratus), Chile (65 peratus) dan di tempat ke-9 adalah Malaysia. (Pew Research Center 2016).

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 (Mohd Uzir Mahidin 2020).

1.2 LATAR BELAKANG KAJIAN

Apabila melibatkan organisasi yang menjalankan tugas dan projek bernilai jutaan ringgit faktor keselamatan maklumat perlu dijaga dengan rapi. Kesannya, apabila tahap kesedaran dalam kalangan pekerja tidak dititikberatkan menyebabkan berlakunya risiko kecurian data dan kebocoran maklumat. Ini akan memberi kesan dan imej yang buruk kepada syarikat terutama syarikat swasta. Sehingga Mei 2019, sebanyak 3,743 insiden keselamatan maklumat telah dilaporkan kepada *Malaysia Computer Emergency Response Team* (MyCERT) (CyberSecurity Malaysia 2019). Oleh itu, insiden keselamatan maklumat perlu diminimumkan dan organisasi perlu melindungi maklumat dan data terutamanya di syarikat swasta yang berisiko. Setiap pekerja syarikat swasta pastinya ada peranti-peranti yang dibawa ke tempat kerja yang boleh menjadi risiko kepada syarikat. Dalam kajian ini, saya telah memilih salah sebuah syarikat swasta yang mempunyai anak syarikat di bawahnya. BIT Group Sdn Bhd, sebuah syarikat besar yang terdiri daripada tujuh (7) anak syarikat yang menjalankan urusan bisnes berasaskan IT di Cyberjaya dengan nilai jumlah projek mencecah nilaian ribuan dan jutaan ringgit berkaitan sistem, aplikasi dan teknologi.

Penggunaan telefon pintar yang semakin meningkat dengan ramalan jualan yang menunjukkan bilangan telefon pintar kini melebihi daripada pembelian telefon asas (Urban et al. 2012). Ini menunjukkan majoriti pengguna lebih gemar menggunakan telefon pintar disebabkan fungsi yang memudahkan kebanyakan kerja mereka. Namun, peranti mudah alih ini mudah terdedah kepada kecurian, kehilangan dan kerosakan yang menimbulkan risiko keselamatan maklumat kepada individu mahupun organisasi.

Secara tradisinya, kurang perhatian diberi kepada kesedaran keselamatan pengguna peranti mudah alih berbanding dengan kawalan keselamatan teknikal seperti tembok api (*firewall)*. Rangkaian tidak boleh dikawal oleh sesuatu organisasi disebabkan ia merupakan sebuah dunia tanpa sempadan di mana serangan virus ke atas rangkaian mudah berlaku dan amat sukar untuk dihapus. Menurut Furnell dan Clarke (2012), pada era teknologi yang semakin mencabar, adalah penting untuk menganalisis faktor-faktor yang menyumbang kepada kesedaran keselamatan pengguna gajet peribadi kerana teknologi sahaja tidak dapat memberikan penyelesaian keselamatan yang lengkap kepada sesebuah organisasi. Kesedaran yang tidak mencukupi dalam kalangan pengguna dalam cara mengendalikan peranti dengan selamat seringkali membuka pintu kepada penjenayah siber untuk menggodam peranti tersebut. Terdapat juga dalam kalangan mereka yang mempunyai pengetahuan yang mencukupi tetapi tidak menggunakan pengetahuan yang ada untuk melindungi gajet peribadi mereka (Al-Sehri 2012; Allam et al. 2014). Ini adalah kerana segelintir pengguna peranti mudah alih menyimpan maklumat peribadi mahupun maklumat organisasi di dalam telefon mereka.

Justeru itu adalah wajar bagi pihak organisasi, khususnya organisasi swasta untuk mengambil tindakan supaya pekerja lebih prihatin terhadap penggunaan peranti mudah alih di tempat kerja dan juga mengenai maklumat yang disimpan di dalam peranti tersebut. Merujuk kepada ISO 27001, pekerja yang bekerja di bawah peraturan organisasi sepatutnya mengambil maklum mengenai organisasi untuk memastikan pekerja menerima pendidikan mengenai kesedaran dan latihan yang sesuai serta sentiasa memberi maklumat yang terkini mengenai polisi organisasi dan prosedur berkaitan bidang tugas. Lagipun, pengesanan, pencegahan dan pemulihan kawalan untuk melindungi daripada perisian hasad (*malware*) perlu dilaksana dan digabung dengan kesedaran penggunaan peranti mudah alih di tempat kerja.

Di BIT Group Sdn Bhd, kami sentiasa memantau dan memastikan tahap keselamatan syarikat sentiasa dalam keadaan baik. Sebagai contoh, setiap pintu masuk diletakkan alat pengesan kehadiran di mana hanya staf yang sah sahaja yang boleh masuk dalam pejabat tersebut. Para pekerja juga masing-masing diberikan emel khas syarikat masing-masing untuk mengelakkan daripada kebocoran maklumat atau

kecurian data. Email ini akan memberi maklum balas kepada pengguna supaya menukar kata laluan setiap tiga (3) bulan sekali. Ini antara langkah-langkah yang diambil oleh pihak syarikat BIT Group.

Namun, dari segi penggunaan peranti mudah alih para pekerja apabila di bawa ke pejabat tidak diberikan penekanan. Sebagai sebuah syarikat swasta, lebih-lebih lagi syarikat berasaskan IT, tahap kesedaran keselamatan maklumat terhadap peranti mudah alih perlu diberi perhatian. Penggunaan peranti mudah alih ini boleh meningkatkan produktiviti dan prestasi syarikat dalam masa yang sama berpotensi mendedahkan kepada risiko keselamatan maklumat jika tidak dikawal dengan baik.

1.3 PENYATAAN MASALAH

Pada akhir tahun 1990, serangan disebabkan virus komputer seperti *Melissa* dan *Code Red* telah mengancam keselamatan maklumat digital dan mendapat perhatian di seluruh dunia (Ramalingam et al. 2014). Semenjak itu, terdapat banyak ancaman baharu seperti emel *spam*, pencurian identiti, kebocoran data, pancingan data, pencerobohan data dan banyak lagi terus berkembang dan memberi impak yang besar terhadap keselamatan maklumat organisasi dan individu (Ramalingam et al. 2014).

Menurut Parsons et al. (2014), banyak ancaman terhadap sistem komputer organisasi boleh dikaitkan dengan tingkah laku pengguna komputer. Sebagai contoh tingkah laku manusia yang boleh membahayakan organisasi adalah memasukkan kata laluan secara tidak sengaja atau sengaja kepada orang lain, menjadi mangsa emel pancingan data dengan mengklik pautan laman sesawang tertanam, atau memasukkan peranti media yang tidak dikenali ke dalam komputer kerja atau rumah (Parsons et al. 2014). Kurangnya kesedaran terhadap keselamatan maklumat boleh menyebab pelanggaran keselamatan (*security breaches*) walaupun organisasi telah melaksana kawalan keselamatan yang kuat (Gibson 2011). Di samping itu, kelalaian dan tingkah laku yang tidak disengajakan oleh staf boleh mengakibatkan ancaman berbahaya terhadap keselamatan aset (Hina & Dominic 2016).

Risiko dan ancaman keselamatan maklumat jelas meningkat sejak beberapa tahun kebelakangan ini. Pada tahun 2018, dunia telah menyaksikan kes-kes jenayah

siber yang dahsyat berkaitan dengan keselamatan maklumat seperti pelanggaran data, *crypto jacking*, dan banyak lagi (Belani 2020). Malaysia juga menerima ancaman keselamatan maklumat ini. Perkara ini telah dilaporkan oleh *CyberSecurity Malaysia* menerusi *Malaysia Computer Emergency Response Team* (MyCERT) dengan menerima lebih 30,000 laporan pelbagai jenis insiden keselamatan siber dalam tempoh sejak 2017 sehingga September 2019.

Selain itu, pada tahun 2018, berlaku penyebaran virus komputer yang meluas sehingga hampir keseluruhan komputer di PDRM Kontinjen Melaka dijangkiti (Farouk 2020). Penyebaran virus tersebut bukan sahaja merosakkan sistem komputer, malah menyebabkan mengganggu operasi harian organisasi keselamatan tersebut. Insiden keselamatan maklumat ini perlu diambil serius dan ditangani dengan cara yang betul oleh semua kakitangan yang menggunakan peranti masing-masing. Menurut Sari dan Candiwan (2014), penyebaran virus dalam rangkaian organisasi boleh berlaku sekiranya gajet peribadi pekerja telah dijangkiti virus apabila pekerja tersebut menggunakan *WiFi* percuma di luar organisasi. Situasi ini berlaku kerana tiada pendidikan atau latihan rasmi diberi kepada staf mengenai kesedaran keselamatan penggunaan gajet peribadi di tempat kerja (Jacey Mariadass et al. 2017). Lagipun gajet peribadi terutamanya telefon pintar dan tablet telah digodam (*hack*) dari luar organisasi apabila staf menggunakan *open* WiFi di luar organisasi. penyataan ini turut dipersetujui oleh Lazau dan George (2011) di mana kajian beliau menyatakan pengguna tidak sedar akan bahaya menggunakan *open* WiFi untuk mengakses internet dengan menggunakan gajet peribadi.

Sebagai strategi permulaan untuk mengelak daripada berlakunya insiden keselamatan maklumat, syarikat swasta memerlukan staf yang berpengetahuan mengenai keselamatan maklumat dengan cara mengukur tahap kesedaran keselamatan maklumat mereka. Pengukuran akan dilakukan melalui kaji selidik berdasarkan pengetahuan, sikap dan tingkah laku mereka serta menilai faktor-faktor lain yang mempengaruhi tahap kesedaran keselamatan maklumat terutamanya pada penggunaan peranti mudah alih. Dengan adanya aktiviti ini, pengurusan atasan diharap mengenal pasti tahap kesedaran dan pengetahuan staf tentang keselamatan maklumat dan risiko peranti mudah alih sama ada tinggi atau rendah. Maklumat ini boleh membantu pihak

pengurusan untuk membuat tindakan susulan, perancangan, strategi dan langkah pencegahan selanjutnya mengenai keselamatan maklumat.

Menurut Parsons et al. (2014), 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 (Parsons et al. 2014). 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 (Parsons et al. 2014).

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.

1.4 PERSOALAN KAJIAN

Berdasarkan penyataan masalah yang dinyatakan di atas, persoalan kajian adalah seperti berikut:

1) Apakah tahap kesedaran dalam kalangan pekerja swasta terhadap keselamatan maklumat terutama dalam penggunaan peranti mudah alih di tempat kerja?
2) Apakah faktor dominan yang mempengaruhi tahap kesedaran keselamatan maklumat dalam kalangan pekerja syarikat swasta?
3) Bagaimanakah reka bentuk model untuk menilai tahap kesedaran keselamatan maklumat dan sejauh mana keberkesanan model yang dibangunkan?

1.5 OBJEKTIF KAJIAN

Objektif utama yang dikemukan untuk kajian ini adalah:

1) Mengenal pasti tahap kesedaran dalam kalangan pekerja swasta terhadap keselamatan maklumat terutama dalam penggunaan peranti mudah alih di tempat kerja.
2) Mengenal pasti faktor dominan yang mempengaruhi tahap kesedaran keselamatan maklumat di tempat kerja.
3) Membina model tahap kesedaran keselamatan maklumat peranti mudah alih dan mengesahkan model yang dibangunkan.

1.6 SKOP KAJIAN

Skop kajian melibatkan perkara berikut:

a. Tertumpu kepada tahap kesedaran keselamatan maklumat terutama penggunaan peranti mudah alih dalam kalangan pekerja syarikat swasta khususnya syarikat yang berasaskan IT.

b. Kajian dijalankan menggunakan kaedah temu bual bersama pakar dan kaedah kaji selidik dalam kalangan pekerja syarikat swasta seperti BIT Group Sdn Bhd.

c. Kaji selidik yang dijalankan adalah berdasarkan model kesedaran sedia ada bagi menilai tahap kesedaran keselamatan maklumat terhadap penggunaan peranti mudah alih di tempat kerja.

1.7 MODEL AWAL

Kajian ini menggunakan gabungan model konseptual yang sedia ada iaitu:

1) Model *Knowledge-Attitude-Behavior* (KAB) (Kruger and Kearney 2006)

2) Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) (Parsons et al. 2014).

3) Model *Information Security Awareness Identification* (ISAIM) (Ramalingam et al. 2014).

4) Model Kesedaran Keselamatan Maklumat (Bharathi & Suguna 2014)

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.

1.8 KEPENTINGAN KAJIAN

Aktiviti kaji selidik yang dijalankan dapat membantu organisasi untuk mengenal pasti tahap kesedaran keselamatan maklumat terutama dalam penggunaan peranti mudah alih terhadap warga kerjanya. Aktiviti ini boleh dijalankan secara berkala, dan tidak melibatkan kos. Selain itu, hasil analisis dapat membantu organisasi untuk menentukan program kesedaran dan latihan keselamatan maklumat yang bersesuaian.

Model kaji selidik yang dibangunkan boleh diguna pakai oleh organisasi swasta yang lain. Seterusnya dapat mengurangkan kos kepada organisasi kerana tidak perlu menggunakan pihak ketiga di dalam menjalankan aktiviti soal selidik. Soal selidik yang dibangunkan dan dilaksanakan secara beretika menjadikan amalan terbaik keselamatan maklumat kepada organisasi. Secara tidak langsung, amalan terbaik ini dapat menyumbang kepada pengukuhan persekitaran keselamatan maklumat yang lebih selamat.

Kajian ini dibuat untuk mendedahkan tahap kesedaran keselamatan maklumat dalam kalangan pekerja syarikat swasta terutamanya pekerja di syarikat BIT Group Sdn Bhd di samping mendedahkan risiko dalam penggunaan peranti mudah alih seperti telefon pintar dan komputer riba semoga ia dapat membuka mata para pekerja tentang pentingnya menjaga keselamatan peranti mudah alih masing-masing.

1.9 ORGANISASI DISERTASI

Disertasi ini mengandungi lima (5) bab seperti berikut:

BAB I merangkumi gambaran keseluruhan kajian yang mengandungi pengenalan, latar belakang kajian, penyataan masalah, persoalan kajian, objektif kajian, skop kajian, model konseptual dan kepentingan kajian.

BAB II merupakan sorotan kajian atau lebih dikenali sebagai kajian kesusasteraan yang mengandungi kerangka sorotan kajian secara umum bagi menentukan jurang pengetahuan dan indikator faktor kajian. Dalam bab ini juga akan memberi tumpuan khusus bagi konsep asas dan terminologi, aspek kesedaran dan kajian lampau. Penjelasan awal model kajian juga dinyatakan secara ringkas dalam bab ini sebagai gambaran sumbangan teori kajian yang hendak dicapai pada akhir kajian ini.

BAB III menerangkan mengenai metodologi kajian yang digunakan untuk mencapai objektif kajian. Metodologi kajian merangkumi reka bentuk kajian, proses pengumpulan dan penentusahan maklumat, penganalisisan, kaedah pengiraan dan proses pengujian kaji selidik kajian akan dihuraikan dalam bab ini.

BAB IV akan menghuraikan hasil analisis data yang diperolehi berdasarkan analisis penilaian pakar, analisis daripada soalan kaji selidik serta pengumpulan instrumen kajian dan penilaian tahap kesedaran organisasi yang dipilih sebagai kajian kes bagi mengesahkan keberkesanannya

BAB V merupakan bab terakhir kajian yang mengandungi perbincangan dan ulasan sebagai rumusan hasil kajian menerusi dapatan kajian untuk mengukur pencapaian objektif kajian dan menentukan sama ada menyokong atau tidak cadangan model kesedaran yang dicadangkan.

1.10 KESIMPULAN

Daripada kajian yang dilaksanakan, kajian ini diharap dapat dilaksanakan dengan teratur dan mencapai semua objektif yang telah ditetapkan. Hasil kajian juga diharap mampu menghasilkan model kesedaran keselamatan maklumat peranti mudah alih terhadap syarikat swasta terutamanya warga kerja di BIT Group Sdn Bhd, dan seterusnya membantu membuat penilaian tahap kesedaran dan faktor yang terlibat dalam menggunakan peranti mudah alih mereka seperti telefon pintar dan komputer riba.

BAB II

KAJIAN KESUSASTERAAN

2.1 PENGENALAN

Kajian kesusasteraan merupakan penelitian sistematik yang jelas untuk mengenali, menilai dan mentafsir hasil penulisan oleh penyelidik terdahulu dan juga pengamal dalam bidang berkaitan dengan permasalahan yang dikaji (Fink 1998). Dalam bab ini dijelaskan bagaimana kajian kesusasteraan dilaksanakan bertujuan untuk memahami dengan lebih terperinci bagaimana tahap kesedaran keselamatan maklumat peranti mudah alih digunakan.

Bab ini membincangkan dengan lebih terperinci berkenaan takrifan konsep dan kajian lepas yang berkaitan tahap kesedaran keselamatan maklumat pengguna, tahap penggunaan peranti mudah alih dan kajian lepas berkaitan model penilaian sedia ada dalam organisasi berbeza sebelum ini. Di dalam kajian kesusasteraan ini juga, sumber-sumber kajian adalah dirujuk daripada jurnal, artikel, garis panduan, tesis, laporan kajian, laporan akhbar dan kenyataan daripada pakar yang berkaitan. Selain itu, proses penelitian secara terperinci, penilaian dan pemahaman secara mendalam terhadap hasil kajian dan penulisan lepas yang mempunyai kaitan dengan persoalan kajian turut dilakukan. Hasil dari penelitian ini akan menampakkan kelompangan dalam pengetahuan berkaitan yang harus dilengkapkan bagi melengkapkan objektif kajian. Bab ini penting dalam memberi input kepada penyelidik untuk memahami setiap persoalan kajian secara lebih mendalam selain dari dapat mengetahui wujudnya masalah itu serta dapat membantu dalam melaksanakan kajian secara lebih berkesan.

Proses penulisan dokumentasi bab ini dibahagikan kepada lima (5) bahagian memudahkan pemahaman untuk setiap kajian yang dilaksanakan. Jadual 2.1 menunjukkan sumber rujukan untuk setiap bahagian.

Jadual 2.1 Sumber rujukan

Bahagian	Sumber rujukan
Model *Knowledge-Attitude-Behavior* (KAB) untuk mengkaji faktor-faktor yang mempengaruhi tahap kesedaran keselamatan maklumat pengguna.	(Kruger and Kearney 2006)
Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) untuk mengkaji bidang fokus penggunaan internet, penggunaan email, pengurusan kata laluan, penggunaan rangkaian medial sosial, pelaporan insiden, pengendalian maklumat dan pengkomputeran mudah alih.	(Parsons et al. 2014)
Model *Information Security Awareness Identification* (ISAIM) untuk mengkaji elemen kesedaran keselamatan maklumat seperti kesedaran organisasi, ancaman, perlindungan, kandungan dan keselamatan.	(Ramalingam et al. 2014)
Model Kesedaran Keselamatan Maklumat untuk mengkaji dan menyesuaikan langkah pencegahan yang bersesuaian pada setiap peringkat dalam organisasi.	(Bharathi & Suguna 2014)
Kajian lampau berkenaan penilaian model tahap kesedaran keselamatan maklumat dan tahap risiko peranti sedia ada dalam organisasi berbeza.	(Jacey Mariadass et. al 2017), (Mohd Rafizam Mohamed et. al 2018) & (Mainar Swari Mahardika et. al 2020)

2.2 KESELAMATAN MAKLUMAT

Fokus utama perlindungan maklumat adalah untuk menjaga keaslian maklumat bagi mencapai pelbagai objektif perniagaan organisasi. Namun, serangan daripada pengganas siber ke atas sistem maklumat mampu mengakibatkan kerugian kewangan, reputasi, dan aset yang serius (Safa et al. 2015). Organisasi perlu menyampaikan penyelesaian teknikal dan tingkah laku pekerjanya untuk melindungi aset maklumat (Siponen et al. 2014). Kurangnya garis panduan, dasar/polisi, kesedaran mengenai ancaman keselamatan maklumat, dan kurang pemantauan tingkah laku pekerja sering menimbulkan situasi yang mengancam kepada keselamatan maklumat organisasi.

Menurut kajian daripada Da Veiga (2015), pekerja yang membaca dan memahami polisi keselamatan maklumat organisasi mereka menunjukkan sikap yang

lebih positif untuk mengembangkan budaya keselamatan maklumat. Oleh yang demikian, kerangka keselamatan yang menyeluruh untuk melaksanakan prosedur keselamatan strategik dengan fokus pada semua pengguna di syarikat swasta adalah perlu dibangunkan untuk memastikan kepatuhan terhadap perlindungan sumber dan keselamatan maklumat.

Terdapat peningkatan pengiktirafan mengenai pentingnya keselamatan maklumat dalam organisasi di seluruh dunia (AlKalbani et al. 2015; Bulgurcu et al. 2010). Ini membawa kepada undang-undang, peraturan, piawaian dan polisi tertentu yang telah dikembang untuk membantu organisasi melindungi maklumat mereka dengan secukupnya. Organisasi akan memastikan pekerja mematuhi keselamatan maklumat dengan merujuk kepada undang-undang, peraturan, piawaian dan polisi yang telah ditetapkan.

Menurut MAMPU, keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima, dan penjagaan keselamatan adalah suatu proses yang berterusan. Ini memerlukan proses dan aktiviti berkala yang dilakukan dari semasa ke semasa bagi memastikan keselamatan sentiasa terjamin. Ancaman keselamatan maklumat sentiasa ada dan sesebuah organisasi perlu bersedia menghadapi sebarang kemungkinan berlakunya serangan siber.

Keselamatan maklumat membawa maksud keadaan yang mana perkhidmatan berasaskan sistem teknologi maklumat berjalan berterusan tanpa sebarang gangguan yang boleh menjejaskan keselamatan maklumat dan aset teknologi yang mengandungi empat (4) komponen asas iaitu, (i) melindungi maklumat rahsia rasmi kerajaan dari capaian tanpa sah; (ii) menjamin setiap maklumat adalah sempurna dan tepat; (iii) memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan (iv) memastikan capaian kepada hanya pengguna yang sah atau penerimaan maklumat dari sumber yang sah (MAMPU 2010). Oleh kerana projek-projek BIT Group Sdn Bhd banyak melibatkan projek kerajaan, jadi banyak kerahsiaan dan data yang sulit yang perlu dilindungi. Selain daripada itu, langkah-langkah ke arah menjamin keselamatan maklumat hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset teknologi; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan

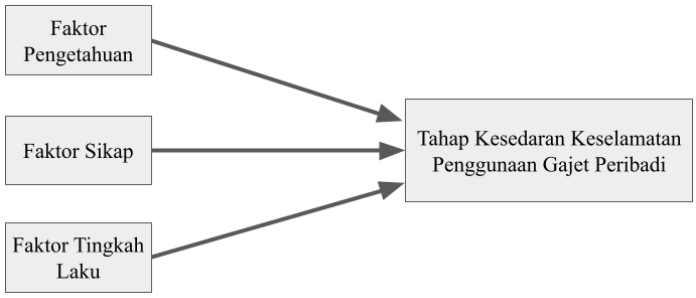
langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan (MAMPU 2010).

2.3 MODEL KESEDARAN KESELAMATAN MAKLUMAT SEDIA ADA

Pemahaman mengenai model dan kerangka kesedaran sedia ada adalah penting untuk membina model kesedaran keselamatan maklumat. Kajian semula kerangka 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.

2.3.1 MODEL *KNOWLEDGE-ATTITUDE-BEHAVIOR* (KAB)

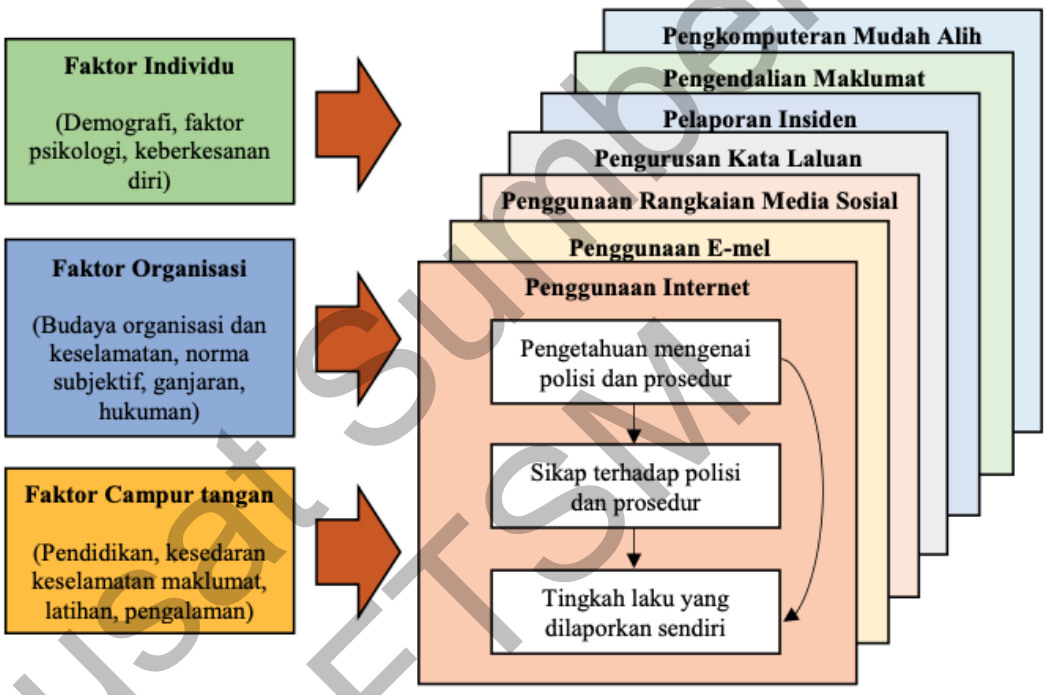
Rajah 2.1 menunjukkan kerangka kajian yang telah diubahsuai daripada Model KAB (*Knowledge-Attitude-Behavior*) oleh Kruger dan Kearney (2006) di mana model ini merujuk kepada teori psikologi sosial yang mencadangkan tiga komponen yang terlibat adalah i) kognitif, ii) kesan dan iii) tingkah laku. Komponen 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 2.1 : Kerangka kajian yang diubahsuai daripada Model Kruger dan Kearney (2006)

2.3.2 MODEL *HUMAN ASPECT OF INFORMATION SECURITY QUESTIONNAIRE* (HAIS-Q)

Parsons et al. (2014) 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 2.2.



Rajah 2.2: Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) (Parsons et al. 2014).

Untuk setiap tujuh bidang fokus tersebut, Parsons et al. (2014) mengembangkan lagi kepada tiga sub-bidang seperti di Jadual 2.2. Seperti bidang fokus, sub-bidang ini dikembangkan berdasarkan kajian daripada beberapa polisi keselamatan maklumat dan temu bual yang telah dijalankan.

Jadual 2.2: Bidang fokus dan sub-bidang Model HAIS-Q.

Bidang Fokus	Sub-bidang
Penggunaan Internet	● Memasang perisian yang tidak dibenarkan. ● Melayari laman sesawang yang meragukan. ● Penggunaan Internet yang tidak sesuai.
Penggunaan emel	● Memajukan (*forwarding*) emel. ● Membuka lampiran emel.
Penggunaan rangkaian media sosial	● Jumlah masa kerja yang dihabiskan di rangkaian media sosial. ● Akibat daripada rangkaian media sosial. ● Memuat naik mengenai kerja di rangkaian media sosial.
Pengurusan kata laluan	● Mengunci komputer. ● Perkongsian kata laluan. ● Memilih kata laluan yang baik.
Pelaporan insiden	● Melaporkan individu yang mencurigakan. ● Melaporkan tingkah laku buruk oleh rakan sekerja. ● Melaporkan semua insiden keselamatan.
Pengendalian maklumat	● Melindungi peranti peribadi elektronik secara fizikal. ● Menghantar maklumat sensitif melalui rangkaian mudah alih. ● Memeriksa emel kerja melalui rangkaian percuma.
Pengkomputeran mudah alih	● Membuang dokumen sensitif. ● Memasukkan peranti DVD/USB. ● Membiarkan bahan sensitif tidak dilindungi.

2.3.3 MODEL *INFORMATION SECURITY AWARENESS IDENTIFICATION* (ISAIM)

Model *Information Security Awareness Identification* (ISAIM) yang dibangunkan oleh Ramalingam et al. (2014) 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 2.3.

1. Penggunaan yang berkesan - elemen untuk mengenal pasti berapa kerap pengguna menggunakan peranti bagi tujuan penggunaan dan lokasi capaian.

2. Kesedaran organisasi - elemen untuk mengenal pasti pengetahuan pengguna tentang persekitaran mereka seperti ketersediaan infrastruktur teknologi maklumat, dasar keselamatan, dan piawaian keselamatan.

3. Kesedaran ancaman - elemen untuk mengenal pasti pengalaman ancaman seseorang, kekerapan, kerugian akibat serangan, pengetahuan mengenai polisi keselamatan dan mekanisme pelaporan.

4. Kesedaran perlindungan - elemen untuk mengenal pasti keberkesanan identiti individu untuk memilih dan mengurus.

5. Kesedaran kandungan - elemen untuk mengenal pasti bagaimana pengguna menilai kesahihan kandungan emel.

6. Amalan keselamatan - elemen untuk mengenal pasti komponen keselamatan kemahiran yang diperlukan, latihan yang dihadiri dan latihan yang diperlukan.

Rajah 2.3: Model *Information Security Awareness Identification* (ISAIM) (Ramalingam et al. 2014).

2.3.4 MODEL KESEDARAN KESELAMATAN MAKLUMAT

Model Kesedaran Keselamatan Maklumat Bharathi & Suguna (2014) diklasifikasikan kepada tiga (3) peringkat iaitu peringkat atas, peringkat pertengahan dan peringkat bawah seperti di Rajah 2.4.

Rajah 2.4: Model Kesedaran Keselamatan Maklumat (Bharathi & Suguna 2014).

Berdasarkan kajian daripada Bharathi & Suguna (2014), 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.

Menurut Bharathi & Suguna (2014), pengurusan pengetahuan membantu individu untuk melakukan pekerjaan mereka dengan cekap dalam membuat keputusan dan penyelesaian masalah yang lebih baik. Perkara ini berguna untuk membantu pengguna sentiasa dilengkapi pengetahuan terkini dan secara langsung boleh

meminimumkan penipuan komputer. Pada peringkat organisasi, pengetahuan pengguna akan ditingkatkan apabila pengalaman dan pengetahuan mereka dikongsi. Pengurusan pengetahuan akan mendorong pengguna untuk memberi idea dan inovasi baharu serta memberi penghargaan yang sewajarnya. Malah, program latihan dan kesedaran keselamatan maklumat merangkumi isu-isu terkini dalam keselamatan maklumat dan memerlukan motivasi untuk meningkatkan kesedaran mengenai keselamatan maklumat.

Bharathi & Suguna (2014) menjelaskan bahawa, organisasi perlu mencipta imej jenama organisasi. Imej jenama positif membawa kepada keuntungan organisasi dan imej jenama negatif membawa kesan buruk kepada fikiran pengguna. Tambahan pula, kaedah keselamatan maklumat digunakan untuk melindungi maklumat daripada capaian yang tidak dibenarkan. Kaedah ini disampaikan untuk memahami prinsip dan peraturan dalam situasi yang berbeza. Menurut Bharathi & Suguna (2014) lagi, tanggungjawab merangkumi bagaimana seseorang individu menangani maklumat dengan berhati-hati dan mesti dilatih untuk menyedari kelemahan sedia ada. Pembangunan kesedaran keselamatan maklumat memerlukan gabungan latihan dan kempen kesedaran untuk meningkatkan pemahaman keselamatan maklumat.

2.4 KAJIAN LAMPAU

Bahagian ini terbahagi kepada tiga (3) bahagian. Bahagian pertama menerangkan kajian berkenaan model *Knowledge-Attitude-Behavior* (KAB) dalam menentukan faktor kesedaran keselamatan penggunaan gajet peribadi, bahagian kedua pula menerangkan kajian berkenaan model tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam, manakala bahagian ketiga menerangkan secara terperinci berkenaan pengukuran tahap keselamatan maklumat dalam kalangan pekerja di Pusat Analisis dan Perkhidmatan Maklumat Suruhanjaya Kehakiman Republik Indonesia (*Center of Analysis and Information Services Judicial Commission Republic of Indonesia*) sebagai justifikasi pemilihan model bagi membentuk model awal kajian. Pembangunan model awal dalam kajian ini pula adalah berdasarkan gabungan model konseptual yang sedia ada seperti Model *Knowledge-Attitude-Behavior* (KAB) (Kruger dan Kearney 2006), Model *Human Aspect of Information Security Questionnaire* (HAIS-Q) (Parsons et al. 2014), Model *Information Security Awareness*

Identification (ISAIM) (Ramalingam et al. 2014), dan model kesedaran sedia ada Model Kesedaran Keselamatan Maklumat (Bharathi & Suguna 2014).

2.4.1 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 (Ajzen & Fishbein 1980). Menurut Bulgurcu et al. (2010), 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 Mylonas et al. (2012); Ophoff dan Robinson (2014), mendapati responden yang mempunyai pengetahuan (*Knowledge*) mengenai keselamatan, lebih menyedari kewujudan perisian hasad (*malware*) di dalam telefon pintar mereka. Selain daripada itu, kajian yang dilakukan oleh Ophoff dan Robinson (2014) mendapati responden melakukan penyulitan ke atas data mereka. Bagaimanapun, dapatan kajian mereka dikata berat sebelah. Terdapat perbezaan yang ketara wujud dalam menentukan kesedaran keselamatan telefon pintar pengguna iaitu dari segi umur di mana 81% responden adalah dalam lingkungan 15-30 tahun. Pengguna dalam lingkungan umur 15 hingga 30 tahun merupakan golongan awal yang mengadaptasi teknologi.

Menurut Benenson (2012), sikap (*Attitude*) dipengaruhi oleh beberapa faktor seperti pengalaman peribadi, kebudayaan, pengaruh orang lain yang dianggap penting, media massa serta faktor emosi dalaman seseorang individu. Pengguna yang cuai seringkali mendedahkan maklumat peribadi disebabkan terperangkap dengan teknik

social engineering yang diguna oleh penjenayah siber. Sikap mengabaikan mesej memberi kebenaran (*need access to*) semasa memuat turun atau memasang aplikasi memberi implikasi besar kepada diri sendiri dan juga organisasi (Felt et al. 2012). Menurut Markelj dan Bernin (2012), situasi ini akan membenarkan pihak ketiga untuk mengakses data peribadi pengguna tanpa pengetahuan pengguna kerana aplikasi tersebut dapat mengakses data peribadi pengguna di belakang aplikasi (*running at the back of the application*) di mana pengguna tidak nampak. Merujuk kepada kajian yang dilakukan oleh Felt et al. (2012), minoriti responden sahaja yang membaca mesej mengenai kebenaran mengakses data peribadi pengguna sebelum memasang aplikasi. Keadaan ini menunjukkan pengguna gajet peribadi tidak mengambil langkah-langkah keselamatan yang sewajarnya untuk melindungi gajet peribadi (Lazau & George 2011). Sikap ini secara tidak langsung membuka ruang kepada penjenayah siber untuk mengancam gajet peribadi untuk mendapatkan data peribadi pengguna mahupun data organisasi (Benenson 2012).

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 (Sari & Candiwan, 2014). Jika pengguna mempunyai sikap yang baik tidak semestinya pengguna bertindak mengikut sikap tersebut. Kadang-kadang pengguna sedar bahawa sesuatu perkara itu salah untuk dipraktikkan, namun bila tiba masa untuk bertindak pengguna menggunakan jalan mudah supaya kerja dapat diselesaikan dengan cepat. Ini dapat dibuktikan dalam kajian yang dilaku oleh Sari dan Candiwan (2014) yang mana tahap kesedaran terhadap tingkah laku berada pada tahap yang memuaskan sahaja. Rajah 2.5 menunjukkan ringkasan kepada faktor yang mempengaruhi kesedaran keselamatan maklumat dalam kalangan pengguna gajet.

Faktor Kesedaran Manusia	1.	Pengetahuan (*Knowledge*)
	2.	Sikap (*Attitude*)
	3.	Tingkah Laku (*Behavior*)

Rajah 2.5 Ringkasan kepada faktor-faktor yang mempengaruhi kesedaran keselamatan maklumat dalam kalangan pengguna gajet (Adel Ismail Al-Alawi et. al 2016)

2.4.2 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 (Ahlan et al. 2011). 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 (Mohd Rafizam et al 2018).

Sikap adalah perasaan umum atau pendapat seseorang mengenai sesuatu (Oladosu 2012), Ia adalah pengawal tingkah laku sebenar seseorang secara sedar atau tidak secara sedar. Sikap adalah sebahagian daripada struktur kognitif yang digunakan oleh penjawat awam untuk mengatur, menstrategikan pengalaman dan tingkah laku mereka (Mohd Rafizam et al 2018). Sikap merupakan respon atau reaksi yang masih tertutup dari seseorang terhadap sesuatu perkara. Menurut Hu et al. (2012), sikap dipengaruhi oleh beberapa faktor seperti pengalaman peribadi, kebudayaan, pengaruh orang lain yang dianggap penting, media massa serta faktor emosi dalaman seseorang individu. Oleh kerana sikap merupakan sesuatu yang difikir di dalam fikiran individu maka ia sukar dilihat oleh orang lain dengan segera. Sikap penjawat awam terhadap kesedaran dalam keselamatan maklumat adalah berkenaan penerimaan atau penolakan mengaplikasikan keselamatan maklumat di persekitaran tempat kerja (Mohd Rafizam et al 2018). Cheng et al. (2013) menjelaskan bahawa penjawat awam menunjukkan minat dan motivasi yang tinggi ke arah mempelajari teknologi maklumat dan komunikasi namun tidak berminat untuk mengekalkan tahap keselamatannya. Ia juga

berpendapat bahawa penjawat awam mempunyai sikap konstruktivisme dan kepercayaan tradisional mengenai pembelajaran teknologi maklumat dan komunikasi. Faktor sikap ini juga sangat penting untuk dikaji dalam kalangan pekerja swasta dan boleh dibandingkan dengan penjawat awam.

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 (Safa et al. 2015; Hu et al. 2012; Brady 2011). Sokongan pihak pengurusan merujuk kepada komitmen daripada pihak pengurusan di dalam organisasi seperti yang dilihat oleh pekerja (Al-Salihy et al. 2003). Walau bagaimanapun, sokongan pihak pengurusan masih di peringkat awal di dalam kajian keselamatan maklumat dengan kebanyakan kajian terdahulu yang lebih fokus kepada teknologi keselamatan (Brady 2011; Santos et a. 2008). Latihan keselamatan maklumat dan program kesedaran adalah antara kaedah untuk memaklumkan kepada pekerja tentang ilmu keselamatan maklumat dalam organisasi (Martin & Rice 2011). Menurut Mohd Rafizam et al. (2018) ilmu seperti ini bertujuan untuk memperkenalkan dan menyediakan maklumat mengenai pentingnya penggunaan langkah balas atau tindakan balas keselamatan untuk mengelakkan maklumat ancaman keselamatan dan kesan ancaman kepada organisasi. Para pemimpin di dalam organisasi perlu menunjukkan tingkah laku keselamatan yang positif dan menggalakkan pekerja mereka untuk menghadiri mana-mana latihan keselamatan maklumat dan mewajibkan para pekerja mereka untuk mematuhi dasar dan peraturan keselamatan yang dilaksanakan di dalam organisasi (Safa et al. 2015). Menurut Ahlan et al. (2011), kemahiran kepimpinan adalah penting di dalam mewujudkan asas untuk kesedaran keselamatan dan telah dikatakan bahawa kepimpinan mempunyai kesan terhadap kesedaran para pekerja mengenai pentingnya mematuhi polisi atau dasar keselamatan yang digariskan oleh organisasi.

Latihan dan pendidikan dasar keselamatan maklumat adalah program yang bertujuan untuk memperkenalkan dan menyediakan maklumat mengenai kepentingan sistem keselamatan, yang mana semua pekerja harus mematuhinya. Kesedaran keselamatan maklumat boleh dicapai melalui latihan keselamatan pekerja kerana latihan adalah salah satu cara untuk menyampaikan maklumat keselamatan siber

organisasi (Sipone et al. 2014). Selain itu, latihan keselamatan maklumat juga dapat meningkatkan kemahiran pekerja untuk menggunakan sistem keselamatan dengan betul yang dapat mencegah ancaman keselamatan (Beas & Salanova 2006; Torkzadeh & Van Dyke 2002). Program latihan atau kempen kesedaran keselamatan telah dilaporkan sebagai cara terbaik untuk meningkatkan kesedaran para pekerja kerana mesej keselamatan dapat mencapai para pekerja dengan lebih efisien (Rezgui & Marks 2008). Pelaksanaan latihan keselamatan maklumat dan program kesedaran keselamatan adalah tanggungjawab pihak pengurusan. Pihak pengurusan harus mempertimbangkan dan memberi sokongan sepenuhnya kepada isu-isu keselamatan maklumat bagi memastikan tingkah laku keselamatan para pekerja boleh diterima dan diamalkan. Kandungan latihan keselamatan maklumat dan program kesedaran keselamatan maklumat harus merangkumi maklumat terperinci dan menyeluruh termasuk tahap kerosakan jika ancaman keselamatan ini tersebar di dalam sesebuah organisasi (Siponen et al. 2014).

Polisi atau dasar keselamatan maklumat amat perlu bagi sebuah organisasi swasta sediakan dalam bentuk dokumen yang mudah dibaca, difahami dan diamalkan oleh para pekerja. Kajian semasa menunjukkan bahawa polisi atau dasar keselamatan maklumat yang didokumentasi dengan baik dengan penerangan yang jelas dapat meningkatkan kesedaran pengguna tentang keselamatan maklumat (Al-Omari et al. 2013). Dengan adanya polisi atau dasar ini, insiden keselamatan di dalam organisasi dapat dikurangkan. Kajian terdahulu menegaskan bahawa polisi atau dasar keselamatan maklumat adalah penting kerana ia menyediakan satu set peraturan dan prosedur yang membantu menentukan tahap keselamatan maklumat yang disyorkan di dalam organisasi yang harus diikuti oleh para pekerja (Yildirim Y. et al. 2011). Secara umumnya, Safa et al. (2016) menyatakan bahawa polisi atau dasar keselamatan maklumat adalah penyataan niat dan objektif dasar syarikat yang bertujuan a) Untuk menunjukkan lembaga pengarah dan pengurusan tertinggi syarikat komitmen terhadap keselamatan maklumat; b) Untuk menetapkan arahan untuk perlaksanaan dan menekankan bahawa mereka melihatnya sebagai bahagian penting dalam operasi harian syarikat; c) Untuk mengekalkan kesinambungan operasi dan meneruskan perjalanan syarikat dalam menyediakan perkhidmatan yang berkualiti dan terjamin dan d) Untuk melindungi aset syarikat. Rajah 2.6 menunjukkan secara ringkas

bagaimana faktor-faktor ini mempengaruhi tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam.

Rajah 2.6 Ringkasan kepada faktor-faktor yang mempengaruhi model tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam (Mohd Rafizam et al 2018).

2.4.3 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, Mainar Swari Mahardika et al. (2020) mencadangkan tujuh (7) bidang fokus, sepuluh (10) pendekatan teknologi maklumat dan latihan yang dijalankan dalam pelbagai cara bagi mengekalkan aspek keselamatan maklumat.

Oleh itu, kajian lanjut diperlukan untuk mengukur tahap kesedaran keselamatan maklumat untuk mengenal pasti bidang keselamatan maklumat yang masih perlu bagi mengembangkan strategi atau kaedah kesedaran keselamatan maklumat yang lebih sesuai. Pelbagai kerangka yang telah digunakan untuk mengukur tahap kesedaran keselamatan maklumat. Mainar Swari Mahardika et al. (2020) memilih Model *Knowledge Attitude Behavior* (KAB) yang dihasilkan oleh Kruger dan Kearney (2006) 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 (E.A. Puspitaningrum 2018).

HAIS-Q (Parsons et al., 2014) adalah model yang dapat digunakan untuk mengukur pengetahuan, sikap dan tingkah laku pekerja, iaitu komponen yang ada dalam Model KAB. Model KAB ini juga digunakan sebagai penanda aras untuk organisasi bagi menyelesaikan pelbagai masalah (Mainar Swari Mahardika et al. 2020). Sebagai contoh, penggunaan Model KAB boleh digunakan untuk mengukur tahap keselamatan maklumat sesebuah organisasi dan ia juga boleh digunakan merancang strategi teknologi maklumat organisasi tersebut (Mainar Swari Mahardika et al. 2020). HAIS-Q mempunyai tujuh (7) bidang fokus termasuk Pengurusan kata laluan, *Password Management* (PM), Penggunaan emel, *Email Use* (EU), Penggunaan Internet*, Internet Use* (IU), Penggunaan rangkaian media sosial, *Social Media Use* (SMU), Pengkomputeran mudah alih, *Mobile Devices* (MD), Pengendalian maklumat, *Information Handling* (IH), dan Pelaporan Insiden, *Incident Reporting* (IR). Bidang fokus ini mempunyai sub-bidang sendiri seperti dalam Jadual 2.2.

2.5 CADANGAN MODEL AWAL

Berdasarkan kajian kesusasteraan yang dijalankan, didapati aspek kesedaran keselamatan maklumat adalah penting dalam mengukur tahap kesedaran keselamatan maklumat dalam kalangan kakitangan organisasi swasta bagi memastikan keselamatan perkhidmatan teknologi maklumat adalah terjamin selamat. Selain itu, komponen daripada model sedia ada juga turut membantu dalam penghasilan cadangan model awal kajian. Pemilihan komponen yang mempengaruhi kesedaran keselamatan maklumat dalam penggunaan peranti mudah alih adalah berdasarkan faktor-faktor seperti faktor pengetahuan, faktor sikap, faktor tingkah laku, faktor sokongan pihak

pengurusan, faktor latihan dan pendidikan dan faktor polisi/dasar keselamatan maklumat.

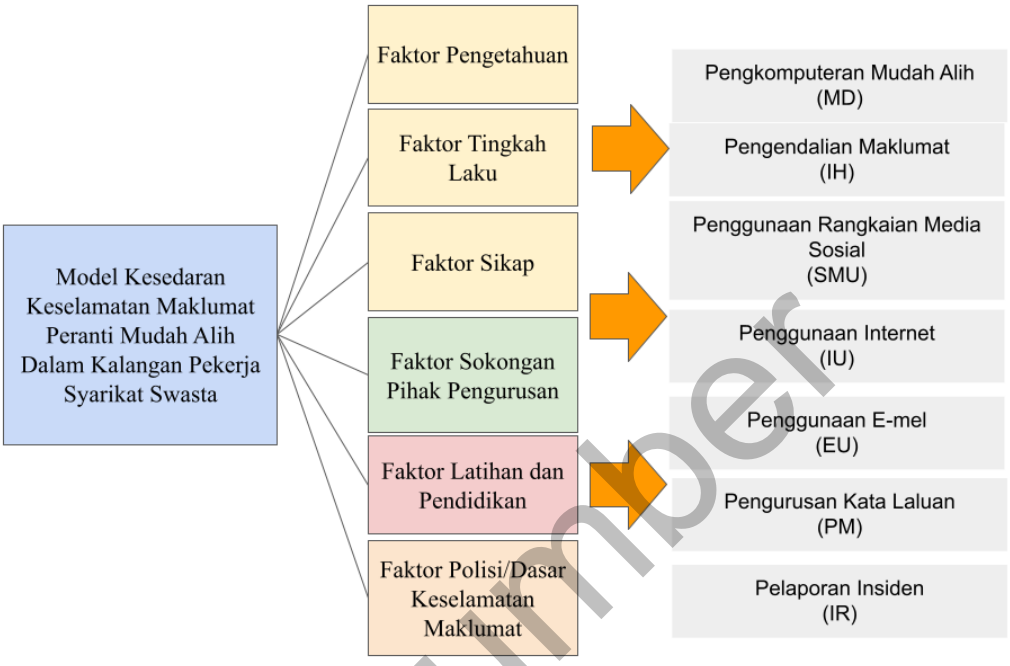
Oleh yang demikian, pembangunan model awal dalam kajian ini adalah gabungan daripada beberapa komponen kajian sedia ada dan enam (6) faktor telah dipilih sebagai komponen untuk pembangunan model awal adalah seperti di Jadual 2.3.

Jadual 2.3 : 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 (Susanto et al. 2012). ● Kajian oleh Mylonas et al. (2012); Ophoff dan Robinson (2014), 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 Ophoff dan Robinson (2014) 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 Pattinson & Anderson (2007). ● Kajian menunjukkan segelintir pengguna tahu tindakan mereka boleh memberi implikasi kepada diri sendiri mahupun organisasi, mereka memilih jalan mudah untuk membuat sesuatu kerja (Sari & Candiwan 2014).
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 (Oladosu 2012), 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 (Hu et al. 2012) bersambung...

...sambungan	● 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 (Benenson 2012)
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 (Al-Salihy et al. 2003). ● 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 (Safa et al. 2015; Hu et al. 2012; Brady 2011).
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 (Siponen et al. 2014). ● Latihan keselamatan maklumat juga dapat meningkatkan kemahiran pekerja untuk menggunakan sistem keselamatan dengan betul yang dapat mencegah ancaman keselamatan (Beas & Salanova 2006; Torkzadeh & Van Dyke 2002).
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 (Bharathi & Suguna 2014). ● Kajian semasa menunjukkan bahawa polisi atau dasar keselamatan maklumat yang didokumentasi dengan baik dengan penerangan yang jelas dapat meningkatkan kesedaran pengguna tentang keselamatan maklumat (Al-Omari et al. 2013).

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 2.7.



Rajah 2.7 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).

2.6 KESIMPULAN

Pengukuran tahap kesedaran keselamatan maklumat merupakan satu aktiviti penting untuk organisasi menilai sejauh manakah tahap kesedaran dan kesediaan mereka terutama dalam penggunaan telefon pintar dan komputer riba di pejabat. Keputusan dari aktiviti penilaian tahap kesediaan ini boleh dijadikan indikator awal dalam menentukan jurang yang perlu ditambah baik oleh organisasi. Berdasarkan kajian kesusasteraan ini mendapati bahawa setiap kajian dan model yang sedia ada mempunyai kekuatan dan kecenderungan yang berbeza berdasarkan kumpulan sasaran yang berlainan. Oleh itu, komponen yang dipilih daripada kajian dan model sedia ada adalah berdasarkan faktor-faktor penting dalam memberi kesan secara langsung kepada tahap kesedaran keselamatan maklumat pengguna telefon pintar dan komputer riba dalam kalangan pekerja syarikat swasta.

Kajian kesusasteraan juga dilaksanakan bagi meneliti kajian lampau kerangka kerja teknologi maklumat dan model sedia ada bagi mendapatkan faktor kesedaran keselamatan maklumat dan seterusnya membentuk model awal kajian. Model awal kajian adalah terdiri daripada enam (6) faktor dan tujuh (7) sub-bidang berdasarkan kajian kesusasteraan yang dijalankan di dalam bab ini. Seterusnya, model awal ini akan digunakan dalam bab seterusnya sebagai penanda aras sebelum mendapat pengesahan dan idea penambahbaikan dari perspektif pakar bidang untuk menambah baik model yang dicadangkan.

BAB III

METODOLOGI KAJIAN

3.1 PENGENALAN

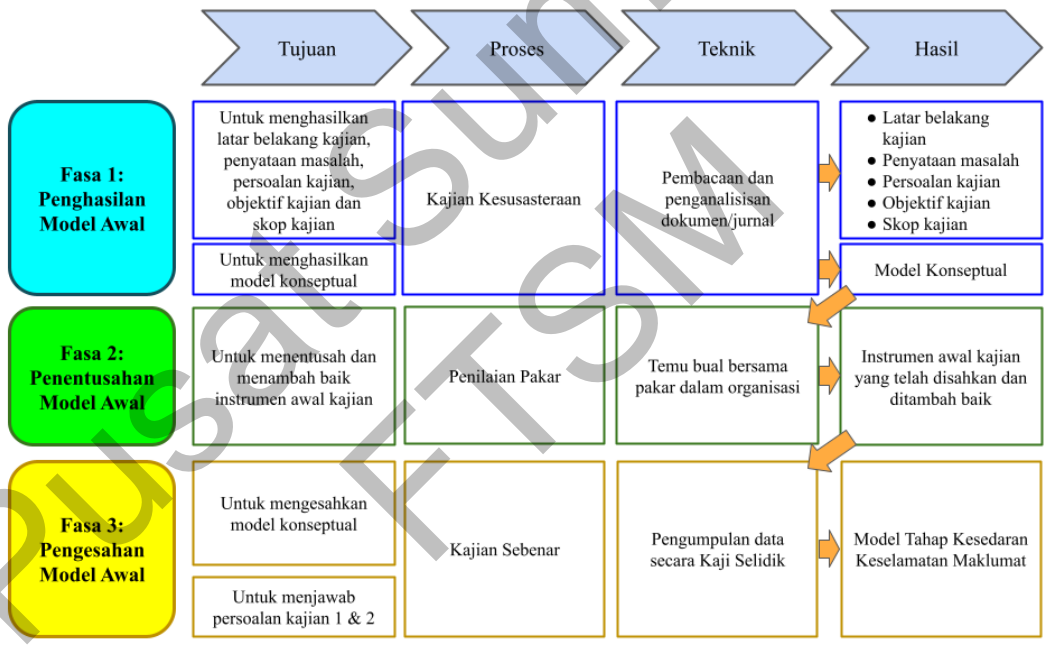
Bab III ini membincangkan tentang metodologi digunakan sebagai pendekatan dalam melaksanakan kajian ini. Metodologi merupakan prinsip, amalan, dan prosedur yang digunakan untuk bidang pengetahuan dan teknologi khusus yang membantu penyelidik sistem maklumat untuk menghasilkan penyelidikan sistem maklumat yang berkualiti tinggi, bernilai, padat, dan layak diterbitkan (Peffers et al. 2008). Metodologi kajian pula merupakan satu kaedah dan teknik dalam mereka bentuk, mengumpul dan menganalisis data bagi menghasilkan bukti yang boleh menyokong sesuatu kajian.

Oleh itu, dalam kajian ini, kaedah kualitatif digunakan untuk pembangunan model awal berdasarkan asas teori kajian terdahulu dan faktor yang dipilih mengikut komponen domain berdasarkan perspektif pakar. Kajian ini turut menggunakan kaedah kuantitatif untuk menilai tahap kesedaran keselamatan maklumat melalui kaji selidik dan analisis sampel data. Kaedah ini adalah bertujuan menghasilkan kesimpulan yang lebih baik selain meningkatkan kesahihan dan penghasilan hasil analisis yang mantap (Creswell 2012). Gabungan kaedah kualitatif dan kuantitatif adalah sangat penting bagi melaksanakan kaedah kerja yang efektif semasa menjalankan kajian dan menjawab masalah kajian.

Bagi menyempurnakan tujuan kajian ini, kelulusan daripada pihak pengurusan organisasi BIT Group Sdn Bhd perlu diperoleh bagi memastikan keseluruhan kajian dapat dilaksanakan dengan lancar. Sesi penerangan dilaksanakan untuk memaklumkan (i) objektif dan kepentingan kajian; (ii) perancangan kajian; dan (iii) mendapatkan input bagi membantu kelancaran kajian.

3.2 METODOLOGI KAJIAN

Dalam kajian ini, metodologi yang digunakan adalah gabungan kaedah kualitatif iaitu secara temu bual dengan pakar dan kaedah kuantitatif iaitu penggunaan kaji selidik. Pendekatan kajian melibatkan tiga (3) fasa utama iaitu (i) Fasa 1 - penghasilan model awal; (ii) Fasa 2 - penentusahan model awal; dan (iii) Fasa 3 - pengesahan model. Setiap fasa mempunyai beberapa aktiviti yang dirancang mengikut keutamaan berdasarkan kesesuaian organisasi yang dikaji. Setiap fasa juga diperincikan kepada proses-proses yang terlibat; tujuan pelaksanaan setiap proses, teknik yang digunakan bagi setiap proses dan hasil akhir bagi setiap proses. Gambaran metodologi kajian iaitu Fasa 1, Fasa 2 dan Fasa 3 seperti yang diterangkan di dalam Rajah 3.1 berikut:



Rajah 3.1 : Metodologi Kajian

Rajah 3.1 menerangkan proses mengenal pasti masalah kajian. Menerusi proses kajian kesusasteraan yang dijalankan akan dapat mengenal pasti penemuan jurang dan seterusnya menghasilkan persoalan kajian. Penerangan secara terperinci berkenaan pendahuluan, penyataan masalah, persoalan kajian, matlamat dan objektif kajian, kepentingan serta skop kajian telah diterangkan di dalam Bab I.

3.3 FASA 1: PENGHASILAN MODEL AWAL

Kajian kesusasteraan telah dilaksanakan melalui pembacaan dan analisis artikel dan jurnal berkaitan kesedaran keselamatan maklumat, faktor-faktor yang mempengaruhi kesedaran keselamatan maklumat dan sub-bidang yang berkaitan dengan penggunaan peranti mudah alih seperti telefon pintar dan komputer riba. Hasil pembacaan dan analisis ini telah berjaya menghasilkan penyataan masalah, objektif, persoalan dan skop kajian.

Kajian kesusasteraan juga meliputi pembacaan dan penelitian asas teori kajian terdahulu berkenaan model kesedaran sedia ada untuk menghasilkan model awal.

3.3.1 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 seperti yang dibincangkan di dalam Bab II.

Analisis tersebut bertujuan untuk mendapatkan latar belakang kajian, penyataan masalah, persoalan kajian, objektif kajian dan skop kajian serta untuk menghasilkan model konseptual seperti di Bab I. Rumusan komponen penting yang telah dikenal pasti menerusi kajian kesusasteraan yang dijalankan adalah seperti di Jadual 3.1.

Jadual 3.1 : 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

3.3.2 Merangka Model Awal

Proses penghasilan model konseptual, kajian kesusasteraan telah dilakukan yang merangkumi aktiviti pembacaan jurnal, buku dan artikel yang berkaitan dengan model kesedaran keselamatan maklumat. Kajian kesusasteraan dapat meningkatkan pemahaman tentang bidang kajian dan aspek yang berkaitan dengan penyelidikan dapat diterokai. Menerusi kajian kesusasteraan juga, ianya dapat membantu memahami dan mengenal pasti jurang pengetahuan yang dihasilkan dari kajian terdahulu dalam bidang yang dikaji. Proses yang terlibat dalam merangka model konseptual kajian adalah seperti di Jadual 3.2.

Jadual 3.2 : 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 3.2 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 di dalam Bab II.

Pembangunan model konseptual dibangunkan dengan mengenal pasti model kesedaran yang dibincangkan di dalam Bab II iaitu model daripada (i) Model *Knowledge-Attitude-Behavior* (KAB) (Kruger and Kearney 2006) (ii) Model Tahap Kesedaran Keselamatan Maklumat Dalam Kalangan Penjawat Awam (Mohd Rafizam et al 2018); dan (iii) *Human Aspect of Information Security Questionnaire* (HAIS-Q) (Parsons et al. 2014).

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 3.3.

Jadual 3.3 : Pemilihan komponen setiap model

Bil	Model	Komponen
1	Model *Knowledge-Attitude-Behavior* (KAB)	• Faktor Pengetahuan • 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 3.4:

Jadual 3.4 : 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.

bersambung...

	...sambungan	
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.
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.

3.4 FASA 2: PENENTUSAHAN 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 3.5.

Jadual 3.5 : Penentusahan model awal

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 3.4. Komponen tersebut kemudiannya ditentusah dan dikomen oleh pakar di organisasi yang dikaji menerusi kaedah temu bual seperti di dalam Borang Penilaian dan Pengesahan Pakar di Lampiran A. Penilaian dan komen yang dibuat oleh pakar diambil kira dan dimasukkan dalam Borang Penilaian dan Pengesahan Pakar (Kemaskini) seperti di Lampiran B untuk ditentusahkan. Kaedah temu bual ini digunakan agar penentuan komponen dapat ditentusahkan 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 Sumber Manusia & Transformasi (HR) di BIT Group Sdn Bhd. Pakar tersebut merupakan daripada kumpulan Pengurusan dan Profesional yang telah berkhidmat di organisasi selama lebih 10 tahun dan

berpengalaman selama 38 tahun. Beliau juga memegang jawatan sebagai Pengurus Besar Sumber Manusia & Transformasi di BIT Group Sdn Bhd dan terlibat secara langsung dalam pengoperasian syarikat dan pelaksanaan dasar serta polisi organisasi. Bagi mengukuhkan lagi soalan kaji selidik ini, pakar kedua dipilih daripada salah sebuah anak syarikat BIT Group iaitu NexQuadrant Sdn Bhd (BIT Group Managed Services). Pakar tersebut merupakan Ketua Pegawai Operasi (COO) kepada syarikat NexQuadrant Sdn Bhd dan terlibat secara langsung dengan aktiviti berkaitan keselamatan siber. Beliau telah berkhidmat hampir 30 tahun dan mengendalikan dan menguruskan hampir lima puluh (50) projek-projek berkaitan keselamatan siber.

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) seperti di Lampiran C. 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]. Rajah 3.2 menunjukkan soalan kaji selidik yang diedarkan secara digital.

Rajah 3.2: Soalan kaji selidik di platform *Google Forms*

3.5 FASA 3: 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. Analisis pengesahan model ini akan dibincangkan lanjut di bab seterusnya. Proses yang terlibat dalam mengesahkan model kajian adalah seperti di Jadual 3.6.

Jadual 3.6 : Pengesahan model awal

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

3.5.1 MENENTUKAN KUMPULAN SASARAN

Sebelum soalan kaji selidik diedarkan, kumpulan sasaran perlu ditentukan terlebih dahulu. Bagi memudahkan mendapat responden, keseluruhan staf di BIT Group Sdn Bhd dipilih untuk dijadikan populasi responden disebabkan di bawah BIT Group Sdn Bhd ada tujuh (7) anak syarikat dan ini lebih sesuai untuk mengkaji tahap kesedaran keselamatan maklumat dalam setiap syarikat. Selain itu, pengkaji juga merupakan salah seorang staf dari syarikat BIT Academy, iaitu anak syarikat yang menguruskan hal berkaitan latihan kepada keseluruhan syarikat di bawah BIT Group Sdn Bhd dan ini memudahkan mendapat responden untuk kajian ini.

Untuk kajian ini, kumpulan sasaran yang dikenali sebagai responden selepas ini adalah 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. Syarikat BIT Group Sdn Bhd mempunyai ketiga-tiga jenis kumpulan sasaran ini dan juga jenis kumpulan dalam organisasi. Oleh itu, adalah relevan responden dipilih sebagai populasi untuk menjawab kaji selidik ini.

3.5.2 PENGUJIAN SOALAN

Pada ketika kajian ini dibuat, negara berada dalam Fasa 1 dan 2 Pelan Pemulihan Negara (PPN) dan semua pekerja bekerja dari rumah dan tiada orang di pejabat. Jadi, soalan yang dibangunkan adalah dalam bentuk digital dan diuji terlebih dahulu. Soalan dalam bentuk digital ini diuji, ditentusahkan dan dipersetujui oleh pakar. Soalan kaji selidik juga diuji oleh pakar dengan menjawab soalan tersebut terlebih dahulu untuk memastikan keberkesanan soalan yang ditanya. Soalan juga dibahagi

beberapa bahagian supaya responden menjawab dengan mudah, mengambil masa yang pendek untuk menjawab setiap sub-bahagian dan dapat memberi tumpuan untuk menjawabnya.

Bagi soalan dalam bentuk digital ini, platform dalam talian *Google Forms* digunakan. Pengujian soalan versi digital ini dilakukan oleh pakar untuk memastikan perjalanan proses kaji selidik berjalan dengan lancar. Pengujian ini juga penting untuk memastikan semua soalan berfungsi sepenuhnya dan data yang dijawab oleh responden masuk ke dalam pangkalan data *Google Forms* untuk memudahkan analisis dibuat. Selain daripada itu, alamat URL juga diuji untuk memastikan alamat tersebut sahih dan boleh dicapai oleh semua responden.

3.5.3 PENGAGIHAN SOALAN

Setelah soalan soal selidik siap dibina dan diuji, soalan tersebut kemudiannya diagih secara serentak kepada responden yang telah ditetapkan iaitu sebanyak 176 orang dalam kalangan ke semua staf di bawah naungan BIT Group Sdn Bhd. Kesemua 176 orang responden ini adalah terdiri daripada pelbagai jenis jawatan dan mereka diberikan soalan dalam bentuk digital iaitu menggunakan menggunakan platform dalam talian *Google Forms* kerana semua staf bekerja dari rumah dan berada di pelbagai negeri. Tempoh menjawab kaji selidik ini diberikan selama tiga (3) hari iaitu pada 11 hingga 13 Ogos 2020.

3.6 ANALISIS DATA

Analisis data merupakan aktiviti yang penting dan amat diperlukan dalam proses kajian. Menurut Muhson (2006), 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.

3.6.1 UJIAN KEBOLEHPERCAYAAN

Sebelum sesuatu instrumen ditadbir dalam kajian sebenar, ia perlu melalui proses mengukur kesahan dan kebolehpercayaan item bagi menjamin kualiti instrumen dan data yang diperolehi. Tahap ini penting bagi memastikan ketepatan data dalam penyelidikan data yang sebenar dapat menjawab semua persoalan kajian yang telah digariskan.

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 Joseph et al. (2010), 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. Skor kebolehpercayaan adalah seperti di Jadual 3.7.

Jadual 3.7 : Skor kebolehpercayaan *Cronbach Alpha*.

Skor	Kebolehpercayaan
0.9 hingga 1.0	Sangat baik dan efektif dengan tahap konsistensi yang tinggi
0.7 hingga 0.8	Baik dan boleh diterima
0.6 hingga 0.7	Boleh diterima
< 0.6	Item perlu dibaiki
< 0.5	Item perlu digugurkan

3.6.2 KEKERAPAN DAN UJIAN SKOR MIN

Analisis deskriptif digunakan untuk mendapatkan kekerapan, min dan sisihan piawai untuk memenuhi keperluan objektif yang ditentukan. Menurut Siddharth Kalla (2009),

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 Deborah (2009), min atau purata adalah statistik yang umum digunakan untuk mengukur pusat kumpulan data berangka dan jumlah semua nilai dalam kumpulan data dibahagi dengan jumlah nilai dalam kumpulan data. Manakala tafsiran statistik min yang digunakan diubah suai daripada Landell (1997) adalah seperti di Jadual 3.8.

Jadual 3.8 : Skor tafsiran min Landell (1997).

Skor (*r*)	**Tahap**
1.00 hingga 3.26	Rendah
3.27 hingga 5.14	Sederhana
5.15 hingga 7.00	Tinggi

3.6.3 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 Joseph et al. (2010) menyatakan bahawa, analisis faktor adalah bertujuan untuk mengurangkan dan merumuskan data yang melibatkan item yang berulang digabungkan dan item yang tidak berkaitan digugurkan. Menurut Costello & Osborne (2005) 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.

Kepentingan pemuatan memberikan sedikit petunjuk tentang pentingnya pemboleh ubah kepada faktor. Nilai ini dapat dijumpai dengan kuasa dua oleh pemboleh ubah. Dalam hal ini Stevens (2002) mengesyorkan untuk penafsiran hanya pemuatan faktor dengan nilai mutlak lebih besar daripada .4 (yang menjelaskan sekitar 16% varian dalam pemboleh ubah).

3.6.4 UJIAN KORELASI

Menurut Syazwani (2017), 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 Hussin (2011) 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 Chong et al. (2013), 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.

Ujian korelasi *Pearson* digunakan bagi menjawab soalan-soalan kajian ini. Hubungan di antara pemboleh ubah dalam kajian ini adalah dengan mengambil kira kekuatan

hubungan yang berpandukan kepada skala kekuatan hubungan oleh Cohen et al. (2011) seperti ditunjukkan di Jadual 3.9.

Jadual 3.9 : Skor kekuatan hubungan korelasi

Skor (*r*)	Kekuatan Korelasi
±.81 hingga 1.00	Sangat kuat
±.51 hingga .80	Kuat
±.31 hingga .50	Sederhana
±.21 hingga .30	Lemah
±.01 hingga .20	Sangat lemah

3.7 KESIMPULAN

Secara keseluruhannya, Bab III menerangkan tentang kaedah metodologi kajian secara terperinci merangkumi reka bentuk kajian, merangka model awal, pengumpulan dan penentusahan maklumat oleh pakar, penganalisisan hasil ulasan dari pakar, hasil kaji selidik dan ujian rintis. Pendekatan kajian yang digunakan bagi mencapai objektif kajian seterusnya menjawab persoalan kajian yang ditetapkan. Hasil akhir kajian ini merupakan satu model kesedaran keselamatan maklumat bagi penggunaan peranti mudah alih dalam kalangan pekerja syarikat swasta yang dikaji, iaitu BIT Group Sdn Bhd dan tujuh (7) anak syarikatnya. Secara keseluruhannya, metodologi kajian merupakan kaedah untuk menjalankan eksperimen dalam mencapai objektif kajian ini seperti yang dibincangkan di Bab I.

BAB IV

DAPATAN KAJIAN

4.1 PENGENALAN

Bab IV melaporkan dapatan kajian dan analisis data yang diperolehi berdasarkan kajian kes yang dijalankan. Berdasarkan kepada objektif kajian, terdapat tiga analisis yang dilakukan dalam kajian ini iaitu analisis pertama adalah pengesahan instrumen oleh pakar, diikuti analisis kedua merupakan hasil kaji selidik daripada kajian kes, dan analisis ketiga penghasilan reka bentuk model akhir kajian. Analisis statistik secara deskriptif diguna bagi menjawab objektif kajian untuk mengenal pasti tahap kesedaran keselamatan maklumat dalam kalangan pekerja syarikat swasta. Hasil kajian menjawab persoalan kajian dan objektif kajian yang dinyatakan di dalam Bab I. Semua hasil analisis dibentangkan dalam bentuk ilustrasi grafik hasil daripada kajian menggunakan *Google Form* dan dianalisis menggunakan sistem *Statistical Package for Social Science* (SPSS), versi 28.

4.2 PENGHASILAN 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.

4.3 PENENTUSAHAN MODEL AWAL

Bagi menentusah model awal kajian, enam (6) komponen yang telah dikenal pasti pada fasa penghasilan model awal diperincikan dalam bentuk soalan kaji selidik

seperti di dalam Borang Penilaian dan Pengesahan Pakar (Kemaskini) (rujuk Lampiran B). 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) (Kruger and Kearney 2006) (ii) Model Tahap Kesedaran Keselamatan Maklumat Dalam Kalangan Penjawat Awam (Mohd Rafizam et al 2018); dan (iii) *Human Aspect of Information Security Questionnaire* (HAIS-Q) (Parsons et al. 2014). Jadual 4.1 berikut menunjukkan rumusan aktiviti dan hasil yang diperolehi daripada sesi penentusahan pakar yang telah dijalankan.

Jadual 4.1 : Rumusan aktiviti dan hasil penentusahan pakar

Tarikh	Aktiviti	Hasil
5 Ogos hingga 10 Ogos 2021	Sesi temu bual dan perbincangan bersama dua (2) orang pakar masing-masing dari syarikat BIT Group Sdn Bhd dan NexQuadrant Sdn Bhd secara atas talian	Penentusahan model awal dan soalan kaji selidik

Dalam kajian ini, seramai dua (2) orang pakar dipilih dan pemilihan pakar adalah berdasarkan bidang kepakaran dalam bidang sumber manusia, transformasi dan keselamatan siber. Kedua-dua pakar memberi kebenaran untuk maklumat mereka diterbitkan. Jadual 4.2 menunjukkan maklumat ringkas berkenaan pakar yang dipilih.

Jadual 4.2 : Maklumat pakar bidang

Pakar	Syarikat	Jawatan	Kepakaran
Pakar 1	BIT Group Sdn Bhd	Pengurus Besar (GM) Sumber Manusia dan Servis Korporat (Transformasi)	38 tahun pengalaman dalam bidang IT, Telekomunikasi, Pengurusan dan Transformasi.
Pakar 2	NexQuadrant Sdn Bhd (BIT Group Managed Services)	Ketua Pegawai Operasi (COO) NexQuadrant Sdn Bhd	30 tahun pengalaman dalam bidang operasi, keselamatan maklumat, rangkaian dan sistem.

4.4 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. Jadual 4.3 berikut menunjukkan rumusan penentusahan pakar berkenaan bentuk soalan kaji selidik yang perlu ditanyakan dan dipersetujui oleh mereka berdasarkan apa yang dicadangkan dalam model awal.

Jadual 4.3 : Rumusan penentusahan pakar terhadap soalan kaji selidik

Bahagian	Kod Item	Soalan kaji selidik	Penentusahan Pakar
Faktor Pengetahuan	A1	Apakah peranti peribadi mudah alih yang dibawa ke tempat kerja anda? ● Telefon Pintar ● Komputer Riba ● Lain-lain (Sila Nyatakan)	Pakar 1 Setuju & Pakar 2 Setuju
	A2	Apakah sistem pengoperasian peranti peribadi bagi telefon pintar yang digunakan? ● Android ● Apple iOS ● Lain-lain (Sila Nyatakan)	Pakar 1 Setuju & Pakar 2 Setuju
	A3	Apakah sistem pengoperasian peranti peribadi bagi komputer riba yang digunakan? ● Windows ● Linux ● macOS ● Lain-lain (Sila Nyatakan)	Pakar 1 Setuju & Pakar 2 Setuju
	A4	Apakah peranan anda di dalam organisasi? ● Pengguna biasa (tidak melibatkan sistem) ● Pengguna sistem ● Pentadbir sistem	Pakar 1 Setuju & Pakar 2 Setuju
	A5	Tukar soalan "Adakah anda mengunci atau meletakkan kata laluan pada telefon pintar anda?" kepada penyataan "Anda mengunci atau meletakkan kata laluan pada telefon pintar anda."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju

bersambung...

...sambungan			
	A6	Tukar soalan "Adakah anda mengunci atau meletakkan kata laluan pada komputer riba anda?" kepada penyataan "Anda mengunci atau meletakkan kata laluan pada komputer riba anda."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
Faktor Tingkah Laku	B1	Tukar soalan "Adakah anda pernah menggunakan WiFi Awam (*Public WiFi*)?" kepada penyataan "Anda pernah menggunakan WiFi Awam (*Public WiFi*)."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
	B2	Tukar soalan "Adakah anda menghantar emel/memuat turun dokumen pejabat menggunakan sambungan WiFi yang selamat (*Secured WiFi*)?" kepada penyataan "Anda menghantar emel/memuat turun dokumen pejabat menggunakan sambungan WiFi yang selamat (*Secured WiFi*)."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
	B3	Tukar soalan "Adakah anda pernah memuat turun (*download*) perisian dari Internet tanpa pengetahuan dan kebenaran daripada syarikat anda?" kepada penyataan "Anda pernah memuat turun (*download*) perisian dari Internet tanpa pengetahuan dan kebenaran daripada syarikat anda."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak.
	B4	Tukar soalan "Adakah anda pernah memuat turun (*download*) perisian dari Internet tanpa pengetahuan tetapi mematuhi apa yang dibenarkan oleh polisi syarikat anda?" kepada penyataan "Anda pernah memuat turun (*download*) perisian dari Internet tanpa pengetahuan tetapi mematuhi apa yang dibenarkan oleh polisi syarikat anda."	Pakar 2 cadangkan tambah satu lagi soalan "...tanpa pengetahuan tetapi mematuhi polisi syarikat"
	B5	Tukar soalan "Adakah anda menggunakan akaun emel pejabat untuk kegunaan peribadi?" kepada penyataan "Anda menggunakan akaun emel pejabat untuk kegunaan peribadi."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
	B6	Tukar soalan "Adakah Anda pernah memuat turun (*download*) dokumen/fail yang dihantar oleh penerima yang tidak dikenali?" kepada penyataan "Anda pernah memuat turun (*download*) dokumen/fail yang dihantar oleh penerima yang tidak dikenali."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju

bersambung...

...sambungan			
	B7	Tukar soalan "Adakah anda pernah menerima emel yang mencurigakan dan mengklik pada URL (*link*) di dalam kandungan emel tersebut?" kepada penyataan "Anda pernah menerima emel yang mencurigakan dan mengklik pada URL (*link*) di dalam kandungan emel tersebut."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
Faktor Sikap	C1	Tukar soalan "Adakah anda mempunyai kata laluan yang berbeza bagi setiap sistem yang digunakan?" kepada penyataan "Anda mempunyai kata laluan yang berbeza bagi setiap sistem yang digunakan."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
	C2	Berapa kalikah anda menukar kata laluan? ● 1-3 bulan sekali ● 4-6 bulan sekali ● 7-9 bulan sekali ● 10-12 sebulan sekali ● Tidak pernah tukar	Pakar 1 Setuju & Pakar 2 Setuju
	C3	Apakah cara anda mengingat kata laluan? ● Tukar "Dengan hati" kepada "Menulis dan simpan di tempat rahsia" ● Menulis dan letak atas meja ● Menulis dan letak di bawah keyboard ● Menulis dan tampal di dinding/papan kenyataan ● Menulis dan simpan di dalam telefon ● Lain-lain (Sila Nyatakan)	Pakar 1 Setuju & Pakar 2 cadangkan tukar "Dengan hati" kepada "Menulis dan simpan di tempat rahsia" dalam pilihan jawapan.
	C4	Tukar soalan "Adakah kata laluan ada mengandungi nombor & simbol?" kepada penyataan "Kata laluan anda ada mengandungi huruf besar, huruf kecil, nombor & simbol (kompleks)."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 cadangkan untuk tambah huruf besar dan huruf kecil (kompleks)
	C5	Tukar soalan "Adakah anda pernah menggunakan dan melayari media sosial untuk tujuan peribadi di tempat kerja?" kepada penyataan "Anda pernah menggunakan dan melayari media sosial untuk tujuan peribadi di tempat kerja dalam tempoh waktu bekerja."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 cadangkan untuk tambah "...dalam tempoh waktu bekerja."

bersambung...

...sambungan			
	C6	Tukar soalan "Adakah anda pernah berkongsi maklumat rasmi atau sulit tentang syarikat di media sosial?" kepada penyataan "Anda pernah berkongsi maklumat rasmi atau sulit tentang syarikat di media sosial."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
Faktor Sokongan Pihak Pengurusan	D1	Tukar soalan "Adakah pihak pengurusan membenarkan anda bawa peranti peribadi anda seperti telefon pintar dan komputer riba ke pejabat?" kepada penyataan "Pihak pengurusan membenarkan anda bawa peranti peribadi anda seperti telefon pintar dan komputer riba ke pejabat."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
	D2	Tukar soalan "Adakah pihak pengurusan menyediakan emel khas dari syarikat untuk tujuan kerja?" kepada penyataan "Pihak pengurusan menyediakan emel khas dari syarikat untuk tujuan kerja."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
	D3	Tukar soalan "Adakah pihak pengurusan menyarankan penukaran kata laluan pada emel pejabat dan peranti peribadi anda setiap 3-6 bulan?" kepada penyataan "Pihak pengurusan menyarankan penukaran kata laluan pada emel pejabat dan peranti peribadi anda setiap 3-6 bulan."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
	D4	Tukar soalan "Adakah pihak pengurusan pernah membuat sesi taklimat keselamatan maklumat kepada semua staf?" kepada penyataan "Pihak pengurusan pernah membuat sesi taklimat keselamatan maklumat kepada semua staf."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju
	D5	Tukar soalan "Jika ya, pernahkah anda menandatangani sebarang surat pematuhan taklimat keselamatan maklumat tersebut?" kepada soalan "Jika setuju, pernahkah anda menandatangani sebarang surat pematuhan taklimat keselamatan maklumat tersebut?"	Pakar 1 cadangkan tukar soalan "Jika ya" kepada "Jika setuju" Pakar 2 Setuju
Faktor Latihan dan Pendidikan	E1	Tukar soalan "Adakah pihak syarikat menjalankan sesi latihan berkenaan kesedaran keselamatan maklumat kepada semua staf?" kepada penyataan "Pihak syarikat menjalankan sesi latihan berkenaan kesedaran keselamatan maklumat kepada semua staf."	Pakar 1 cadangkan tukar soalan kepada penyataan responden boleh bersetuju atau tidak. Pakar 2 Setuju

bersambung...

...sambungan	E2	Tukar soalan "Jika ya, adakah anda memahami dan mempraktikkan apa yang dipelajari dari segi keselamatan maklumat?" kepada soalan "Jika setuju, adakah anda memahami dan mempraktikkan apa yang dipelajari dari segi keselamatan maklumat?"	Pakar 1 cadangkan tukar soalan "Jika ya" kepada "Jika setuju" Pakar 2 Setuju
	E3	Pernahkah anda melihat risalah atau poster berkenaan keselamatan maklumat di tempat kerja?	Pakar 1 Setuju & Pakar 2 Setuju
	E4	Pada pandangan anda, adakah taklimat/latihan keselamatan maklumat perlu dilaksanakan secara berkala?	Pakar 1 Setuju & Pakar 2 Setuju
Faktor Polisi/Dasar Keselamatan Maklumat	F1	Adakah anda tahu kewujudan Dasar Keselamatan ICT di syarikat anda?	Pakar 1 Setuju & Pakar 2 menyatakan bahawa polisi/dasar ada di dalam Sistem Portal Syarikat
	F2	Jika ya, adakah anda pernah baca Dasar Keselamatan ICT di syarikat anda?	Pakar 1 Setuju & Pakar 2 menyatakan bahawa beliau individu yang bertanggungjawab menulis polisi/dasar keselamatan syarikat
	F3	Pada pandangan anda, wajarkah syarikat mengeluarkan satu dokumen berkaitan Dasar Keselamatan ICT di syarikat anda?	Pakar 1 Setuju & Pakar 2 Setuju

Selepas selesai aktiviti penentusahan model awal dan soalan kaji selidik, kedua-dua pakar bersetuju dengan cadangan model awal seperti yang dibentangkan dalam Bab II (Rajah 2.7) tanpa sebarang perubahan kerana komponen yang dipilih sudah mencukupi dan memadai bagi syarikat swasta. Penambahbaikan hanya dilakukan kepada bentuk dan kaedah soalan kaji selidik ditanya sahaja. Jadi, tiada perubahan daripada model awal.

4.5 PENGUMPULAN DATA

Soalan kaji selidik diagih secara serentak dan secara dalam 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. Ringkasan maklumat pengumpulan data adalah seperti di Jadual 4.4.

Jadual 4.4 : Maklumat pengumpulan data

Tarikh	11 hingga 13 Ogos 2021
Tajuk	Kaji Selidik Tahap Kesedaran Keselamatan Maklumat Peranti Mudah Alih Dalam Kalangan Pekerja Syarikat BIT Group Of Companies.
Organisasi terlibat	BIT Group Sdn Bhd (Syarikat Induk) dan 7 anak syarikat dibawahnya iaitu BIT Sdn Bhd, BIT Software Sdn Bhd, BIT Academy Sdn Bhd, NexQuadrant Sdn Bhd, Sadiqin Sdn Bhd dan As Sehah Digital Sdn Bhd
Kumpulan Sasaran	Kumpulan Pengurusan dan Profesional dan Kumpulan Sokongan dan Pelaksana yang terdiri daripada ● Pengguna biasa (tidak melibatkan sistem secara langsung) ● Pengguna sistem ● Pentadbir sistem
Bilangan responden	75 daripada 176 responden
Kaedah agihan	Secara email melalui *Google Form* (kaji selidik secara atas talian)

Lampiran C yang disediakan adalah soalan kaji selidik yang telah ditentusahkan oleh pakar dan ia dijalankan bagi tujuan pengumpulan maklumat dan data dari pelbagai jenis responden dari seluruh Malaysia. Setiap instrumen kajian telah diteliti dan dinilai oleh pakar disamping ujian kebolehpercayaan juga diadakan bagi

mengesahkan setiap bentuk soalan kaji selidik yang akan diedarkan kepada semua staf.

4.6 UJIAN KEBOLEHPERCAYAAN

Nilai *Cronbach Alpha* dicari untuk menentukan kebolehpercayaan setiap item dalam soalan kaji selidik. Menurut George dan Mallery (2003), 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 Taber (2018), nilai *Cronbach's Coefficient Alpha* boleh mengukur tahap kebolehpercayaan items untuk menguji kesahihan soalan kaji selidik yang dibangunkan. Seramai sebelah (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 4.5. Nilai ini menunjukkan indeks kebolehpercayaan item adalah baik dan boleh diterima serta memenuhi ciri-ciri yang dikehendaki.

Jadual 4.5 : 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

Menurut Nunnally and Bernstein (1994), nilai 0.70 cukup untuk peringkat awal penyelidikan sebagai panduan dalam penafsiran pekali kebolehpercayaan. Namun, penyelidikan asas memerlukan skor ujian pekali kebolehpercayaan 0.80 atau

lebih tinggi. Ini sangat berbeza bagi pembuat keputusan, standard yang diinginkan pada pekali kebolehpercayaan adalah diantara julat 0.90 hingga 0.95 atau lebih tinggi.

4.7 ANALISIS DESKRIPTIF

Analisis deskriptif merupakan salah satu bentuk di dalam penyelidikan jenis kuantitatif (Chua Yan Piaw, 2006). Secara asasnya, di dalam kajian deskriptif, data yang dipungut bagi tujuan penganalisisan kebiasaannya dibuat melalui analisis frekuensi, peratusan, min, sisihan piawai, dan taburan skor dilaporkan. Analisis deskriptif kajian ini dibahagikan kepada dua bahagian utama iaitu Bahagian Pertama yang berkaitan dengan maklumat demografi responden manakala Bahagian Kedua yang berkaitan komponen faktor tahap kesedaran keselamatan maklumat dalam penggunaan peranti mudah alih dalam kalangan pekerja BIT Group of Companies. Secara keseluruhan maklum balas, terdapat 75 orang yang berjaya memberikan respon berbanding 176 orang staf bernaung di bawah syarikat BIT Group of Companies iaitu sebanyak 43% daripada keseluruhan responden. Kadar ini sedikit rendah berbanding yang dijangka memandangkan bilangan pekerja sebenar telah dikemaskini dan faktor masa (iaitu 3 hari sahaja) untuk menjawab memberi kekangan dari segi mendapatkan lebih banyak respon.

4.7.1 ANALISIS MAKLUMAT DEMOGRAFI

Dalam Bahagian Pertama, analisis deskriptif melihat nilai peratusan dan kekerapan responden berdasarkan jantina, umur, kelulusan tertinggi akademik, syarikat responden bekerja, kedudukan dalam organisasi, tempoh berkhidmat dan negeri responden.

a. Soalan 1 : Jantina

Soalan 1 menunjukkan pecahan maklum balas responden mengikut jantina. Daripada 75 responden yang memberikan maklum balas terhadap kaji selidik, seramai 53 (70.7%) orang responden adalah lelaki, manakala seramai 22 (29.3%) adalah perempuan. Peratusan maklum balas kaji selidik adalah seperti di Jadual 4.6.

Jadual 4.6 : Taburan Kekerapan dan Peratus Responden Mengikut Jantina

Jantina	Frekuensi (*f*)	Peratus (%)
Lelaki	53	70.7
Perempuan	22	29.3

(n=75)

b. Soalan 2 : Umur

Soalan 2 menunjukkan pecahan maklum balas responden mengikut umur. Daripada 75 responden yang memberikan maklum balas terhadap kaji selidik, seramai 31 (41.3%) orang responden yang berumur 31 - 40 tahun, 21 (28.0%) orang responden yang berumur 41 - 50 tahun, 18 (24.0%) orang responden yang berumur 21 - 30 tahun, manakala seramai 5 (6.7%) orang responden yang berumur 51 - 60 tahun. Peratusan maklum balas kaji selidik adalah seperti di Jadual 4.7.

Jadual 4.7 : Taburan Kekerapan dan Peratus Responden Mengikut Umur

Umur	Frekuensi (*f*)	Peratus (%)
21 - 30 tahun	18	24.0
31 - 40 tahun	31	41.3
41 - 50 tahun	21	28.0
51 - 60 tahun	5	6.7

(n=75)

c. Soalan 3 : Kelulusan tertinggi akademik

Soalan 3 menunjukkan pecahan maklum balas responden mengikut kelulusan tertinggi dalam bidang akademik. Daripada 75 responden yang memberikan maklum balas terhadap kaji selidik, seramai 40 (53.3%) orang responden yang berkelulusan Sarjana Muda (Ijazah), 27 (36.0%) orang responden yang berkelulusan Diploma, 5 (6.7%) orang responden yang berkelulusan Sarjana (Master), manakala seramai 3 (4.0%) orang responden yang berkelulusan STPM/SPM/SPMV/Sijil. Tiada pekerja yang mempunyai kelulusan tertinggi akademik pada tahap PHD. Peratusan maklum balas kaji selidik adalah seperti di Jadual 4.8.

Jadual 4.8 : Taburan Kekerapan dan Peratus Responden Mengikut Kelulusan Tertinggi Akademik

Kelulusan tertinggi akademik	Frekuensi (*f*)	Peratus (%)
PHD	0	0
Sarjana (Master)	5	6.7
Sarjana Muda (Ijazah)	40	53.3
Diploma	27	36.0
STPM/SPM/SPMV/Sijil	3	4.0

(n=75)

d. Soalan 4 : Syarikat anda bekerja

Soalan 4 menunjukkan pecahan maklum balas responden mengikut syarikat mereka bekerja. Daripada 75 responden yang memberikan maklum balas terhadap kaji selidik, seramai 27 (36.0%) orang responden yang bekerja di syarikat BIT Sdn Bhd, diikuti oleh 26 (34.7%) orang responden yang bekerja di syarikat BIT Group Sdn Bhd, 8 (10.7%) orang responden yang bekerja di syarikat BIT Software Sdn Bhd dan NexQuadrant Sdn Bhd, 3 (4.0%) orang responden yang bekerja di syarikat Sadiqin Sdn Bhd, 2 (2.7%) orang responden yang bekerja di syarikat BIT Academy Sdn Bhd, manakala seramai 1 (1.3%) orang responden yang bekerja di syarikat As Sehah Digital Sdn Bhd. Peratusan maklum balas kaji selidik adalah seperti di Jadual 4.9.

Jadual 4.9 : Taburan Kekerapan dan Peratus Responden Mengikut Syarikat Mereka Bekerja

Syarikat	Frekuensi (*f*)	Peratus (%)
BIT Group Sdn Bhd	26	34.7
BIT Software Sdn Bhd	8	10.7
BIT Academy Sdn Bhd	2	2.7
BIT Sdn Bhd	27	36.0
NexQuadrant Sdn Bhd	8	10.7
Sadiqin Sdn Bhd	3	4.0
As Sehah Digital Sdn Bhd	1	1.3

(n=75)

e. Soalan 5 : Kedudukan dalam organisasi

Soalan 5 menunjukkan pecahan maklum balas responden mengikut kedudukan mereka dalam organisasi. Daripada 75 responden yang memberikan maklum balas terhadap kaji selidik, seramai 49 (65.3%) orang responden adalah daripada Kumpulan Pengurusan dan Profesional, manakala seramai 26 (34.7%) adalah daripada Kumpulan Sokongan dan Pelaksana. Peratusan maklum balas kaji selidik adalah seperti di Jadual 4.10.

Jadual 4.10 : Taburan Kekerapan dan Peratus Responden Mengikut Kedudukan Dalam Organisasi

Kedudukan dalam organisasi	Frekuensi (*f*)	Peratus (%)
Kumpulan Pengurusan dan Profesional	49	65.3
Kumpulan Sokongan dan Pelaksana	26	34.7

(n=75)

4.7.2 ANALISIS RESPONDEN TERHADAP KOMPONEN FAKTOR

Dalam Bahagian Kedua, analisis deskriptif melihat bilangan kekerapan (frekuensi), nilai peratusan, skor min dan analisis faktor berdasarkan maklum balas responden terhadap setiap item dalam soalan kaji selidik.

Dalam kajian ini, tahap kesedaran keselamatan maklumat di antara penggunaan peranti mudah alih dalam kalangan pekerja swasta dinilai berdasarkan bilangan kekerapan (frekuensi), nilai peratusan dan analisis skor min mengikut faktor-faktor yang dikenal pasti pada model awal. Terdapat dua (2) bentuk skala dalam soalan kaji selidik ini iaitu skala nominal iaitu dwi pilihan/fakta dan skala ordinal. Skala nominal adalah skala pengukuran yang tidak boleh disusun mengikut urutan dan tidak boleh diukur. Skala pengukuran nominal digunakan untuk mengklasifikasikan objek, individu dan kelompok. Sebagai contoh ada soalan kaji selidik yang menggunakan pilihan jawapan dalam bentuk fakta di mana responden boleh memilih fakta yang sesuai dan tambah pilihan jawapan sekiranya perlu dan ada yang menggunakan skala ‘Ya’, ‘Tidak’ dan ‘Tidak Pasti’. Bagi bentuk soalan ini, pengukuran dalam bentuk bilangan kekerapan (frekuensi) dan nilai peratusan akan digunakan.

Skala ordinal adalah skala pengukuran boleh memberikan nilai numerik tetapi tidak dapat melakukan operasi matematik. Skala pengukuran ordinal terdiri daripada data yang boleh disusun mengikut tertib atau nilai tertentu yang lazimnya boleh disusun dengan menggunakan skala Likert. Bagi bentuk soalan ini, pengukuran skala Likert digunakan dan boleh ditentukan melalui skor min dan analisis faktor. Skala Pengukuran Likert yang digunakan pula adalah Skala Likert tujuh (7) mata terdiri dari ‘1’ yang bermaksud sangat tidak setuju, kepada ‘7’ bermaksud sangat bersetuju dengan penyataan yang diberikan. Bagi bentuk soalan ini, pengukuran dalam bentuk

ujian skor min, analisis faktor dan ujian korelasi *Pearson* akan digunakan. Jadual 4.11 menunjukkan Skala Likert dan penilaiannya.

Jadual 4.11 : Skala Likert dan penilaiannya

Skala Likert	Penilaian
1	Sangat Tidak Bersetuju
2	Tidak Bersetuju
3	Kurang Bersetuju
4	Berkecuali
5	Agak Bersetuju
6	Bersetuju
7	Sangat Bersetuju

4.7.2.1 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 Landell (1997) 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.

a. Bahagian A : Faktor Pengetahuan

Dalam kaji selidik ini, tahap kesedaran keselamatan maklumat peranti mudah alih dalam kalangan pekerja swasta dinilai melalui bilangan kekerapan (frekuensi), nilai peratusan responden yang menjawab soalan kaji selidik dan ujian skor min pada Bahagian A : Faktor Pengetahuan. Bahagian ini adalah bagi mengukur tahap pengetahuan sedia ada mengenai keselamatan maklumat, ancaman siber dan langkah-langkah keselamatan maklumat. Bilangan kekerapan dan nilai peratusan

responden yang menjawab kaji selidik bagi bahagian ini adalah seperti dalam Jadual 4.12.

Jadual 4.12 : Bilangan kekerapan (frekuensi) dan nilai peratusan bagi Faktor Pengetahuan

Kod Item	Soalan	Jawapan	Frekuensi (*f*)	Peratus (%)
A1	Apakah peranti peribadi mudah alih yang dibawa ke tempat kerja?	Telefon Pintar	74	98.7
		Komputer Riba	61	81.3
		iPad	1	1.3
A2	Apakah sistem pengoperasian peranti peribadi bagi telefon pintar yang digunakan?	Android	42	56.0
		Apple iOS	33	44.0
A3	Apakah sistem pengoperasian peranti peribadi bagi komputer riba yang digunakan?	Windows	67	89.3
		Linux	0	0
		macOS	6	8.0
		Tidak membawa laptop peribadi	2	2.6
A4	Apakah peranan anda di dalam organisasi?	Pengguna biasa (tidak melibatkan sistem)	26	34.7
		Pengguna sistem	38	50.7
		Pentadbir sistem	11	14.7

Daripada 75 responden yang memberi maklum balas, seramai 74 (98.7%) orang responden membawa peranti peribadi mudah alih iaitu telefon pintar mereka ke tempat kerja. Manakala seramai 61 (81.3%) orang responden membawa peranti peribadi mudah alih iaitu komputer riba mereka ke tempat kerja. Hanya 1 (1.3%) orang responden membawa peranti peribadi mudah alih iaitu iPad mereka ke tempat kerja. Peratusan ini menunjukkan bahawa majoriti responden ada membawa peranti peribadi mudah alih masing-masing iaitu telefon pintar dan komputer riba ke tempat kerja. Ini meningkatkan risiko peranti peribadi dan juga meningkatkan risiko tahap keselamatan maklumat dalam kalangan pekerja BIT Group of Companies.

Seramai 42 (56%) orang responden yang menggunakan sistem pengoperasian Android dalam telefon pintar mereka, manakala seramai 33 (44%) orang responden yang menggunakan sistem pengoperasian Apple iOS dalam telefon pintar mereka. Seterusnya, seramai 67 (89.3%) orang responden yang menggunakan sistem pengoperasian Windows dalam komputer riba, manakala seramai 6 (8.0%) orang responden yang menggunakan sistem pengoperasian macOS dalam komputer riba. Seramai 2 (2.7%) orang responden pula tidak membawa komputer riba (laptop)

peribadi ke tempat kerja. Peratusan ini menunjukkan bahawa majoriti responden menggunakan sistem pengoperasian Android bagi telefon pintar dan Windows bagi komputer riba. Sistem pengoperasian Android dan Windows banyak bergantung kepada kod sumber terbuka (*open-source code*) yang bermaksud bahawa pemilik peranti ini dapat mengubahsuai sistem operasi telefon dan komputer riba mereka. Terlalu banyak pengubahsuaian dan modifikasi, mungkin menimbulkan kelemahan dan risiko dalam keselamatan peranti mereka.

Dari segi peranan dalam organisasi pula, seramai 38 (50.7%) orang responden yang terdiri daripada pengguna sistem yang terlibat dengan penggunaan sistem di dalam syarikat masing-masing. Manakala seramai 26 (34.7%) orang responden adalah pengguna biasa iaitu yang tidak melibatkan penggunaan sistem secara langsung dan selebihnya iaitu seramai 11 (14.7%) adalah pentadbir sistem. Peratusan ini menunjukkan bahawa majoriti responden memainkan peranan yang sangat penting dalam syarikat kerana mereka menggunakan sistem yang disediakan oleh pihak syarikat.

Bagi mengetahui tahap kesedaran keselamatan maklumat di antara penggunaan peranti mudah alih dalam kalangan pekerja swasta dari komponen faktor pengetahuan, analisis skor min dilakukan. Faktor pengetahuan bertujuan mengukur tahap pengetahuan sedia ada mengenai keselamatan maklumat para pekerja terutamanya pada peranti peribadi mereka. Jadual 4.13 menunjukkan hasil analisis skor min terhadap faktor pengetahuan.

Jadual 4.13 : Skor min dan tahap kesedaran responden bagi Faktor Pengetahuan

Kod Item	**Soalan**	**Min (μ)**	**Tahap Kesedaran**
A5	Anda mengunci atau meletakkan kata laluan pada telefon pintar anda.	6.56	Tinggi
A6	Anda mengunci atau meletakkan kata laluan pada komputer riba anda	6.55	Tinggi

Secara keseluruhannya, dapat dirumuskan kebanyakan responden mengetahui tentang perlunya mengunci atau meletakkan kata laluan pada telefon pintar dan komputer riba mereka dengan keputusan skor min masing-masing bagi soalan A5 dan

A6 iaitu 6.56 dan 6.55. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai tersebut menunjukkan tahap yang tinggi. Skor ini juga menunjukkan bahawa tahap kesedaran keselamatan maklumat peranti mudah alih responden berada pada tahap yang tinggi dari segi faktor pengetahuan.

b. Bahagian B : Faktor Tingkah Laku

Dalam kaji selidik ini, tahap kesedaran keselamatan maklumat peranti mudah alih dalam kalangan pekerja swasta dinilai melalui ujian skor min berdasarkan responden yang menjawab soalan kaji selidik pada Bahagian B : Faktor Tingkah Laku. Faktor tingkah laku bertujuan untuk mengukur tahap kepantasan, ketepatan dan kesediaan seseorang dalam melakukan tindakan berkaitan keselamatan maklumat pada peranti peribadi mereka. Jadual 4.14 menunjukkan hasil analisis skor min terhadap faktor tingkah laku.

Jadual 4.14 : Skor min dan tahap kesedaran responden bagi Faktor Tingkah Laku

Kod Item	Soalan	Min (μ)	Tahap Kesedaran
B1	Anda pernah menggunakan WiFi Awam (*Public WiFi*).	3.95	Sederhana
B2	Anda menghantar emel/memuat turun dokumen pejabat menggunakan sambungan WiFi yang selamat (*Secured WiFi*).	6.23	Tinggi
B3	Anda pernah memuat turun (*download*) perisian dari Internet tanpa pengetahuan dan kebenaran daripada syarikat anda.	4.85	Sederhana
B4	Anda pernah memuat turun (*download*) perisian dari Internet tanpa pengetahuan tetapi mematuhi apa yang dibenarkan oleh polisi syarikat anda.	4.05	Sederhana
B5	Anda menggunakan akaun emel pejabat untuk kegunaan peribadi.	6.57	Tinggi
B6	Anda pernah memuat turun (*download*) dokumen/fail yang dihantar oleh penerima yang tidak dikenali.	6.52	Tinggi
B7	Anda pernah menerima emel yang mencurigakan dan mengklik pada URL (*link*) di dalam kandungan emel tersebut.	6.29	Tinggi

Bagi soalan faktor tingkah laku iaitu B1, B3, B5, B6 dan B7 ianya mendorong kecenderungan kepada soalan yang berbentuk negatif. Oleh yang demikian, bagi memastikan tiada sebarang ralat yang berlaku, nilai likert 7 mata yang diperolehi melalui jawapan dari responden perlu ditukar terlebih dahulu kepada skala yang berlawanan iaitu pilihan sangat tidak bersetuju (7), tidak bersetuju (6), kurang bersetuju (5), berkecuali (4), agak bersetuju (3), bersetuju (2) dan sangat bersetuju (1).

Secara keseluruhannya, dapat dirumuskan kebanyakan responden mempunyai tahap kepantasan, ketepatan dan kesediaan tentang perlunya menghantar emel/memuat turun dokumen pejabat menggunakan sambungan WiFi yang selamat *(Secured WiFi)*, tidak menggunakan akaun emel pejabat untuk kegunaan peribadi, tidak pernah memuat turun (*download*) dokumen/fail yang dihantar oleh penerima yang tidak dikenali dan tidak pernah menerima emel yang mencurigakan dan mengklik pada URL (*link*) di dalam kandungan emel tersebut pada telefon pintar dan komputer riba mereka. Keputusan skor min masing-masing bagi soalan B2, B5, B6 dan B7 iaitu 6.23, 6.57, 6.52 dan 6.29. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai tersebut menunjukkan tahap yang tinggi. Skor ini juga menunjukkan bahawa tahap kesedaran keselamatan maklumat peranti mudah alih responden berada di tahap yang tinggi dari segi faktor tingkah laku.

Namun, bagi soalan B1, B3 dan B4 keputusan skor min masing-masing adalah 3.95, 4.85 dan 4.05. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai tersebut menunjukkan tahap yang sederhana. Skor ini juga menunjukkan bahawa perlunya diberikan penekanan agar perubahan tingkah laku berlaku dari segi penggunaan WiFi awam *(Public WiFi)*, memuat turun (*download*) perisian dari Internet tanpa pengetahuan dan kebenaran daripada syarikat dan memuat turun (*download*) perisian dari Internet tanpa pengetahuan tetapi mematuhi apa yang dibenarkan oleh polisi syarikat anda. Tahap kesedaran keselamatan maklumat bagi item-item ini perlu dipertingkatkan.

c. Bahagian C : Faktor Sikap

Dalam kaji selidik ini, tahap kesedaran keselamatan maklumat peranti mudah alih dalam kalangan pekerja swasta dinilai melalui bilangan kekerapan (frekuensi), nilai peratusan responden yang menjawab soalan kaji selidik dan ujian skor min pada

Bahagian C : Faktor Sikap. Bahagian ini adalah bagi mengukur tahap kepekaan seseorang terhadap kesedaran keselamatan maklumat dari segi pengalaman peribadi, pengaruh dari orang lain dan pengaruh media massa. Bilangan kekerapan dan nilai peratusan responden yang menjawab kaji selidik bagi bahagian ini adalah seperti dalam Jadual 4.15.

Jadual 4.15 : Bilangan kekerapan (frekuensi) dan nilai peratusan bagi Faktor Sikap

Kod Item	Soalan	Jawapan	Frekuensi (*f*)	Peratus (%)
C2	Berapa kalikah anda menukar kata laluan?	1 - 3 bulan sekali	28	37.7
		4 - 6 bulan sekali	21	28.0
		7 - 9 bulan sekali	2	2.7
		10 - 12 bulan sekali	12	16.0
		Tidak pernah tukar	12	16.0
C3	Apakah cara anda mengingat kata laluan?	Menulis dan simpan di tempat rahsia	17	22.7
		Menulis dan letak atas meja	0	0
		Menulis dan letak di bawah keyboard	0	0
		Menulis dan tampal di dinding/papan kenyataan	1	1.3
		Menulis dan simpan di dalam telefon	27	36.0
		Kombinasi nama dan nombor	3	4.0
		Menghafal	16	21.3
		Hafal, kalau lupa klik Forgot *Password*	2	2.7
		Rahsia *(Confidential)*	2	2.7
		Hint	1	1.3
		Buku catatan	1	1.3
		Password manager	1	1.3
		Simpan di tempat tertentu yang saya ketahui sahaja	1	1.3
		Menggunakan aplikasi yang memerlukan pengesahan *password*	1	1.3
		Sesuatu yang berkaitan dengan diri	1	1.3
		Tiada	1	1.3

Daripada 75 responden yang memberi maklum balas, seramai 28 (37.3%) orang responden menukar kata laluan mereka 1 - 3 bulan sekali, diikuti 21 (28.0%) orang responden menukar kata laluan mereka 4 - 6 bulan sekali, 2 (2.7%) orang responden menukar kata laluan mereka 7 - 9 bulan sekali dan 12 (16%) orang

responden menukar kata laluan mereka 10 - 12 bulan sekali. Manakala seramai 12 (16%) orang responden yang tidak pernah menukar kata laluan mereka. Peratusan ini menunjukkan bahawa majoriti responden mengamalkan menukar kata laluan setiap 1 - 3 bulan dan 4 - 6 bulan sekali. Proses penukaran kata laluan dalam tempoh yang dinyatakan adalah sangat praktikal dan terdapat dalam polisi syarikat. Ini dapat mengurangkan risiko digodam atau risiko tahap keselamatan maklumat dalam peranti masing-masing.

Seterusnya, kajian terhadap cara pekerja mengingati kata laluan mereka pula ditanya. Perkara ini sangat penting kerana mahu menilai sejauh mana kepekaan pekerja dalam menjaga keselamatan kata laluan mereka. Seramai 27 (36.0%) orang responden memilih untuk menulis dan simpan kata laluan di dalam telefon mereka, diikuti 17 (22.7%) orang responden memilih untuk menulis dan simpan kata laluan di tempat rahsia mereka dan 16 (21.3%) orang responden memilih untuk menghafal dan mengingat kata laluan mereka. Manakala seramai 3 (4.0%) orang responden yang memilih untuk mengingat kata laluan dengan kombinasi nama dan nombor dan 2 (2.7%) orang responden memilih untuk mengingat kata laluan dengan menghafal, namun apabila mereka lupa, mereka akan klik *Forgot Password*. Menariknya, hanya seramai 1 (1.3%) orang responden memilih untuk mengingat kata laluan dengan cara berikut (1) Menulis dan tampal di dinding/papan kenyataan, (2) Menggunakan fungsi *Hint,* (3) Menulis pada buku catatan, (4) Menggunakan *Password manager,* (5) Menyimpan di tempat tertentu yang mereka ketahui sahaja, (6) Menggunakan aplikasi yang memerlukan pengesahan kata laluan, dan (7) Sesuatu yang berkaitan dengan diri mereka. Seramai 1 (1.3%) orang responden memilih tiada, iaitu tiada cara spesifik mereka mengingati kata laluan. Peratusan ini menunjukkan bahawa majoriti responden memilih untuk menulis dan menyimpan di dalam telefon mereka dan menulis dan menyimpan di tempat rahsia mereka. Menyimpan kata laluan di dalam telefon meningkatkan lagi risiko peranti sekiranya ia digodam, melainkan telah diaktifkan fungsi kawalan keselamatan pada telefon masing-masing. Cara yang terbaik adalah dengan menghafal atau mengingat kata laluan anda tanpa menulis di mana-mana.

Seterusnya, kita ingin mengkaji skor min bagi faktor sikap. Faktor sikap bertujuan mengukur tahap kepekaan seseorang terhadap kesedaran keselamatan

maklumat pada peranti peribadi mereka dari segi pengalaman peribadi, pengaruh dari orang lain dan pengaruh media massa. Jadual 4.16 menunjukkan hasil analisis skor min terhadap faktor sikap.

Jadual 4.16 : Skor min dan tahap kesedaran responden bagi Faktor Sikap

Kod Item	Soalan	Min (μ)	Tahap Kesedaran
C1	Anda mempunyai kata laluan yang berbeza bagi setiap sistem yang digunakan.	5.51	Tinggi
C4	Kata laluan anda ada mengandungi huruf besar, huruf kecil, nombor & simbol (kompleks).	6.60	Tinggi
C5	Anda pernah menggunakan dan melayari media sosial untuk tujuan peribadi di tempat kerja dalam tempoh waktu bekerja.	4.36	Sederhana
C6	Anda pernah berkongsi maklumat rasmi atau sulit tentang syarikat di media sosial.	6.79	Tinggi

Bagi soalan faktor sikap iaitu C5 dan C6 ianya mendorong kecenderungan kepada soalan yang berbentuk negatif. Oleh yang demikian, bagi memastikan tiada sebarang ralat yang berlaku, nilai likert 7 mata yang diperolehi melalui jawapan dari responden perlu ditukar terlebih dahulu kepada skala yang berlawanan iaitu pilihan sangat tidak bersetuju (7), tidak bersetuju (6), kurang bersetuju (5), berkecuali (4), agak bersetuju (3), bersetuju (2) dan sangat bersetuju (1).

Secara keseluruhannya, dapat dirumuskan kebanyakan responden mempunyai tahap kepekaan yang tinggi terhadap kesedaran keselamatan maklumat dari segi pengalaman peribadi, pengaruh dari orang lain dan pengaruh media massa pada peranti mudah alih mereka. Keputusan skor min masing-masing bagi soalan C1, C4 dan C6 iaitu 5.51, 6.60 dan 6.79. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai tersebut menunjukkan tahap yang tinggi. Skor ini juga menunjukkan bahawa tahap kesedaran keselamatan maklumat peranti mudah alih responden berada di tahap yang tinggi dari segi faktor sikap.

Namun, bagi soalan C5 keputusan skor min adalah 4.36. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai tersebut menunjukkan tahap yang sederhana. Skor ini juga menunjukkan bahawa perlunya diberikan penekanan kepada

para pekerja agar perubahan sikap berlaku dari segi menggunakan dan melayari media sosial untuk tujuan peribadi di tempat kerja dalam tempoh waktu bekerja. Tahap kesedaran keselamatan maklumat bagi item ini perlu dipertingkatkan

d. Bahagian D : Faktor Sokongan Pihak Pengurusan

Dalam kaji selidik ini, tahap kesedaran keselamatan maklumat peranti mudah alih dalam kalangan pekerja swasta dinilai melalui bilangan kekerapan (frekuensi), nilai peratusan responden yang menjawab soalan kaji selidik dan ujian skor min pada Bahagian D : Faktor Sokongan Pihak Pengurusan. Bahagian ini adalah bagi mengukur tahap kepimpinan pihak pengurusan terhadap keselamatan maklumat dari segi sokongan, galakkan dan pelaksanaan pematuhan. Bilangan kekerapan dan nilai peratusan responden yang menjawab kaji selidik bagi bahagian ini adalah seperti dalam Jadual 4.17.

Jadual 4.17 : Bilangan kekerapan (frekuensi) dan nilai peratusan bagi Faktor Sokongan Pihak Pengurusan

Kod Item	Soalan	Jawapan	Frekuensi (*f*)	Peratus (%)
D5	Jika setuju, pernahkah anda menandatangani sebarang surat pematuhan taklimat keselamatan maklumat tersebut?	Ya	7	9.6
		Tidak	14	19.2
		Tidak Pasti	52	71.2

Soalan kaji selidik ini ingin mengkaji sama ada para pekerja pernah atau tidak menandatangani sebarang surat pematuhan taklimat keselamatan maklumat tersebut, sekiranya mereka memilih bersetuju. Daripada 75 responden yang memberi maklum balas, seramai 52 (71.2%) orang responden menjawab ‘Tidak Pasti’, diikuti 14 (19.2%) orang responden menjawab ‘Tidak’ dan hanya seramai 7 (9.6%) orang responden sahaja yang menjawab ‘Ya’. Peratusan ini menunjukkan bahawa majoriti responden tidak pasti sama ada mereka pernah menandatangani sebarang surat pematuhan taklimat keselamatan maklumat. Di sini jelas bahawa pihak pengurusan tidak ada mengeluarkan sebarang surat pematuhan taklimat keselamatan maklumat dan tidak juga mengadakan sesi taklimat keselamatan tersebut. Ini mampu mengurangkan lagi tahap kesedaran keselamatan maklumat dalam kalangan pekerja kerana kurangnya pendedahan kepada perkara-perkara berkaitan keselamatan.

Seterusnya, kita ingin mengkaji skor min bagi faktor sokongan pihak pengurusan. Faktor sokongan pihak pengurusan bertujuan mengukur tahap kepimpinan pihak pengurusan terhadap keselamatan maklumat dari segi sokongan, galakkan dan pelaksanaan pematuhan. Jadual 4.18 menunjukkan hasil analisis skor min terhadap faktor sokongan pihak pengurusan.

Jadual 4.18 : Skor min dan tahap kesedaran responden bagi Faktor Sokongan Pihak Pengurusan

Kod Item	Soalan	Min (μ)	Tahap Kesedaran
D1	Pihak pengurusan membenarkan anda bawa peranti peribadi anda seperti telefon pintar dan komputer riba ke pejabat.	6.56	Tinggi
D2	Pihak pengurusan menyediakan emel khas dari syarikat untuk tujuan kerja.	6.77	Tinggi
D3	Pihak pengurusan menyarankan penukaran kata laluan pada emel pejabat dan peranti peribadi anda setiap 3-6 bulan.	6.36	Tinggi
D4	Pihak pengurusan pernah membuat sesi taklimat keselamatan maklumat kepada semua staf.	3.48	Sederhana

Secara keseluruhannya, dapat dirumuskan kebanyakan responden percaya bahawa pihak pengurusan mempunyai tahap kepimpinan yang tinggi terhadap keselamatan maklumat dari segi sokongan, galakkan dan pelaksanaan pematuhan. Keputusan skor min masing-masing bagi soalan D1, D2 dan D3 iaitu 6.56, 6.77 dan 6.36. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai tersebut menunjukkan tahap yang tinggi. Skor ini juga menunjukkan bahawa tahap kesedaran keselamatan maklumat di syarikat responden berada di tahap yang tinggi dari segi faktor sokongan pihak pengurusan. Malah, pihak pengurusan menyokong dan membenarkan para pekerja membawa telefon pintar dan komputer riba masing-masing.

Namun, bagi soalan D4 keputusan skor min adalah 3.48. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai tersebut menunjukkan tahap yang sederhana. Skor ini juga menunjukkan bahawa pihak pengurusan perlu meneliti perkara ini iaitu membuat sesi taklimat keselamatan maklumat kepada semua staf sebagai memberi pendedahan asas tentang pentingnya kesedaran keselamatan

maklumat. Tahap kesedaran keselamatan maklumat bagi item ini perlu dititikberatkan dan dipertingkatkan.

e. Bahagian E : Faktor Latihan dan Pendidikan

Dalam kaji selidik ini, tahap kesedaran keselamatan maklumat peranti mudah alih dalam kalangan pekerja swasta dinilai melalui bilangan kekerapan (frekuensi), nilai peratusan responden yang menjawab soalan kaji selidik dan ujian skor min pada Bahagian E : Faktor Latihan dan Pendidikan. Bahagian ini adalah bagi mengukur tahap kesediaan dan kewajaran mengadakan sesi latihan kesedaran keselamatan maklumat dan kaedah pendidikan berterusan kepada semua pekerja. Bilangan kekerapan dan nilai peratusan responden yang menjawab kaji selidik bagi bahagian ini adalah seperti dalam Jadual 4.19.

Jadual 4.19 : Bilangan kekerapan (frekuensi) dan nilai peratusan bagi Faktor Latihan dan Pendidikan

Kod Item	Soalan	Jawapan	Frekuensi (*f*)	Peratus (%)
E2	Jika setuju, adakah anda memahami dan mempraktikkan apa yang dipelajari dari segi keselamatan maklumat?	Ya	24	34.8
		Tidak	6	8.7
		Tidak Pasti	39	56.5
E3	Pernahkah anda melihat risalah atau poster berkenaan keselamatan maklumat di tempat kerja?	Ya	14	16.7
		Tidak	31	41.3
		Tidak Pasti	30	40.0

Soalan kaji selidik seterusnya, ingin mengkaji sama ada para pekerja memahami dan mempraktikkan atau tidak apa yang dipelajari dari segi keselamatan maklumat. Daripada 75 responden yang memberi maklum balas, seramai 39 (56.5%) orang responden menjawab ‘Tidak Pasti’, diikuti 24 (34.8%) orang responden menjawab ‘Ya’ dan hanya seramai 6 (8.7%) orang responden sahaja yang menjawab ‘Tidak’. Peratusan ini menunjukkan bahawa majoriti responden tidak pasti sama ada mereka memahami dan mempraktikkan apa yang dipelajari dari segi keselamatan maklumat. Di sini jelas bahawa sekiranya latihan tidak diadakan sewajarnya, maka ini boleh mengurangkan tahap kesediaan dan kesedaran keselamatan maklumat dalam kalangan pekerja. Namun, terdapat juga responden yang memahami dan mempraktikkan apa yang dipelajari dari segi keselamatan maklumat kerana mereka menghadiri sesi latihan berkaitan kesedaran keselamatan maklumat.

Soalan kaji selidik berikutnya, ingin mengkaji sama ada para pekerja pernah melihat risalah atau poster berkenaan keselamatan maklumat di tempat kerja. Seramai 31 (41.3%) orang responden menjawab 'Tidak', diikuti 30 (40.0%) orang responden menjawab 'Tidak Pasti' dan hanya seramai 14 (18.7%) orang responden sahaja yang menjawab 'Ya'. Peratusan ini menunjukkan bahawa majoriti responden tidak pernah atau tidak pasti mereka ada melihat risalah atau poster berkenaan keselamatan maklumat di tempat kerja mereka. Di sini jelas bahawa sekiranya pendidikan tidak diadakan sewajarnya, maka ini boleh merendahkan tahap kesediaan dan kesedaran keselamatan maklumat dalam kalangan pekerja. Namun, terdapat juga responden yang pernah melihat risalah atau poster berkenaan keselamatan maklumat di tempat kerja mereka.

Seterusnya, kita ingin mengkaji skor min bagi faktor latihan dan pendidikan. Faktor latihan dan pendidikan bertujuan mengukur tahap kesediaan dan kewajaran mengadakan sesi latihan kesedaran keselamatan maklumat dan kaedah pendidikan berterusan kepada semua pekerja. Jadual 4.20 menunjukkan hasil analisis skor min terhadap faktor latihan dan pendidikan.

Jadual 4.20 : Skor min dan tahap kesedaran responden bagi Faktor Latihan dan Pendidikan

Kod Item	Soalan	Min (μ)	Tahap Kesedaran
E1	Pihak syarikat menjalankan sesi latihan berkenaan kesedaran keselamatan maklumat kepada semua staf.	3.60	Sederhana
E4	Pada pandangan anda, adakah taklimat/latihan keselamatan maklumat perlu dilaksanakan secara berkala?	5.60	Tinggi

Secara keseluruhannya, dapat dirumuskan kebanyakan responden percaya bahawa perlunya kepada pelaksanaan taklimat/latihan keselamatan maklumat secara berkala. Keputusan skor min bagi soalan E4 iaitu 5.60. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai tersebut menunjukkan tahap yang tinggi. Skor ini juga menunjukkan bahawa tahap kesedaran keselamatan maklumat di syarikat responden berada di tahap yang tinggi dari segi faktor latihan dan pendidikan. Malah, mereka sedar dan percaya bahawa pentingnya latihan dan pendidikan dalam

meningkatkan kefahaman, pengetahuan dan pratikaliti mengenai keselamatan maklumat.

Namun, bagi soalan E1 keputusan skor min adalah 3.60. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai tersebut menunjukkan tahap yang sederhana. Skor ini juga menunjukkan bahawa perlunya pihak pengurusan atau syarikat yang terlibat mengendalikan latihan meneliti perkara ini iaitu membuat sesi latihan dan pendidikan tentang kesedaran keselamatan maklumat kepada semua staf. Tahap kesedaran keselamatan maklumat bagi item ini perlu difikirkan dan dipertingkatkan.

f. Bahagian F : Faktor Polisi/Dasar Keselamatan Maklumat

Dalam kaji selidik ini, tahap kesedaran keselamatan maklumat peranti mudah alih dalam kalangan pekerja swasta dinilai melalui bilangan kekerapan (frekuensi), nilai peratusan responden yang menjawab soalan kaji selidik dan ujian skor min pada Bahagian F : Faktor Polisi/Dasar Keselamatan Maklumat. Bahagian ini adalah bagi mengukur tahap penyediaan polisi dan dasar keselamatan maklumat oleh pihak pengurusan tertinggi kepada seluruh syarikat. Bilangan kekerapan dan nilai peratusan responden yang menjawab kaji selidik bagi bahagian ini adalah seperti dalam Jadual 4.21.

Jadual 4.21 : Bilangan kekerapan (frekuensi) dan nilai peratusan bagi Faktor Polisi/Dasar Keselamatan Maklumat

Kod Item	Soalan	Jawapan	Frekuensi (*f*)	Peratus (%)
F1	Adakah anda tahu kewujudan Dasar Keselamatan ICT di syarikat anda?	Ya	26	34.7
		Tidak	11	14.7
		Tidak Pasti	38	50.7
F2	Jika ya, adakah anda pernah baca Dasar Keselamatan ICT di syarikat anda?	Ya	10	14.3
		Tidak	21	30.0
		Tidak Pasti	39	55.7

Daripada 75 responden yang memberi maklum balas, seramai 38 (50.7%) orang responden menjawab ‘Tidak Pasti’, diikuti 26 (34.7%) orang responden menjawab ‘Ya’ dan hanya seramai 11 (14.7%) orang responden sahaja yang menjawab ‘Tidak’. Peratusan ini menunjukkan bahawa majoriti responden tidak pasti sama ada

mereka tahu tentang kewujudan Dasar Keselamatan ICT di syarikat mereka. Ini menunjukkan pihak pengurusan perlu menyediakan satu Polisi/Dasar Keselamatan ICT di setiap syarikat dan perkara ini perlu diwar-warkan kepada seluruh pekerja supaya mereka mengetahui kewujudannya.

Seterusnya, jika pekerja mengetahui tentang kewujudan Polisi/Dasar Keselamatan ICT di syarikat masing-masing, soalan seterusnya ingin mengkaji sama ada mereka membaca atau tidak Polisi/Dasar Keselamatan ICT tersebut. Seramai 39 (55.7%) orang responden menjawab 'Tidak Pasti', diikuti 21 (30.0%) orang responden menjawab 'Tidak' dan hanya seramai 10 (14.3%) orang responden sahaja yang menjawab 'Ya'. Peratusan ini menunjukkan bahawa majoriti responden tidak pernah atau tidak pasti mereka ada baca atau tidak Polisi/Dasar Keselamatan ICT di syarikat masing-masing. Polisi/Dasar Keselamatan ICT perlu ada di setiap syarikat dan setiap pekerja perlu mengetahui kewujudannya dan membacanya. Ini kerana polisi/dasar ini sangat diperlukan untuk memberi panduan kepada pekerja tentang keselamatan maklumat dan secara tak langsung melatih tahap kesedaran keselamatan maklumat dalam kalangan pekerja.

Akhir sekali, kita ingin mengkaji skor min bagi faktor polisi/dasar keselamatan maklumat. Faktor polisi/dasar keselamatan maklumat bertujuan mengukur tahap penyediaan polisi dan dasar keselamatan maklumat oleh pihak pengurusan tertinggi kepada seluruh syarikat. Jadual 4.22 menunjukkan hasil analisis skor min terhadap faktor polisi/dasar keselamatan maklumat.

Jadual 4.22 : Skor min dan tahap kesedaran responden bagi Faktor Polisi/Dasar Keselamatan Maklumat

Kod Item	Soalan	Min (μ)	Tahap Kesedaran
F3	Pada pandangan anda, wajarkah syarikat mengeluarkan satu dokumen berkaitan Dasar Keselamatan ICT di syarikat anda?	6.21	Tinggi

Secara keseluruhannya, dapat dirumuskan kebanyakan responden percaya bahawa sangat wajar untuk setiap syarikat mengeluarkan satu dokumen khas berkaitan Dasar Keselamatan ICT di syarikat masing-masing. Keputusan skor min bagi soalan F3 iaitu 6.21. Berdasarkan tafsiran skor min yang ditetapkan oleh Landell (1997), nilai

tersebut menunjukkan tahap yang tinggi. Skor ini juga menunjukkan bahawa tahap kesedaran keselamatan maklumat di syarikat responden berada di tahap yang tinggi dari segi faktor polisi/dasar keselamatan maklumat. Malah, mereka sedar dan percaya bahawa wajarnya setiap syarikat mempunyai dokumen dasar keselamatan maklumat mereka yang tersendiri atau boleh dibuat dalam syarikat induk dan dikongsi kepada semua anak syarikat. Ini dapat meningkatkan kefahaman, pengetahuan tentang polisi dan dasar yang perlu diikuti oleh setiap pekerja.

4.7.2.2 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 Kass & Tinsley (2018), 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)*.

a. Bahagian A : Faktor Pengetahuan

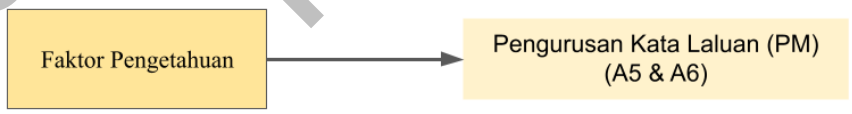
Ujian analisis faktor pengetahuan ini dijalankan dengan menggunakan analisis komponen prinsipal dan hasil penganalisisan item ditunjukkan seperti di dalam Jadual 4.23.

Jadual 4.23 :Matriks komponen bagi Faktor Pengetahuan

Faktor Pengetahuan	**Komponen Matrix (Sebelum)**	**Komponen Matrix *(Selepas putaran Varimax*)**
	1	1
A5	.905	Hanya satu (1) komponen sahaja diekstrak. Penyelesaian tidak boleh diputarkan.
A6	.905	

Kaedah pengekstrakan: *Principal Component Analysis*

Data-data tersebut kemudiannya diputar dengan menggunakan putaran *varimax* dan hasilnya adalah seperti di dalam Jadual 4.23. Sebelum putaran *varimax* dijalankan, item A5 dan A6 mempunyai nilai melebihi .4 dan dikategorikan dalam komponen 1 iaitu Pengurusan Kata Laluan (*Password Management (PM)*) pada peranti peribadi. Hasil putaran *varimax* menunjukkan, hanya satu (1) komponen sahaja diekstrak. Ini membuktikan bahawa hubungan korelasi di antara item dengan faktor pengetahuan dan ini merupakan kunci untuk memahami sifat faktor tersebut. Bagaimanapun, kedua-dua item tersebut adalah wajar dipertimbang untuk dijadikan sebahagian komponen di dalam model kesedaran berdasarkan hasil analisis daripada putaran *varimax*. Secara keseluruhannya, kedua-dua item di dalam komponen faktor pengetahuan digunakan untuk mereka bentuk model tahap kesedaran seperti dalam Rajah 4.1.



Rajah 4.1 : Komponen bagi Faktor Pengetahuan

b. Bahagian B : Faktor Tingkah Laku

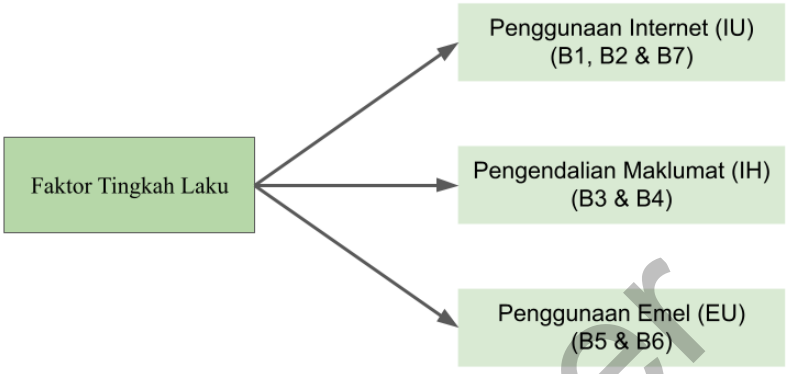
Ujian analisis faktor tingkah laku pula dijalankan dengan menggunakan analisis komponen prinsipal dan hasil penganalisisan item ditunjukkan seperti di dalam Jadual 4.24.

Jadual 4.24 : Matriks komponen bagi Faktor Tingkah Laku

Faktor Tingkah Laku	**Komponen Matrix (Sebelum)**			**Komponen Matrix *(Selepas putaran Varimax*)**		
	1	2	3	1	2	3
B1	.544			.550		
B2	-.582	.333	.447	-.785		
B3	.707	.561			.874	
B4	.535	.708			.901	
B5	.333		.848			.900
B6	.642	-.329	.427	.448		.706
B7	.463	-.502		.726		

Kaedah pengekstrakan: *Principal Component Analysis*
Kaedah putaran: *Varimax with Kaiser Normalization*

Data-data tersebut kemudiannya diputar dengan menggunakan putaran *varimax* dan hasilnya adalah seperti di dalam Jadual 4.24. Setelah putaran *varimax* dijalankan, hampir ke semua item B1, B2, B3, B4, B5, B6 dan B7 mempunyai nilai melebihi .4 dan dikategorikan dalam komponen 1 iaitu Penggunaan Internet (*Internet Use (IU)*), komponen 2 iaitu Penggunaan Emel (*Email Use (EU)*) dan komponen 3 iaitu Pengendalian Maklumat (*Information Handling (IH)*). Ini membuktikan bahawa hubungan korelasi di antara item dengan faktor tingkah laku dan ini merupakan kunci untuk memahami sifat faktor tersebut. Bagaimanapun, kesemua item tersebut adalah wajar dipertimbang untuk dijadikan sebahagian komponen di dalam model kesedaran berdasarkan hasil analisis daripada putaran *varimax* walaupun ada yang negatif. Secara keseluruhannya, semua item di dalam komponen faktor tingkah laku digunakan untuk mereka bentuk model tahap kesedaran seperti dalam Rajah 4.2.



Rajah 4.2 : Komponen bagi Faktor Tingkah Laku

c. Bahagian C : Faktor Sikap

Ujian analisis faktor sikap ini dijalankan dengan menggunakan analisis komponen prinsipal dan hasil penganalisisan item ditunjukkan seperti di dalam Jadual 4.25.

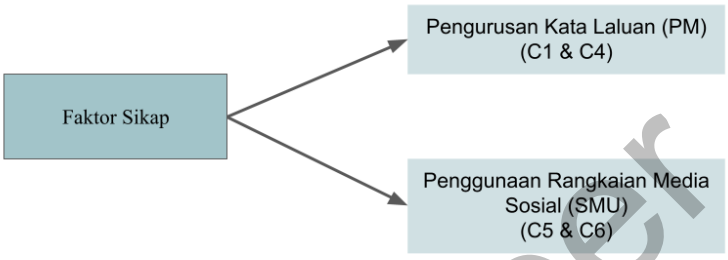
Jadual 4.25 : Matriks komponen bagi Faktor Sikap

Faktor Sikap	**Komponen Matrix (Sebelum)**		**Komponen Matrix *(Selepas putaran Varimax*)**	
	1	2	1	2
C1	.747		.788	
C4	.723	.405	.829	
C5	-.525	.538		.721
C6		.779		.817

Kaedah pengekstrakan: *Principal Component Analysis*
Kaedah putaran: *Varimax with Kaiser Normalization*

Data-data tersebut kemudiannya diputar dengan menggunakan putaran *varimax* dan hasilnya adalah seperti di dalam Jadual 4.25. Setelah putaran *varimax* dijalankan, item C1, C4, C5 dan C6 mempunyai nilai melebihi .4 dan dikategorikan dalam komponen 1 iaitu Pengurusan Kata Laluan (*Password Management (PM)*) pada peranti peribadi dan komponen 2 iaitu Penggunaan Rangkaian Media Sosial (*Social Media Use (SMU)*). Ini membuktikan bahawa hubungan korelasi di antara item dengan faktor sikap dan ini merupakan kunci untuk memahami sifat faktor tersebut. Bagaimanapun, kesemua item tersebut adalah wajar dipertimbang untuk dijadikan

sebahagian komponen di dalam model kesedaran berdasarkan hasil analisis daripada putaran *varimax*. Secara keseluruhannya, semua item di dalam komponen faktor sikap digunakan untuk mereka bentuk model tahap kesedaran seperti dalam Rajah 4.3.



Rajah 4.3 : Komponen bagi Faktor Sikap

d. Bahagian D : Faktor Sokongan Pihak Pengurusan

Ujian analisis faktor sokongan pihak pengurusan ini dijalankan dengan menggunakan analisis komponen prinsipal dan hasil penganalisisan item ditunjukkan seperti di dalam Jadual 4.26.

Jadual 4.26 : Matriks komponen bagi Faktor Sokongan Pihak Pengurusan

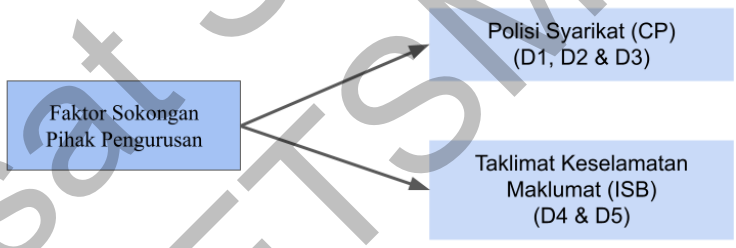
Faktor Sokongan Pihak Pengurusan	**Komponen Matrix (Sebelum)**		**Komponen Matrix *(Selepas putaran Varimax*)**	
	1	2	1	2
D1	.730		.731	
D2	.905		.914	
D3	.791		.790	
D4		.830		.828
D5		.808		.826

Kaedah pengekstrakan: *Principal Component Analysis*
Kaedah putaran: *Varimax with Kaiser Normalization*

Bagi soalan faktor sokongan pihak pengurusan iaitu D5, item adalah dalam bentuk teks (*string*) dan ia perlu ditukar ke nombor (*numerical*) untuk membuat analisis faktor. Oleh yang demikian, bagi memastikan tiada sebarang ralat yang berlaku, nilai teks yang diperolehi melalui jawapan dari responden perlu ditukar

terlebih dahulu kepada nombor iaitu pilihan ‘Ya’ (4), ‘Tidak Pasti’ (3), ‘Tidak’ (2) dan tiada respon (1).

Data-data tersebut kemudiannya diputar dengan menggunakan putaran *varimax* dan hasilnya adalah seperti di dalam Jadual 4.26. Setelah putaran *varimax* dijalankan, item D1, D2, D3, D4 dan D5 mempunyai nilai melebihi .4 dan dikategorikan dalam komponen 1 iaitu Polisi Syarikat (*Company Policy (CP)*) dan komponen 2 iaitu Taklimat Keselamatan Maklumat *(Information Security Briefing (ISB)*). Ini membuktikan bahawa hubungan korelasi di antara item dengan faktor sokongan pihak pengurusan dan ini merupakan kunci untuk memahami sifat faktor tersebut. Bagaimanapun, kesemua item tersebut adalah wajar dipertimbang untuk dijadikan sebahagian komponen di dalam model kesedaran berdasarkan hasil analisis daripada putaran *varimax*. Secara keseluruhannya, semua item di dalam komponen faktor sokongan pihak pengurusan digunakan untuk mereka bentuk model tahap kesedaran seperti dalam Rajah 4.4.



Rajah 4.4 : Komponen bagi Faktor Sokongan Pihak Pengurusan

e. Bahagian E : Faktor Latihan dan Pendidikan

Ujian analisis faktor latihan dan pendidikan ini dijalankan dengan menggunakan analisis komponen prinsipal dan hasil penganalisisan item ditunjukkan seperti di dalam Jadual 4.27.

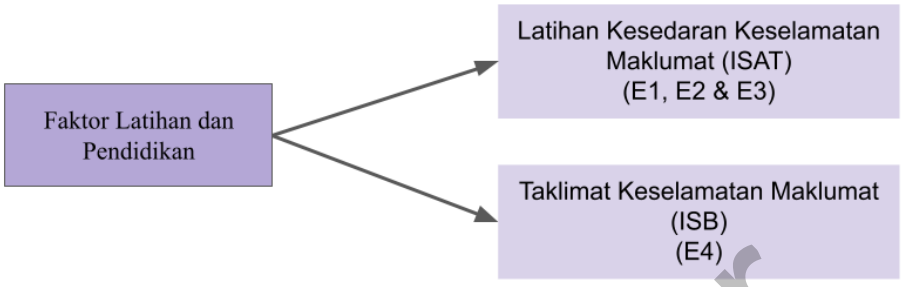
Jadual 4.27 : Matriks komponen bagi Faktor Latihan dan Pendidikan

Faktor Latihan dan Pendidikan	**Komponen Matrix (Sebelum)**		**Komponen Matrix *(Selepas putaran Varimax*)**	
	1	2	1	2
E1	.766	.330	.828	
E2	.837		.859	
E3	.788		.698	-.419
E4		.917		.960

Kaedah pengekstrakan: *Principal Component Analysis*
Kaedah putaran: *Varimax with Kaiser Normalization*

Bagi soalan faktor sokongan pihak pengurusan iaitu E2 dan E3, item adalah dalam bentuk teks (*string*) dan ia perlu ditukar ke nombor (*numerical*) untuk membuat analisis faktor. Oleh yang demikian, bagi memastikan tiada sebarang ralat yang berlaku, nilai teks yang diperolehi melalui jawapan dari responden perlu ditukar terlebih dahulu kepada nombor iaitu pilihan 'Ya' (4), 'Tidak Pasti' (3), 'Tidak' (2) dan tiada respon (1) untuk item E2, manakala pilihan 'Ya' (3), 'Tidak Pasti' (2), 'Tidak' (1) untuk item E3.

Data-data tersebut kemudiannya diputar dengan menggunakan putaran *varimax* dan hasilnya adalah seperti di dalam Jadual 4.27. Sebelum putaran *varimax* dijalankan, item E1, E2, E3 dan E4 mempunyai nilai melebihi .4 dan dikategorikan dalam komponen 1 iaitu Latihan Kesedaran Keselamatan Maklumat (*Information Security Awareness Training (ISAT)*) dan komponen 2 iaitu Taklimat Keselamatan Maklumat *(Information Security Briefing (ISB)*). Ini membuktikan bahawa hubungan korelasi di antara item dengan faktor latihan dan pendidikan dan ini merupakan kunci untuk memahami sifat faktor tersebut. Bagaimanapun, kesemua item tersebut adalah wajar dipertimbang untuk dijadikan sebahagian komponen di dalam model kesedaran berdasarkan hasil analisis daripada putaran *varimax* walaupun ada yang negatif. Secara keseluruhannya, semua item di dalam komponen faktor latihan dan pendidikan digunakan untuk mereka bentuk model tahap kesedaran seperti dalam Rajah 4.5.



Rajah 4.5 : Komponen bagi Faktor Latihan dan Pendidikan

f. Bahagian F : Faktor Polisi/Dasar Keselamatan Maklumat

Ujian analisis faktor polisi/dasar keselamatan maklumat ini dijalankan dengan menggunakan analisis komponen prinsipal dan hasil penganalisisan item ditunjukkan seperti di dalam Jadual 4.28.

Jadual 4.28 : Matriks komponen bagi Faktor Polisi/Dasar Keselamatan Maklumat

Faktor Polisi/Dasar Keselamatan Maklumat	**Komponen Matrix (Sebelum)**	**Komponen Matrix *(Selepas putaran Varimax*)**
	1	1
F1	.862	Hanya satu (1) komponen sahaja diekstrak. Penyelesaian tidak boleh diputarkan.
F2	.860	
F3	-.311	

Kaedah pengekstrakan: *Principal Component Analysis*

Bagi soalan faktor polisi/dasar keselamatan maklumat iaitu F1 dan F2, item adalah dalam bentuk teks (*string*) dan ia perlu ditukar ke nombor (*numerical*) untuk membuat analisis faktor. Oleh yang demikian, bagi memastikan tiada sebarang ralat yang berlaku, nilai teks yang diperolehi melalui jawapan dari responden perlu ditukar terlebih dahulu kepada nombor iaitu pilihan 'Ya' (3), 'Tidak Pasti' (2) dan 'Tidak' (1) untuk item F1, manakala pilihan 'Ya' (4), 'Tidak Pasti' (3), 'Tidak' (2) dan tiada respon (1) untuk item F2.

Data-data tersebut kemudiannya diputar dengan menggunakan putaran *varimax* dan hasilnya adalah seperti di dalam Jadual 4.28. Sebelum putaran *varimax* dijalankan, item F1 dan F2 mempunyai nilai yang sama melebihi .4 dan boleh dikategorikan dalam komponen 1 iaitu Polisi Syarikat (*Company Policy (CP)*). Hasil putaran *varimax* menunjukkan, hanya satu (1) komponen sahaja diekstrak. Ini membuktikan bahawa hubungan korelasi di antara item dengan faktor polisi/dasar keselamatan maklumat dan ini merupakan kunci untuk memahami sifat faktor tersebut. Bagaimanapun, kesemua item tersebut adalah wajar dipertimbang untuk dijadikan sebahagian komponen di dalam model kesedaran berdasarkan hasil analisis daripada putaran *varimax* walaupun ada yang negatif. Secara keseluruhannya, semua item di dalam komponen faktor polisi/dasar keselamatan maklumat digunakan untuk mereka bentuk model tahap kesedaran seperti dalam Rajah 4.6.

Rajah 4.6 : Komponen bagi Faktor Polisi/Dasar Keselamatan Maklumat

4.7.2.3 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).

a. Bahagian A : Faktor Pengetahuan

Hasil kajian analisis korelasi *Pearson* dalam Jadual 4.29 menunjukkan nilai indeks korelasi bagi komponen faktor pengetahuan adalah .637. Kekuatan hubungan antara item A5 dengan A6 (.637) adalah kuat.

Jadual 4.29 : Analisis korelasi *Pearson* bagi Faktor Pengetahuan

Dimensi		A5	A6
A5	*Pearson Correlation*	1	.637**
	Sig. (2-tailed)		< .001
	N	75	75
A6	*Pearson Correlation*	.637**	1
	Sig. (2-tailed)	< .001	
	N	75	75

**. Korelasi adalah signifikan pada aras 0.01 *(2-tailed)*.

Keputusan nilai signifikan menunjukkan bahawa kesemua hubungan adalah signifikan iaitu item A5 dengan A6 *(p = .001; p < .01)*.

b. Bahagian B : Faktor Tingkah Laku

Hasil kajian analisis korelasi *Pearson* dalam Jadual 4.30 menunjukkan nilai indeks korelasi bagi komponen faktor tingkah laku adalah di antara .013 hingga .387. Kekuatan hubungan antara item-item secara umumnya adalah sangat lemah, lemah dan sederhana. Kekuatan hubungan antara item B1 dengan B3 (.229), B1 dengan B6 (.238), B3 dengan B6 (.228) dan B6 dengan B7 (.273) adalah lemah namun signifikan dan positif. Manakala, kekuatan hubungan antara item B2 dengan B3 (.315) dan B5 dengan B6 (.387) pula adalah sederhana namun signifikan dan positif.

Jadual 4.30 : Analisis korelasi *Pearson* bagi Faktor Tingkah Laku

Dimensi		B1	B2	B3	B4	B5	B6	B7
B1	*Pearson Correlation*	1	.026	.229*	.208	.092	.238*	.182
	Sig. (2-tailed)		.823	.048	.074	.430	.040	.119
	N	75	75	75	75	75	75	75
B2	*Pearson Correlation*	.026	1	.315**	-.103	.055	.060	.054
	Sig. (2-tailed)	.823		.006	.381	.640	.610	.648
	N	75	75	75	75	75	75	75

bersambung...

	...sambungan							
B3	*Pearson Correlation*	.229*	.315**	1	.055	.154	.228*	.062
	Sig. (2-tailed)	.048	.006		.640	.187	.049	.599
	N	75	75	75	75	75	75	75
B4	*Pearson Correlation*	.208	-.103	.055	1	-.013	-.061	.066
	Sig. (2-tailed)	.074	.381	.640		.915	.602	.576
	N	75	75	75	75	75	75	75
B5	*Pearson Correlation*	.092	.055	.154	-.013	1	.387**	.003
	Sig. (2-tailed)	.430	.640	.167	.915		<.001	.981
	N	75	75	75	75	75	75	75
B6	*Pearson Correlation*	.238*	.060	.228*	-.061	.387**	1	.273*
	Sig. (2-tailed)	.040	.610	.049	.602	<.001		.018
	N	75	75	75	75	75	75	75
B7	*Pearson Correlation*	.182	.054	.062	.066	.003	.273*	1
	Sig. (2-tailed)	.119	.648	.599	.576	.981	.018	
	N	75	75	75	75	75	75	75

*. Korelasi adalah signifikan pada aras 0.05 *(2-tailed).*
**. Korelasi adalah signifikan pada aras 0.01 *(2-tailed).*

Keputusan nilai signifikan menunjukkan bahawa ada dua (2) hubungan yang signifikan iaitu item B2 dengan B3 *(p = .006; p < .01)* dan B5 dengan B6 *(p = .001; p < .01)*. Bagaimanapun, terdapat hubungan yang tidak signifikan iaitu item B1 dengan B2 *(p = .823; p > .01)*, B1 dengan B3 *(p = .048; p > .01),* B1 dengan B4 *(p = .074; p > .01),* B1 dengan B5 *(p = .430; p > .01),* B1 dengan B6 *(p = .040; p > .01)* dan B1 dengan B7 *(p = .119; p > .01).* Namun begitu, hubungan antara kesemua item tersebut adalah positif tetapi tidak signifikan.

c. Bahagian C : Faktor Sikap

Hasil kajian analisis korelasi *Pearson* dalam Jadual 4.31 menunjukkan nilai indeks korelasi bagi komponen faktor sikap adalah di antara .038 hingga .344. Kekuatan hubungan antara item-item secara umumnya adalah sangat lemah dan sederhana. Kekuatan hubungan antara item C1 dengan C5 (.131), C4 dengan C5 (.079) dan C5 dengan C6 (.197) adalah sangat lemah namun signifikan dan positif. Manakala,

kekuatan hubungan antara item C1 dengan C4 (.344) pula adalah sederhana namun signifikan dan positif.

Jadual 4.31 : Analisis korelasi *Pearson* bagi Faktor Sikap

Dimensi		C1	C4	C5	C6
C1	*Pearson Correlation*	1	.344**	.131	-.038
	Sig. (2-tailed)		.002	.263	.744
	N	75	75	75	75
C4	*Pearson Correlation*	.344**	1	.079	-.159
	Sig. (2-tailed)	.002		.501	.174
	N	75	75	75	75
C5	*Pearson Correlation*	.131	.079	1	.197
	Sig. (2-tailed)	.263	.501		.090
	N	75	75	75	75
C6	*Pearson Correlation*	-.038	-.159	.197	1
	Sig. (2-tailed)	.744	.174	.090	
	N	75	75	75	75

**. Korelasi adalah signifikan pada aras 0.01 *(2-tailed)*.

Keputusan nilai signifikan menunjukkan bahawa ada satu (1) hubungan yang signifikan iaitu item C1 dengan C4 *(p = .002; p < .01)*. Bagaimanapun, terdapat hubungan yang tidak signifikan iaitu item C1 dengan C5 *(p = .263; p > .01)*, C1 dengan C6 *(p = .744; p > .01),* C4 dengan C5 *(p = .501; p > .01),* C4 dengan C6 *(p = .174; p > .01)* dan C5 dengan C6 *(p = .090; p > .01).* Namun begitu, hubungan antara kesemua item tersebut adalah positif tetapi tidak signifikan.

d. Bahagian D : Faktor Sokongan Pihak Pengurusan

Hasil kajian analisis korelasi *Pearson* dalam Jadual 4.32 menunjukkan nilai indeks korelasi bagi komponen faktor sokongan pihak pengurusan adalah di antara .006 hingga .650. Kekuatan hubungan antara item-item secara umumnya adalah sangat lemah, sederhana dan kuat. Kekuatan hubungan antara item D1 dengan D3 (.270) dan D4 dengan D5 (.369) adalah sederhana namun signifikan dan positif, manakala D1 dengan D2 (.559) dan D2 dengan D3 (.650) adalah kuat dan signifikan.

Jadual 4.32 : Analisis korelasi *Pearson* bagi Faktor Sokongan Pihak Pengurusan

Dimensi		D1	D2	D3	D4	D5
D1	*Pearson Correlation*	1	.559**	.270*	-.052	.136
	Sig. (2-tailed)		<.001	.019	.655	.244
	N	75	75	75	75	75
D2	*Pearson Correlation*	.559**	1	.650**	-.007	.013
	Sig. (2-tailed)	<.001		<.001	.952	.910
	N	75	75	75	75	75
D3	*Pearson Correlation*	.270*	.650**	1	-.006	.112
	Sig. (2-tailed)	.019	<.001		.960	.338
	N	75	75	75	75	75
D4	*Pearson Correlation*	-.052	-.007	-.006	1	.369*
	Sig. (2-tailed)	.655	.952	.960		.001
	N	75	75	75	75	75
D5	*Pearson Correlation*	.136	.013	.112	.369*	1
	Sig. (2-tailed)	.244	.910	.338	.001	
	N	75	75	75	75	75

*. Korelasi adalah signifikan pada aras 0.05 *(2-tailed)*.
**. Korelasi adalah signifikan pada aras 0.01 *(2-tailed)*.

Keputusan nilai signifikan menunjukkan bahawa ada tiga (3) hubungan yang signifikan iaitu item D1 dengan D2 *(p = .001; p < .01)*, D2 dengan D3 *(p = .001; p < .01)* dan D4 dengan D5 *(p = .001; p < .01)* . Bagaimanapun, terdapat hubungan yang tidak signifikan iaitu item D1 dengan D3 *(p = .019; p > .01)*, D1 dengan D4 *(p = .655; p > .01),* D1 dengan D5 *(p = .244; p > .01),* D2 dengan D4 *(p = .952; p > .01),* D2 dengan D5 *(p = .910; p > .01),* D3 dengan D4 *(p = .60; p > .01)* dan D3 dengan D5 *(p = .338; p > .01).* Namun begitu, hubungan antara kesemua item tersebut adalah positif tetapi tidak signifikan.

e. Bahagian E : Faktor Latihan dan Pendidikan

Hasil kajian analisis korelasi *Pearson* dalam Jadual 4.33 menunjukkan nilai indeks korelasi bagi komponen faktor latihan dan pendidikan adalah diantara .021 hingga

.540. Kekuatan hubungan antara item-item secara umumnya adalah sangat lemah, sederhana dan kuat. Kekuatan hubungan antara item E3 dengan E4 (.251) adalah sederhana namun signifikan dan negatif, manakala E1 dengan E2 (.540) adalah kuat dan E1 dengan E3 (.380) adalah sederhana dan signifikan.

Jadual 4.33 : Analisis korelasi *Pearson* bagi Faktor Latihan Dan Pendidikan

Dimensi		E1	E2	E3	E4
E1	*Pearson Correlation*	1	.540**	.380**	-.021
	Sig. (2-tailed)		<.001	<.001	.856
	N	75			75
E2	*Pearson Correlation*	.540**	1	.498**	-.077
	Sig. (2-tailed)	<.001		<.001	.509
	N	75	75	75	75
E3	*Pearson Correlation*	.380**	.498**	1	-.251*
	Sig. (2-tailed)	<.001	<.001		.030
	N	75	75	75	75
E4	*Pearson Correlation*	-.021	-.077	-.251*	1
	Sig. (2-tailed)	.856	.509	.030	
	N	75	75	75	75

*. Korelasi adalah signifikan pada aras 0.05 *(2-tailed).*
**. Korelasi adalah signifikan pada aras 0.01 *(2-tailed).*

Keputusan nilai signifikan menunjukkan bahawa ada tiga (3) hubungan yang signifikan iaitu item E1 dengan E2 *(p = .001; p < .01)*, E1 dengan E3 *(p = .001; p < .01)* dan E2 dengan E3 *(p = .001; p < .01)*. Bagaimanapun, terdapat hubungan yang tidak signifikan iaitu item E1 dengan E4 *(p = .856; p > .01)*, E2 dengan D4 *(p = .509; p > .01),* dan E3 dengan E4 *(p = .030; p > .01)*. Namun begitu, hubungan antara kesemua item tersebut adalah positif tetapi tidak signifikan.

f. Bahagian F : Faktor Polisi/Dasar Keselamatan Maklumat

Hasil kajian analisis korelasi *Pearson* dalam Jadual 4.34 menunjukkan nilai indeks korelasi bagi komponen faktor polisi/dasar keselamatan maklumat di antara .100 hingga .541. Kekuatan hubungan antara item-item secara umumnya adalah sangat

lemah dan kuat. Kekuatan hubungan antara item F1 dengan F2 (.541) adalah kuat, manakala dan F1 dengan F3 (.109) adalah sangat lemah dan tidak signifikan.

Jadual 4.34 : Analisis korelasi *Pearson* bagi Faktor Polisi/Dasar Keselamatan Maklumat

Dimensi		F1	F2	F3
F1	*Pearson Correlation*	1	.541**	-.109
	Sig. (2-tailed)		<.001	.350
	N	75	75	75
F2	*Pearson Correlation*	.541**	1	-.100
	Sig. (2-tailed)	<.001		.394
	N	75	75	75
F3	*Pearson Correlation*	-.109	-.100	1
	Sig. (2-tailed)	.350	.394	
	N	75	75	75

**. Korelasi adalah signifikan pada aras 0.01 *(2-tailed)*.

Keputusan nilai signifikan menunjukkan bahawa ada satu (1) hubungan yang signifikan iaitu item F1 dengan F2 *($p = .001; p < .01$)*. Bagaimanapun, terdapat hubungan yang tidak signifikan iaitu item F1 dengan F3 *($p = .350; p > .01$)* dan F2 dengan F3 *($p = .394; p > .01$)*. Hubungan antara item-item tersebut adalah negatif dan tidak signifikan.

4.8 HASIL KESELURUHAN ANALISIS

Kajian ini melibatkan seramai 75 orang responden di dalam sebuah syarikat swasta iaitu BIT Group Sdn Bhd yang merupakan syarikat induk yang mempunyai tujuh (7) anak syarikat dibawahnya. Soalan kaji selidik telah diedar kepada 176 orang staf seluruh Malaysia, namun 75 orang responden sahaja yang memberi maklum balas dalam tempoh menjawab soalan kaji selidik selama tiga (3) hari iaitu 11 hingga 13 Ogos 2021.

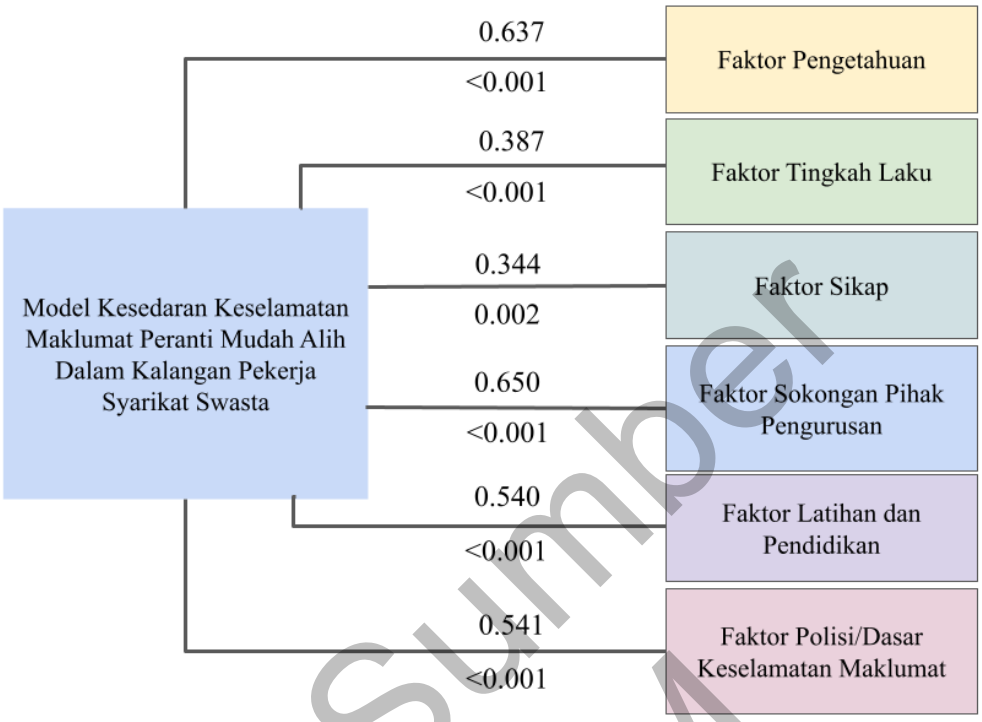
Data yang diperolehi kemudiannya dianalisis dengan menggunakan perisian SPSS versi 28. Menerusi ujian kebolehpercayaan, nilai yang diperoleh daripada *Cronbach Alpha* adalah di antara 0.700 hingga 0.889. Nilai ini menunjukkan indeks

kebolehpercayaan item adalah baik, boleh diterima dan memenuhi ciri-ciri yang dikehendaki.

Hasil ujian skor min pula adalah di antara 3.48 hingga 6.79 untuk setiap komponen yang terlibat. Berdasarkan tafsiran skor min tersebut, nilai tersebut menunjukkan tahap yang sederhana dan tinggi. Skor ini juga menunjukkan bahawa tahap kesedaran keselamatan maklumat peranti mudah alih responden berada di tahap yang sederhana dan tinggi. Jika diperhatikan faktor tingkah laku, faktor sikap, faktor sokongan pihak pengurusan dan faktor latihan dan pendidikan adalah sederhana. Tahap kesedaran keselamatan maklumat responden dalam faktor-faktor ini perlu dipertingkatkan. Faktor pengetahuan dan faktor polisi/dasar keselamatan maklumat pula adalah tinggi. Ini bermaksud majoriti responden mempunyai pengetahuan tentang keselamatan maklumat di tempat kerja dan begitu juga ada polisi di syarikat masing-masing yang menekankan aspek keselamatan maklumat.

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*.

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*. Rajah 4.7 menunjukkan hubungan korelasi antara keenam-enam faktor berdasarkan analisis korelasi *Pearson*.



Rajah 4.7 : Hubungan keenam-enam faktor berdasarkan Analisis Korelasi *Pearson*

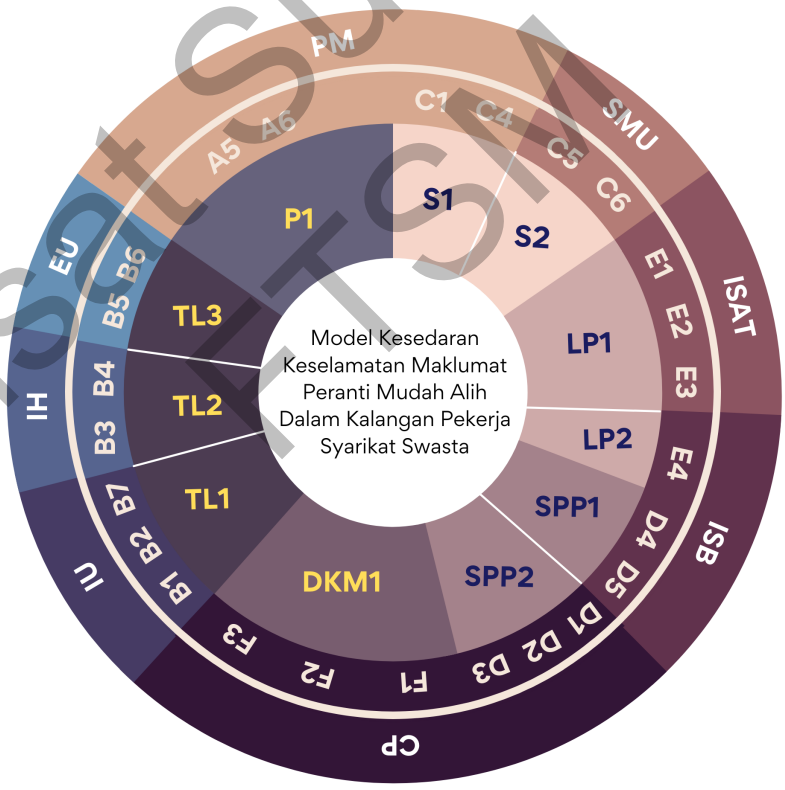
4.9 MODEL AKHIR

Berdasarkan penentusahan dan pengesahan yang dibuat oleh pakar, model akhir kajian adalah sama dengan model awal kajian dengan sedikit penambahbaikan seperti dalam Rajah 4.8. 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 4.8 menunjukkan keseluruhan komponen model akhir yang dipecahkan mengikut kategori berdasarkan ujian analisis faktor dan hasil putaran *varimax*.



Rajah 4.8 : Model akhir kajian

Jadual 4.35 menunjukkan keseluruhan item-item dalam setiap faktor dalam komponen model akhir kajian beserta dengan kategori bagi setiap item yang diterangkan secara terperinci berdasarkan Rajah 4.8.

Jadual 4.35 : 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.
		E2	Memahami dan mempraktikkan apa yang dipelajari tentang 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.

bersambung...

...sambungan **DKM1** Faktor Dasar Keselamatan Maklumat Syarikat	**Polisi Syarikat (CP)**	**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.

4.10 KESIMPULAN

Melalui analisis statistik yang dijalankan ini, secara keseluruhan hasil analisis dapat menyokong teori dan model yang dibincangkan dalam Bab I dan Bab II. Hasil analisis kajian ini juga, melalui ujian skor min yang dijalankan mendapati tahap kesedaran yang tinggi terhadap faktor kesedaran keselamatan maklumat dalam kalangan pekerja BIT Group of Companies. Ujian analisis faktor yang dijalankan juga melihatkan hampir setiap item di dalam komponen faktor mempunyai hubungan yang sederhana dan tinggi. Ujian korelasi *Pearson* pula dijalankan bagi menunjukkan faktor pengetahuan, faktor sokongan pihak pengurusan, faktor latihan dan pendidikan dan faktor polisi/dasar keselamatan maklumat mempunyai hubungan korelasi yang kuat dan signifikan, manakala faktor tingkah laku dan faktor sikap mempunyai hubungan yang sederhana dan signifikan.

Secara keseluruhannya, bab ini menerangkan pengesahan instrumen kajian daripada pakar dan seterusnya analisis terhadap data yang diperolehi daripada soalan kaji selidik. Analisis yang dilaksanakan telah dapat mengenal pasti tahap kesedaran keselamatan maklumat peranti mudah alih dalam kalangan pekerja syarikat swasta

seperti di BIT Group of Companies. Hasil gabungan analisis faktor dan hubungan keenam-enam faktor dengan pemboleh ubah telah membentuk model akhir kajian seperti dalam Rajah 4.8. Bab V seterusnya akan membincangkan rumusan, cadangan dan kesimpulan yang diperolehi bagi keseluruhan kajian yang dijalankan.

BAB V

PERBINCANGAN DAN KESIMPULAN

5.1 PENGENALAN

Bab terakhir ini akan membincangkan penemuan hasil dapatan kajian daripada Bab IV dan merumuskan keseluruhan kajian. Hasil kajian yang dibincang ialah ringkasan dan pencapaian objektif, sumbangan kajian, kekangan dan cadangan kajian masa depan serta penutup. Selain itu, berdasarkan pengalaman yang diperolehi sepanjang melaksanakan kajian ini, bab ini juga memberi beberapa cadangan yang boleh dilaksanakan pada masa hadapan berkaitan dengan hasil kajian. Objektif kajian ini adalah untuk mengenal pasti tahap kesedaran dalam kalangan pekerja swasta terhadap keselamatan maklumat dan juga mengenal pasti faktor dominan yang mempengaruhi tahap kesedaran keselamatan maklumat melalui peranti mudah alih seperti penggunaan telefon pintar dan komputer riba di tempat kerja.

5.2 PENCAPAIAN OBJEKTIF

Secara keseluruhannya, kajian ini berjaya memenuhi tiga (3) objektif kajian yang dinyatakan di dalam Bab I iaitu untuk (i) mengenal pasti tahap kesedaran dalam kalangan pekerja swasta terhadap keselamatan maklumat terutama dalam penggunaan peranti mudah alih di tempat kerja; (ii) mengenal pasti faktor dominan yang mempengaruhi tahap kesedaran keselamatan maklumat di tempat kerja; dan (iii) membina model tahap kesedaran keselamatan maklumat peranti mudah alih dan mengesahkan model yang dibangunkan. Berikut adalah rumusan penemuan kajian terhadap persoalan kajian.

5.2.1 Mengenal pasti tahap kesedaran dalam kalangan pekerja swasta terhadap keselamatan maklumat terutama dalam penggunaan peranti mudah alih di tempat kerja.

Objektif pertama adalah untuk mengenal pasti tahap kesedaran dalam kalangan pekerja swasta terhadap keselamatan maklumat terutamanya dalam penggunaan peranti mudah alih di tempat kerja. Pembangunan model dalam kajian ini adalah

bermula dengan melakukan kajian kesusasteraan terhadap model kesediaan dan kajian yang lepas yang berkaitan dengan 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. Kemudian dalam Bab II faktor persekitaran tersebut 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).

5.2.2 Mengenal pasti faktor dominan yang mempengaruhi tahap kesedaran keselamatan maklumat di tempat kerja.

Objektif kedua adalah mengenal pasti faktor dominan yang mempengaruhi tahap kesedaran keselamatan maklumat di tempat kerja. Berdasarkan kajian kesusasteraan terhadap model kesedaran keselamatan maklumat yang lepas, kajian terhadap faktor kesedaran dan peranti mudah alih dalam kalangan penjawat awam, pihak kerajaan sudah pun mempunyai polisi mereka tersendiri yang dipanggil DKICT dan BYOD dan ia dikawal selia oleh pihak MAMPU. Namun, untuk syarikat swasta, perkara ini hanya boleh dikawal selia oleh syarikat tersebut. Jadi, kajian ini membantu syarikat swasta mengenal pasti faktor-faktor kesedaran keselamatan maklumat dalam kalangan pekerja. 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.

Terdapat beberapa penemuan yang tidak dijangka daripada kajian ini iaitu:

1. Tahap kesedaran adalah sederhana dan tinggi bagi syarikat swasta yang berteraskan IT. Dijangkakan syarikat swasta yang berasaskan IT sepatutnya mempunyai tahap kesedaran yang tinggi kerana adanya pengetahuan tentang keselamatan maklumat secara tidak langsung.
2. Faktor tingkah laku dan sikap adalah pada tahap sederhana dan faktor latihan dan pendidikan serta faktor polisi perlu ada dibuat secara berkala dalam syarikat swasta kerana ia boleh menjadi faktor penting dalam memastikan keselamatan maklumat dalam organisasi.

5.2.3 Membina model tahap kesedaran keselamatan maklumat peranti mudah alih dan mengesahkan model yang dibangunkan.

Objektif kajian yang ketiga 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. Di dalam fasa tiga (3) kajian ini, beberapa analisis diadakan ke atas data yang diterima daripada responden menerusi kaji selidik yang dijalankan. 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. 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.* 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.

5.3 SUMBANGAN KAJIAN

Berdasarkan kajian yang telah dijalankan, terdapat enam (6) sumbangan utama yang telah diberikan dalam kajian ini. Sumbangan-sumbangan tersebut ialah:

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.

5.4 CADANGAN KAJIAN MASA HADAPAN

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

5.5 PENUTUP

Secara keseluruhannya kajian ini telah berjaya mencapai objektif kajian dan menjawab persoalan kajian seperti yang dinyatakan dalam Bab I. Sumbangan kajian ini telah berjaya menghasilkan model kesedaran keselamatan maklumat peranti mudah alih dalam kalangan pekerja syarikat swasta yang merangkumi soalan kaji selidik

yang dibangunkan berdasarkan model sedia ada dan kajian lepas dalam bahasa yang lebih mudah difahami dan bersesuaian, dan juga sebagai garis panduan kepada syarikat swasta lain. Hasil keputusan yang diperolehi daripada pengesahan pakar dan soal selidik yang dihantar kepada responden, secara puratanya membuktikan model ini berkesan dalam menilai tahap kesedaran keselamatan maklumat dalam kalangan pekerja serta dapat dijadikan penanda aras untuk syarikat membenarkan pekerja membawa peranti mudah alih seperti telefon pintar dan komputer riba untuk kegunaan di tempat kerja dengan diberikan polisi yang bersesuaian. Model yang dibangunkan diharap akan dimanfaatkan sebaiknya dan terus ditambahbaik di masa hadapan.

RUJUKAN

Adel Ismail Al-Alawi, Sulaiman M.H. Al-Kandari and Refaat Hassan Abdel-Razek. 2016. *Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University*. Journal of Innovation & Business Best Practice, DOI: 10.5171/2016.329374.

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

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

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.

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.

Al-Sehri, Yasser. 2021. *Information Security Awareness and Culture*. British Journal of Arts and Social Sciences. Vol.6 (No.1): 61-69.

AlKalbani, A., Deng, H. & Kam, B. 2015. *Organisational Security Culture and Information Security Compliance for e-Government Development: The Moderating Effect of Social Pressure*. Pacific Asia Conference on Information Systems, PACIS 2015.

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.

Allam, S., Stephen, V.F. & Ethan, F. 2014. *Smartphone Information Security Awareness: A Victim of Operational Pressures*. Computer & Security 42: 56-65.

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

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.

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

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

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.

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.

Cheng, L., Li, Y., Li. W., Holm, E. & Zhai, Q. 2013. *Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory*. Computers and Security, 39(PART B), 447-459. doi:10.1016/j.cose.2013.09.009

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.

Cohen, L., Manion, L. & Morrison, K. 2011. *Research Methods in Education*. hlm. 7th Edisi . New York: Routledge Taylor & Francis Group.

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).

Creswell, J. W. 2012. *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research 4th Edition*. Pearson.

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].

CyberSecurity Malaysia. 2020. Infografik: Perlindungan Kata Laluan. https://www.cybersecurity.my/properties_v3/images/infographic/6-kata-laluan-bm.jpg [15 Ogos 2021].

Da Veiga, A. 2015. *The Influence of Information Security Policies on Information Security Culture: Illustrated Through a Case Study*. Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015 (July): 22–33.

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

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

Farouk Jani Basha. 2020. *Model Tahap Kesedaran Dan Kepatuhan Terhadap Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Polis Diraja Malaysia (PDRM)*. Fakulti Sains dan Teknologi Maklumat (FTSM), UKM.

Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E. & Wagner, D. 2012. *Android Permissions: User Attention, Comprehension and Behavior*. Symposium on Usable Privacy and Security (SOUPS)1-14.

Fink, A. 1998. *Conducting Research Literature Reviews: From the Internet to Paper*. (Arlene Fink, Ed.), hlm. 5th Edisi. SAGE Publications.

Furnell, S., Clarke, N. 2012. *Power to People? The Evolving Recognition of Human Aspects of Security*. Computer & Security 31(8): 983-988.

Gaurav Belani. 2020. 5 Cybersecurity Threats to Be Aware of in 2020. https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020 [12 Jun 2021].

George, D., & Mallery, P. (2003). *SPSS for Windows Step By Step: A Simple Guide and Reference (4th edn.)*. Boston: Allyn & Bacon

Gibson, D. 2011. *Managing Risk in Information Systems*. Jones & Barlett Learning.

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.

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.

Hina, S. & Dominic, P. D. D. 2018. *Information Security Policies' Compliance: A Perspective for Higher Education Institutions*. Journal of Computer Information Systems 1–11. doi:10.1080/08874417.2018.1432996

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

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

Jacey Mariadass, Hazura Mohamed & Rossilawati Sulaiman. 2017. *Kesedaran Keselamatan Penggunaan Gajet Peribadi Dalam Kalangan Staf Akademik Politeknik Malaysia*. Politeknik Ungku Omar dan UKM.