MODEL TAHAP KESEDARAN KESELAMATAN MAKLUMAT DALAM KALANGAN PENJAWAT AWAM

Mohd Rafizam bin Mohamed
Ibrahim Mohamed
Hasimi Sallehuddin

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Tujuan kajian ini dilakukan adalah untuk melihat tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam. Kajian kes dilakukan di salah sebuah agensi sektor awam iaitu Ibu Pejabat Suruhanjaya Pilihan Raya (SPR) Malaysia yang terletak di Putrajaya. Pemilihan SPR sebagai agensi terpilih adalah kerana agensi ini mempunyai maklumat yang penting dan sensitif seperti rekod pendaftaran pemilih, maklumat persempadanan dan rekod pengundi rakyat Malaysia. Berdasarkan kepada kajian dari pengkaji yang lepas, adalah didapati faktor pekerja menyumbang kepada isu keselamatan maklumat. Maka jelaslah bahawa perlu ada kesedaran keselamatan maklumat dalam kalangan penjawat awam yang bertugas di sektor awam bagi melindungi dan menjaga keselamatan maklumat di setiap agensi. Kesedaran keselamatan maklumat penjawat awam diukur dengan merujuk kepada empat faktor yang telah dikenalpasti melalui ulasan kepustakaan yang terdiri daripada faktor sikap, latihan dan pendidikan, sokongan pihak pengurusan dan polisi/dasar keselamatan maklumat. Kaedah kajian ini dimulakan dengan pencarian kajian terdahulu mengenai isu berkaitan kesedaran keselamatan maklumat bagi mencari jurang kajian. Seterusnya, ulasan kepustakaan yang lebih mendalam dilakukan untuk membangunkan instrumen bagi soalan kaji selidik. Borang kaji selidik secara atas talian dan manual digunakan untuk mendapat maklumbalas daripada 132 responden. Perisian *Statistical Package for Social Science* (SPSS) versi 24.0 digunakan untuk tujuan analisis dan dipersembahkan dalam bentuk jadual dan graf bagi mendapatkan keputusan yang dikehendaki. Dapatan kajian menunjukkan tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam untuk faktor yang dikenalpasti adalah di tahap yang baik dan saling berhubungkait. Pada akhir kajian, satu cadangan model telah dibangunkan yang telah mendapat pengesahan daripada pakar yang berpengalaman dan boleh dijadikan sebagai panduan bagi kaedah untuk mempertingkatkan tahap kesedaran keselamatan maklumat dalam kalangan penjawat awam.

1.0 LATAR BELAKANG

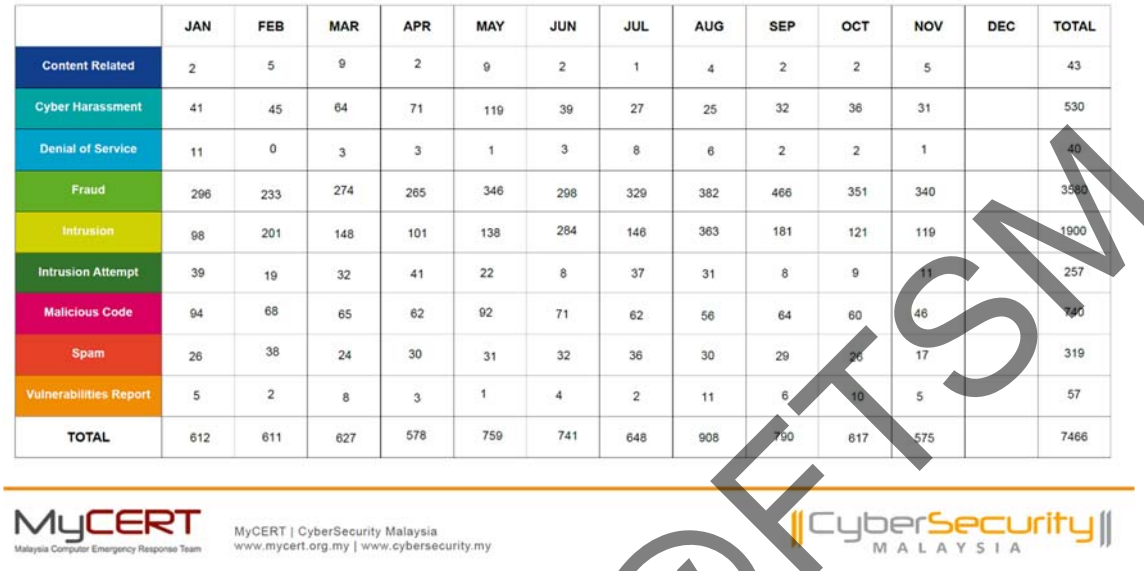
Penggunaan teknologi maklumat dan komunikasi telah mempengaruhi kehidupan manusia dengan ketara pada masa kini. Teknologi berasaskan web telah membawa banyak kelebihan kepada organisasi dan pelanggan tetapi pelanggaran keselamatan maklumat masih menjadi kebimbangan di setiap agensi kerajaan. *Anti-virus, anti-malware, anti-spam, anti-phishing, anti-spyware, firewall*, dan sistem pengesanan pencerobohan adalah antara aspek teknologi yang digunakan untuk menangani keselamatan maklumat, tetapi teknologi ini tidak dapat menjamin persekitaran yang selamat untuk perlindungan maklumat (Safa et al. 2015).

Keselamatan maklumat masih merupakan isu penting bagi kedua-dua pengguna dan organisasi. Teknologi tidak semata-mata menjamin persekitaran yang selamat untuk maklumat; aspek manusia bagi menjamin keselamatan maklumat harus dipertimbangkan, selain aspek teknologi. Kekurangan kesedaran keselamatan maklumat, kejahilan, kecuaian, sikap tidak peduli, kerosakan, dan ketahanan adalah asas kesalahan yang dilakukan oleh ramai pekerja (Safa et al. 2016).

Di Malaysia, agensi kerajaan juga turut digesa untuk meningkatkan tahap kecekapan dan keberkesanan mengawal ancaman luar yang boleh mengugat isu keselamatan maklumat (MAMPU 2016). Walaupun terdapat kelebihan dari segi penyampaian maklumat kepada orang ramai dengan menggunakan perkhidmatan atas talian, namun agensi juga terdedah kepada risiko keselamatan melalui penggantungan kepada penggunaan teknologi maklumat dan komunikasi untuk menjalankan perkhidmatan mereka, khususnya organisasi yang menawarkan perkhidmatan atas talian. Terdapat pelbagai langkah yang diambil oleh pihak kerajaan bagi menangani masalah keselamatan maklumat. Antara yang terkini adalah, pihak *Malaysian Administrative Modernization and Management Planning Unit* (MAMPU) telah mengeluarkan satu rangka kerja keselamatan siber sektor awam (RAKKSA) bertujuan memberi panduan asas serta merangkumi kesemua komponen keselamatan yang perlu diambil kira oleh kementerian dan agensi sektor awam untuk melindungi maklumat dalam ruang siber mereka.

Menurut statistik yang dikeluarkan oleh MyCert pada tahun 2017 (Rajah 1.1), terdapat 7,466 kes insiden keselamatan yang telah berlaku sehingga November 2017. Rajah

1.1 menunjukkan statistik pelbagai jenis insiden keselamatan maklumat dari Januari hingga November 2017.



	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
Content Related	2	5	9	2	9	2	1	4	2	2	5		43
Cyber Harassment	41	45	64	71	119	39	27	25	32	36	31		530
Denial of Service	11	0	3	3	1	3	8	6	2	2	1		40
Fraud	296	233	274	265	346	298	329	382	466	351	340		3580
Intrusion	98	201	148	101	138	284	146	363	181	121	119		1900
Intrusion Attempt	39	19	32	41	22	8	37	31	8	9	11		257
Malicious Code	94	68	65	62	92	71	62	56	64	60	46		740
Spam	26	38	24	30	31	32	36	30	29	26	17		319
Vulnerabilities Report	5	2	8	3	1	4	2	11	6	10	5		57
TOTAL	612	611	627	578	759	741	648	908	790	617	575		7466

Rajah 1.1 Statistik Insiden Keselamatan Maklumat Tahun 2017
(Sumber : https://www.mycert.org.my/statistics/2017.php)

Oleh yang demikian, bagi memastikan keselamatan maklumat adalah bebas daripada ancaman virus, serangan pengodam, cacing *(worm), spam* dan sebagainya maka keperluan untuk meningkatkan kesedaran keselamatan maklumat dalam kalangan penjawat awam perlu dititikberatkan. Justuru itu, selain menyediakan polisi dan dasar berkaitan keselamatan maklumat, usaha untuk mempertingkatan kesedaran keselamatan maklumat dalam kalangan penjawat awam adalah perlu dilakukan bagi memelihara keselamatan maklumat dalam agensi kerajaan.

2.0 KAJIAN KESUSASTERAAN

2.1 Keselamatan Maklumat

Menurut takrifan *Malaysian Administrative Modernization and Management Planning Unit* MAMPU (2010), maklumat merupakan hasil terakhir sesuatu sistem pengkomputeran dan dengan itu ianya amat penting dan bernilai bagi sesebuah organisasi. Kehilangan atau kemusnahan data/maklumat yang disimpan di dalam komputer sering berlaku disebabkan oleh kejadian seperti kebakaran, pengkhianatan, kecuaian dan kecurian. Bagi mengatasi masalah ini, kawalan ke atas capaian data/ maklumat dan keselamatan fizikal perlu diperketatkan.

Keselamatan maklumat pula ditakrifkan sebagai perlindungan sistem maklumat daripada ancaman akses dan maklumat yang tidak dibenarkan (Cavalli et al. 2004; Tamjidyamcholo et al. 2013). Keselamatan maklumat adalah salah satu unsur penting yang perlu dipertimbangkan dalam pembangunan sistem maklumat. Banyak organisasi telah pun melaksanakan teknologi keselamatan canggih seperti kad pintar dan biometrik bagi memantapkan keselamatan maklumat organisasi (Kreicberga 2010).

2.2 Faktor Kesedaran Keselamatan Maklumat

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, Arshad & Lubis 2011).

2.2.1 Faktor Sikap

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.

Sikap merupakan respon atau reaksi yang masih tertutup dari seseorang terhadap sesuatu perkara. Ianya merupakan kesediaan untuk bertindak dan bukan merupakan pelaksanaan motif tertentu. 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 ianya 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. 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.

2.2.2 Faktor Sokongan Pihak Pengurusan

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 al. 2008).

Seperti yang telah dibincangkan sebelum ini, pihak pengurusan dapat menunjukkan sokongan mereka terhadap tingkah laku keselamatan maklumat melalui penganjuran dan membangunkan latihan keselamatan maklumat, program kesedaran dan pelaksanaan ISP. Latihan keselamatan maklumat, program kesedaran dan pelaksanaan ISP adalah kaedah untuk memaklumkan kepada pekerja tentang ISP organisasi (Martin & Rice 2011), yang bertujuan untuk memperkenalkan dan menyediakan maklumat mengenai pentingnya penggunaan langkah balas/tindakan balas keselamatan untuk mengelakkan maklumat ancaman keselamatan dan kesan ancaman kepada organisasi.

Para pemimpin di dalam sesebuah 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 ISP organisasi.

2.2.3 Faktor Latihan Dan Pendidikan

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 ISP organisasi (Siponen, Adam Mahmood & Pahnila 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; Liang, & Xue 2009; 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 ini bagi memastikan tingkah laku keselamatan para pekerja boleh diterima. Kandungan latihan keselamatan maklumat dan program kesedaran keselamatan harus merangkumi maklumat terperinci termasuklah tahap kerosakkan jika ancaman keselamatan ini tersebar di dalam sesebuah organisasi (Siponen et al. 2014).

2.2.4 Faktor Polisi/Dasar Keselamatan Maklumat

Adalah penting bagi organisasi menyediakan dokumentasi ISP yang betul supaya para pekerja dapat memahami dan mengamalkannya. Kajian semasa menunjukkan bahawa ISP yang didokumentasi dengan baik dengan penerangan yang jelas dapat meningkatkan kesedaran pengguna tentang keselamatan maklumat (Al-Omari et al. 2013).

Dengan itu, insiden keselamatan di dalam organisasi dapat dikurangkan. Kajian terdahulu menegaskan bahawa ISP adalah penting kerana ia menyediakan satu set peraturan dan prosedur yang membantu menentukan tahap keselamatan maklumat yang disyorkan di dalam organisasi yang harus dikuti oleh para pekerja (Yildirim Y. et al. 2011).

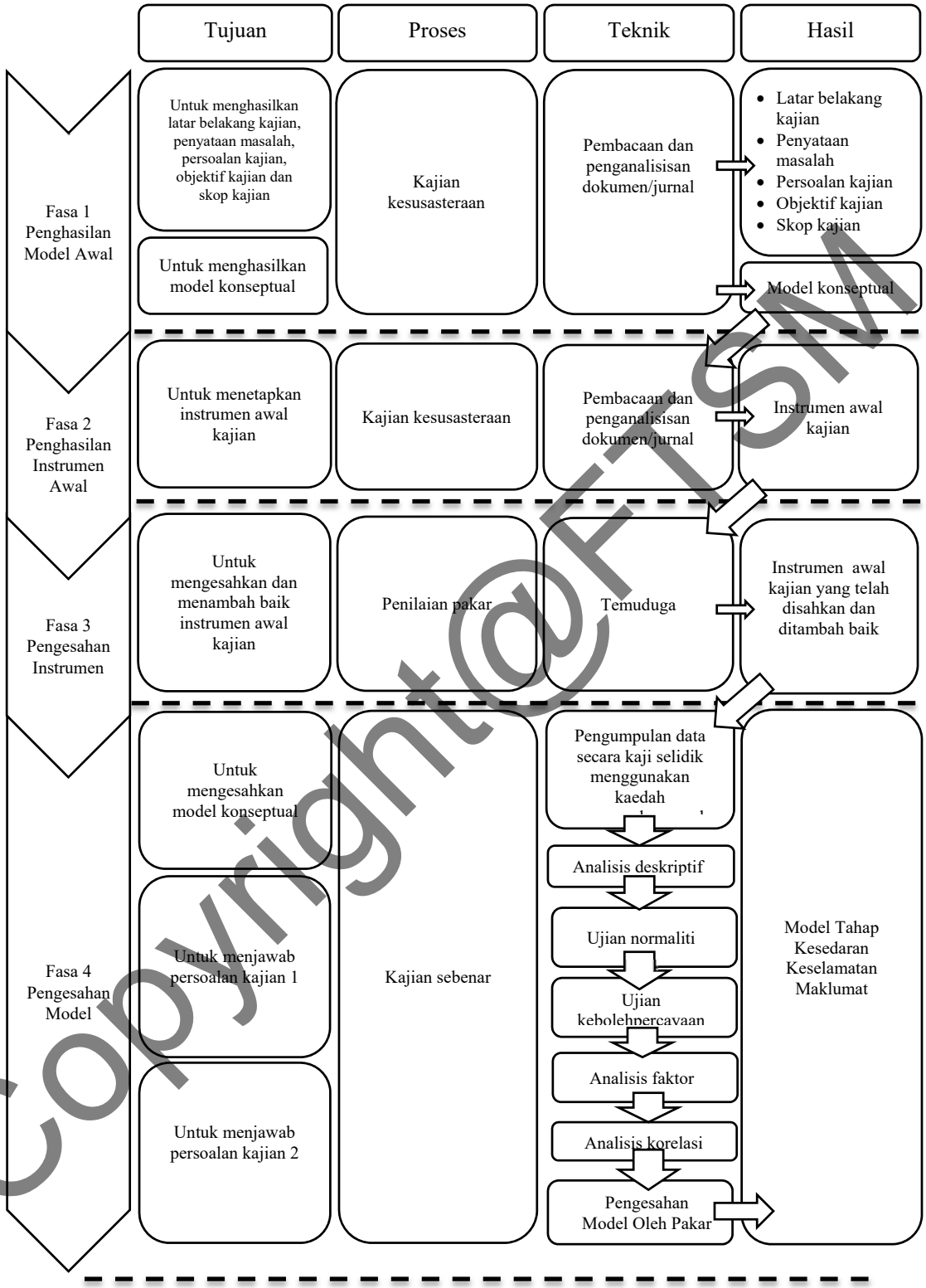
Secara umumnya, Safa et al. (2016) menyatakan bahawa ISP adalah pernyataan niat dan objektif dasar syarikat yang bertujuan a) Untuk menunjukkan lembaga dan pengurusan kanan syarikat komitmen terhadap keselamatan maklumat. B) Untuk menetapkan arahan untuk pelaksanaan dan menekankan bahawa mereka melihatnya sebagai bahagian penting dari operasi harian syarikat c) Untuk mengekalkan kesinambungan operasi dan seterusnya meneruskan untuk menyediakan perkhidmatan d) Untuk melindungi aset syarikat.

.

3.0 METODOLOGI KAJIAN

3.1 Pendekatan Kajian

Pendekatan kajian distrukturkan kepada empat (4) fasa utama iaitu penghasilan model konseptual, penghasilan instrumen awal, pengesahan instrumen kajian dan pengesahan model. Setiap fasa diperincikan kepada proses-proses yang terlibat, tujuan pelaksanaan setiap proses, teknik yang digunakan bagi setiap proses dan hasil akhir bagi setiap proses. Gambaran pendekatan kajian adalah seperti yang ditunjukkan dalam Rajah 1.3.



Rajah 1.3 Pendekatan kajian

4.0 PENGUJIAN DAN ANALISIS

4.1 Analisis Korelasi

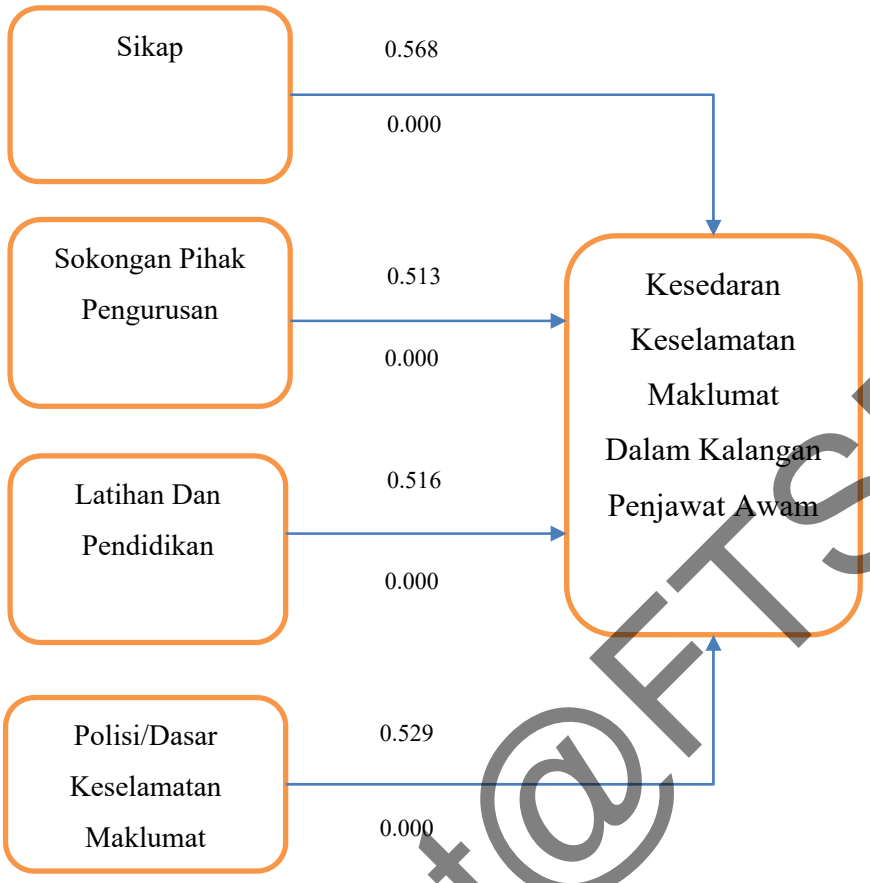
Analisis korelasi antara dimensi kesedaran keselamatan maklumat dibuat bagi menguji dan menerangkan arah serta kekuatan hubungan bagi empat (4) dimensi keselamatan maklumat dengan satu (1) dimensi kesedaran keselamatan maklumat. Hasil korelasi adalah seperti di Jadual 4.1.

Jadual 4.1 Korelasi antara dimensi

Kod	Dimensi	Arah dan Kekuatan				
		Positif Lemah	**Positif Baik**	**Positif Sangat Baik**	**Positif Kuat**	**Tiada korelasi**
A	Sikap	Tiada	B (.441) C (.349) D (.498)	E (.568)	Tiada	Tiada
B	Sokongan Pihak Pengurusan	Tiada	A (.441)	C (.610) E (.513)	D (.762)	Tiada
C	Latihan Dan Pendidikan	Tiada	A (.349)	B (.610) D (.601) E (.513)	Tiada	Tiada
D	Polisi/Dasar Keselamatan Maklumat	Tiada	A (.498)	C (.601) E (.529)	B (.762)	Tiada
E	Kesedaran Keselamatan Maklumat	Tiada	Tiada	A (.568) B (.513) C (.516) D (.529)	Tiada	Tiada

Secara keseluruhannya, hasil analisis korelasi antara dimensi menunjukkan wujud hubungan sangat baik dan kuat antara setiap dimensi kesedaran keselamatan maklumat. Hasil analisis korelasi antara dimensi sikap, sokongan pihak pengurusan, latihan dan pendidikan serta polisi/dasar keselamatan maklumat dengan dimensi kesedaran keselamatan maklumat menunjukkan semua dimensi mempunyai hubungan yang sangat baik. Analisis korelasi ini telah menjawab persoalan pertama kajian iaitu adakah wujud hubungan antara dimensi keselamatan maklumat dengan dimensi kesedaran keselamatan maklumat iaitu di tahap yang sangat baik dan kuat.

4.2 Pengesahan Model Oleh Pakar



Rajah 4.2 Model Akhir Tahap Kesedaran Keselamatan Maklumat Dalam Kalangan Penjawat Awam

5.0 RUMUSAN DAN KESIMPULAN

5.1 Rumusan

Kesedaran keselamatan maklumatmerupakan salah satu faktor yang penting dalam menentukan kejayaan dalam menjaga kerahsiaan maklumat organsiasi. Kegagalan untuk menilai dan menambah baik kesedaran keselamatan maklumat secara langsung memberi kesan kepada prestasi organisasi.

Sehubungan dengan itu, kajian ini dijalankan bertujuan untuk mencapai dua objektif utama iaitu:

a) Mengenal pasti faktor kesedaran keselamatan maklumat dan hubung kaitnya dalam kalangan penjawat awam.

b) Membangunkan model kesedaran keselamatan maklumat.

Bagi memenuhi objektif pertama kajian iaitu mengenal pasti dimensi kesedaran keselamatan maklumat dan hubung kaitnya, kajian kesusasteraan telah dijalankan secara sistematik ke atas kajian-kajian terdahulu dalam bidang kualiti maklumat.

5.1.1 Korelasi Sikap

Secara keseluruhan dari dapatan analisis, angka koefisien korelasi bagi faktor sikap adalah dalam julat 0.26 – 0.50. Ini bererti tingkat kekuatan hubungan antara dimensi adalah sangat baik. Angka korelasi adalah bernilai positif dan bermakna hubungan adalah searah. Oleh yang demikian, dapat disimpulkan bahawa semakin tinggi sikap pekerja semakin meningkatkan kesedaran keselamatan maklumat.

Nilai Sig. (2 tailed) adalah 0.000 dan ini bermakna lebih kecil dari 0.05 atau 0.01, maka ertinya ada hubungan yang signifikan antara dimensi sikap dan kesedaran keselamatan maklumat.

5.1.2 Korelasi Sokongan Pihak Pengurusan

Secara keseluruhan dari dapatan analisis, angka koefisien korelasi bagi faktor sokongan pihak pengurusan adalah dalam julat 0.26 – 0.99. Ini bererti tingkat kekuatan hubungan antara dimensi adalah sangat baik dan kuat. Angka korelasi adalah bernilai positif dan bermakna hubungan adalah searah. Oleh yang demikian, dapat disimpulkan bahawa semakin tinggi sokongan pihak pengurusan semakin bertambah kesedaran keselamatan maklumat dalamkalangan pekerja.

Nilai Sig. (2 tailed) adalah 0.000 dan ini bermakna lebih kecil dari 0.05 atau 0.01, maka ertinya ada hubungan yang signifikan antara dimensi sokongan pihak pengurusan dan kesedaran keselamatan maklumat.

5.1.3 Korelasi Latihan dan Pendidikan

Secara keseluruhan dari dapatan analisis, angka koefisien korelasi bagi faktor latihan dan pendidikan adalah dalam julat 0.26 – 0.75. Ini bererti tingkat kekuatan hubungan antara dimensi adalah sangat baik dan kuat. Angka korelasi adalah bernilai positif dan bermakna hubungan adalah searah. Oleh yang demikian, dapat disimpulkan bahawa semakin banyak latihan dan pendidikn semakin tinggi kesedaran keselamatan maklumat pekerja tersebut.

Nilai Sig. (2 tailed) adalah 0.000 dan ini bermakna lebih kecil dari 0.05 atau 0.01, maka ertinya ada hubungan yang signifikan antara dimensi latihan dan pendidikan dan kesedaran keselamatan maklumat.

5.1.4 Korelasi Polisi dan Dasar Keselamatan Maklumat

Secara keseluruhan dari dapatan analisis, angka koefisien korelasi bagi faktor latihan dan pendidikan adalah dalam julat 0.26 – 0.99. Ini bererti tingkat kekuatan hubungan antara dimensi adalah sangat baik dan kuat. Angka korelasi adalah bernilai positif dan bermakna hubungan adalah searah. Oleh yang demikian, dapat disimpulkan bahawa semakin jelas polisi dan dasar keselamatan maklumat akan meningkatkan kesedaran keselamatan maklumat dalam kalangan pekerja.

Nilai Sig. (2 tailed) adalah 0.000 dan ini bermakna lebih kecil dari 0.05 atau 0.01, maka ertinya ada hubungan yang signifikan antara dimensi polisi dan dasar keselamatan maklumat dan kesedaran keselamatan maklumat.

5.2. Cadangan dan Kajian Masa Depan

Model dihasilkan berdasarkan analisis data ke atas dimensi sikap, latihan dan pendidikan, sokongan pihak pengurusan dan polisi/dasar keselamatan maklumat. Oleh itu, dicadangkan agar pengujian lanjut dilaksanakan menggunakan dimensi daripada jenis berbeza seperti pengetahuan, tingkahlaku dan lain-lain bagi tujuan pemantapan model.

5.2.1. Menguji model yang dihasilkan ke jumlah penjawat awam yang lebih ramai

Model yang dihasilkan adalah terdiri daripada kalangan penjawat awam yang bertugas di Ibu Pejabat SPR Putrajaya. Ini secara tidak langsung, dapatan kajian tidak mencerminkan dapatan bagi seluruh penjawat awam. Oleh itu pengujian lanjut disarankan ke atas penjawat awam yang bertugas di kementerian atau pasukan beruniform.

5.2.2 Menggunakan pendekatan kajian secara kualitatif

Kajian ini merupakan kajian kuantitatif di mana pengkaji cuba untuk mengenal pasti dimensi kesedaran keselamatan maklumat dalam konteks sektor awam. Kajian secara kualitatif diharapkan dapat memberi pemahaman yang lebih mendalam terhadap model yang telah dihasilkan.

5.2.3. Mewujudkankan suasana mesra keselamatan maklumat kepada penjawat awam

Penjawat awam perlu didedahkan kepada kesedaran keselamatan maklumat walaupun mempunyai latarbelakang tugas yang berbeza. Setiap penjawat awam sebolehnya diwajibkan menghadiri latihan dan kursus sekurang-kurangnya sekali setahun bagi memberi pendedahan kepada teknologi maklumat yang senantiasa berubah.

5.3. Kesimpulan

Secara keseluruhannya, kajian ini telah berjaya membangunkan Model Tahap Kesedaran Keselamatan Maklumat Dalam Kalangan Penjawat Awam dalam konteks sektor awam di Malaysia. Model ini dapat dijadikan garis panduan dalam menilai dan menambah baik kesedaran keselamatan maklumat dalam kalangan penjawat awam supaya kesedaran keselamatan maklumat dapat ditingkatkan dan maklumat dapat diselenggara dengan lebih baik dan selamat. Seterusnya, sistem penyampaian kerajaan bertambah baik dan keselamatan maklumat dapat diurus dengan lebih sempurna.

RUJUKAN

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

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 Sciences*, 3018–3027.

Al-Salihy, Ann, Jannet, W, Sures, R. 2003. Effectivess of Information Systems Security in IT Organizations in Malaysia. *The 9th Asia-Pacific Conference*, 716–720.

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*, *22*(6), 1043–1058.

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

Cavalli, E., Mattasoglio, A., Pinciroli, F. & Spaggiari, P. 2004. Information security concepts and practices: The case of a provincial multi-specialty hospital. *International Journal of Medical Informatics*,. doi:10.1016/j.ijmedinf.2003.12.008

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

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

Kreicberga, L. 2010. Internal threat to information security. *Pure.Ltu.Se*,.

Liang, H. & Xue, Y. 2009. Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly*, *33*(1), 71–90.

MAMPU. 2010. Dasar Keselamatan ICT Unit Pemodenan Tadbiran Dan Perancangan Pengurusan Malaysia (MAMPU) Jabatan Perdana Menteri. *Garis Panduan*,. Retrieved from http://www.mampu.gov.my/documents/10228/3486670/DKICT_53.pdf/

MAMPU. 2016. Rangka Kerja Keselamatan Siber Sektor Awam.

Martin, N. & Rice, J. 2011. Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers and Security*, *30*(8), 803–814.

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

Rezgui, Y. & Marks, A. 2008. Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7–8), 241–253. doi:10.1016/j.cose.2008.07.008

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A. & Herawan, T. 2015. Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78. doi:10.1016/j.cose.2015.05.012

Safa, Von Solms, R. & Furnell, S. 2016. Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82.

Santos, R., Correia, M. E. & Antunes, L. 2008. Securing a health information system with a government issued digital identification card. *Proceedings - International Carnahan Conference on Security Technology*, 135–141.

Siponen, M., Adam Mahmood, M. & Pahnila, S. 2014. Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224.

Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H. & Gholipour, R. 2013. Information security - Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers and Education*, *68*, 223–232. doi:10.1016/j.compedu.2013.05.010

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

Yildirim Y., E., Akalp, G., Aytac, S. & Bayram, N. 2011. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31*(4), 360–365. doi:10.1016/j.ijinfomgt.2010.10.006