KESEDARAN KESELAMATAN PENGGUNAAN GAJET PERIBADI DALAM KALANGAN STAF AKADEMIK POLITEKNIK MALAYSIA

Jacey Mariadass[1], Hazura Mohamed[2] & Rossilawati Sulaiman[2]

[1]Politeknik Ungku Omar
jacey@puo.edu.my
[2]Universiti Kebangsaan Malaysia
hazura.mohamed@ukm.edu.my
rossilawati@ukm.edu.my

ABSTRAK

Ledakan teknologi membawa arus dalam penggunaan pelbagai peranti canggih untuk berkomunikasi di antara satu sama lain. Gajet peribadi atau lebih dikenali sebagai *Bring Your Own Device* (*BYOD*) merupakan situasi apabila pekerja di sesebuah organisasi diberi kebenaran menggunakan gajet dan aplikasi milik sendiri serta diberi kebenaran untuk menggunakan rangkaian organisasi. Kebenaran yang diberi oleh pihak organisasi harus diberi perhatian terhadap implikasi yang bakal dihadapi oleh organisasi. Penceroboh meletakkan target yang tinggi terhadap rangkaian organisasi untuk mendapatkan maklumat penting yang dapat memanfaatkan mereka. Tujuan kajian dilaksana adalah untuk mengetahui kesedaran keselamatan penggunaan gajet peribadi dalam kalangan staf akademik Politeknik Malaysia. Kesedaran diuji dengan merujuk kepada tiga faktor yang dikenal pasti melalui sorotan susastera yang terdiri daripada faktor pengetahuan, faktor sikap dan faktor tingkah laku. Kaedah tinjauan dan persampelan rawak mudah diguna untuk mendapatkan maklum balas daripada responden. Borang soal selidik secara atas talian diguna untuk mendapatkan maklum balas daripada responden. Statistik deskriptif dan statistik inferensi diguna untuk menganalisis data yang diperolehi. Data dianalisis dengan menggunakan *International Business Machine Statistical Package for Social Science* (IBM SPSS) *Statistics 21*. Dapatan kajian bagi persoalan kajian pertama menunjukkan min purata faktor pengetahuan (4.08), faktor sikap (3.89) dan faktor tingkah laku (3.83) yang menunjukkan responden mempunyai tahap kesedaran keselamatan penggunaan gajet peribadi yang tinggi. Hasil dapatan melalui analisis regresi pelbagai menunjukkan faktor sikap (0.517) yang merupakan faktor yang paling dominan yang mempengaruhi tahap kesedaran keselamatan penggunaan gajet peribadi. Ini diikuti oleh faktor tingkahlaku (0.291) dan faktor pengetahuan (0.285). Hasil kajian yang diperolehi menyumbang dalam perkongsian amalan terbaik asas yang perlu diamal oleh setiap pengguna bagi menjamin keselamatan penggunaan gajet peribadi di tempat kerja.

Kata kunci: BYOD, rangkaian organisasi, faktor manusia

1. Pengenalan

Teknologi maklumat semakin berkembang dari hari ke hari. Pelbagai jenis peranti diguna untuk berkomunikasi melalui internet. Salah sebuah peranti yang pesat berkembang adalah gajet peribadi. Gajet peribadi atau lebih dikenali sebagai *Bring Your Own Device* (BYOD) merupakan situasi apabila pekerja di sesebuah organisasi diberi kebenaran menggunakan gajet dan aplikasi milik sendiri. Gajet peribadi (contohnya: komputer riba, peranti storan mudah alih, telefon pintar dan tablet) amat diminati di kalangan staf di sesebuah organisasi. Segala maklumat boleh dipadat di dalam gajet peribadi masing-masing (Lazau & George 2011). Kebanyakan pengguna gajet peribadi menggunakan gajet peribadi untuk mengurus maklumat peribadi dan organisasi. Golongan profesional seperti staf akademik, staf pengurusan dan sebagainya melihat gajet peribadi sebagai satu keperluan di dalam kehidupan kerana gajet peribadi merupakan peranti terminal yang mempunyai pelbagai fungsi yang memudahkan kerja mereka. Menurut Parakovic et al. (2012), cabaran yang paling utama adalah untuk melindungi maklumat yang di simpan di dalam gajet peribadi pengguna disebabkan nilai maklumat tersebut sangat penting bagi seseorang individu mahupun bagi sesebuah organisasi. Ini adalah kerana penjenayah siber cuba menggodam gajet peribadi pengguna untuk memperoleh maklumat penting yang terdapat di dalam gajet mereka. Penggunaan telefon pintar yang semakin meningkat dengan ramalan jualan yang menunjukkan bilangan telefon pintar kini melebihi daripada pembelian telefon asas (Urban, Hoofnsgle dan Li 2012). Justeru itu, reka bentuk telefon pintar kecil dan ringan menyebabkan semua kategori umur suka menggunakannya terutama jika terdapat kemudahan internet (Uffen et al. 2013).

Selain itu, kebanyakan telefon pintar dan tablet mempunyai kemudahan *built-in WiFi* yang membolehkan pengguna untuk membuat sambungan internet sama ada melalui internet *hotspot* peribadi mahupun yang terbuka (*open Wireless Fidility* (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. 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 dilaku oleh pengguna yang menggunakan gajet peribadi mereka. Ada juga pengguna yang menyimpan maklumat sulit mereka dan organisasi di dalam gajet peribadi tanpa melakukan penyulitan data (Lazau & George 2011; Mylonas et al. 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.

Secara tradisinya, kurang perhatian diberi kepada kesedaran keselamatan pengguna gajet peribadi berbanding dengan kawalan keselamatan teknikal seperti firewall. Rangkaian tidak boleh dikawal oleh sesuatu organisasi disebabkan ianya merupakan sebuah dunia tanpa sempadan di mana serangan virus ke atas rangkaian mudah berlaku dan amat sukar untuk dihapus. Oleh yang demikian, amatlah tipis peluang Pegawai Teknologi Maklumat untuk membina sebuah sistem rangkaian keselamatan yang mutlak (Zhao et al. 2012). 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 di kalangan pengguna dalam cara mengendalikan gajet dengan selamat seringkali membuka pintu kepada penjenayah siber untuk menggodam gajet.

Berikutan pelaksanaan dasar dan prinsip e-pembelajaran yang dikuatkuasa mulai sesi Disember 2012 (Surat Edaran Pelaksanaan Dasar dan Prinsip ePembelajaran Politeknik, Jabatan Pengajian Politeknik, Kementerian Pengajian Tinggi), pihak pengurusan Politeknik Malaysia membenarkan staf akademik untuk membawa gajet peribadi masing-

masing untuk membantu pembelajaran teradun atau lebih dikenali sebagai *Blended Learning*. Walaupun keselamatan belum menjadi budaya kampus, namun pihak pengurusan Politeknik harus memastikan risiko yang perlu ditanggung disebabkan memberi kebenaran membawa gajet peribadi ke Politeknik dan langkah yang perlu diambil supaya ianya tidak memberi impak kepada keselamatan maklumat dan rangkaian Politeknik.

Sering kali gajet peribadi menjadi agen kepada aktiviti spam dan virus ke dalam rangkaian Politeknik. Menurut Sari dan Candiwan (2014), penyebaran virus dalam rangkaian organisasi boleh berlaku sekiranya gajet pekerja telah dijangkiti virus apabila pekerja tersebut menggunakan WiFi percuma di luar organisasi. Situasi ini berlaku kerana tiada pendidikan atau latihan yang rasmi diberi kepada staf mengenai kesedaran keselamatan penggunaan gajet peribadi di tempat kerja. 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. Ini adalah kerana, gajet peribadi pengguna boleh diintip di mana penjenayah siber mampu memintas komunikasi antara gajet peribadi dan *open WiFi*. Ianya telah menjadi sasaran penjenayah siber untuk mencuri data peribadi pengguna mahupun organisasi tanpa disedari oleh pengguna.

Bertitik tolak daripada itu, menurut Allam et al. (2014), kesedaran keselamatan penggunaan gajet peribadi mempunyai kaitan dengan faktor manusia. Gajet peribadi dikendali oleh orang dan ini bermakna bahawa keselamatan maklumat juga merupakan isu faktor manusia. Faktor manusia mempengaruhi cara individu berinteraksi dengan teknologi di mana interaksi sering memudaratkan keselamatan (Parsons et al. 2010). Pengguna gajet peribadi kurang mengambil tahu mengenai isu-isu keselamatan penggunaan gajet peribadi di mana situasi ini menimbulkan ancaman terbesar kepada keselamatan maklumat (Mylonas et al. 2012). Kajian yang dilaku oleh Khan et al. (2012) pula membuktikan bahawa segelintir sahaja pengguna telefon pintar yang sebenarnya mengamalkan garis panduan keselamatan maklumat penggunaan telefon pintar.

Kebanyakan pengguna tidak faham bahawa gajet peribadi terutamaya telefon pintar dan tablet menjadi sasaran kebanyakan penjenayah siber (Mylonas et al. 2012) kerana terdapat banyak maklumat sulit di dalamnya. Kebanyakan pengguna gajet peribadi menyimpan maklumat sulit di dalam gajet peribadi mereka tanpa melakukan penyulitan data. Menurut Lazau dan George (2011) dan Mylonas et al. (2012), penyimpanan maklumat sulit pengguna dan organisasi di dalam gajet peribadi pengguna boleh memberi implikasi kepada pengguna mahupun organisasi. Oleh yang demikian, kajian dilakukan untuk mengenal pasti tahap kesedaran keselamatan penggunaan gajet peribadi di tempat kerja dan mengenal pasti faktor paling dominan yang mempengaruhi kesedaran keselamatan penggunaan gajet peribadi di tempat kerja dalam kalangan staf akademik Politeknik Malaysia.

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 mengenai keselamatan, lebih menyedari kewujudan perisian hasad (*malware*) di dalam telefon pintar mereka. Selain daripada itu, kajian yang dilaksana 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 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 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 diimplemen, 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 tingkahlaku berada pada tahap yang memuaskan sahaja.

Kajian yang dilaku oleh Mylonas et al. (2012); Ophoff dan Robinson (2014) dan Verkasalo et al. (2010); mendapati majoriti responden pengkaji terdiri daripada golongan yang mahir dalam mengendalikan keselamatan penggunaan gajet peribadi. Dapatan kajian tidak dapat digeneralisasikan kepada orang yang kurang mahir dalam mengendalikan keselamatan penggunaan gajet peribadi. Kajian lanjut perlu dilaku untuk mengetahui kesedaran keselamatan penggunaan gajet peribadi di kalangan latar belakang pendidikan responden yang berbeza contohnya berbeza jabatan dalam sesebuah organisasi.

Manakala kajian yang dilaksana oleh Ophoff dan Robinson (2014) dan Verkasalo (2010) mencadangkan kajian kesedaran keselamatan penggunaan gajet peribadi perlu dilaku ke atas negara lain disebab perbezaan kebudayaan juga boleh memberi implikasi kepada dapatan kajian. Perbezaan budaya dipengaruhi oleh faktor pengetahuan, sikap dan tingkah laku pengguna gajet peribadi terhadap kesedaran keselamatan. Oleh yang demikian, kajian dilakukan terhadap kesedaran keselamatan penggunaan gajet peribadi dengan melihatkan faktor pengetahuan, sikap dan tingkah laku dengan memberi tumpuan kepada lima dimensi (peggunaan kata laluan - *screen lock*, menyimpan maklumat sulit, antivirus, memuat turun / memasang aplikasi dan pautan yang diterima melalui emel / SMS / *WhatsApps*) supaya item yang dibina dapat menjawab persoalan kajian.

2. Metodologi

2.1. Reka bentuk kajian

Kaedah tinjauan dipilih berdasarkan kesesuaian dengan bentuk kajian yang dibuat. Menurut Noraini (2013), kajian tinjauan dapat mengumpul jawapan terus daripada responden kajian. Menurut Othman (2015), dalam kajian tinjauan, sekumpulan responden daripada populasi dipilih sebagai responden kajian, memungut maklumat daripada responden dan seterusnya menganalisis maklumat tersebut untuk menjawab persoalan kajian.

Kaedah kuantitatif digunakan untuk menganalisis data. Bagi menganalisis data kajian, statistik deskriptif (purata) dan statistik inferensi (analisis regresi) digunakan. Menurut Othman (2015), statistik deskriptif diguna untuk memperihalkan set-set data mentah yang diambil dari sampel bagi memahami ciri-ciri sampel yang terpilih dari satu-satu populasi. Manakala statistik inferensi diguna untuk menganalisis data yang diperolehi dari sampel dengan tujuan membuat inferensi atau generalisasi kepada populasi yang diwakili oleh sampel tersebut. Generalisasi boleh dilaku disebabkan sampel yang dipilih adalah secara rawak.

2.2. Populasi dan sampel kajian

Populasi bagi kajian ini ialah staf akademik Jabatan Pengajian Politeknik Malaysia. Sebanyak 441 staf akademik di Politeknik dipilih secara rawak daripada 7800 orang staf akademik Politeknik Malaysia (sumber daripada Unit Pembangunan Kerjaya, Bahagian Kecemerlangan Profesional, Jabatan Pengajian Politeknik). Menurut Krejcie dan Morgan (1970), sampel sebanyak 367 orang mencukupi untuk mewikili bilangan populasi sebanyak 7800 orang.

2.3. Instrumen kajian

Soal selidik secara atas talian diguna untuk mendapat maklumat bagi meninjau maklum balas responden untuk mengenal pasti tahap dan faktor yang mempengaruhi kesedaran keselamatan penggunaan gajet di tempat kerja dalam kalangan staf akademik Politeknik Malaysia. Emel rasmi kerajaan webmail.1govuc.gov.my digunakan untuk menghantar emel yang diserta alamat pautan soal selidik kepada semua staf akademik Politeknik Malaysia. Staf akademik dikelompokkan mengikut Politeknik masing-masing. Tempoh penerimaan respon adalah selama 2 bulan. Skala Likert diguna untuk mengukur respons yang diberi bagi setiap item dalam borang soal selidik. Responden dikehendaki klik pada jawapan mereka pada item yang terdapat dalam borang soal selidik atas talian berdasarkan skala iaitu 1 : sangat tidak setuju kepada 5 : sangat setuju.

Borang soal selidik terbahagi kepada dua bahagian iaitu:

a) Bahagian A: Profil responden
b) Bahagian B terdiri daripada 3 seksyen iaitu:
- B1 (Bagi mengukur Faktor Pengetahuan – 8 item)
- B2 (Bagi mengukur Faktor Sikap – 10)
- B3 (Bagi mengukur Faktor Tingkah laku – 14 item)

Penentuan kesahan bagi soal selidik adalah untuk menentukan sejauh mana alat kajian dapat mengukur item-item bagi mewakili faktor pengetahuan, sikap dan tingkah laku. Penggubalan item-item instrumen kajian dilaku dengan merujuk kepada beberapa orang pakar yang mempunyai kepakaran dan pengalaman luas dalam bidang keselamatan maklumat penggunaan gajet peribadi. Bagi tujuan ini, empat orang pakar telah di kenal pasti untuk membuat pengesahan terhadap item borang soal selidik yang terdiri daripada dua pensyarah Universiti Kebangsaan Malaysia dan dua orang pakar daripada Cyber Security Malaysia.

Kebolehpercayaan merujuk kepada konsep yang diguna untuk menilai tahap konsistensi sesuatu item yang mengukur objektif tertentu. Kajian rintis dijalan bagi memastikan kesahihan dan kebolehpercayaan item-item dalam borang soal selidik. Oleh sebab kaji selidik dilaksana secara atas talian menggunakan *Google Form*, maka kajian rintis juga dijalan secara atas talian bagi memastikan tiada masalah teknikal dengan platfom yang diguna oleh pengkaji untuk melaksanakan kajian sebenar. Nilai cronbach alfa yang berada di antara 0.9-1.0 bermakna nilai kebolehpercayaan tinggi, julat di antara 0.6-0.7 masih boleh diterima manakala jika melebihi 0.8 adalah sangat baik. Kesemua nilai *Alpha Cronbach* yang diperolehi melebihi 0.8 (Bahagian B-I: Faktor Pengetahuan = 0.875, Bahagian B-II: Faktor Sikap = 0.876, Bahagian B-III: Faktor Tingkah laku = 0.901 dan Pemboleh ubah bersandar = 0.828). Maka semua item diterima.

3. Dapatan Kajian

Pengukuran tahap kesedaran keselamatan penggunaan gajet peribadi amat penting kerana kebanyakan serangan dilaku ke atas gajet peribadi. Bagi mengukur tahap kesedaran keselamatan penggunaan gajet peribadi dalam kalangan staf akademik Politeknik Malaysia, item-item soal selidik secara tidak langsung membolehkan responden untuk berfikir sambil menjawab mengenai faktor pengetahuan, sikap dan tingkah laku mereka terhadap keselamatan penggunaan gajet peribadi. Analisis skor min dalam kajian dibuat untuk mengetahui persepsi responden mengenai tahap kesedaran terhadap amalan keselamatan penggunaan gajet peribadi di tempat kerja. Jadual 1 diguna untuk menjawab persoalan kajian pertama.

Jadual 1. Ukuran tahap persetujuan min

Skor min	Intepretasi	Tahap kecenderungan
1.0 – 2.33	Tidak setuju	Rendah
2.34 – 3.66	Agak setuju	Sederhana
3.67 – 5.00	Setuju	Tinggi

Sumber : Mohd Najib 2003

3.1. Analisis Bahagian A : Maklumat latar belakang staf akademik

Seramai 441 staf akademik dari Politeknik Malaysia (24 buah Politeknik) terlibat dalam menjawab soal selidik. Majoriti responden adalah dalam kategori umur di antara 23 hingga 38 tahun iaitu seramai 300 (68%) responden diikuti dengan kategori umur di antara 39 hingga 49 tahun seramai 118 (26.8%) dan kategori umur 50 hingga 60 tahun seramai 23 (5.2%) responden.

3.2. Analisis persoalan kajian pertama

Persoalan kajian pertama: Adakah tahap kesedaran tinggi dalam kalangan staf akademik Politeknik terhadap keselamatan penggunaan gajet peribadi di tempat kerja?

Jadual 2 menunjukkan pada keseluruhannya majoriti responden memberikan respons positif. Lima daripada lapan item mempunyai skor min 4.00 ke atas. Skor min yang tertinggi iaitu 4.52 merupakan item P1. Ini menunjukkan responden tahu bahawa penetapan kata laluan (*screen lock*) untuk gajet peribadi adalah sangat penting. Manakala nilai skor min yang paling rendah iaitu 3.74 ialah item P2 ("Saya tahu cara selamat untuk menyimpan maklumat sulit (cth: memo, surat dan lain-lain) di dalam gajet peribadi saya"), item P3 ("Saya tahu bahawa maklumat peribadi saya dikongsi dengan pihak ketiga apabila saya memuat turun / memasang sebarang aplikasi percuma") dan item P8 ("Saya tahu pemilik aplikasi yang dimuat turun berkemungkinan dapat mengakses maklumat yang terdapat di dalam gajet peribadi tanpa pengetahuan saya"). Secara keseluruhan, tahap pengetahuan terhadap keselamatan penggunaan gajet peribadi di tempat kerja adalah tinggi dengan min purata keseluruhan ialah 4.08.

Jadual 2. Nilai min dan sisihan piawai bagi Faktor Pengetahuan

	Min
P1	4.52
P2	3.74
P3	3.74
P4	4.48
P5	4.20
P6	4.01
P7	4.19
P8	3.74
Purata	4.08

Jadual 3 menunjukkan responden memberi persetujuan yang tinggi terhadap faktor sikap. Skor min yang tertinggi ialah item S5 iaitu 4.30. Item ini menunjukkan responden mengambil berat mengenai bahaya klik pada pautan daripada sumber yang tidak boleh dipercayai. Manakala item S9 iaitu "Saya terganggu (*annoying*) apabila amaran keselamatan sentiasa keluar semasa saya memuat turun sebarang aplikasi percuma." merupakan nilai skor min yang terendah iaitu 3.35. Ini menunjukkan ada segelintir responden yang berasa terganggu apabila amaran keselamatan sentiasa keluar semasa mereka memuat turun sebarang aplikasi. Min purata keseluruhan faktor sikap adalah 3.89, iaitu pada tahap tinggi.

Jadual 3. Nilai min dan sisihan piawai bagai Faktor Sikap

	Min
S1	4.10
S2	4.02
S3	3.79
S4	3.91
S5	4.30
S6	3.56
S7	4.11
S8	3.49
S9	3.35
S10	4.28
Purata	3.89

Jadual 4 menunjukkan responden memberi persetujuan yang tinggi terhadap faktor tingkah laku. Skor min yang paling tinggi adalah item T5 iaitu 4.43. Ini menunjukkan responden akan pastikan maklumat di dalam gajet peribadi dipadam sebelum menjual balik gajet. Skor min yang paling rendah adalah item T11 iaitu 3.48 di mana item ini menunjukkan segelintir responden tidak sentiasa mengemaskini antivirus yang terdapat di dalam gajet peribadi. Min purata keseluruhan faktor tingkah laku adalah 3.83, iaitu pada tahap tinggi.

Jadual 4. Nilai min dan sisihan piawai bagi Faktor Tingkah Laku

	Min
T1	3.99
T2	3.53
T3	4.20
T4	3.54
T5	4.43
T6	4.07
T7	3.92
T8	4.07
T9	4.08
T10	3.55
T11	3.48
T12	3.56
T13	3.55
T14	3.72
Purata	3.83

3.3 Analisis persoalan kajian kedua

Persoalan kajian kedua: Apakah faktor paling dominan yang mempengaruhi kesedaran keselamatan penggunaan gajet peribadi di tempat kerja dalam kalangan staf akademik Politeknik Malaysia?

Keputusan analisis regresi menunjukkan bahawa tiga pembolehubah peramal iaitu Faktor Pengetahuan (FP), Faktor Sikap (FP) dan Faktor Tingkah laku (FP) merupakan peramal kepada tahap kesedaran keselamatan penggunaan gajet peribadi. Tahap kesedaran keselamatan diuji dari segi (i) penggunaan kata laluan – *screen lock*, (ii) menyimpan maklumat sulit, (iii) antivirus, (iv) memuat turun aplikasi dan (v) klik pautan yang diterima melalui e-mel atau sistem pesanan ringkas (sms). Merujuk Jadual 5, tiga pembolehubah bebas iaitu FP, FS dan FT, kesemuanya menunjukkan 69.3% menyumbang terhadap tahap kesedaran keselamatan penggunaan gajet peribadi di tempat kerja. Manakala sebanyak 30.7% dipengaruhi oleh faktor yang tidak dipertimbang dalam kajian.

Jadual 5. Analisis keputusan regresi pengaruh FP, FS dan FT terhadap tahap kesedaran keselamatan pengunaan gajet peribadi

Ringkasan Model				
Model	R	R kuasa dua	R kuasa dua diselaraskan	Anggaran ralat piawai
1	0.833[a]	0.693	0.691	0.42825

Peramal: (Pemalar), Faktor Pengetahuan, Faktor Sikap, Faktor Tingkah laku

Jadual 6 menunjukkan model regresi linear bagi model FP, FS dan FT. Model Linear diguna untuk mencari perkaitan antara pembolehubah bersandar dan pembolehubah bebas. Berdasarkan Jadual 3, koefisien antara FP, FS dan FT mempengaruhi tahap kesedaran keselamatan penggunaan gajet peribadi di tempat kerja. Hasil dapatan menunjukkan faktor pengetahuan (0.285), faktor sikap (0.517) dan faktor tingkah laku (0.291). Faktor pengetahuan (t = 6.446, p=0.000), faktor sikap (t = 8.299, p=0.000), dan faktor tingkah laku (t = 5.766, p=0.000) menunjukkan terdapat hubungan yang siginifikan dengan tahap kesedaran keselamatan penggunaan gajet peribadi di tempat kerja.

Jadual 6. Analisis keputusan koefisien pengaruh faktor manusia terhadap kesedaran keselamatan penggunaan gajet peribadi

Model		Pekali tak terpiawai B	Ralat piawaian	Pekali seragam Beta	Nilai t	Signifikan
1	(Pemalar)	-0.390	0.139		-2.797	0.005
	Pengetahuan	0.285	0.044	0.253	6.446	0.000
	Sikap	.517	.062	.403	8.299	0.000
	Tingkahlaku	.291	.050	.259	5.766	0.000

Pemboleh ubah bersandar: Tahap kesedaran keselamatan penggunaan gajet peribadi

4. Perbincangan

Berdasarkan dapatan kajian, dapat dirumus tahap kesedaran keselamatan penggunaan gajet peribadi di tempat kerja dalam kalangan staf akademik di Politeknik Malaysia adalah pada tahap tinggi. Purata min bagi faktor pengetahuan (skor min = 4.08), faktor sikap (skor min = 3.89) dan faktor tingkahlaku (skor min = 3.83) berada pada tahap tinggi. Dapatan kajian turut menyokong kajian-kajian yang dijalankan oleh Mylonas et al. (2012), Ophoff dan Robinson (2014) serta Sari dan Candiwan (2014) kecuali dapatan Sari dan Candiwan (2014) bagi tahap kesedaran terhadap tingkah laku berada pada tahap yang memuaskan sahaja.

Walaupun secara keseluruhan skor min menunjukkan responden mempunyai tahap kesedaran keselamatan penggunaan gajet peribadi yang tinggi, namun terdapat juga beberapa item soalan yang mempunyai dapatan kajian yang bercanggah dengan dapatan kajian-kajian yang lepas. Di antaranya adalah mengenai kesedaran mengenai penetapan kata laluan (*screen lock*). Dapatan kajian ini bagi item berbeza dengan kajian yang dilaku oleh Lazau dan George (2011) yang mendapati sebanyak 53% daripada responden tidak menggunakan kata laluan (*screen lock*) untuk melindungi telefon pintar manakala responden bagi kajian ini mendapati majoriti responden menetapkan kata laluan (*screen lock*) supaya orang lain tidak dapat mengakses gajet peribadi. Ini adalah kerana responden bagi kajian terdiri daripada staf akademik Politeknik Malaysia. Golongan ini lebih peka dan prihatin terhadap kesedaran keselamatan penggunaan gajet peribadi di tempat kerja disebabkan tahap pendidikan di mana majoriti responden memiliki Ijazah Sarjana Muda dan tahap pendidikan yang lebih tinggi.

Kesemua faktor-faktor yang dikaji iaitu faktor pengetahuan, faktor sikap dan faktor tingkah laku mempengaruhi satu sama lain dalam menentukan kesedaran keselamatan penggunaan gajet peribadi di tempat kerja dalam kalangan staf akademik Politeknik Malaysia. Faktor paling dominan adalah faktor sikap (0.517) diikuti dengan faktor tingkahlaku (0.291) dan faktor pengetahuan (0.285). Ini menunjukkan faktor sikap memainkan peranan penting dalam menentukan tahap kesedaran keselamatan penggunaan gajet peribadi.

5. Kesimpulan

Melalui kajian ini, amalan terbaik yang paling asas dapat dijadikan penanda aras oleh organisasi yang membenarkan staf membawa gajet peribadi untuk diguna di tempat kerja:

a. Menggunakan *screen lock* sama ada menggunakan pin, password, pattern, voice unlock dan sebagainya. Kemudahan ini disedia di dalam setiap gajet peribadi (telefon pintar ataupun tablet) pada bahagian *Settings* > *Security*. Penggunaan screen lock amat penting supaya orang lain tidak dapat mengakses maklumat peribadi di dalam gajet peribadi pengguna.
   Cadangan: Perlu menukar *screen lock* (*pin, password, pattern*) secara berkala.
b. Memuat turun aplikasi, permainan dan muzik hanya dari sumber yang dipercayai. Sebagai contoh, hanya memuat turun permainan yang diketahui daripada vendor bereputasi dan disah atau dari kedai komersial yang disokong oleh pengeluar peranti atau pembekal.
   Cadangan: Sebelum memuat turun aplikasi dan permainan, perlu mengenal pasti apa yang diakses oleh pihak ketiga sebelum klik download.
c. Mengimbas (*scan*) gajet peribadi menggunakan perisian *anti-malware* pada peranti dan mengambil tindakan yang sewajarnya apabila pengguna mengenal pasti aplikasi yang mencurigakan.
   Cadangan:
   i. Mengimbas gajet peribadi secara berkala untuk mengesan malware.
   ii. Mengemaskini (*update*) antivirus yang terdapat di dalam gajet peribadi.
   iii. Guna *firewall* yang terdapat pada gajet peribadi untuk menapis trafik masuk dan trafik keluar untuk menyekat perisian berniat jahat.

Peranti mudah alih seperti telefon pintar dan tablet memudahkan pengguna untuk mengakses data organisasi mahupun data peribadi di mana sahaja. Oleh kerana penggunaan telefon pintar dan tablet semakin lama semakin meningkat dengan ledakan teknologi, risiko juga harus ditanggung oleh pengguna jika pengguna tiada kesedaran terhadap keselamatan penggunaan gajet peribadi. Gajet peribadi mempunyai ciri-ciri untuk disambung ke pelbagai rangkaian tidak kira di mana pengguna berada asalkan tempat yang mereka kunjungi mempunyai akses internet. Situasi ini menjadikan pengguna terdedah kepada kerugian kawalan fizikal dan pelanggaran keselamatan rangkaian. Menggunakan gajet peribadi boleh meningkatkan risiko kehilangan data (apabila peranti fizikal hilang), pendedahan data (apabila data sensitif terdedah kepada orang ramai atau pihak ketiga tanpa kebenaran) dan peningkatan pendedahan kepada rangkaian berasaskan serangan

dari mana-mana gajet peribadi yang disambung secara langsung dan melalui rangkaian melalui internet.

Pengguna gajet peribadi yang memproses maklumat rahsia rasmi diluar pejabat hendaklah memastikan supaya ianya sentiasa dilindungi daripada kehilangan dan kerosakan. Perkara ini amat penting supaya maklumat yang terkandung di dalam gajet peribadi tidak dikompromi. Pengguna gajet peribadi perlu memastikan pelaksanaan langkah kawalan keselamatan bagi perlindungan fizikal, kawalan akses dan perlindungan daripada serangan *malware* dititik berat. Setelah *malware* menjangkiti gajet peribadi pengguna untuk mencuri atau merosakkan data pengguna, ia mungkin merebak ke peranti lain di rangkaian organisasi. Gajet peribadi adalah kaedah mudah untuk penyerang menyebarkan malware dengan merebak di semua peranti yang bersambung dan boleh memasang *malware* dalam mana-mana *firewall* di dalam rangkaian organisasi. Kehadiran *malware* tidak dapat dikesan sehingga kerosakan besar dikenalpasti.

Walaupun kajian ini mendapati kesedaran keselamatan penggunaan gajet peribadi dalam kalangan staf akademik Politeknik Malaysia adalah tinggi, namun kajian lanjut perlu dilakukan bagi memastikan dapatan kajian lebih kukuh. Pengkaji akan datang boleh menggunakan instrumen kajian yang lain seperti temubual dan melakukan pemerhatian ke atas aktiviti yang dilaku oleh semua kakitangan kerajaan menggunakan gajet peribadi masing-masing. Selain itu, sampel perlu diluaskan dengan melibatkan semua staf sokongan dan pelajar di Politeknik Malaysia untuk memantapkan hasil kajian yang dilaku. Penambahan saiz sampel dan skop kajian yang diperluas supaya hasil dapatan kajian lebih bermakna dan lebih mudah diterima oleh pelbagai pihak sebagai rujukan. Penggunaan gajet peribadi di tempat kerja mendatangkan manafaat kepada pengguna dan organisasi namun ianya perlu diurus secara terancang dan sistematik supaya maklumat tidak dikompromi. Kesedaran keselamatan penggunaan gajet peribadi perlu dipupuk oleh setiap pengguna gajet peribadi. Kelalaian seorang pengguna di dalam organisasi boleh menyebabkan kesemua pengguna rangkaian organisasi mendapat kesan buruk. Oleh yang demikian, organisasi boleh menyediakan latihan kesedaran keselamatan penggunaan gajet peribadi dari semasa ke semasa supaya pengguna faham tanggungjawab terhadap rangkaian organisasi apabila mengguna pakai rangkaian. Kesedaran perlu supaya pengguna tahu limitasi apabila menggunakan rangkaian di tempat kerja.

Rujukan

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

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

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

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. 2010. Information Security Policy Compliance: An empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly 34(3): 523-548.

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.

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

Khan, S., Nauman, M., Othman, A. T. & Musa, S. 2012. How Secure is Your Smartphone: An Analysis of Smartphone Mechanisms. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), International Conference 76-81.

Krejcie, R.V. & Morgan, D.W. 1970. Determining Sample Size for Research Activities. Education and Psychological Measurement 30: 607-610.

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

Lazau, A. & George, W. 2011. Perceived Risk and Sensitive Data on Mobile Devices. Cyberforensics 183-196.

Markelj, B., & Bernik, I. 2012. Mobile Devices and Corporate Data Security. International Journal of Education and Information Technologies 6(1): 97-104.

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

Noraini Idris. 2013. Penyelidikan dalan Pendidikan. Kuala Lumpur: McGraw-Hill (Malaysia) Sdn. Bhd.

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

Othman Talib. 2015. SPSS - Analisis Data Kuantitatif untuk Penyelidik Muda. Bangi: MPWS Rich Publication Sdn Bhd.

Perakovic, D., Remenar, V., & Husnjak, S. 2012. Reseach of Security Threats in the Use of Modern Terminal Devices. Annals & Proceedings of DAAAM International 23(1):545-548.

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. 2010. Human Factors and Information Security: Individual, Culture and Security Environment. Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation. 1-45.

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

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

Urban, J,F., Hoofnagle, C.J. & Li. 2012. Mobile Phones and Privacy. UC Berkeley, Public Law and Legal Theory Research Paper Series.

Verkasalo, H., Nicolas, C.L., Castillo, F.J.M. & Bouwman, H. 2010. Analysis of Users and Non-Users of Smartphone Applications. Telematics and Informatics 27:242–255.

Zhao, J., Zhou, Y., & Shuo, L. (2012). A Situation Awareness Model of System Saurvibality Based on Variable Fuzzy Set. TELKOMNIKA 10 (8): 2239-2246.