KESEDARAN AHLI FARMASI KOMUNITI DI NEGERI KELANTAN TERHADAP KESELAMATAN SIBER

MOHAMMAD IZANI BIN AB RASHID

UNIVERSITI KEBANGSAAN MALAYSIA

KESEDARAN AHLI FARMASI KOMUNITI DI NEGERI KELANTAN TERHADAP KESELAMATAN SIBER

MOHAMMAD IZANI BIN AB RASHID

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

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2023

PENGAKUAN

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

07 September 2023

MOHAMMAD IZANI BIN AB RASHID
P106788

PENGHARGAAN

Alhamdulillah, dengan izin Allah S.W.T, saya telah berjaya menyiapkan kajian ini bagi memenuhi keperluan pengajian saya di peringkat sarjana.

Jutaan terima kasih diucapkan kepada Ts. Dr. Khairul Azmi bin Abu Bakar, penyelia saya bagi projek kajian ini yang sentiasa sabar dalam memberi bimbingan dan tunjuk ajar sepanjang perjalanan menyiapkan kajian ini. Ribuan terima kasih juga diucapkan kepada koordinator program, para pensyarah, kakitangan dan rakan pelajar di fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia yang telah memberi panduan di dalam pelbagai bentuk sehingga kajian ini berjaya disiapkan.

Ucapan khas terima kasih kepada Kementerian Kesihatan Malaysia atas kesudian menaja pengajian saya menerusi Hadiah Latihan Persekutuan. Segala ilmu yang diperolehi akan saya gunakan untuk memberi sumbangan dan khidmat bakti terbaik kepada rakyat dan negara.

Akhirnya, terima kasih juga diucapkan kepada ibu, isteri dan keluarga atas dorongan dan motivasi tanpa jemu seterusnya memastikan semangat saya tidak padam sepanjang menyiapkan kajian ini. Tidak lupa juga kepada rakan-rakan pengajian yang sudi memberi inspirasi, bantuan dan nasihat.

Tanpa tunjuk ajar, dorongan dan sokongan pihak-pihak yang dinyatakan di atas, adalah mustahil untuk kajian ini dapat disiapkan. Semoga kajian ini dapat memberi manfaat dan sumbangan kepada negara serta menjadi rujukan kepada pengkaji seterusnya pada masa akan datang.

ABSTRAK

Pindaan Akta Racun 1952 pada sidang parlimen 2022 telah membolehkan rekod ubatan dan pesakit disimpan di dalam bentuk digital secara sepenuhnya di farmasi komuniti. Dengan pergantungan yang semakin tinggi terhadap teknologi digital dalam menyediakan khidmat kesihatan kepada pesakit, ahli farmasi komuniti terdedah kepada risiko ancaman keselamatan siber yang boleh menjejaskan keselamatan data pesakit dan integriti perkhidmatan farmaseutikal yang diberi. Kajian ini mengkaji tahap kesedaran keselamatan siber dalam kalangan ahli farmasi komuniti di negeri Kelantan kerana adalah penting untuk memahami risiko insiden keselamatan siber yang berkaitan dengan faktor manusia, yang biasa berlaku dalam pencerobohan data penjagaan kesihatan. Kajian ini menggunakan kaedah kuantitatif dengan melakukan tinjauan secara atas talian berpandukan model "Human Aspects of Information Security Questionnaire" (HAIS-Q) sebagai asas, yang menilai tahap kesedaran keselamatan siber berdasarkan pengetahuan, sikap dan tingkah laku melibatkan seramai 59 orang responden. Hasil kajian mendapati bahawa tahap kesedaran ahli farmasi komuniti di negeri Kelantan berada di tahap yang sangat baik dari sudut pengurusan maklumat dan pelaporan insiden keselamatan siber, tahap baik bagi pengurusan kata laluan dan penggunaan e-mel manakala tahap yang sederhana bagi penggunaan Internet. Adalah diyakini hasil kajian ini nanti akan dapat menjadi rujukan kepada para penyelidik di dalam kajian seterusnya serta membantu pihak berwajib dan pembuat polisi dalam merangka pelan penambahbaikan di dalam aspek keselamatan siber melibatkan petugas kesihatan di Malaysia.

AWARENESS OF COMMUNITY PHARMACISTS IN KELANTAN STATE TOWARDS CYBER SECURITY

ABSTRACT

Amendments to the Poisons Act 1952 in the 2022 parliamentary session have enabled medical and patient records to be stored in digital form in a fully digital format in community pharmacies. With the increasing reliance on digital technology in providing health services to patients, community pharmacists are exposed to cyber security risks that may affect data security of the patients and the integrity of the pharmaceutical services provided. This study examines the level of cyber security awareness among community pharmacists in the state of Kelantan because it is important to understand the risk of cyber security incidents related to human factors, which are common in healthcare data breaches. This study uses a quantitative method by conducting an online survey based on the "Human Aspects of Information Security Questionnaire" (HAIS-Q) model as a basis, which assesses the level of cyber security awareness based on knowledge, attitude and behavior involving a total of 59 respondents. The results of the study found that the level of awareness of community pharmacists in the state of Kelantan is at a very good level in terms of information management and cyber security incident reporting, a good level for password management and email use while a moderate level for Internet use.. It is believed that the results of this study will later be able to be a point of reference for researchers in future studies as well as helping the authorities and policy makers in drawing up an improvement plan in the aspect of cyber security awareness involving healthcare workers in Malaysia.

KANDUNGAN

Halaman

SENARAI JADUAL

SENARAI ILUSTRASI

SENARAI SINGKATAN

%	Peratus
A	*Attitude*
ATP	*Advance Persistence Threat*
B	*Behavior*
CIA	*Confidentiality, Integrity, Availability*
CSM	Cybersecurity Malaysia
DBIR	*Data Breach Investigations Report*
DDoS	*Distributed Denial-of-Service*
DLP	*Data Loss Prevention*
DoS	*Denial-of-Service*
FRP	*Fully Registered Pharmacist*
HAIS-Q	*Human Aspects of Information Security Questionnaire*
K	*Knowledge*
KAB	*Knowledge, Attitude and Behavior*
KKM	Kementerian Kesihatan Malaysia
MBR	*Master Boot Record*
NIST	*National Institute of Standards and Technology*
PRP	*Provisionally Registered Pharmacist*
RC	*Reverse Coding*
SeBIS	*The Security Behavior Intentions Scale*
SPSS	*Statistical Package for the Social Sciences*

TPB	*Theory of Planned Behaviour*
UISAQ	*Users' Information Security Awareness Questionnaire*
USB	*Universal Serial Bus*
USD	*United States Dollar*
WMI	*Windows Management Infrastructure*
α	*Alpha*

BAB I

PENGENALAN

1.1 PENDAHULUAN

Menurut NIST, keselamatan siber ialah “Pencegahan kerosakan, perlindungan dan pemulihan komputer, sistem komunikasi elektronik, perkhidmatan komunikasi elektronik, komunikasi wayar dan komunikasi elektronik, termasuk maklumat yang terkandung di dalamnya, untuk memastikan ketersediaan, integriti, pengesahan, kerahsiaan, dan tanpa sangkalan.” (NIST 2021). Ia juga boleh ditakrifkan sebagai "organisasi dan pengumpulan sumber, proses dan struktur yang digunakan untuk melindungi ruang siber dan sistem yang dijana oleh ruang siber daripada kejadian yang menyelewengkan ‘de jure’ daripada hak harta ‘de facto’." (Craigen et al. 2014).

Keselamatan siber merupakan elemen penting di dalam sistem keselamatan sesebuah organisasi dan negara, bagi mengelakkan pencerobohan data yang boleh menyebabkan kerugian wang ringgit dan kebocoran maklumat peribadi. Pada tahun 2020, sebanyak 10,790 kes insiden keselamatan siber direkodkan oleh Cyber Security Malaysia (2020), berbanding 10,772 kes pada tahun sebelumnya (Cyber Security Malaysia 2019). Pada tahun 2017 pula, terdapat laporan bahawa 46.2 juta maklumat peribadi pelanggan syarikat telekomunikasi di Malaysia telah dicuri pada tiga tahun sebelumnya (Bernama 2017).

Keselamatan siber bukanlah tanggungjawab pegawai keselamatan maklumat semata-mata, tetapi merupakan tanggungjawab bersama setiap tenaga kerja yang terlibat dengan sistem tersebut. Sebabnya adalah walaupun pelbagai kaedah dapat digunakan oleh penggodam untuk menyerang sistem dan rangkaian komputer, salah satu permukaan serangan yang paling mudah dieksploit dalam sistem komputer adalah kelemahan manusia, yang sering menjadi rantaian paling lemah di dalam sistem

keselamatan siber seterusnya menjadi punca sistem rangkaian komputer sesebuah organisasi diceroboh. Menurut Verison DBIR 2019, e-mel ialah kaedah pilihan untuk 94% kiriman perisian hasad dan kaedah pancingan data digunakan dalam 32% daripada jumlah pencerobohan yang direkodkan (Verison 2019). Satu kajian mendapati bahawa dua punca utama pautan hasad daripada e-mel dipetik oleh mangsa adalah disebabkan oleh perasaan minat dan kurangnya perhatian oleh mangsa (Caputo et al. 2014).

Eksploitasi terhadap kelemahan tersebut lebih berjaya apabila ia diburukkan lagi oleh faktor-faktor lain seperti salah maklumat, kelalaian, dan kekurangan kesedaran keselamatan siber dikalangan warga kerja. Tinjauan oleh SANS mendapati bahawa 51% respondennya menganggap bahawa ancaman utama keselamatan siber ialah kecuaian orang dalam. Hasil tinjauan juga mendapati bahawa kebocoran maklumat sulit secara tidak sengaja adalah 83% lebih tinggi dalam sektor kesihatan berbanding sektor lain, menunjukkan bahawa pelanggaran juga boleh berlaku walaupun tanpa wujudnya penyerang yang berniat jahat (Filkins 2014). Kajian yang dilakukan keatas sebuah agensi kerajaan mendapati bahawa faktor kelemahan manusia memberi risiko tertinggi kepada insiden keselamatan siber di agensi. Semua ini memberi petunjuk bahawa kesedaran siber dan keprihatinan anggota memainkan peranan penting dalam perlindungan siber sesebuah organisasi.

1.1.1 Prinsip Asas Keselamatan Siber

Keselamatan siber terdiri daripada prinsip asas yang utama iaitu kerahsiaan, integriti dan ketersediaan yang turut dikenali sebagai *CIA triad* (Lundgren 2019). Kerahsiaan ialah sekatan ke atas orang tertentu dari pengetahuan kandungan, capaian, penggunaan dan penyimpanan pelbagai jenis data dan aset. Integriti ialah jaminan bahawa sesuatu aset atau data itu adalah masih sama seperti di dalam keadaan asalnya tanpa diusik oleh mana-mana pihak tanpa kebenaran. Manakala ketersediaan ialah sifat aset dan data tersebut yang sentiasa boleh dicapai oleh pengguna tanpa halangan apabila diperlukan. Kesemua prinsip ini menjadi asas yang kemudiannya dikembangkan untuk membentuk prinsip-prinsip lain keselamatan siber oleh pelbagai pihak dan organisasi yang mempunyai penilaian berbeza terhadap keselamatan siber dari sudut pandang mereka. Berikut ialah perbincangan lebih mendalam berkaitan kerahsiaan, integriti dan ketersediaan:

1. Kerahsiaan: Tujuan utama prinsip pertama keselamatan siber iaitu kerahsiaan ialah untuk memastikan bahawa data atau aset yang terlibat adalah sentiasa dipelihara dari sudut capaian dan pendedahan daripada pihak yang tidak dibenarkan. Ia memainkan peranan penting di dalam pemeliharaan aset dan data kritikal seperti rahsia perniagaan, data peribadi, rekod kewangan, hak harta intelek, maklumat pelanggan dan maklumat sulit. Insiden kebocoran maklumat sebegini boleh membawa kepada kesan besar terhadap pihak yang terlibat seperti kerosakan imej, kerugian kewangan, kehilangan kepercayaan dan implikasi perundangan (Whitman et al. 2018).

   Kerahsiaan boleh dicapai melalui pelbagai pendekatan dan biasanya digabung bagi mendapatkan kesan terbaik seperti penyulitan, kawalan capaian, pengelasan data, pengasingan rangkaian dan penggunaan teknologi *Data Loss Prevention* (DLP). Penyulitan ialah proses mengekod data bagi memastikan hanya pihak yang dibenarkan boleh mencapai dan membacanya semula. Ia melibatkan proses transformasi data dari format yang boleh dibaca kepada format yang tidak boleh dibaca menggunakan teknik kriptografi. Ini seterusnya memastikan bahawa walaupun data tersebut berjaya dicapai atau dicuri oleh pihak yang tidak dibenarkan, kandungannya tetap tidak boleh dibaca atau difahami.

   Kawalan capaian dari sudut keselamatan siber ialah penyelesaian keselamatan melalui cara kawalan capaian terhadap data dan aset kepada pihak tertentu. Ia memainkan peranan penting dalam melindungi maklumat sensitif, menghalang capaian yang tidak dibenarkan dan memastikan keselamatan dan integriti keseluruhan infrastruktur digital organisasi. Kawalan capaian boleh dicapai melalui teknik sekatan terpilih akses kepada data dan aset, samada fizikal atau digital, berdasarkan tahap kebenaran yang diberikan kepada pengguna atau individu. Ia bertujuan untuk memastikan bahawa hanya kakitangan yang diberi kuasa boleh mencapai sumber tertentu sambil mengekalkan pengguna yang tidak dibenarkan. Kawalan capaian yang biasa digunakan termasuklah penggunaan kata laluan, pengesahan pelbagai faktor, kad identiti, bilik berkunci dan penggunaan sistem biometrik. Dengan membuat kawalan capaian, pihak

yang tidak diberi keizinan tidak dapat mencapai data atau aset yang dikawal seterusnya memastikan kerahsiaan data atau aset tersebut kekal terpelihara.

Pengelasan data ialah proses mengelaskan data mengikut tahap sensitiviti dan kerahsiaannya. Proses ini dapat membantu organisasi yang mengawal data tersebut di dalam menentukan tahap kawalan yang berpatutan sesuai dengan kelas data tersebut. Perkara ini dapat mengurangkan penggunaan sumber yang diperlukan untuk memelihara kerahsiaan data tersebut. Ini kerana proses kawalan data memerlukan penggunaan sumber yang banyak dari sudut tenaga kerja manusia dan kewangan serta boleh menjejaskan ketersediaan data untuk digunakan oleh pihak yang dibenarkan. Dengan menggunakan proses pengelasan data, data yang kurang sulit adalah lebih mudah dicapai kepada lebih ramai pengguna berbanding data dan aset yang lebih sulit dan sensitif.

Pengasingan rangkaian bermaksud memecahkan rangkaian di dalam organisasi kepada keperluan capaian dan tugas. Biasanya proses ini yang menghasilkan lebih banyak rangkaian yang lebih kecil di dalam organisasi seterusnya menghalang capaian diantara rangkaian kecuali kepada komunikasi dan data yang dibenarkan diantara rangkaian. Perkara ini dapat memelihara organisasi tersebut dengan memastikan halangan terhadap capaian yang tidak diingini atau insiden keselamatan siber yang berlaku kepada satu rangkaian tidak berjangkit ke rangkaian yang lain seterusnya memelihara kerahsiaan sesuatu data dan aset.

Penggunaan teknologi DLP merupakan cara yang berkesan bagi melindungi data dari insiden keselamatan siber yang menyebabkan kehilangan, kecurian atau pendedahan data. Ia mampu untuk mengesan, memantau, serta mengawal pemindahan, penggunaan dan penyimpanan data daripada berlaku tanpa kebenaran. Antara ciri-ciri utama yang terdapat pada DLP ialah analisis dan tapisan kandungan, pemantauan trafik rangkaian, penyulitan data, penyamaran data serta analisis tingkah laku pengguna. Gabungan elemen-elemen perlindungan ini membolehkan DLP memelihara kerahsiaan data secara berkesan (Kharraz et al. 2015).

2. Integriti: Prinsip kedua keselamatan siber iaitu integriti pula merujuk kepada kualiti yang terdapat di dalam keselamatan siber untuk memelihara data bagi memastikan ia sentiasa tepat, dipercayai dan tidak melalui sebarang perubahan yang tidak dibenarkan. Perubahan data yang menjejaskan integritinya boleh berlaku pada mana-mana proses termasuklah perjalanan, pemprosesan dan penyimpanan. Kegagalan memastikan integriti data dipelihara juga boleh mengakibatkan pelbagai implikasi seperti kerosakan imej, kerugian kewangan, kehilangan kepercayaan dan implikasi perundangan (Whitman et al. 2018). Terdapat pelbagai cara yang boleh digunakan bagi memelihara integriti data seperti teknik hashing, tandatangan digital, kawalan capaian dan data sandaran.

   Hashing ialah proses menjana nilai hash unik yang terhasil daripada data asal tersebut. Nilai hash adalah unik dan ia boleh mewakili data asalnya kerana sebarang perubahan pada data asal walaupun kecil sekalipun akan menyebabkan perubahan nilai pada nilai hash baru yang dijana. Nilai hash biasanya disimpan bersama dengan data asal bagi tujuan mengesahkan integritinya. Terdapat pelbagai teknik hashing yang selalu digunakan contohnya SHA-1, SHA-2, MD5, LANMAN dan NTML, namun pemilihan kepada teknik-teknik yang digunakan bergantung kepada pelbagai faktor seperti kredibiliti, bebas perlanggaran, dan kadar kepantasan.

   Tandatangan digital ialah teknik yang biasa digunakan untuk memastikan integriti dan keaslian sesuatu data itu dipelihara dan dijamin. Ia memanfaatkan proses kriptografi dan hashing bagi memastikan dua pihak yang berinteraksi diantara satu sama lain meyakini data yang dikirim dan dikongsi adalah tulen dan berintegriti tanpa pengubahan oleh pihak ketiga. Tandatangan digital mempunya manfaat yang besar di dalam pelbagai bidang seperti kesihatan, ketenteraan, kewangan, dan perundangan kerana ia selamat, mudah serta menjimatkan kos dan masa.

   Selain melindungi kerahsiaan data dan aset seperti yang dibincangkan sebelum ini, kawalan capaian juga berfungsi untuk melindungi integriti data dan aset. Ia adalah aspek asas di dalam keselamatan siber melibatkan proses mengurus dan

menyekat capaian individu atau sistem kepada data dan aset yang cuba dilindungi.

Satu teknik pengurusan yang biasa digunakan untuk kawalan capaian ialah penggunaan model yang terdiri daripada tiga peringkat, yang terdiri daripada pengenalpastian, pengesahan dan keizinan. Pengenalpastian menggunakan ciri unik pengguna sebagai bukti kelayakan seperti nama pengguna, alamat e-mel atau pengecam unik. Pengesahan pula memastikan identiti pengguna dengan menjalankan pengesahan terhadap kelayakan mereka melalui pelbagai mekanisme contohnya kata laluan, sijil digital, pengesahan dua faktor, dan biometrik. Keizinan pula ialah tahap ketiga setelah pengguna melepasi tahap pertama dan kedua.

Setelah identiti pengguna disahkan melalui pengenalpastian dan pengesahan, mereka akan diberi tahap capaian sesuai dengan identiti mereka. Organisasi biasanya mempunyai dasar kawalan capaian yang mengandungi ketetapan hak capaian pengguna berdasarkan prinsip keistimewaan pengguna, peranan, dan tanggungjawab (Whitman et al. 2019). Penentuan capaian yang betul adalah penting bagi melindungi integriti data dan aset.

Pemulihan data: Data adalah aset yang sangat berharga bagi sesebuah organisasi dan kehilangan atau kerosakannya boleh membawa akibat buruk dan kerugian dari sudut kewangan, reputasi, perjalanan operasi, dan pelanggaran undang-undang atau garis panduan. Oleh itu, adalah penting untuk mempunyai pelan proses pemulihan data yang mantap apabila berlaku insiden keselamatan siber bagi mengurangkan risiko ini dan memastikan kesinambungan operasi dan perniagaan (Kessler 2018).

Pemulihan data dari sudut keselamatan siber ialah proses mendapatkan semula dan memulihkan data daripada pelbagai sistem, peranti storan, atau sandaran yang dipadamkan, rosak atau hilang. Ia merupakan aspek kritikal keselamatan siber kerana ia membantu organisasi pulih daripada pelanggaran data, kegagalan sistem, pemadaman tidak sengaja atau insiden lain yang boleh mengakibatkan

kehilangan data. Setelah tahap dan punca pemadaman, kerosakan atau kehilangan data disedari, organisasi terlibat biasanya boleh menggunakan pelbagai cara untuk pemulihan data, bergantung kepada kesesuaian (Casey et al. 2014):

Salinan data: Kewujudan salinan kepada data kritikal secara kerap adalah amalan asas dalam pemulihan data kerana ia akan menjadi pengganti kepada data asal dalam proses pemulihan. Salinan perlu disimpan di dalam peranti storan berasingan atau di tempat lain bagi memastikan ia lebih selamat dan berdaya tahan. Sekiranya kehilangan data berlaku, organisasi dapat memulihkan data serta meneruskan operasi seperti biasa.

Pembinaan Semula dan Pembaikan Data: Data yang rosak juga boleh dipulihkan dengan cara pembinaan semula atau melakukan pembaikan pada fail atau struktur storan yang rosak. Teknik ini kadangkala melibatkan penggunaan alat forensik khas atau memerlukan khidmat pakar pemulihan data jika kerosakan yang dialami adalah besar dan rumit.

3. Ketersediaan: Dari sudut keselamatan siber, ketersediaan merujuk kepada keadaan sesuatu data atau aset di mana ia sentiasa boleh dicapai dan beroperasi dengan masa yang ditetapkan untuk pengguna yang dibenarkan apabila mereka perlu mencapai data atau aset tersebut. Ia adalah elemen penting bagi memastikan fungsi, kebolehpercayaan dan kualiti capaian data atau aset adalah pada tahap yang sepatutnya. Perlindungan kepada prinsip ketersediaan merangkumi pencegahan kepada gangguan luar jangka yang tidak dirancang dan juga pencegahan dari serangan yang disengajakan, berniat jahat yang bertujuan untuk menafikan atau mengurangkan jumlah capaian dari pengguna kepada sumber aset atau data yang dilindungi

   Mengekalkan sifat ketersediaan di dalam keselamatan siber adalah penting di dalam organisasi dan perniagaan kerana tempoh putus perkhidmatan boleh mengakibatkan kerugian besar dari sudut kerosakan imej, kewangan, kehilangan kepercayaan dan implikasi perundangan. Bagi mencapai perlindungan tersebut,

organisasi biasanya menggunakan pelbagai strategi termasuklah dengan melakukan pertindihan, pengimbangan beban, pemantauan sistem, mitigasi DDoS, serta pembinaan infrastruktur yang berdaya tahan (Whitman et al. 2019):

Pertindihan: Ia merupakan amalan membuat pertindihan aset atau data kritikal bagi memastikan semua aset dan data tersebut mempunyai pengganti yang berterusan dalam menghadapi aktiviti berniat jahat atau kegagalan luar jangka. Walaupun meningkatkan kos, amalan ini penting bagi melindungi aset digital, mengekalkan kesinambungan operasi dan meminimumkan masa henti operasi. Pertindihan boleh dilakukan dari pelbagai sudut seperti pertindihan perkakasan, pertindihan data, pertindihan rangkaian, pertindihan tempat, dan pertindihan aplikasi (Whitman et al. 2019).

Pengimbangan beban: Ia merupakan amalan mengagihkan beban seperti beban trafik di dalam rangkaian atau beban kerja pengkomputeran yang terdapat pada sumber, sistem atau pelayan untuk mengoptimumkan prestasi seterusnya memastikan ketersediaan dan mengelakkan kesesakan trafik atau beban berlebihan. Ia dapat memainkan peranan penting dalam memastikan penggunaan sumber pengkomputeran berfungsi dengan lancar dan cekap sambil mengekalkan daya tahan dan keselamatan sesebuah organisasi terhadap ancaman siber. Pengimbangan beban boleh dibuat menggunakan pengimbang beban berasaskan perisian atau perkakasan pengimbang beban khusus.

Pemantauan sistem: pemantauan sistem melibatkan pelbagai proses seperti pengumpulan, perekodan, analisis dan kemudiannya pemahaman berterusan kepada corak data sistem dan rangkaian untuk mengesan insiden keselamatan atau sebarang anomali lain. Ia berkemampuan untuk mengenal pasti tanda-tanda capaian tanpa kebenaran, petunjuk kompromi, jangkitan perisian hasad atau sebarang aktiviti mencurigakan lain yang berkemungkinan menjejaskan keselamatan siber. Pemantauan sistem merangkumi pelbagai aktiviti termasuklah pemantauan trafik rangkaian, analisis log, pengimbasan kelemahan dan pengesanan anomali.

Dengan melaksanakan pemantauan sistem yang baik, sesebuah organisasi boleh mengenal pasti insiden keselamatan atau potensi kelemahan secara proaktif sebelum ia meningkat kepada kejadian buruk yang lebih besar. Ia memberi gambaran lebih jelas sistem dan tingkah laku normal pengguna sistem, membolehkan tindakan pengesanan awal bagi ancaman keselamatan, seterusnya membolehkan pihak keselamatan membuat tindak balas pantas bagi sebarang insiden yang berlaku (Whitman et al. 2019). Selain itu, pemantauan sistem juga mempunyai peranan penting kepada organisasi dalam mematuhi peraturan dan keselamatan yang ditetapkan oleh pihak berkuasa.

Mitigasi DDoS: DDoS atau DoS merupakan satu bentuk ancaman keselamatan siber yang boleh dilakukan oleh penjenayah siber. Serangan DoS menyasarkan sambungan komunikasi diantara pengguna sebenar dan pelayan oleh penyedia perkhidmatan dengan cara mengurangkan kualiti sambungan atau menghalangnya terus. Cara yang digunakan oleh penyerang ialah dengan menghantar paket di dalam jumlah yang sangat besar sehingga aset penyedia perkhidmatan tidak dapat menampung permintaan servis yang dibuat oleh penyerang dan juga pengguna sebenar. Jika pelayan masih dapat menampung permintaan servis yang terlalu banyak tersebut sekalipun, ia telah membazirkan banyak sumber sehingga boleh menjejaskan perkhidmatan kepada pelanggan sebenar (Prakash et al. 2016).

Ancaman utama serangan DoS ialah jumlah besar paket yang dihantar, bukanlah kandungannya. Paket yang dihantar pula tidaklah mudah untuk dikesan dan dikendalikan disebabkan oleh jumlahnya yang besar. Serangan Dos boleh dipecahkan kepada beberapa kategori berdasarkan jenis serangan yang dilakukan iaitu di tahap rangkaian, tahap aplikasi, tahap operasi, dan tahap data (Prakash et al. 2016).

Pelbagai cara digunakan oleh organisasi untuk menangani ancaman DoS, antaranya ialah penggunaan teka-teki seperti bentuk dan soalan matematik, kemudian penapisan MAC dengan cara mengasingkan MAC pengguna sebenar dan penyerang. Dalam kes ini, capaian MAC pengguna akan dibenarkan

manakala MAC penyerang akan dihalang. Manakala yang terakhir ialah pengesahan berdasarkan kriptografi (Prakash et al. 2016).

Latihan: Faktor manusia adalah penting di dalam keselamatan siber sesebuah organisasi. Setiap individu di dalam organisasi tanpa mengira jawatan dan peranan perlu dilatih tentang amalan terbaik dan kesedaran keselamatan siber bagi mengelakkan mereka menjadi punca pencerobohan siber terhadap organisasi mereka. Individu yang terlatih bukan sahaja tidak berisiko untuk menjadi mangsa serangan siber, bahkan mereka boleh membentuk budaya kerja yang mementingkan keselamatan siber di samping melaporkan aktiviti mencurigakan yang berlaku di dalam organisasi.

Terdapat pelbagai sudut latihan yang boleh diberikan kepada anggota organisasi. Secara umumnya, mereka perlu dilatih tentang risiko dan akibat ancaman keselamatan siber, prosedur dan keselamatan yang digunakan di organisasi, kesedaran teknik kejuruteraan sosial dan pancingan data, tingkah laku selamat dan amalan terbaik, pelaporan insiden keselamatan, serta kerahsiaan dan perlindungan data. Di samping berjaya menjalani latihan, anggota organisasi juga perlu sentiasa menjalani latihan berterusan dan melalui simulasi insiden keselamatan siber secara berkala.

1.1.2 Insiden-Insiden Keselamatan Siber Berskala Besar

Terdapat banyak insiden keselamatan siber yang menjejaskan prinsip asas keselamatan siber seterusnya memberi kesan kepada ribuan organisasi dan jutaan manusia di seluruh dunia. Ia memberi kesan bukan sahaja dari sudut kerugian wang ringgit yang boleh mencecah nilai ribuan juta ringgit, namun juga kepada kerahsiaan data syarikat dan pengguna yang boleh memberi kesan privasi, keselamatan dan emosi seumur hidup kepada pihak yang terlibat akibat daripada kecurian data, kehilangan data dan kehilangan capaian kepada perkhidmatan yang disediakan. Sesetengah organisasi juga terdedah kepada tindakan undang-undang disebabkan oleh kegagalan melindungi data pengguna. Beberapa insiden keselamatan siber yang mencuri tumpuan dunia termasuklah:

1. Stuxnet: Ketika ketegangan berlaku diantara negara Amerika Syarikat dan Iran berkaitan teknologi nuklearnya, terdapat insiden keselamatan siber yang menyerang loji nuklear Iran yang disebabkan oleh perisian hasad Stuxnet. Ia merupakan perisian hasad yang sangat canggih pada masa tersebut dan mula dikesan pada tahun 2010. Stuxnet menggunakan 4 kelemahan hari-sifar yang hampir mustahil dapat dihasilkan oleh penggodam biasa. Walaupun sukar untuk mengetahui bagaimana perisian hasad dihasilkan, penyelidik menilai bahawa perisian hasad ini memerlukan sumber yang besar untuk dicipta, termasuklah dari sudut kewangan, manusia dan masa. Dianggarkan sekurang-kurangnya 5 hingga 10 orang diperlukan untuk bekerja selama beberapa bulan untuk menghasilnya (Chen et al. 2011).

   Fungsi utama perisian hasad ini ialah khusus untuk menjejaskan mesin emparan nuklear di loji nuklear di Natanz, Iran. Loji nuklear Natanz mempunyai rangkaian komputer yang terkawal dan tertutup, bermakna tidak mungkin ia dapat disebarkan mengguna sambungan Internet atau rangkaian dalaman. Oleh itu, siasatan mendapati kemungkinan besar rangkaian komputer tersebut dijangkiti Stuxnet melalui vektor pemacu USB (De Falco et al. 2012). Ini bermakna bahawa pencipta cacing memerlukan seseorang untuk menghantar cacing dan menjangkiti rangkaian.

   Kesan paling langsung daripada serangan perisian hasad ini ialah kesan fizikal kepada emparan nuklear di loji nuklear Natanz. Adalah jelas Stuxnet direka khusus untuk menjejaskan kemampuan emparan di loji tersebut untuk berfungsi secara penggunaannya yang biasa. Perisian hasad ini berfungsi dengan menjejaskan kelajuan emparan menjadikan kelajuannya berubah diantara tinggi dan rendah secara berselang-seli. Walaubagaimanapun, perubahan kelajuan ini tidak dapat disedari oleh pengendalinya kerana perisian hasad ini membuat seolah-olah tiada apa perubahan yang berlaku pada sistem. Akibatnya emparan menjadi rosak dengan cepat dan tidak dapat dibaiki dengan baik. Dianggarkan terdapat kira-kira 6000 hingga 9000 emparan terdapat di loji nuklear Nathan ketika itu (De Falco et al. 2012).

Insiden ini juga memberi kesan besar kepada Iran dari sudut ekonomi dan imej negara. Insiden ini memberi mesej jelas bahawa perisian hasad boleh dihasilkan untuk melakukan sabotaj terhadap sasaran khusus dan bernilai tinggi. Insiden ini juga telah membuka mata dan memberi kesedaran kepada banyak pihak terutamanya kerajaan terhadap keselamatan siber.

2. Sony Pictures Entertainment (SPE): Ini bukanlah kali pertama SPE menjadi mangsa serangan siber. Namun, pada 24 November 2014, SPE didapati telah menjadi mangsa kepada salah satu serangan siber terbesar dalam sejarah. Pekerja yang cuba log masuk ke stesen kerja mereka disambut dengan rangka merah menyala dengan mesej dari penggodam. Penjenayah tersebut yang menggelarkan diri mereka Guardian of Peace telah melanggar menceroboh data dan aset SPE, menyebabkan kerugian besar yang tidak dapat dibayangkan kepada SPE (Peter 2015).

   Sebelum mana-mana juruteknik IT SPE boleh mengambil sebarang tindakan, perisian hasad oleh penjenayah telah menjangkiti semua komputer dalam rangkaian syarikat tersebut. Data daripada 3262 komputer dan 837 pelayan telah dicuri serta dipadamkan. Semua data dalam rangkaian telah disulitkan menggunakan algoritma yang kompleks oleh penggodam, menjadikan tugas memulihkannya hampir mustahil. Lebih memburukkan keadaan, penggodam juga merosakkan perisian pengendalian komputer yang dijangkiti seterusnya menjadikannya tidak berguna. Dilaporkan bahawa dalam beberapa hari berikutnya selepas serangan itu, kakitangan terpaksa bekerja menggunakan papan putih menggantikan komputer yang tidak dapat digunakan (Desimone et al. 2017).

   Lebih memburukkan keadaan, ini bukan penamat mimpi ngeri SPE apabila mereka mendapati bahawa penggodam telah menyebarkan 9 kumpulan data sulit pada tapak perkongsian awam dalam tempoh 3 minggu. Data tersebut mengandungi maklumat e-mel, maklumat kewangan, lebih daripada 47,000 nombor keselamatan sosial pekerja, maklumat peribadi lain, skrip filem yang belum siap, dan lima filem Sony, di mana empat daripadanya belum dipasarkan

pada masa serangan itu. Kumpulan penggodam itu juga menyiarkan mesej yang mengancam ahli keluarga pekerja dan juga mengancam untuk melakukan serangan ke atas pawagam yang merancang untuk menayangkan filem The Interview. Dianggarkan 100 *terabyte* data telah dicuri di dalam insiden ini (Li 2018).

Beberapa sumber menyatakan bahawa SPE kurang bersedia untuk serangan siber sebesar itu. Ed Skoudis, penggodam "topi putih" yang melatih profesional keselamatan IT korporat tentang ujian pertahanan siber di Institut SANS berkata bahawa kemahiran penggodaman yang digunakan di dalam insiden Sony kelihatan sederhana dan pada tahap yang boleh dilakukan oleh pelajar dalam kelas peringkat pertengahannya sahaja. Beliau dipetik sebagai berkata "Ia menunjukkan pertahanan Sony tidaklah begitu baik." (Peter 2015).

Beberapa pakar keselamatan dan perisikan sebenarnya telah memberi amaran sebelum ini kepada pegawai bertanggungjawab di Sony tentang ancaman dan risiko serangan siber oleh akibat penghasilan filem The Interview. Namun, Sony tidak mengambil berat akan kemungkinan tersebut dan juga akibat daripada serangan tersebut kepada organisasi mereka (Peter 2015).

3. Pencerobohan data Yahoo: Pada tahun 2016, Yahoo telah mengumumkan bahawa mereka telah mengalami insiden keselamatan siber iaitu pencerobohan data melibatkan 500 juta akaun penggunanya pada tahun 2014, dan kemudiannya mengumumkan sekali lagi pencerobohan data melibatkan 1 bilion akaun penggunanya pada tahun 2023. Data yang terlibat termasuklah nama, alamat e-mel, kata laluan, nombor telefon, dan soalan keselamatan serta jawapannya bagi sesetengah pengguna (Castillo 2017).

   Pencerobohan data ini memberi kesan yang sangat besar kepada Yahoo apabila imej mereka terjejas teruk serta saham mereka merudum. Pelanggan Yahoo turut terjejas kerana kecurian data akaun mereka menyebabkan mereka terdedah kepada pelbagai ancaman siber yang lain seperti pancingan data, kecurian identiti dan kecurian data. Lebih diburukkan lagi apabila ramai diantara

pengguna Yahoo menggunakan e-mel dan kata laluan yang sama di laman sesawang dan perkhidmatan lain menyebabkan data mereka di tempat lain turut terdedah kepada pencerobohan (Perlroth 2017).

4. WannaCry: Pada 12 Mei 2017, dunia dikejutkan dengan insiden keselamatan siber iaitu serangan siber melalui perisian hasad tebusan yang dikenali sebagai WannaCry. Turut dikenali sebagai WannaCry 2.0, WanaCrypt0r 2.0, Wanna Decryptor, WCry atau WannaCrypt, ia menyasarkan sistem operasi Windows yang dijual oleh Microsoft. Dianggarkan kira-kira 230, 000 komputer dan 150 negara telah dilanda WannaCry di seluruh dunia dalam masa yang sangat singkat (Bistarelli et al. 2018).

   WannaCry bukan sahaja menyerang komputer peribadi tetapi juga komputer pelbagai syarikat dan institusi kerajaan. Ia menyulitkan fail mereka dan meminta wang tebusan USD300 - USD600 (kira-kira RM1400 – RM2800) dalam nilai Bitcoin ketika itu untuk setiap komputer yang dijangkiti. Di United Kingdom, perkhidmatan National Health Service terjejas teruk oleh serangan ini yang menjejaskan perkhidmatan penjagaan kesihatannya. Syarikat lain yang terjejas oleh perisian tebusan WannaCry termasuklah Telefonica, Renault, FedEx, Nissan, Hitachi, Bank pusat Russia, MegaFon, Sberbank, Bank of China, pejabat kerajaan Jepun, Sandvik, Petrobras dan Portugal Telecom. Kerugian kewangan global akibat serangan itu dianggarkan sekitar $4 bilion (kira-kira RM16.2 bilion) (Berr 2017).

   Terdapat beberapa serangan perisian tebusan sebelum ini, tetapi tidak pada skala ini. Banyak perisian tebusan yang lebih lama bergantung pada mangsa yang memuat turun perisian hasad dengan menipu mereka untuk membuka lampiran atau mengklik pautan yang mengandungi perisian hasad. Apa yang menjadikan WannaCry pada Mei 2017 berbeza dan lebih berbahaya daripada yang lain ialah ia merupakan perisian tebusan generasi baharu, dengan keupayaan seperti cacing untuk menyebarkan dirinya sendiri, kemudian menjangkiti komputer berisiko yang bersambung antara satu sama lain (Zeichick 2017)

Terdapat beberapa sebab bagaimana serangan berlaku begitu pantas di seluruh dunia. Pertama, WannaCry mengeksploitasi kerentanan CVE-2017-0144. Pada hari pertama serangan, Microsoft belum lagi mengeluarkan kemaskini keselamatan untuk versi Windows yang tidak disokong termasuk Windows XP (berakhir 8 April 2014) (Microsoft. n.d) dan Windows 8 (berakhir 12 Januari 2016) (Microsoft. n.d). Pada April 2017, didapati bahawa sekitar 7% daripada semua komputer di seluruh dunia masih menggunakan Windows XP, menjadikan jumlahnya sekitar 140 juta komputer.

Kedua, WannaCry mempunyai keupayaan untuk menjangkiti komputer lain tanpa memerlukan interaksi pengguna (Brenner 2017). Ini juga sukar untuk dipertahankan kerana langkah pertahanan iaitu kemaskini keselamatan perisian pengendalian Windows perlu dilakukan pantas namun tidak disediakan oleh pihak Microsoft. Terdapat tiga kumpulan komputer yang didapati lebih terdedah kepada serangan ini iaitu pemain permainan komputer dalam talian, pengguna perisian Teamviewer dan komputer yang sebelum ini pernah dijangkiti oleh perisian hasad (Einav 2017). Ini kerana komputer-komputer ini mempunyai lebih banyak interaksi dengan komputer lain berbanding komputer yang mempunyai sambungan biasa. Jadi, semakin banyak komputer terjejas yang disambungkan ke rangkaian dalaman dan luaran, semakin besar kemungkinan ia dijangkiti oleh perisian hasad WannaCry.

Ketiga, WannaCry juga memanfaatkan DoublePulsar, satu lagi alat penggodaman selain EternalBlue yang dibocorkan oleh pihak yang dikenali sebagai Shadow Broker (Zeichick 2017). Ia mengeksploitasi kelemahan di dalam perisian pengendalian Windows yang tidak dikemaskini, memberikan keistimewaan penuh perisian hasad tersebut terhadap komputer mangsa.

5. Pencerobohan data Equifax: Equifax Information Services LLC merupakan salah 1 daripada 3 syarikat pelaporan kad kredit utama di Amerika Syarikat selain Experian Information Solutions dan TransUnion LLC (White 2023). Syarikat ini mengambil, mengumpul, dan melaporkan maklumat pengguna kad kredit yang merupakan rakyat negara tersebut dari sudut laporan kredit. Laporan

ini kemudiannya diberikan kepada institusi kewangan dan perniagaan yang dibenarkan untuk memperoleh maklumat tersebut.

Pada 7 September 2017, mengumumkan insiden keselamatan siber yang menjejaskan lebih kurang 145 juta pengguna di Amerika Syarikat akibat dari pencerobohan sistem dalamannya (Caitlin 2018). Pencerobohan ini membolehkan penjenayah tersebut memperoleh pelbagai maklumat peribadi pengguna kad kredit yang terjejas seperti nama, tarikh lahir, nombor keselamatan sosial, alamat dan nombor lesen memandu (Caitlin 2018).

Insiden ini memberi kesan yang sangat buruk bukan sahaja kepada Equifax namun juga kepada keselamatan rakyat Amerika Syarikat. Tindakan undang-undang kemudiannya dimulakan oleh banyak pihak yang terjejas dan mengesyaki terdapat kelemahan urus tadbir apabila dilaporkan bahawa Equifax pernah dimaklumkan tentang kelemahan sistemnya oleh Apache Software Foundation yang boleh melindungi Equifax dari insiden ini jika tindakan penambahbaikan mengikut saranan laporan tersebut diambil (Sally. 2017).

6. NotPetya: Ia merupakan perisian hasad tebusan yang muncul pada 27 Jun 2017, menjadi antara insiden serangan siber terbesar di dunia (Solon et al. 2017). Perisian hasad ini sebenarnya merupakan versi penambahbaikan oleh penjenayah siber dari versi asal perisian hasad Petya yang diberi nama baharu baru membezakannya dengan versi asal. Berbeza dengan Petya, NotPetya bukan sahaja menyulitkan fail, tetapi juga keseluruhan sistem termasuklah MBR menjadikan sistem operasi yang digunakan oleh pengguna lumpuh dan tidak dapat digunakan(Yeh et al. 2007).

   Seperti juga perisian hasad WannaCry, NotPetya mengeksploitasi kelemahan EternalBlue yang terdapat di dalam perisian pengendalian Windows yang tidak dikemaskini selain mengeksploitasi beberapa lagi kelemahan yang lain seperti yang terdapat pada WMI dan EternalRomance (CISA. 2018). Hanya satu komputer yang tidak dikemaskini diperlukan untuk dijangkiti seterusnya menyerang rangkaian dalaman sesuatu organisasi kerana perisian hasad ini

boleh mendapatkan hak pentadbir seterusnya menjangkiti komputer lain (Abrams 2016). NotPetya juga disebarkan melalui teknik pancingan data menggunakan e-mel yang mengandungi perisian hasad ini sebagai lampiran (Brewster 2017)

Serangan ini bermula di negara Ukraine, sebelum merebak ke 64 negara dalam masa yang pantas dengan Amerika Syarikat menjadi negara kedua paling terjejas selepas Ukraine (Thomson 2017). Banyak organisasi besar terjejas disebabkan oleh perisian hasad ini terutamanya yang memerlukan perjalanan operasi sistem komputer secara berterusan bagi menjalankan aktiviti perniagaan dan fungsi peranan secara normal.

7. Serangan rantaian bekalan SolarWinds: Antara serangan terbesar yang berlaku di negara Amerika Syarikat pada tahun 2019 ialah serangan ke atas rantaian bekalan SolarWinds yang turut dikenali sebagai UNC2452, Sunburst ataupun Solorigate. SolarWinds ditubuhkan pada tahun 1999, merupakan syarikat teknologi maklumat terkenal dari Amerika Syarikat yang membekalkan perisian kepada pelbagai syarikat-syarikat gergasi seperti CISCO dan Microsoft serta pelbagai organisasi kerajaan (Alkhadra et al. 2021).

   Serangan ke atas SolarWinds dikategorikan sebagai serangan rantaian bekalan. Bagi serangan sebegini, sasaran utama serangan adalah organisasi yang mempunyai sistem keselamatan siber yang lemah. Namun, pencerobohan yang berjaya ke atas organisasi tersebut iaitu Orion dalam kes ini boleh dijadikan pintu masuk kepada serangan ke atas organisasi lain yang lebih besar yang berada di dalam rantaian bekalannya iaitu SolarWinds dan organisasi lain yang menerima bekalan perisian dari SolarWinds. Dalam bidang perniagaan, setiap produk mempunyai rangkaian bekalan termasuklah produk e-dagang dan perisian. Maka pencerobohan ke atas perisian yang dikeluarkan oleh pembekal SolarWinds membolehkan penjenayah menceroboh organisasi yang menerima perisian SolarWinds tanpa disedari mereka lebih-lebih lagi apabila serangan tersebut dibuat dimasukkan terus ke dalam kod sumber perisian dari SolarWinds sebelum ditandatangani secara digital (Alkhadra et al. 2021).

Dianggarkan sebanyak lebih daripada 17000 pelanggan SolarWinds telah memuat turun perisian yang dijangkiti tersebut, menyebabkan mereka terjejas teruk kerana banyak daripada pelanggan SolarWinds merupakan organisasi yang mempunyai banyak data dan aset sensitif. Penggodam juga didapati bijak menggunakan pelbagai teknik berbeza bagi merahsiakan aktiviti mereka sehingga tidak dikesan oleh pengguna dan pihak yang memantau serta mereka telah berjaya mengelak daripada perisian keselamatan yang bertanggungjawab mengesan aktiviti mencurigakan (Gillis 2021). Dianggarkan kerugian yang dialami oleh SolarWinds akibat dari serangan siber ini mencecah USD100 bilion manakala sesetengah pihak pula menjangkakan nilai yang tidak dapat dihitung dengan mengambil kira kebocoran maklumat rahsia dan sensitif yang disimpan oleh banyak organisasi kerajaan yang menjadi pelanggan SolarWinds seterusnya mampu mengancam keselamatan negara Amerika Syarikat (Pexton 2021).

Kebanyakan insiden keselamatan siber samada berskala kecil atau besar mempunyai kaitan dengan tahap kesedaran keselamatan siber atau kegagalan untuk mengamalkan polisi dan amalan piawaian keselamatan siber. Jadual 1.1 di bawah menunjukkan antara punca pencerobohan yang boleh dikaitkan dengan elemen kecuaian manusia bagi insiden-insiden yang dibincangkan:

Jadual 1.1 Punca pencerobohan siber yang boleh dikaitkan dengan elemen kecuaian manusia

Tahun Laporan	**Insiden**	**Elemen Kecuaian Manusia**
2013 & 2014	Pencerobohan data Yahoo	Kejuruteraan sosial dan serangan *spear phising* (Graphus 2020)
2014	Pencerobohan data Sony Pictures Entertainment (SPE)	Katalaluan lemah, tidak mengambil berat akan amaran pihak penyelidik, serta kekurangan latihan keselamatan siber dikalangan kakitangan (Mazzarella 2015)
2017	WannaCry	Kegagalan mengemaskini perisian pengendalian Windows (Kaspersky n.d.)
2017	Pencerobohan data Equifax	Kegagalan komunikasi untuk mengemaskini serta membaiki perisian seperti yang dirancang. Sijil digital telah luput selama 10 bulan (Bisson 2023)
2017	NotPetya	Kegagalan mengemaskini perisian pengendalian Windows, Menekan pautan dan lampiran di e-mel (pancingan data) serta tidak segera menutup komputer yang dijangkiti (Bouldin 2018)

1.1.3 Ahli Farmasi Sebagai Profesional Kesihatan

Ahli farmasi merupakan anggota profesional kesihatan yang mempunyai peranan penting di dalam sistem kesihatan sesebuah negara. Mereka merupakan pakar di dalam ubat-ubatan, termasuklah di dalam penyediaan, penyimpanan, dos, dan cara pengambilan ubat yang betul. Mereka bertanggungjawab untuk membekalkan ubat kepada pesakit dan juga menyemak preskripsi ubat yang ditulis oleh doktor perubatan dan doktor haiwan. Selain itu, mereka mempunyai kepakaran untuk membuat pemantauan dan penilaian di dalam penggunaan ubat sedia ada oleh pesakit. Penilaian ini termasuklah kesesuaian ubat yang digunakan, interaksi antara ubat-ubatan serta interaksi antara ubatan dan makanan yang diambil pesakit.

Dari sudut pembekalan ubat-ubatan kepada pesakit, tanggungjawab utama seorang ahli farmasi ialah memastikan bahawa pesakit yang menerima pembekalan ubat bagi tujuan rawatan tersebut menerima ubatan yang betul, dos yang betul, tempoh rawatan yang betul, jumlah ubat yang betul dan masa pengambilan ubat yang betul. Ubat yang betul bermakna ubat tersebut adalah tepat dan tidak bertindan untuk rawatan penyakit yang diterima serta sesuai dengan pesakit tersebut. Sebarang sejarah alergi ubat yang pernah dialami oleh seseorang pesakit tersebut perlu diambil maklum oleh ahli farmasi yang membekalkan ubat kepada pesakit.

Ahli farmasi juga merupakan pakar di dalam kaunseling pengambilan ubat-ubatan. Terdapat pesakit yang tidak mengambil ubat dengan cara yang disebabkan oleh pelbagai faktor antaranya usia, kesukaran membaca, terlupa, kerisauan terhadap kesan ubat, dan kepercayaan atau ideologi yang sangat berbeza diantara seseorang pesakit dengan yang lain. Kegagalan pesakit untuk mengikuti pelan rawatan melalui ubatan yang dibekalkan sebenarnya meningkatkan beban kewangan kepada pesakit dan menyebabkan pembaziran ubat-ubatan (Jimmy et al. 2011). Maka di sinilah peranan ahli farmasi dalam memberikan kaunseling kepada pesakit bagi memastikan faktor-faktor yang menyebabkan kegagalan mematuhi pelan rawatan ubatan yang diberi tidak gagal. Adalah didapati juga bahawa kualiti pelan rawatan ubatan seseorang pesakit juga bertambah dengan sangat baik apabila mendapat intervensi dari ahli farmasi (Sanii et al. 2016).

Ahli farmasi juga memainkan peranan di dalam merangka pelan rawatan terbaik ubatan pesakit bersama profesional kesihatan yang lain. Maklum balas yang diberikan oleh ahli farmasi kepada doktor perubatan dari sudut kesesuaian ubatan, rekod pesakit, keberkesanan dan keselamatan sesuatu ubat adalah penting di dalam memastikan bahawa pesakit mendapat rawatan terbaik yang boleh diterima olehnya. Pesakit yang datang ke farmasi komuniti juga boleh membuat perbincangan dengan ahli farmasi yang bertugas bagi menentukan jenis ubatan, makanan dan suplemen kesihatan yang terbaik untuk mereka (Mansur JM. 2016).

Ahli farmasi juga merupakan pakar rujuk kepada ahli profesional kesihatan yang lain berkaitan ubat-ubatan terutamanya di dalam organisasi kesihatan. Kebiasaannya hospital kerajaan mempunyai unit maklumat ubat yang diketuai oleh ahli farmasi yang bertanggungjawab untuk menerima panggilan telefon berkaitan ubat-ubatan yang memerlukan jawapan pantas, tepat dan menepati hasil atau penemuan kajian terkini. Kebiasaannya persoalan yang ditanya ialah berkaitan dengan dos ubat berdasarkan maklumat demografi unik seseorang pesakit seperti berat badan, dan maklumat penyakit sedia ada seperti penyakit hati dan buah pinggang yang memerlukan dos ubat yang diselaraskan khas mengikut keperluan individu tersebut.

Ahli farmasi juga mempunyai kemahiran membuat ubat-ubatan menggunakan bahan aktif dan tidak aktif yang boleh dibeli dalam bentuk bahan mentah. Ini kerana mereka mempunyai pengetahuan dan latihan yang cukup untuk membuat ubat-ubatan yang mampu bertahan dan selamat untuk kegunaan pesakit (Carvalho et al. 2022). Keupayaan ini juga membolehkan ahli farmasi membuat ubat-ubatan yang sesuai dengan cita rasa pesakit yang mendapatkan rawatan seperti pemilihan rasa, warna dan bentuk ubat yang memenuhi cita rasa pesakit selain mempunyai kesan rawatan yang diingini. Di dalam sektor pengilangan pula, ahli farmasi bertanggungjawab di dalam merancang peratus bahan, bentuk ubatan dan cara pembuatan ubat-ubatan pada skala besar.

Ahli farmasi juga bertanggungjawab di dalam jaminan ubat-ubatan yang dihasilkan serta memastikan bahawa ia sentiasa mematuhi protokol, garis panduan dan undang-undang yang ditetapkan (Sarantopoulos et al. 1995). Pengilangan ubat-ubatan

perlu mematuhi pelbagai piawaian dan pemantauan dari pelbagai pihak yang mengawal. Antara perkara asas yang perlu dipatuhi ialah amalan pengilangan baik dan amalan pengedaran baik yang merupakan syarat asas sesuatu ubat yang dihasilkan boleh diterima dan lulus untuk dipasarkan kepada masyarakat (Center for Drug Evaluation and Research n.d.). Kegagalan mematuhi keperluan yang ditetapkan setelah produk ubat-ubatan dipasarkan boleh menyebabkan produk dipanggil balik dan pengilang berdepan tindakan undang-undang.

Kebiasaannya di Malaysia, bagi membolehkan seseorang menjadi Ahli Farmasi Berdaftar (FRP), seseorang perlu mempunyai sekurang-kurangnya Ijazah Sarjana Muda Farmasi yang diiktiraf oleh kerajaan Malaysia bagi melayakkan menjalani latihan sebagai Ahli Farmasi Provisional (PRP). Ini merupakan kelayakan sementara bagi membolehkan seseorang itu menjalani latihan wajib sebagai ahli farmasi selama 1 tahun di bawah pemantauan FRP. Latihan ini pula hanya boleh dijalankan di organisasi kesihatan yang diiktiraf oleh kerajaan Malaysia Nam 2002). Di samping itu, seseorang itu juga perlu lulus ujian undang-undang bagi beberapa akta serta garis panduan berkaitan sebelum layak untuk bergelar FRP (Program Perkhidmatan Farmasi. n.d..

Setelah menjadi seorang ahli farmasi yang berdaftar, seseorang itu boleh meneruskan kerjayanya di dalam sektor farmasi yang sesuai. Sejumlah besar ahli farmasi berkhidmat sebagai penjawat awam di institusi pengajian tinggi, pusat kajian, makmal, hospital, klinik, ataupun sebagai anggota pentadbiran dan penguatkuasaan undang-undang. Ahli farmasi yang bekerja di sektor kerajaan bukan sahaja terikat dari sudut perundangan dan etika ahli farmasi, namun juga terikat sebagai seorang penjawat awam yang perlu menjalankan tugas-tugas rasmi yang lain. Di sektor swasta pula, kebiasaannya ahli farmasi memilih kerjaya di institusi pengajian tinggi swasta, kilang, syarikat farmaseutikal, ataupun sebagai ahli farmasi komuniti.

Dikalangan ahli farmasi yang berkhidmat di sektor swasta, ahli farmasi komuniti merupakan ahli farmasi yang paling banyak bertemu dengan pesakit dan menyimpan pelbagai rekod berkaitan ubat-ubatan dan pesakit yang dirawat. Ahli farmasi komuniti perlu mempunyai pengetahuan luas bukan sahaja berkaitan kepakaran seorang ahli farmasi, namun mereka juga perlu tahu juga tentang pelbagai produk yang

terdapat di farmasi seperti peralatan perubatan, alat ujian, dan juga pelbagai jenis makanan tambahan yang sentiasa bertambah dan berubah dari masa ke semasa. Selain itu juga, kebiasaannya mereka perlu menjadi pengurus atau pemilik farmasi komuniti tersebut yang memerlukan mereka mempunyai kemahiran mengurus sumber manusia, kewangan dan inventori bagi memastikan perniagaan dan perkhidmatan farmasi komuniti mereka dapat berjalan lancar dan tidak rugi.

1.2 MOTIVASI KAJIAN

Kajian yang memberi perhatian khusus kepada kesedaran keselamatan siber adalah terhad (Ögütçü et al. 2016). Berdasarkan sorotan kajian yang dijalankan, telah terdapat kajian kesedaran keselamatan siber melibatkan penduduk Malaysia, yang sebahagian besarnya adalah daripada sektor pendidikan. Namun, masih belum ditemui sebarang kajian bagi menilai tahap kesedaran siber khusus dikalangan tenaga kerja di dalam sektor kesihatan. Assenza et al. (2020) pula mendapati bahawa banyak organisasi menjalankan kempen kesedaran siber, namun tidak menilai keberkesanan kempen yang dijalankan. Maka, jurang kajian tersebut menjadi motivasi utama kajian ini, iaitu memberi tumpuan kepada memahami kesedaran keselamatan siber dikalangan profesional kesihatan di Malaysia.

Dikalangan profesional kesihatan di Malaysia, ahli farmasi komuniti dipilih kerana mereka adalah individu yang mempunyai kuasa dan tanggungjawab terbesar di dalam farmasi komuniti tempat mereka berkhidmat. Kebanyakan mereka ialah pengurus jika bukan pemilik kepada farmasi komuniti tersebut, yang bertanggung kepada perjalanan perniagaan serta semua perkara berkaitan farmasi komuniti tempat mereka bertugas termasuklah keselamatan aset dan data. Maka, tahap kesedaran keselamatan siber seseorang ahli farmasi komuniti adalah penting di dalam mendapatkan gambaran risiko ancaman dan akibat insiden keselamatan siber terhadap data pesakit di farmasi komuniti.

1.3 PERNYATAAN MASALAH

Ahli farmasi komuniti merupakan petugas barisan hadapan kesihatan kepada negara yang menyediakan perkhidmatan kaunseling ubatan dan produk kesihatan kepada

masyarakat setempat. Selain itu, mereka turut bertanggungjawab menguruskan keseluruhan perjalanan sesebuah farmasi komuniti termasuklah latihan, stok, kakitangan serta rekod perubatan berkaitan pembekalan ubatan dan maklumat pesakit. Rekod-rekod perubatan ini perlu disimpan bertepatan dengan peruntukan undang-undang sepertimana yang terdapat di dalam Akta Racun 1952.

Pindaan Akta Racun 1952 pada 21 Julai 2022 (Parlimen 2022) telah membenarkan preskripsi dan rekod perubatan disimpan di dalam bentuk elektronik sepenuhnya dengan mematuhi syarat-syarat yang ditetapkan. Rekod ini mengandungi maklumat diagnosis, rawatan, jenis ubat, dos ubat, kad pengenalan, nama penuh, dan alamat pesakit yang mendapatkan rawatan di farmasi tersebut. Apabila ia disimpan di dalam bentuk elektronik, ini meningkatkan risiko ancaman siber kepada farmasi komuniti yang boleh menyebabkan kebocoran maklumat perubatan pesakit.

Di seluruh dunia, banyak pencerobohan data berkaitan rekod perubatan telah berlaku antara tahun 2005 hingga 2019, menjejaskan 249.09 juta individu. Laporan juga menunjukkan bahawa bagi tahun 2018, 536 daripada 2,216 kejadian pencerobohan data melibatkan 65 buah negara adalah berkaitan data perubatan (She AH et al. 2020).Data perubatan dianggap sebagai sasaran yang sangat berharga kerana ia mengandungi pelbagai maklumat peribadi yang sensitif (Chernyshev et al. 2018) dan didapati mempunyai sistem keselamatan yang lemah (Coventry et al. 2018).

Memandangkan telah banyak data perubatan rakyat Malaysia disimpan di dalam talian berbanding sebelum ini, implikasi dari pencerobohan data perubatan tersebut turut meningkat. Pencerobohan terhadap sistem dan pangkalan data perubatan boleh menjadi insiden keselamatan siber yang besar, menjejaskan kerahsiaan rekod perubatan berjuta-juta rakyat Malaysia. Pencerobohan juga meningkatkan risiko manipulasi data, mengakibatkan tafsiran data perubatan yang tidak tepat yang boleh membawa kepada kesilapan diagnosis dan pelan rawatan. Kehilangan data perubatan akibat dari pencerobohan sistem pula boleh menyebabkan keputusan perubatan yang perlu dilakukan segera tidak dapat dilakukan kerana ketiadaan maklumat yang mencukupi.

1.4 MATLAMAT DAN OBJEKTIF KAJIAN

Kajian ini mempunyai matlamat dan objektif seperti berikut:

1. Menentukan model dan petunjuk bagi penilaian tahap kesedaran keselamatan siber yang bersesuaian dengan kajian ini

2. Menentukan instrumen yang bersesuaian dengan kajian ini

3. Mengkaji tahap kesedaran keselamatan siber dikalangan ahli farmasi komuniti di negeri Kelantan

1.5 PERSOALAN KAJIAN

Terdapat juga persoalan yang timbul ketika kajian ini dibuat iaitu:

1. Apakah yang dimaksudkan dengan kesedaran keselamatan siber?

2. Apakah kaedah kajian yang sesuai bagi menentukan tahap kesedaran keselamatan siber?

3. Bagaimana untuk menentukan model dan petunjuk bagi pengukuran tahap kesedaran keselamatan siber?

1.6 SKOP KAJIAN

Kajian ini hanya melibatkan ahli farmasi komuniti di negeri Kelantan yang dianggarkan terdapat seramai 187 orang (KKM 2023). Soal selidik berasaskan tinjauan akan digunakan sebagai kaedah pengumpulan data untuk menilai tahap kesedaran keselamatan siber. Lima aspek kesedaran siber akan dinilai iaitu pengurusan kata laluan, penggunaan e-mel, penggunaan Internet, pengurusan maklumat dan pelaporan insiden.

1.7 KEPENTINGAN KAJIAN

Dapatan dari kajian ini penting kerana ia boleh menjadi sumber rujukan dalam perangkaan strategi masa depan termasuklah penentuan komponen yang sesuai di dalam program latihan anggota kesihatan berkaitan keselamatan siber. Selain itu, pihak berwajib juga akan dapat membuat analisis risiko insiden keselamatan siber berkaitan dengan faktor manusia. Kajian ini juga akan menjadi asas untuk kajian lanjutan yang berkaitan oleh penyelidik lain pada masa hadapan.

1.8 KESIMPULAN

Secara kesimpulannya, tahap kesedaran keselamatan siber yang lemah dari sudut sumber manusia meningkatkan risiko pencerobohan data dan kebocoran maklumat sesebuah organisasi. Banyak organisasi-organisasi termasuklah yang hebat telah menjadi mangsa serangan siber dan pencerobohan data yang telah mengakibatkan kerugian besar dari sudut kewangan, imej, kepercayaan dan meningkatkan risiko mereka untuk terdedah kepada tindakan perundangan. Penggodam juga gemar menyasarkan sektor-sektor kritikal termasuklah sektor kesihatan sebagai sasaran serangan siber kerana ia menjanjikan pulangan lumayan.

Keselamatan siber ialah komponen penting dalam pengurusan siber kerana sistem kesihatan di Malaysia semakin bergantung pada penyelesaian komputer untuk menyimpan rekod, berkongsi maklumat, analisis dan membuat keputusan. Penilaian terhadap kesedaran, pengetahuan dan tingkah laku berkaitan keselamatan siber adalah penting untuk memahami risiko insiden keselamatan siber yang berkaitan dengan faktor manusia, yang biasa berlaku dalam pelanggaran data penjagaan kesihatan. Tanpa penilai tahap keselamatan siber, risiko yang mungkin dihadapi oleh anggota kesihatan terhadap ancaman keselataman siber tidak dapat ditentukan dengan jelas. Kajian ini akan memberi fokus kepada penilaian tahap kesedaran keselamatan siber dikalangan anggota sektor kesihatan iaitu ahli farmasi komuniti di negeri Kelantan.

BAB II

KAJIAN LITERASI

2.1 PENGENALAN

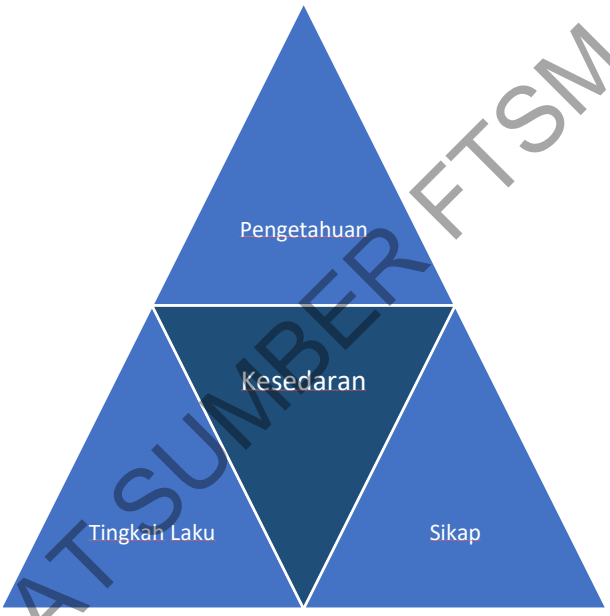
Kebelakangan ini, semakin banyak organisasi yang mengambil berat akan kepentingan melindungi data dan aset mereka dari ancaman siber. Ini kerana kepesatan teknologi telah menyebabkan pelbagai maklumat sensitif disimpan di dalam bentuk digital, dan sepertimana yang telah dibincangkan sebelum ini, pencerobohan data sensitif ini memberi kesan yang sangat buruk bukan sahaja kepada organisasi, tapi juga kepada individu yang terlibat dengan organisasi tersebut seperti pelanggan dan pekerja.

Kesedaran keselamatan siber merupakan komponen penting kepada keselamatan data organisasi tersebut. Individu di dalam organisasi adalah aset penting kepada organisasi tersebut kerana keupayaan mereka untuk membuat keputusan yang penting apabila diperlukan. Organisasi perlu memastikan bahawa setiap individu tahu, sedar dan bersedia untuk memainkan peranan dan tanggungjawab mereka dalam menjaga maklumat organisasi yang ada di dalam simpanan mereka (Amankwa et al. 2014).

Kesedaran keselamatan siber adalah satu konsep yang rumit namun ia dapat dipecahkan kepada pecahan utama iaitu pengetahuan (K), sikap (A) dan tingkah laku (B) berpandukan model KAB (Assenza et al. 2020) (Kruger et al. 2006). Sebagai contoh mudah, walaupun seseorang itu tahu bahawa memakai tali pinggang keledar penting untuk keselamatan ketika pemanduan, namun masih ramai yang mengambil sikap tidak peduli dan bertindak tidak memakai tali pinggan keledar. Maka pengetahuan sahaja tidak menjamin bahawa seseorang itu mempunyai kesedaran yang baik.

Walaupun ketiga-tiga elemen tersebut adalah berbeza, namun ia berkait rapat diantara satu sama lain. Pengetahuan populasi tentang sesuatu perkara adalah perkara

pertama yang akan membentuk sikap dan tingkah laku terhadap perkara tersebut. Tahap pengetahuan terhadap sesuatu perkara memberi kesan kepada sikap, manakala sikap pula menjadi faktor pendorong kepada tingkah laku yang akan diterjemahkan kepada tindakan terhadap perkara tersebut (Fabrigar et al. 2006). Seperti yang digariskan oleh (Shaw et al. 2009), Kesedaran keselamatan siber ialah darjah kefahaman pengguna (pengetahuan) tentang kepentingan keselamatan maklumat serta tanggungjawab (sikap) dan tindakan (tingkah laku) mereka untuk mencapai tahap yang mencukupi dari sudut kawalan keselamatan maklumat untuk melindungi data organisasi dan rangkaian.



Rajah 2.1 Konsep kesedaran berpandukan model pengetahuan, sikap dan tingkah laku

Mempunyai pengetahuan dalam konteks kesedaran keselamatan siber bermaksud mengetahui pelbagai konsep, amalan, risiko dan akibat berkaitan keselamatan siber. Contohnya termasuklah mengetahui pelbagai jenis ancaman siber yang biasa digunakan penjenayah seperti kejuruteraan sosial, pancingan data, dan pelbagai perisian hasad. Dengan mengetahui ancaman ini, individu di dalam organisasi tersebut boleh mengenal pasti e-mel serta pautan atau lampiran di dalamnya yang mencurigakan dengan lebih baik serta mampu mengelakkan diri dari menjadi mangsa taktik penjenayah siber. Tahap pengetahuan mungkin berbeza antara satu dengan yang lain, menyebabkan wujud perbezaan di dalam tahap perlindungan keselamatan siber dari sudut pengetahuan (Madden n.d.).

Komponen sikap mempunyai peranan penting dalam kesedaran keselamatan siber. Ini kerana ia menentukan cara individu melihat serta bertindak balas terhadap sebarang potensi ancaman siber. Ia seterusnya akan menentukan tahap komitmen oleh individu terhadap amalan keselamatan dan komitmen keseluruhan mereka bagi membentuk persekitaran digital yang selamat. Sikap proaktif dan positif adalah penting bagi melindungi data, aset dan infrastruktur kritikal daripada serangan siber (Zwilling et al. 2020).

Dalam konteks kesedaran keselamatan siber, sikap positif memerlukan pengiktirafan tentang kepentingan keselamatan siber dan perasaan ingin mengambil tanggungjawab untuk menjaga keselamatan siber. Ia melibatkan sikap proaktif dalam mencari pengetahuan berterusan tentang potensi ancaman, sentiasa mengikuti perkembangan risiko baharu yang muncul, dan mengambil bahagian secara aktif dalam program latihan dan pendidikan berkaitan keselamatan siber. Dengan sikap yang positif, individu lebih cenderung untuk kemudiannya mengamalkan amalan atau tingkah laku selamat, seperti kerap mengemas kini aplikasi dan perisian, menggunakan kata laluan yang baik, dan sentiasa berhati-hati dalam berkongsi maklumat peribadi secara dalam talian (Klein 2023).

Sikap curiga juga merupakan sikap yang positif dalam konteks kesedaran keselamatan siber. Ia menyebabkan individu mempersoalkan banyak perkara yang meragukan seperti kesahihan e-mel yang diterima, laman sesawang, serta mengambil sikap berhati-hati dalam memenuhi permintaan berkaitan maklumat peribadi atau kewangan. Sikap curiga ini boleh menyelamatkan individu tersebut daripada menjadi mangsa penipuan dan manipulasi oleh penjenayah siber melalui pelbagai teknik seperti pancingan data dan kejuruteraan sosial.

Kemudian, sikap mempunyai tanggungjawab terhadap kesedaran keselamatan siber membentuk komitmen mengelak daripada tingkah laku cuai yang menjejaskan keselamatan siber. Individu yang bertanggungjawab akan berhati-hati dalam tindakan mereka, menyedari bahawa aktiviti mereka boleh memberi kesan yang meluas, bukan sahaja pada diri sendiri tetapi juga kepada individu lain. Ini termasuk seterusnya boleh mengelakkan individu daripada melibatkan diri dalam tingkah laku tidak selamat dan

berisiko seperti melayari laman sesawang yang mencurigakan atau memuat turun fail daripada sumber yang tidak dipercayai yang mungkin mengandungi perisian hasad seterusnya menyebabkan berlaku pencerobohan ke atas organisasi dan individu (Moallem 2019).

Usaha membentuk sikap positif terhadap keselamatan siber ialah usaha berterusan yang memerlukan pembelajaran berterusan, komitmen dan kesediaan untuk berubah sesuai dengan amalan dan teknologi keselamatan siber terkini. Dengan mempunyai sikap yang bertanggungjawab dan proaktif, setiap individu di dalam organisasi boleh menyumbang kepada persekitaran digital yang lebih baik dan selamat, seterusnya melindungi diri mereka, organisasi, dan komuniti daripada ancaman siber (Zwilling et al. 2020).

Dalam konteks kesedaran keselamatan siber, komponen tingkah laku merujuk kepada tabiat, atau tindakan kebiasaan yang dibuat oleh individu dan organisasi yang memberi kesan kepada risiko ancaman siber dan perlindungan data dan aset mereka. Ia merangkumi pelbagai perkara seperti pelaksanaan amalan selamat, pematuhan kepada dasar dan prosedur yang ditetapkan, dan melibatkan diri secara aktif dalam mengamalkan tingkah laku selamat di dalam semua aktiviti yang dijalankan. Tingkah laku positif berkaitan keselamatan siber adalah penting bagi mengekalkan tahap keselamatan yang kukuh serta mengurangkan kemungkinan insiden serangan siber (Kovacevic et al. 2020).

Terdapat pelbagai perkara yang boleh dianggap sebagai budaya tingkah laku positif dari sudut keselamatan siber:

1. Sentiasa mengemaskini perisian dan aplikasi. Pembekal perisian terutamanya perisian pengendalian sentiasa mengeluarkan kemaskini perisian mereka secara berkala bagi menutup eksploitasi dan kelemahan baharu yang mereka temui seterusnya mengurangkan risiko insiden keselamatan siber kepada pengguna perisian mereka (Kim 2014).

2. Menggunakan kata laluan yang kukuh, dengan membuat kata laluan panjang serta menggabungkan huruf kecil, huruf besar, nombor dan aksara khas. Usaha

ini boleh melindungi pengguna daripada cubaan pencerobohan dan penggodam perlu mengambil masa yang lebih panjang untuk memecahkan kata laluan pengguna sesuai dengan tahap kekuatan kata laluan yang digunakan. Kata laluan yang selamat juga dapat dicapai jika ia tidak digunakan di laman sesawang berbeza (Alqahtani 2022).

3. Mengamalkan amalan pelayaran laman sesawang yang baik. Risiko ancaman keselamatan siber dapat dikurangkan jika pengguna memilih laman sesawang dengan tahap keselamatan yang diperakui dan disahkan serta menggunakan perisian keselamatan yang mempunyai reputasi baik (Adholiya et al. 2019).

4. Sentiasa berwaspada dengan sebarang lampiran dan pautan yang dihantar samada melalui e-mel, media sosial atau perisian komunikasi yang lain. Ini kerana lampiran dan pautan yang dihantar mungkin mengandungi perisian hasad atau akan membawa mereka ke laman sesawang berbahaya yang mengandungi perisian hasad yang boleh mencerobohi peranti mereka tanpa disedari (Li et al. 2019).

5. Amalan berhati-hati dengan taktik kejuruteraan sosial. Penjenayah biasanya menggunakan teknik ini untuk mengumpul kelemahan individu sasaran seterusnya memanipulasi kelemahan individu tersebut dengan membuat pancingan, ugutan ataupun penyamaran bagi mencapai tujuan jahat mereka (Aldawood et al. 2018).

6. Sentiasa menjaga maklumat peribadi. Tingkah laku keselamatan siber yang baik ialah dengan tidak mendedahkan maklumat peribadi di Internet kerana maklumat tersebut boleh dicuri dan digunakan oleh pihak-pihak yang berniat jahat . Individu dengan tingkah laku keselamatan siber yang baik juga hanya akan menggunakan rangkaian wi-fi yang selamat, serta menggunakan perisian penyulitan data ketika membuat capaian Internet (ACSC. n.d).

7. Sentiasa bersedia untuk melaporkan sebarang aktiviti atau individu mencurigakan serta juga melaporkan insiden keselamatan siber, kelemahan atau potensi risiko keselamatan yang boleh dihadapi oleh organisasi. Laporan perlu

dibuat dengan kadar segera supaya kerosakan yang dihasilkan oleh sesuatu serangan siber dapat dibendung sebelum merebak menjadi lebih parah. Dengan mengamalkan budaya pelaporan ini, risiko untuk individu dan organisasi terdedah kepada ancaman siber dapat dikurangkan.

2.2 KAJIAN SEDIA ADA TENTANG KESEDARAN KESELAMATAN SIBER

Oleh kerana komuniti keselamatan siber telah memahami bahawa faktor manusia menjadi punca utama insiden keselamatan siber, semakin banyak kajian dan latihan kesedaran keselamatan siber telah dijalankan oleh pelbagai pihak termasuklah institusi pengajian, dengan matlamat meningkatkan tahap kesedaran keselamatan siber (Dodge et al. 2007)(Kumaraguru et al. 2007). Kajian oleh (Zwilling et al. 2020) mendapati bahawa pengguna Internet secara umumnya mengetahui terma "keselamatan siber" serta memahami risiko yang wujud daripada pengguna Internet dari pelbagai sudut seperti pencerobohan privasi, kerosakan peralatan, kehilangan wang, serta wujud pengawasan oleh pihak lain. Mereka juga didapati menggunakan kata laluan yang kuat serta menggunakan perisian keselamatan, namun hanya sebilangan kecil yang mempunyai pengetahuan mendalam tentang keselamatan siber.

Di Malaysia, kajian berkaitan tahap kesedaran keselamatan siber dilihat semakin mendapat perhatian berdasarkan pertambahan kajian berkaitannya yang dijalankan. Pelbagai aspek berkaitan kesedaran siber seperti keberkesanan kempen sedia ada yang dijalankan, cabaran yang dihadapi oleh pelbagai kumpulan berbeza, dan peranan institusi pendidikan di dalam meningkatkan tahap kesedaran siber di Malaysia telah dikaji.

Berdasarkan sorotan kajian yang dijalankan, kebanyakan kajian penilaian tahap kesedaran keselamatan siber yang dijalankan di Malaysia melibatkan responden dari institusi pendidikan. Ini mungkin kerana pelajar adalah kumpulan masyarakat yang mudah untuk dikaji serta mereka merupakan golongan yang mudah untuk terdedah kepada ancaman siber. Jadual 2.1 di bawah menunjukkan kajian-kajian terdahulu dan penemuan mereka berkaitan dengan penilaian tahap kesedaran keselamatan siber di Malaysia

Jadual 2.1 Kajian-kajian terdahulu dan penemuan mereka berkaitan dengan penilaian tahap kesedaran berkaitan siber di Malaysia

No.	Penyelidik & tahun kajian	Responden	Kaedah	Penemuan
1	Thang et al. (2020)	562 orang pelajar tingkatan 4 di 4 buah sekolah	Tinjauan	Umumnya mempunyai pengetahuan risiko dan bahaya penggunaan media sosial
2	Leng et al. (2020)	20 orang pengguna Internet di Lembah Klang berumur 60 tahun ke atas	Tinjauan	Mempunyai kesedaran dalam isu keselamatan siber
3	Zulkarnain et al. (2020)	Murid darjah 6 di 4 buah sekolah di Machang, Kelantan	Tinjauan	Peningkatan kesedaran keselamatan siber selepas didedahkan dengan latihan
4	Zulkifli et al. (2020)	67 orang pelajar sekolah menengah, guru, dan ibu bapa	Tinjauan	Kebanyakannya menyedari ancaman siber, tetapi hanya sedikit yang mengambil langkah keselamatan
5	Rahman et al. (2019)	98 orang pelajar di UKM	Tinjauan	Kesedaran, persepsi dan pengetahuan berkaitan keselamatan siber adalah sederhana
6	Arifin et al. (2019)	872 orang ibu bapa yang mempunyai anak berumur 17 tahun ke bawah	Tinjauan	Kesedaran ibu bapa berkaitan keselamatan siber berada pada tahap sederhana
7	Fatokun et al. (2019)	340 orang pelajar prasiswazah dan pasca siswazah institusi pengajian tinggi di Lembah Klang	Tinjauan	Jantina, umur dan tahap pendidikan memberi kesan kepada tingkah laku melibatkan keselamatan siber
8	Rahim et al. (2019)	384 orang remaja (berumur 13 hingga 19)	Tinjauan	Perlu perhatian lebih bagi pendidikan pada komponen kesedaran perlindungan data peribadi.
9	Pitchan et al. (2019)	35 orang pengguna Internet dan 6 kakitangan kerajaan	Tinjauan	Responden tidak mempunyai pengetahuan jelas tentang undang-undang siber yang ada di Malaysia
10	Markom et al. (2019)	307 orang pelajar Universiti Kebangsaan Malaysia dan Politeknik Ungku Omar	Tinjauan	Kesedaran mengenai undang-undang siber di Malaysia adalah sederhana
11	Thah et al. (2019)	1896 orang pelajar sekolah dari Malaysia dan 1336 dari Thailand	Tinjauan	Ibu bapa memainkan peranan penting dalam isu keselamatan siber kanak-kanak
12	Ahmad et al. (2018)	872 orang ibu bapa kepada kanak-kanak sekolah	Tinjauan	Tahap kesedaran keselamatan siber yang sederhana
13	Othman et al. (2018)	368 orang kakitangan akademik di tiga institut pengajian tinggi yang memperoleh persijilan ISMS (ISO/IEC 27001:2013)	Tinjauan	Kesedaran yang baik tentang keselamatan maklumat

bersambung…

…sambungan

14	Khalid et al. (2018)	142 orang pelajar UKM (Fakulti Pendidikan)	Tinjauan	Kesedaran yang tinggi dalam beberapa komponen yang dinilai tetapi kurang dalam beberapa komponen yang lain
15	Saizan et al. (2018)	231 orang calon dari German-Malaysian Institute (GMI)	Tinjauan	Mempunyai kesedaran sederhana berkaitan keselamatan siber
16	Zainudin et al. (2018)	4 orang pengurus keselamatan siber daripada empat institusi kewangan	Tinjauan	Kebanyakan responden hanya mempunyai kesedaran terhadap *Advance Persistence Threat* (ATP) melalui latihan tidak formal melalui pelbagai medium yang ada. Hasil kajian mendapati latihan tidak formal adalah lebih baik daripada latihan formal untuk meningkatkan kesedaran terhadap ATP
17	Zahri et al. (2017)	9158 orang pelajar sekolah berumur 7 – 18 tahun	Tinjauan	Secara umumnya mempunyai kesedaran keselamatan siber
18	Rani (2017)	318 orang pelajar pra-universiti	Tinjauan	Mempunyai tahap kesedaran sederhana tanpa mengira perbezaan jantina. Kesedaran yang lebih baik bagi pelajar yang mempunyai kemahiran komputer yang baik
19	Er et al. (2017)	103 orang pelajar universiti di Malaysia	Tinjauan	Mempunyai tahap kesedaran keselamatan siber yang baik
20	Muniandy et al. (2017)	128 orang pelajar kolej swasta di Malaysia	Tinjauan	Menunjukkan tingkah laku keselamatan siber yang tidak memuaskan
21	Thang et al. (2016)	4 orang pelajar sekolah menengah di sekolah elit Malaysia	Tinjauan	Secara umumnya sedar risiko dan faedah penggunaan laman sosial
22	Hasan et al. (2015)	342 orang pelajar di Universiti Teknologi Mara (Fakulti Perakaunan)	Tinjauan	Kesedaran terhadap risiko jenayah siber berbeza mengikut jantina, umur dan tahap akademik
23	Ministry of Education, CyberSecurity Malaysia and Digi (2013)	9651 orang pelajar sekolah berumur 7 – 18 tahun	Tinjauan	Tahap kesedaran yang rendah berkaitan keselamatan siber
24	Ishak et al. (2012)	400 orang awam	Tinjauan	Perempuan dan orang awam yang berpendidikan tinggi mempunyai kesedaran yang lebih baik tentang ancaman siber
25	Hazelah et al. (2011)	25 orang penduduk kota di Johor Bharu dan Petaling Jaya	Tinjauan	Kesedaran yang lemah tentang kecurian identiti

2.3 KESEDARAN TENTANG KESELAMATAN SIBER DI DALAM BIDANG KESIHATAN

Insiden keselamatan siber merupakan ancaman yang semakin banyak dihadapi oleh sektor penjagaan kesihatan terutamanya sistem kesihatan seperti hospital (Jalali et al. 2018). Walaupun implikasi insiden keselamatan siber tidak terhad kepada sektor kesihatan sahaja, namun didapati usaha melindungi data dan aset digital di dalam sektor kesihatan adalah ketinggalan berbanding sektor lain (Ahmad et al. 2021).

Dengan perkembangan teknologi yang pesat dan rekod perubatan mula disimpan secara digital secara meluas, implikasi pencerobohan data ke atas organisasi di dalam sistem kesihatan boleh menyebabkan kerosakan besar kepada organisasi, kakitangan dan pesakit dari pelbagai sudut. Walaupun pelbagai langkah dan strategi telah dilakukan bagi mengurangkan risiko pencerobohan data di sektor kesihatan, usaha pencegahan tidak berjaya sepenuhnya tanpa sokongan dan komitmen dari semua individu di dalam organisasi termasuklah profesional kesihatan yang berkhidmat. Ini kerana faktor manusia juga memainkan peranan di dalam perlindungan dari ancaman keselamatan siber (Nifakos et al. 2021).

Salah satu ancaman utama kepada rekod kesihatan elektronik adalah kesilapan manusia. Pelanggaran selepas pelaksanaan rekod kesihatan elektronik oleh organisasi kesihatan kebanyakannya berlaku disebabkan oleh tahap kesedaran yang rendah dan ketidakpedulian kakitangannya berbanding disebabkan oleh aktiviti berniat jahat (Kim et al. 2019). Dalam sektor kesihatan, pendedahan maklumat sulit yang tidak disengajakan adalah perkara yang biasa dan selalu berlaku (PwC 2014). Risiko insiden keselamatan siber boleh dikurangkan dengan program latihan kesedaran keselamatan siber (Hockey et al. 2020).

Kajian oleh Coventry et al. (2020) mendapati bahawa tahap kesedaran yang rendah adalah perkara biasa dalam organisasi kesihatan dan merupakan salah satu faktor utama yang menyumbang kepada tujuh tingkah laku tidak selamat iaitu kelemahan akaun pengguna dan keselamatan komputer, kelemahan penggunaan capaian jarak jauh, amalan kaedah penyulitan yang lemah, simpanan fail dan kemas kini yang lemah, keselamatan capaian fizikal yang lemah, capaian peranti perubatan yang tidak selamat,

dan amalan e-mel yang tidak selamat. Isu ini lebih kritikal kerana responden menunjukkan bahawa mereka juga kurang mendapat latihan kesedaran keselamatan siber. Ini adalah kajian kualitatif yang melibatkan beberapa sesi dengan 50 kakitangan penjagaan kesihatan dari tiga buah negara berbeza iaitu Ireland, Itali dan Greece.

Kajian selanjutnya yang dijalankan oleh Gioulekas et al. (2022) mendapati bahawa terdapat keperluan untuk mewujudkan jabatan atau unit yang membuat pemantauan tahap keselamatan siber berkaitan individu dan aset di fasiliti kesihatan secara berterusan disamping menjadikan program latihan sebagai keutamaan dan dasar yang penting. Perkara ini dapat mengurangkan risiko pencerobohan data di institusi kesihatan kerana pencerobohan data di fasiliti kesihatan terutamanya hospital adalah berkait rapat dengan tahap kesedaran keselamatan siber kakitangannya yang lemah.

Kajian keratan rentas oleh Balaji et al. (2019) yang melibatkan 45 doktor di India menggunakan soal selidik mendapati bahawa tiada perbezaan diantara doktor di bandar dan di pedalaman dari sudut kesedaran keselamatan siber. Namun, hasil kajian mendapati bahawa anggota kesihatan perlu menambah baik pengetahuan dan kesedaran keselamatan siber. Walau bagaimanapun, kajian ini mempunyai limitasi saiz sampel yang kecil.

2.4 KESIMPULAN

Kesimpulannya, kajian literasi mendapati bahawa kurangnya kajian berkaitan kesedaran keselamatan siber di Malaysia berkaitan anggota kesihatan walaupun didapati bahawa sektor kesihatan mempunyai risiko yang tinggi untuk mendapat ancaman keselamatan siber disebabkan oleh kurangnya kesedaran dikalangan petugas kesihatan dan ganjaran lumayan yang boleh diperolehi oleh penjenayah hasil daripada pencerobohan data dan aset yang dilakukan.

BAB III

KAEDAH KAJIAN

3.1 PENGENALAN

Kaedah kajian atau metodologi merupakan elemen penting bagi setiap kajian. Ia menjelaskan pendekatan yang diambil secara sistematik dan terperinci di dalam penyelesaian masalah atau persoalan yang ada di dalam kajian tersebut. Sesuatu kaedah kajian mestilah sesuai dengan objektif kajian, pernyataan masalah dan sumber yang ada. Ini bagi memastikan sesuatu isu yang dikaji dapat disiasat dengan sebenar berdasarkan kaedah kajian yang dipilih, seterusnya menterjemahkan isu-isu yang kompleks ke bentuk yang mudah difahami untuk perbincangan selanjutnya.

Kaedah kajian yang jelas dan sesuai adalah penting bagi memastikan sesuatu kajian itu mempunyai tahap kebolehpercayaan dan kesahihan yang tinggi, serta memastikan sebarang bias atau kesilapan dapat dikesan seterusnya diminimumkan. Dalam bab ini, beberapa komponen kepada kaedah kajian iaitu reka bentuk kajian, instrumen pengumpulan data dan teknik analisis akan dijelaskan.

3.2 PEMILIHAN MODEL SOAL SELIDIK

Tidak ada alat pengukuran piawai untuk mengukur tingkah laku keselamatan siber pengguna akhir (Egelman et al. 2015). Terdapat model kajian yang ditaja oleh penyedia perkhidmatan keselamatan siber menyebabkan percanggahan motif iaitu terdapat kecenderungan soalan yang ditanya menyebabkan sesuatu isu itu terlebih lapor dan isu yang lain kurang dilaporkan. Terdapat para pengkaji sebelum ini yang menggunakan model tingkah laku seperti teori pencegahan secara am, teori motivasi perlindungan, dan tingkah laku berancangan bagi memahami komponen kesedaran keselamatan siber

namun teori-teori yang digunakan tidak menyeluruh kerana terdapat pemboleh ubah yang diabaikan (Parsons et al. 2014).

Teori pencegahan secara am atau *General Deterrence Theory* menerangkan bahawa hukuman yang berat dan tindakan undang-undang yang ketat dapat mengawal seseorang individu dari melakukan jenayah. Ketakutan seseorang terhadap akibat dari hukuman yang berat menjadi elemen penting dalam mengelakkan mereka dari menjadi penjenayah (Nagin et al. 1993).

Teori motivasi perlindungan atau *Protection Motivation Theory* ialah satu lagi teori psikologi yang menerangkan bahawa tindakan perlindungan dan pencegahan seseorang adalah berkait rapat dengan tahap anggapan mereka terhadap ancaman dari sudut kesejahteraan, kesihatan dan hidup mereka. Terdapat empat faktor utama yang dinilai di dalam teori ini iaitu ancaman, penilaian ancaman, penilaian perlindungan dan motivasi diri (Floyd et al. 2000). Teori tingkah laku berancangan atau *Theory of Planned Behaviour* (TPB) pula menerangkan tingkah laku manusia adalah berdasarkan niat, yang berkait rapat dengan tiga faktor utama iaitu sikap, norma subjektif dan kawalan perilaku (Armitage et al. 2001).

Terdapat juga para pengkaji sebelum ini yang menggunakan soalan secara umum bagi mendapatkan maklum balas tahap kesedaran keselamatan siber yang menyebabkan terdapat kecenderungan untuk maklum balas bersifat berat sebelah. Kajian-kajian terkini pula ada yang bersifat lebih menyeluruh dan menjurus kepada komponen kesedaran keselamatan siber iaitu pengetahuan, sikap dan tingkah laku contohnya Galba et al. (2015) yang menghasilkan "Users' Information Security Awareness Questionnaire (UISAQ)". Egelman et al. (2015) pula telah mencadangkan "The Security Behavior Intentions Scale (SeBIS)" manakala Ögütçü et al. (2016) pula telah menghasilkan model yang terdiri daripada empat skala utama.

Parsons et al. (2017) pula telah menghasilkan Human Aspects of Information Security Questionnaire (HAIS-Q) yang telah digunakan untuk penilaian tahap kesedaran keselamatan siber dari sudut pengetahuan, sikap dan tingkah laku bagi pelbagai populasi penduduk di Australia. Setelah meneliti kesemua model yang

dinyatakan, kami mendapati model yang dipilih mestilah bersifat menyeluruh dan menjurus kepada kriteria kesedaran keselamatan siber yang terkini iaitu pengetahuan, sikap dan tingkah laku. Didapati model HAIS-Q adalah yang paling sesuai untuk kajian ini kerana lebih mudah dan sesuai untuk mengukur tahap kesedaran siber responden dan telah mempunyai instrumen soal selidik kajian yang telah disahkan yang boleh dijadikan sebagai sandaran.

HAIS-Q mempunyai tujuh topik tumpuan yang setiap daripadanya terbahagi pula kepada tiga topik pecahan yang menilai komponen pengetahuan, sikap dan tingkah laku responden. Tujuh topik tersebut ialah pengurusan kata laluan, penggunaan e-mel, penggunaan Internet, pengurusan maklumat, penggunaan media sosial, penggunaan peranti mudah alih dan pelaporan insiden. Pemilihan tujuh topik tumpuan ini adalah berdasarkan hasil temuduga bersama pakar keselamatan siber, soal selidik keselamatan siber dan dokumen polisi keselamatan siber yang mendapati bahawa ini adalah topik yang sering menjadi punca pencerobohan data dan aset di sesuatu organisasi dan paling berkait rapat dengan kesedaran keselamatan siber individu di dalam organisasi.

Namun, bagi kajian ini, jumlah soalan di dalam soal selidik asal perlu dihadkan supaya sesuai dengan para responden agar mereka sentiasa memberi sepenuh perhatian dan tidak berasa bosan seterusnya memastikan jawapan yang diberi adalah berkualiti dan mencerminkan situasi sebenar. Kajian oleh Rips et al. (2008) mendapati bahawa menggunakan jumlah soalan yang terlalu banyak di dalam soal selidik boleh menyebabkan jawapan yang diberi oleh responden kurang tepat dan tidak konsisten. Maka adalah penting untuk menyediakan soal selidik yang bersesuaian dengan kumpulan responden yang bakal terlibat di dalam kajian ini kerana mereka menjawab soal selidik secara kendiri dan tidak di dalam persekitaran tertutup.

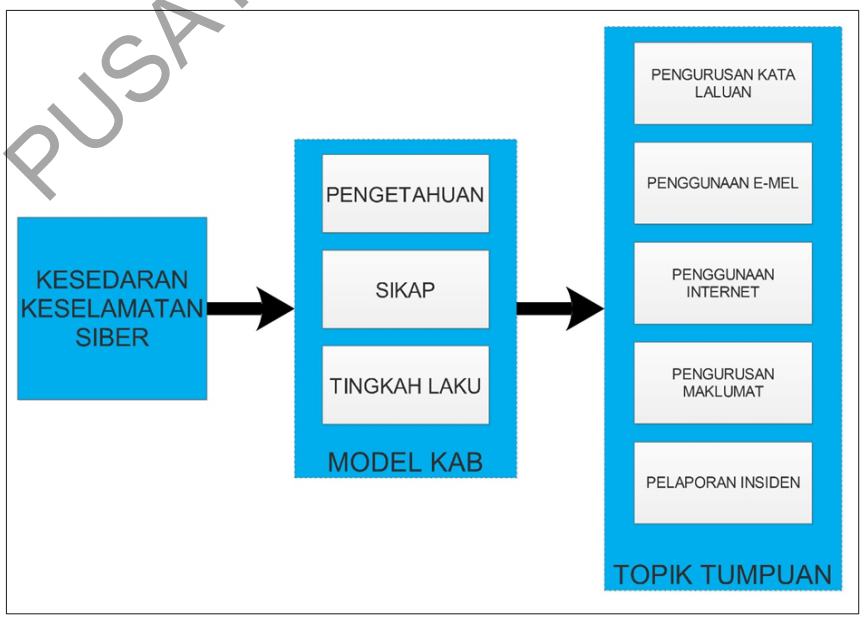
3.3 REKA BENTUK KAJIAN

Kajian ini menggunakan kaedah kuantitatif kerana ia lebih sesuai untuk mengkaji responden yang ramai dalam tempoh yang terhad serta masih menepati objektif kajian. Data akan di kumpul daripada responden menggunakan borang soal selidik sebelum ia dianalisis. Tiga bentuk soalan boleh dihasilkan melalui soal selidik iaitu soalan terbuka,

betul atau salah, dan pilihan jawapan pelbagai (Agresti 2018). Soalan yang panjang dan kompleks boleh menyebabkan responden hilang tumpuan dan minat seterusnya menyebabkan mereka tidak menjawab soalan dengan sebaiknya yang boleh menjejaskan soal selidik yang dijalankan (Bradburn et al. 2004). Kajian juga mendapati bahawa penggunaan bentuk soalan betul atau salah dan pilihan jawapan pelbagai secara umumnya adalah lebih baik daripada bentuk soalan terbuka (Groves et al. 2011) bagi tujuan mendapatkan data yang lebih mudah dianalisis menggunakan kaedah statistik.

Soalan-soalan di dalam borang soal selidik juga terbahagi kepada dua bahagian. Bahagian pertama berkait dengan maklumat demografi responden manakala bahagian kedua adalah berkait dengan penilaian tahap kesedaran keselamatan siber mereka. Bagi bahagian kedua, tiga kriteria penilaian kesedaran seperti yang dibincangkan sebelum ini akan turut dimasukkan iaitu pengetahuan, tingkah laku dan sikap (Kruger et al. 2006).

Bagi memastikan soalan-soalan yang dihasilkan adalah berkualiti dan menepati keperluan kajian, reka bentuk awal soalan-soalan adalah berasaskan daripada model HAIS-Q (Parsons et al. 2017) yang telah mempunyai soalan-soalan yang telah disahkan. Soalan yang dihasilkan kemudiannya dirujuk kepada pakar bagi mendapatkan maklum balas dan proses pengesahan.



Rajah 3.1 Rangka kerja penilaian tahap kesedaran keselamatan siber

Setelah borang soal selidik disahkan, kajian rintis dijalankan kepada beberapa ahli farmasi swasta yang terpilih. Kajian rintis ini penting bagi memastikan sebarang kelemahan dan isu yang timbul ketika proses pengumpulan data dapat dikenal pasti dan bagi mengesahkan kebolehpercayaannya, pekali kebolehpercayaan digunakan berdasarkan kaedah "Cronbach's Alpha". Interpretasi kepada nilai Cronbach's Alpha adalah mengikut kajian oleh Devellis (2016) seperti jadual 3.1 di bawah.

Jadual 3.1 Intepretasi kepada nilai Cronbach Alpha

No.	Nilai Chronbach Alpha (α)	Kesimpulan Kebolehpercayaan
1	α > 0.90	Skala terlalu besar
2	α 0.80 – 0.90	Sangat baik
3	α 0.70 – 0.80	Boleh diterima
4	α 0.65 – 0.70	Kurang diterima
5	α 0.60 – 0.65	Tidak diingini
6	α < 0.60	Ditolak

Hasil kajian rintis yang dijalankan pula adalah seperti jadual 3.2 di bawah. Didapati nilai terendah yang diperolehi ialah 0.75 bagi komponen utama pengurusan maklumat manakala nilai tertinggi yang diperolehi ialah 0.875 bagi komponen utama penggunaan Internet. Nilai yang diperolehi ini juga adalah didapati tidak jauh dari nilai Cronbach Alpha yang diperolehi dari kajian asal HAIS-Q dari kajian oleh Parsons et al. (2017). Maka, instrumen kajian ini bolehlah digunakan di dalam kajian sebenar kepada responden.

Jadual 3.2 Nilai Cronbach Alpha Instrumen Kajian

Komponen Utama Soal Selidik	Jumlah Item	Nilai Chronbach Alpha (α)	Kebolehpercayaan
Pengurusan kata laluan	3	0.824	Sangat baik
Penggunaan e-mel	3	0.804	Sangat baik
Penggunaan Internet	3	0.875	Sangat baik
Pengurusan maklumat	3	0.750	Boleh diterima
Pelaporan insiden keselamatan siber	3	0.814	Sangat baik

Kajian sebenar dimulakan selepas hasil daripada kajian rintis tersebut diperolehi dan dianalisis. Soalan kaji selidik diedarkan secara dalam talian melalui pautan pada perisian WhatsApp kepada responden yang akan membawa kepada soal selidik yang disediakan menggunakan perisian Google Form. Penggunaan perisian ini memudahkan kajian kerana capaian kepada responden dan proses pengumpulan data dapat dibuat secara lebih mudah, cepat, selamat dan menjimatkan kos.

3.4 POPULASI DAN SAMPEL KAJIAN

Populasi bagi kajian ini adalah ahli farmasi komuniti di Kelantan yang dianggarkan seramai 187 orang (KKM 2023). Menggunakan formula Cochrane (Bartlett 2001) dengan margin ralat 5%, tahap keyakinan 95%, saiz sampel minimum yang diperlukan ialah 126 orang. Teknik pensampelan secara mudah digunakan di dalam kajian ini.

3.5 KESIMPULAN

Secara kesimpulan, bab ini menerangkan mengapa kaedah kuantitatif dipilih serta bagaimana proses-proses penghasilan metodologi dan instrumen kajian yang sesuai dijalankan sebelum ia digunakan di dalam kajian ini. Hasil dari ujian rintis pula mendapati bahawa instrumen yang digunakan mempunyai tahap kebolehpercayaan yang baik. Bilangan sampel minimum yang diperlukan daripada populasi kajian telah ditentukan bagi memastikan kajian ini mempunyai tahap keyakinan yang tinggi.

BAB IV

HASIL KAJIAN

4.1 PENGENALAN

Di dalam bab ini, analisis dilakukan terhadap maklum balas responden yang diterima melalui soal selidik yang dijalankan sebelum ini. Data yang diperolehi dianalisis dengan menggunakan rumusan perisian Google Forms, perisian SPSS versi 26 dan perisian Microsoft Excel.

Hasil analisis kemudiannya di buat penilaian berdasarkan nilai min yang diperolehi seperti jadual 4.1 di bawah yang diubahsuai dari kajian Mahamod (2012).

Jadual 4.1 Penilaian tahap kesedaran keselamatan siber

Nilai Min	Penilaian tahap kesedaran
1.0 – 1.5	Kurang kesedaran yang serius
1.5 – 2.5	Kurang kesedaran
2.5 – 3.5	Kesedaran yang sederhana
3.5 – 4.5	Kesedaran yang baik
4.5 – 5.0	Kesedaran yang sangat baik

4.2 TATACARA PEMERIKSAAN DAN ANALISIS DATA

Seramai lima puluh sembilan (59) orang responden telah bersetuju untuk memberi maklum balas di dalam kajian ini melalui borang soal selidik yang dibangunkan melalui perkhidmatan Google Forms yang diedarkan secara manual kepada ahli farmasi komuniti di negeri Kelantan. Jumlah ini sebenarnya tidak mencapai sasaran minimum yang ditetapkan iaitu sebanyak 126 orang. Namun, berdasarkan populasi ahli farmasi komuniti yang terhad dan unik kerana tidak pernah dikaji sebelum ini, dijangka bahawa

kajian ini tetap memberi impak dan manfaat kepada hasil kajian yang diharapkan terutamanya di dalam menjadi asas kepada kajian seterusnya berkaitan populasi tersebut. Kajian ini juga penting di dalam mendapatkan maklumat asas berkaitan ahli farmasi komuniti seterusnya merangka tindakan penambahbaikan seterusnya berkaitan keselamatan siber.

Rajah 4.1 Persetujuan responden untuk terlibat di dalam kajian

Maklumat yang diperolehi dari responden melalui perisian Google Forms kemudiannya dipindahkan ke dalam perisian Microsoft Excel sebelum dipindahkan sekali lagi untuk analisis menggunakan perisian SPSS versi 26. Penelitian mendapati bahawa tiada *missing value* dikesan kerana responden tidak dapat melengkapkan soal selidik jika terdapat soalan yang tidak dijawab. Data yang diperolehi melalui soal selidik yang dijalankan adalah dari dua kategori iaitu nominal dan ordinal. Data nominal tidak dapat diukur menggunakan skala dan ia terhad kepada soalan berkaitan maklumat asas dan demografi responden. Data ordinal pula terdapat di dalam 5 komponen utama soal selidik yang bertujuan untuk menilai tahap pengetahuan, sikap dan tingkah laku responden yang ingin dikaji.

Di dalam kajian ini, data ordinal adalah diambil menggunakan skala Likert 5 mata, dengan ketetapan berikut iaitu 1 = Sangat tidak setuju, 2 = Tidak setuju, 3 = Setuju atau Tidak Setuju, 4 = Setuju, dan 5 = Sangat Setuju. Walaupun ia diasaskan pada tahun 1932 (Likert 1932), skala Likert masih digunakan secara meluas dan dipilih bagi kajian ini kerana ia sesuai dengan jenis kajian yang dijalankan. Responden perlu memilih

jawapan yang dirasakan sesuai yang menggambarkan diri mereka. Jawapan responden menggunakan skala ini kemudiannya diterjemahkan ke dalam bentuk numerik 1 hingga 5 untuk proses analisis. Bagi mengurangkan bias dan memastikan responden membaca dahulu soalan sebelum memberi jawapan, beberapa soalan iaitu B2, C1, C2, C3, D1, D2, D3 dan F2 telah diolah secara negatif, bermakna pengiraan skala perlu dibuat secara reverse coding.

Bagi mengelakkan kekeliruan, cara pengiraan reverse coding perlu diterangkan di dalam kajian ini. Jika pengiraan biasa hanya menukar data ordinal maklumbalas responden dari skala Likert 5 point kepada nilai 1-5 yang bersamaan dengan skala tersebut, pengiraan reverse coding dibuat dengan cara menukar maklumbalas responden dari skala Likert 5 point kepada nilai 1-5 secara terbalik. Nilai akhir tersebut boleh diperolehi dengan cara pengiraan matematik iaitu menolak nilai asal yang diperolehi dari skala Likert 5 point dengan nilai 6 (nilai maximum 5 ditambah dengan 1). Contohnya soalan B2 yang bersifat negatif, nilai min asal yang diperolehi daripada maklumbalas semua 59 orang responden ialah 1.593, namun ia perlu ditukar dengan cara pengiraan 6 - 1.593 menjadikan nilai akhirnya 4.4068. Penentuan nilai akhir bagi semua komponen soalan di dalam kajian ini adalah seperti yang ditunjukkan di dalam jadual 4.2 dibawah:

Jadual 4.2 Penentuan nilai bagi semua komponen soalan

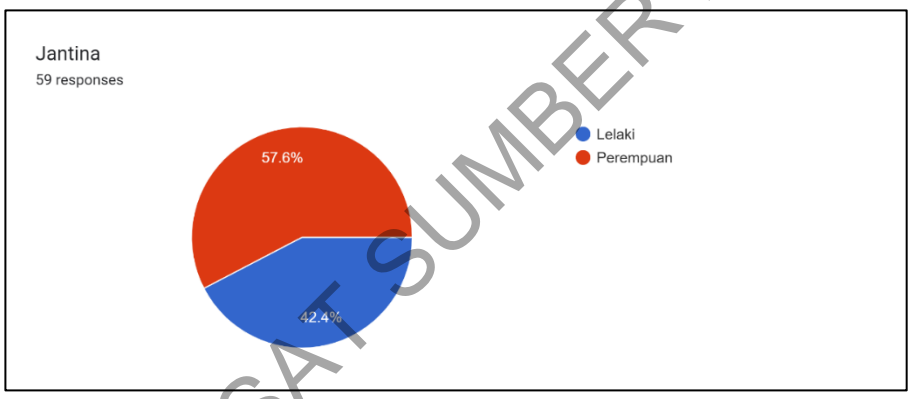
Soalan	Bentuk Olahan Soalan	Nilai Min Skala Likert 5 poin	Nilai Min akhir untuk analisis	Perubahan Nilai
B1	Positif	4.1186	4.1186	Tiada
B2	Negatif	1.5930	4.4068	Berubah
B3	Positif	4.6441	4.6441	Tiada
C1	Negatif	2.2540	3.7458	Berubah
C2	Negatif	1.8480	4.1525	Berubah
C3	Negatif	1.3560	4.6441	Berubah
D1	Negatif	3.3034	2.9661	Berubah
D2	Negatif	2.8640	3.1356	Berubah
D3	Negatif	2.6950	3.3051	Berubah
E1	Positif	4.4407	4.4407	Tiada
E2	Positif	4.6949	4.6949	Tiada
E3	Positif	4.8305	4.8305	Tiada
F1	Positif	4.7119	4.7119	Tiada
F2	Negatif	1.1695	4.8305	Berubah
F3	Positif	4.4407	4.4407	Tiada

4.3 ANALISIS DATA

4.3.1 Analisis Demografi Responden

Demografi responden adalah penting bagi menentukan latar belakang responden yang terlibat di dalam kajian ini. Ia membantu pengkaji mendapatkan gambaran lebih jelas serta membuat perbandingan diantara responden yang terlibat berdasarkan perbezaan demografi. Di dalam kajian ini, maklumat demografi yang diukur dan dinilai ialah jantina, umur, tahap Pendidikan tertinggi, tempoh berkhidmat sebagai ahli farmasi komuniti, dan samada responden pernah menerima latihan berkaitan keselamatan siber. Hasil analisis adalah seperti berikut:

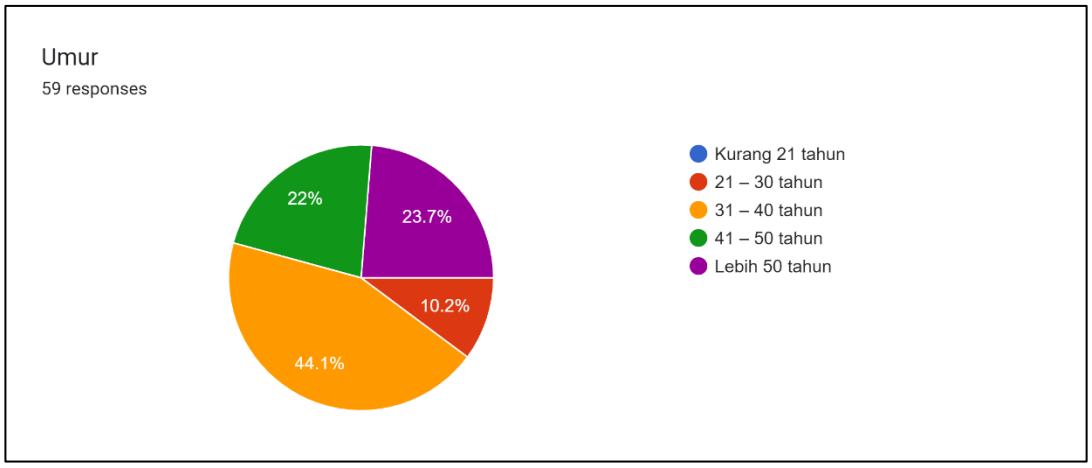
a. Jantina



Rajah 4.2 Jantina responden

Majoriti responden yang menjawab soal selidik bagi kajian ini ialah wanita iaitu seramai 34 orang manakala 25 orang adalah lelaki.

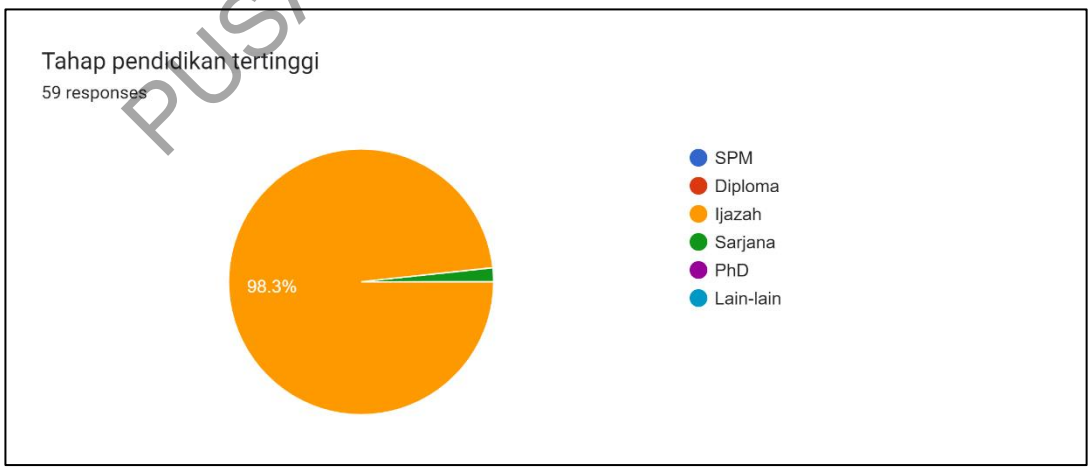
b. Umur



Rajah 4.3 Umur responden

Tiada responden berumur kurang 21 tahun kerana umur normal untuk seseorang memperoleh ijazah sarjana muda farmasi ialah lingkungan 22 tahun. 6 orang berumur 21-30 tahun. Majoriti responden yang menjawab soal selidik bagi kajian ini ialah yang berumur diantara 31-40 tahun iaitu seramai 26 orang. 13 orang berumur diantara 41-50 tahun. Jumlah kedua terbesar iaitu seramai 14 orang (23.7%) responden berumur lebih 50 tahun.

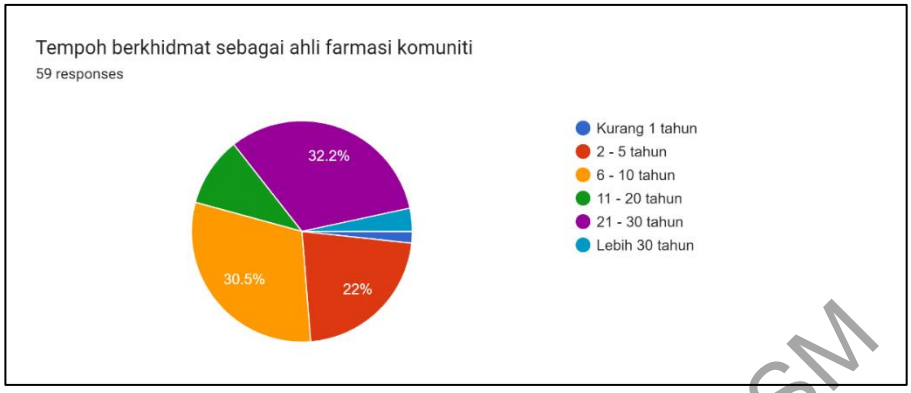
c. Tahap Pendidikan Tertinggi



Rajah 4.4 Tahap pendidikan tertinggi responden

Hampir semua responden mempunyai pendidikan tertinggi di peringkat ijazah, manakala hanya seorang yang melalui pendidikan di peringkat sarjana.

d. Tempoh Berkhidmat Sebagai Ahli Farmasi Komuniti



Rajah 4.5 Tempoh responden berkhidmat sebagai ahli farmasi komuniti

Pertambahan jumlah ahli farmasi di Malaysia pada beberapa tahun yang lepas telah menyebabkan semakin banyak farmasi komuniti di buka di seluruh Kelantan. Lebih separuh daripada responden iaitu seramai 31 orang telah berkhidmat sebagai ahli farmasi komuniti kurang dari 11 tahun iaitu seorang dalam masa setahun, 13 orang diantara 2-5 tahun, dan 18 orang diantara 6-10 tahun. 6 orang telah berkhidmat diantara 11-20 tahun. 10 orang telah berkhidmat diantara 21-30 tahun, manakala hanya 2 orang mempunyai pengalaman berkhidmat lebih 30 tahun di farmasi komuniti.

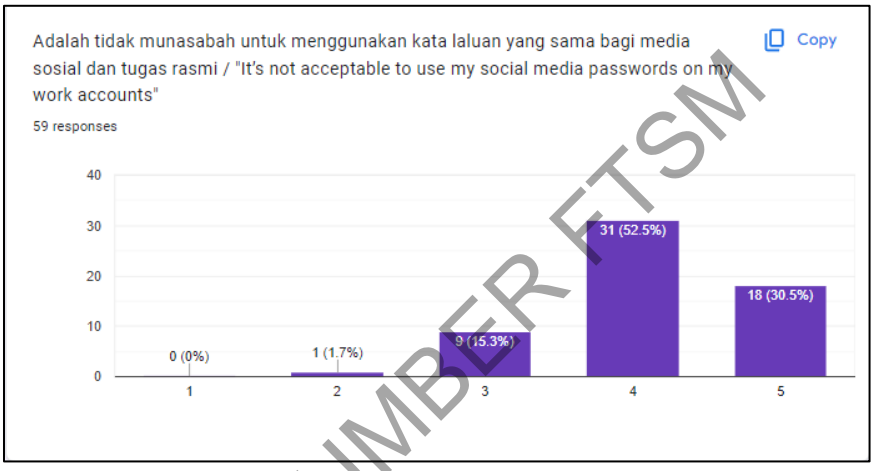
e. Pernah menerima latihan atau penerangan berkaitan keselamatan siber

Rajah 4.6 Pengalaman latihan responden berkaitan keselamatan siber

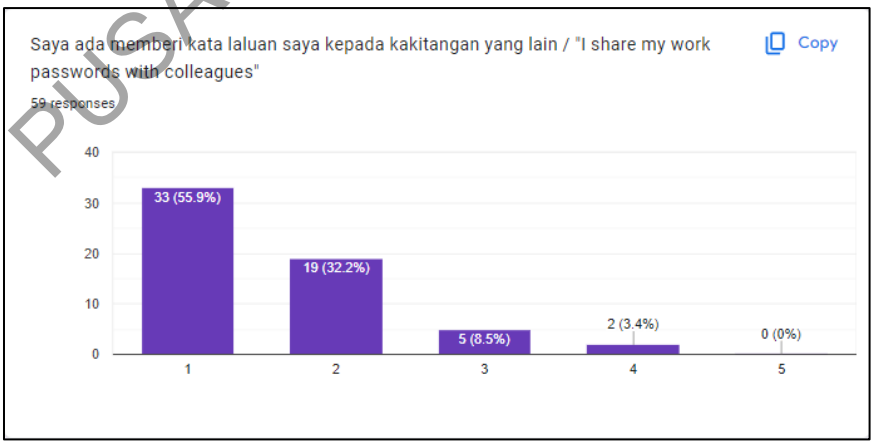
Hasil tinjauan mendapati hanya 4 orang responden pernah menerima latihan berkaitan keselamatan siber manakala selebihnya iaitu 55 orang tidak pernah mendapat sebarang latihan berkaitan keselamatan siber.

4.3.2 Analisis Berkaitan Pengurusan Kata Laluan

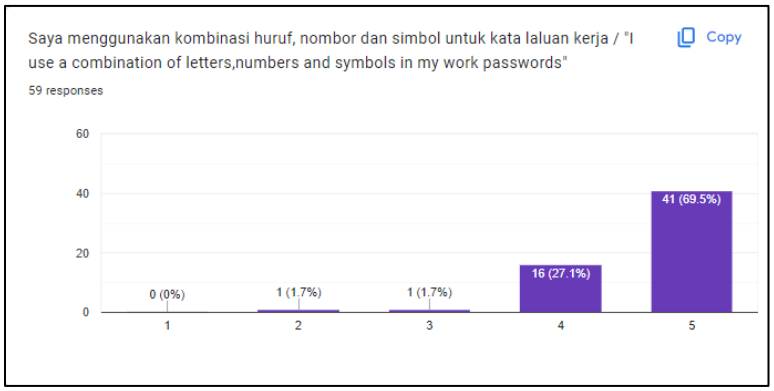
Hasil maklumbalas responden bagi komponen utama pengurusan kata laluan adalah seperti rajah 4.7, 4.8, dan 4.9 dibawah:



Rajah 4.7 Maklumbalas responden bagi soalan komponen B1



Rajah 4.8 Maklumbalas responden bagi soalan komponen B2



Rajah 4.9 Maklumbalas responden bagi soalan komponen B3

Analisis pada hasil soal selidik bagi pengurusan kata laluan seperti jadual 4.3 mendapati min purata bagi nilai semua komponen ialah 4.389831 menjadikan tahap kesedaran ahli farmasi komuniti berada pada tahap 4 iaitu baik. Komponen B1 menunjukkan nilai min terendah (4.1186) berbanding komponen lain iaitu B2 (4.4068) dan B3 (4.6441).

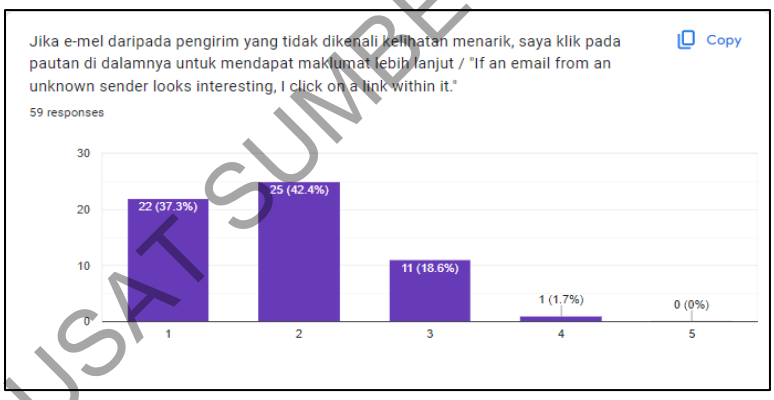
Jadual 4.3 Analisis pengurusan kata laluan

Soalan	Pernyataan	1	2	3	4	5	Nilai Min	Penilaian
B1	Adalah tidak munasabah untuk menggunakan kata laluan yang sama bagi media sosial dan tugas rasmi	0 (0%)	1 (1.7%)	9 (15.3%)	31 (52.5%)	18 (30.5%)	4.1186	Baik
B2 (RC)	Saya ada memberi kata laluan saya kepada kakitangan yang lain	0 (0%)	2 (3.4%)	5 (8.5%)	19 (32.2%)	33 (55.9%)	4.4068	Baik
B3	Saya menggunakan kombinasi huruf, nombor dan simbol untuk kata laluan kerja	0 (0%)	1 (1.7%)	1 (1.7%)	16 (27.1%)	41 (69.5%)	4.6441	Sangat Baik
						Purata	4.389831	Baik

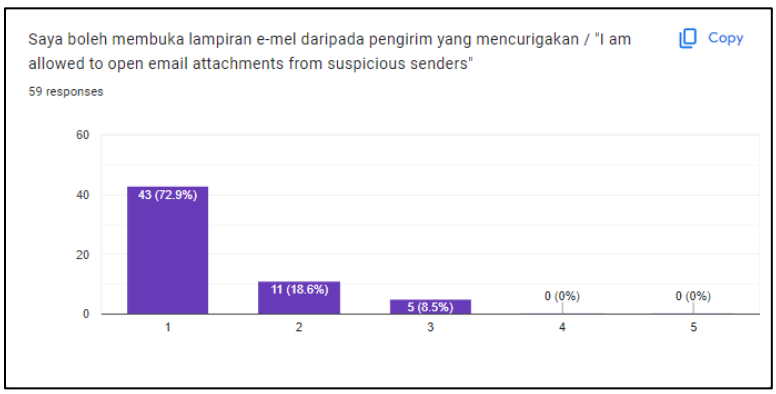
4.3.3 Analisis Berkaitan Penggunaan E-mel

Hasil maklumbalas responden bagi komponen utama penggunaan e-mel adalah seperti rajah 4.10, 4.11, 4.12 dibawah:

Rajah 4.10 Maklumbalas responden bagi soalan komponen C1



Rajah 4.11 Maklumbalas responden bagi soalan komponen C2



Rajah 4.12 Maklumbalas responden bagi soalan komponen C3

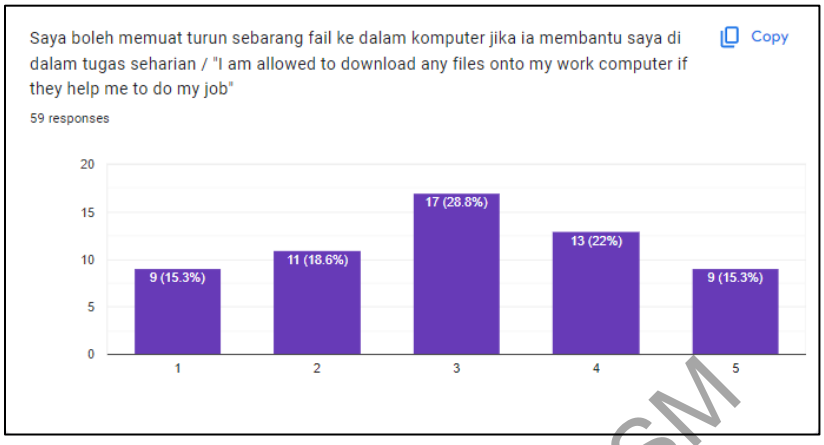
Analisis pada hasil soal selidik bagi penggunaan e-mel seperti jadual 4.4 mendapati bahawa min purata bagi nilai semua komponen ialah 4.180791 menjadikan tahap kesedaran ahli farmasi komuniti berada pada tahap 4 iaitu baik. Komponen C1 menunjukkan nilai min terendah (3.7458) berbanding komponen lain iaitu C2 (4.1525) dan C3 (4.6441).

Jadual 4.4 Analisis penggunaan e-mel

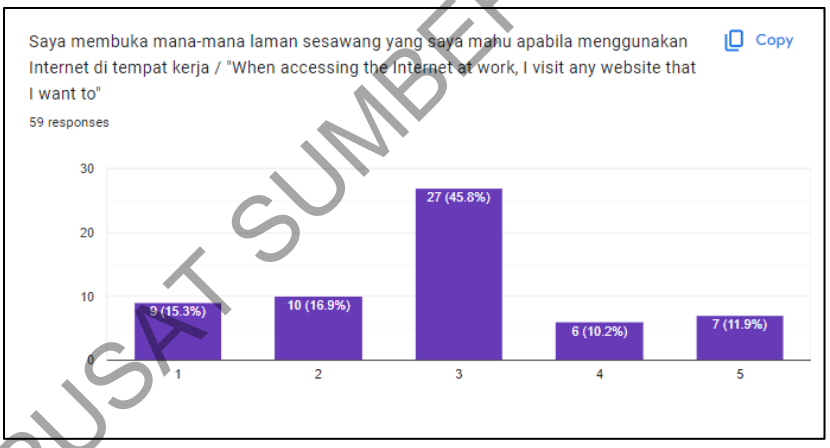
Soalan	Pernyataan	1	2	3	4	5	Nilai Min	Penilaian
C1 (RC)	Adalah sentiasa selamat untuk mengklik pautan dalam e-mel daripada orang yang dikenali	1 (1.7%)	2 (3.4%)	23 (39%)	18 (30.5%)	15 (25.4%)	3.7458	Baik
C2 (RC)	Jika e-mel daripada pengirim yang tidak dikenali kelihatan menarik, saya klik pada pautan di dalamnya untuk mendapat maklumat lebih lanjut	0 (0%)	1 (1.7%)	11 (18.6%)	25 (42.4%)	22 (37.3%)	4.1525	Baik
C3 (RC)	Saya boleh membuka lampiran e-mel daripada pengirim yang mencurigakan	0 (0%)	0 (0%)	5 (8.5%)	11 (18.6%)	43 (72.9%)	4.6441	Sangat Baik
						Purata	4.180791	Baik

4.3.4 Analisis Berkaitan Penggunaan Internet

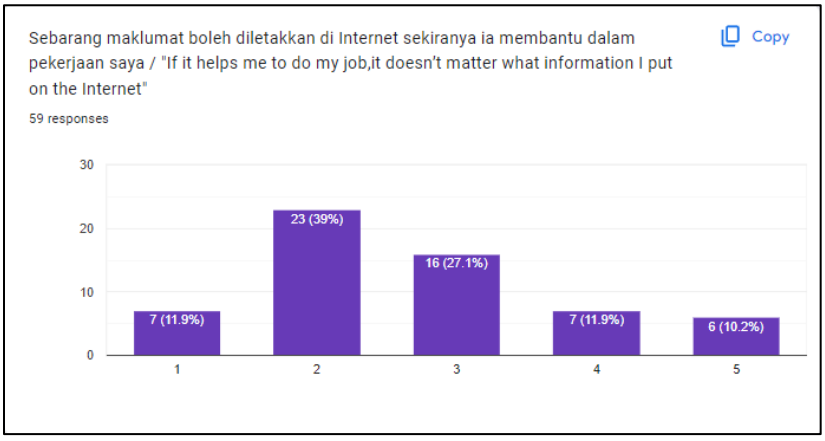
Hasil maklumbalas responden bagi komponen utama penggunaan Internet adalah seperti rajah 4.13, 4.14, 4.15 dibawah:



Rajah 4.13 Maklumbalas responden bagi soalan komponen D1



Rajah 4.14 Maklumbalas responden bagi soalan komponen D2



Rajah 4.15 Maklumbalas responden bagi soalan komponen D3

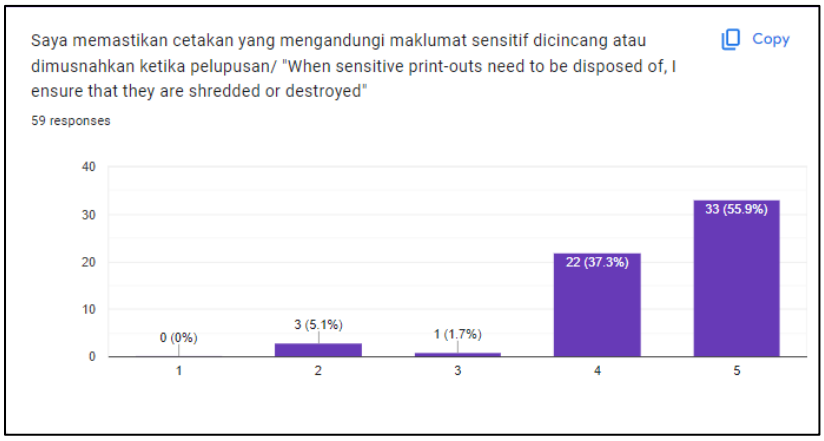
Analisis pada hasil soal selidik bagi penggunaan Internet seperti di jadual 4.5 mendapati bahawa min purata bagi nilai semua komponen ialah 3.135593 menjadikan tahap kesedaran ahli farmasi komuniti berada pada tahap 3 iaitu sederhana. Komponen D1 menunjukkan nilai min terendah (2.9661) berbanding komponen lain iaitu D2 (3.1356) dan D3 (3.3051).

Jadual 4.5 Analisis penggunaan Internet

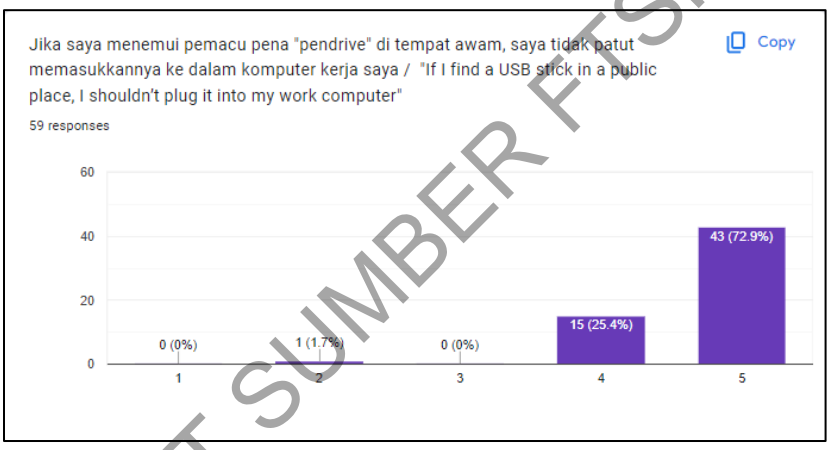
Soalan	Pernyataan	1	2	3	4	5	Nilai Min	Penilaian
D1 (RC)	Saya boleh memuat turun sebarang fail ke dalam komputer jika ia membantu saya di dalam tugas seharian	9 (15.3%)	13 (22%)	17 (28.8%)	11 (18.6%)	9 (15.3%)	2.9661	Sederhana
D2 (RC)	Saya membuka mana-mana laman sesawang yang saya mahu apabila menggunakan Internet di tempat kerja	7 (11.9%)	6 (10.2%)	27 (45.8%)	10 (16.9%)	9 (15.3%)	3.1356	Sederhana
D3 (RC)	Sebarang maklumat boleh diletakkan di Internet sekiranya ia membantu dalam pekerjaan saya	6 (10.2%)	7 (11.9%)	16 (27.1%)	23 (39%)	7 (11.9%)	3.3051	Sederhana
						Purata	3.135593	Sederhana

4.3.5 Analisis Berkaitan Pengurusan Maklumat

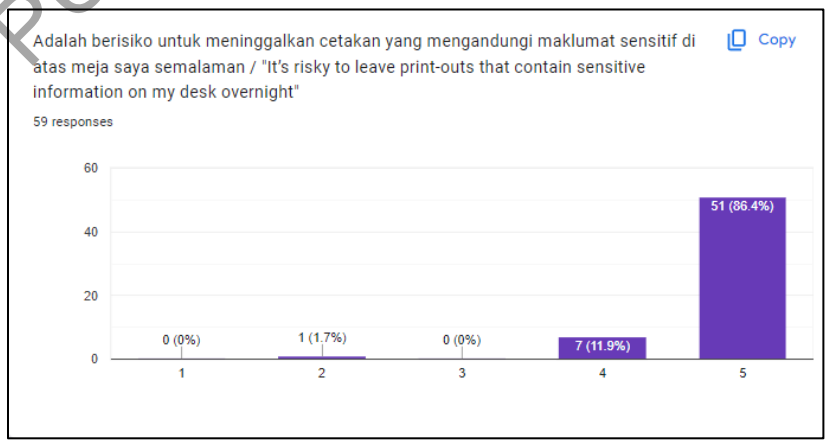
Hasil maklumbalas responden bagi komponen utama pengurusan maklumat adalah seperti rajah 4.16, 4.17, 4.18 dibawah:



Rajah 4.16 Maklumbalas responden bagi soalan komponen E1



Rajah 4.17 Maklumbalas responden bagi soalan komponen E2



Rajah 4.18 Maklumbalas responden bagi soalan komponen E3

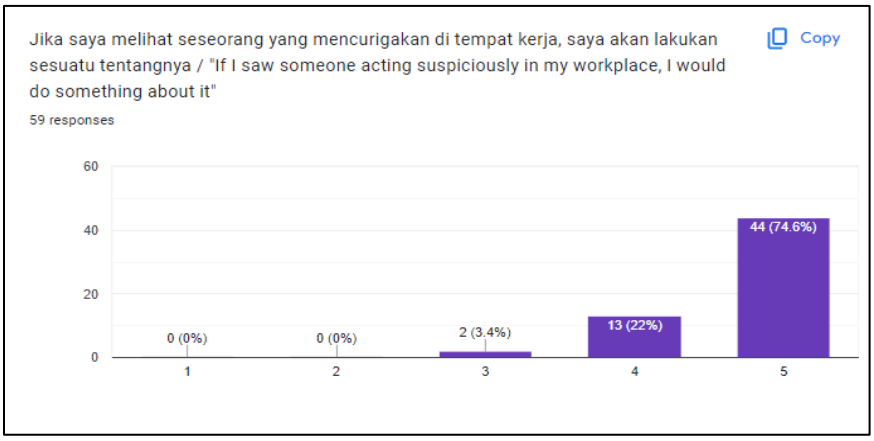
Analisis pada hasil soal selidik bagi pengurusan maklumat seperti di jadual 4.6 mendapati bahawa min purata bagi nilai semua komponen ialah 4.65536. Ini bermakna tahap kesedaran ahli farmasi komuniti berada pada tahap 5 iaitu sangat baik. Komponen D1 menunjukkan nilai min terendah (4.4407) berbanding komponen lain iaitu D2 (4.6949) dan D3 (4.8305).

Jadual 4.6 Analisis pengurusan maklumat

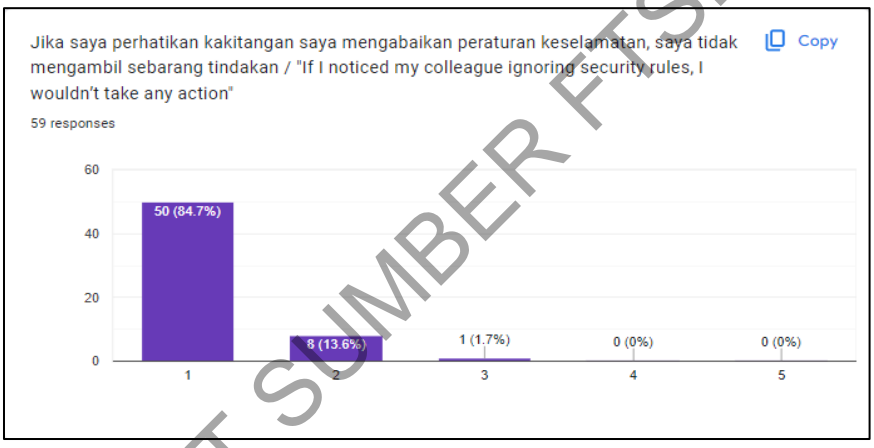
Soalan	Pernyataan	1	2	3	4	5	Nilai Min	Penilaian
E1	Saya memastikan cetakan yang mengandungi maklumat sensitif dicincang atau dimusnahkan ketika pelupusan	0 (0%)	3 (5.1%)	1 (1.7%)	22 (37.3%)	33 (55.9%)	4.4407	Baik
E2	Jika saya menemui pemacu pena "pendrive" di tempat awam, saya tidak patut memasukkannya ke dalam komputer kerja saya	0 (0%)	1 (1.7%)	0 (0%)	15 (25.4%)	43 (72.9%)	4.6949	Sangat Baik
E3	Adalah berisiko untuk meninggalkan cetakan yang mengandungi maklumat sensitif di atas meja saya semalaman	0 (0%)	1 (1.7%)	0 (0%)	7 (11.9%)	51 (86.4%)	4.8305	Sangat Baik
						Purata	4.655367	Sangat Baik

4.3.6 Analisis Berkaitan Pelaporan Insiden Keselamatan Siber

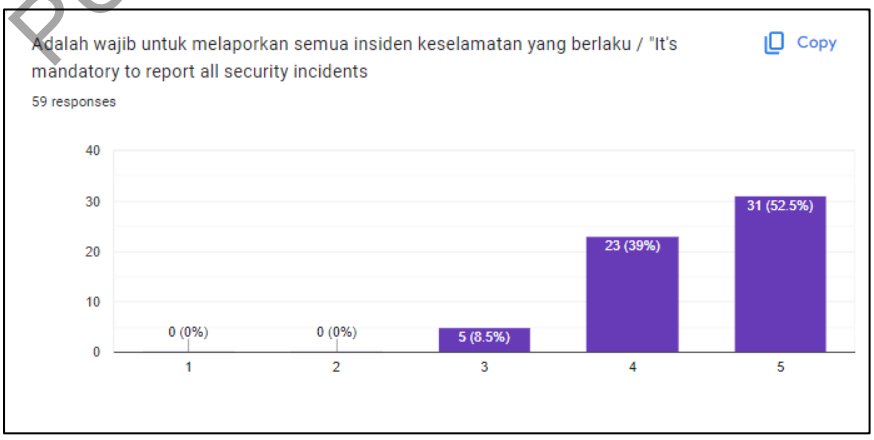
Hasil maklumbalas responden bagi komponen utama pelaporan insiden keselamatan siber adalah seperti rajah 4.19, 4.20, 4.21 dibawah:



Rajah 4.19 Maklumbalas responden bagi soalan komponen F1



Rajah 4.20 Maklumbalas responden bagi soalan komponen F2



Rajah 4.21 Maklumbalas responden bagi soalan komponen F3

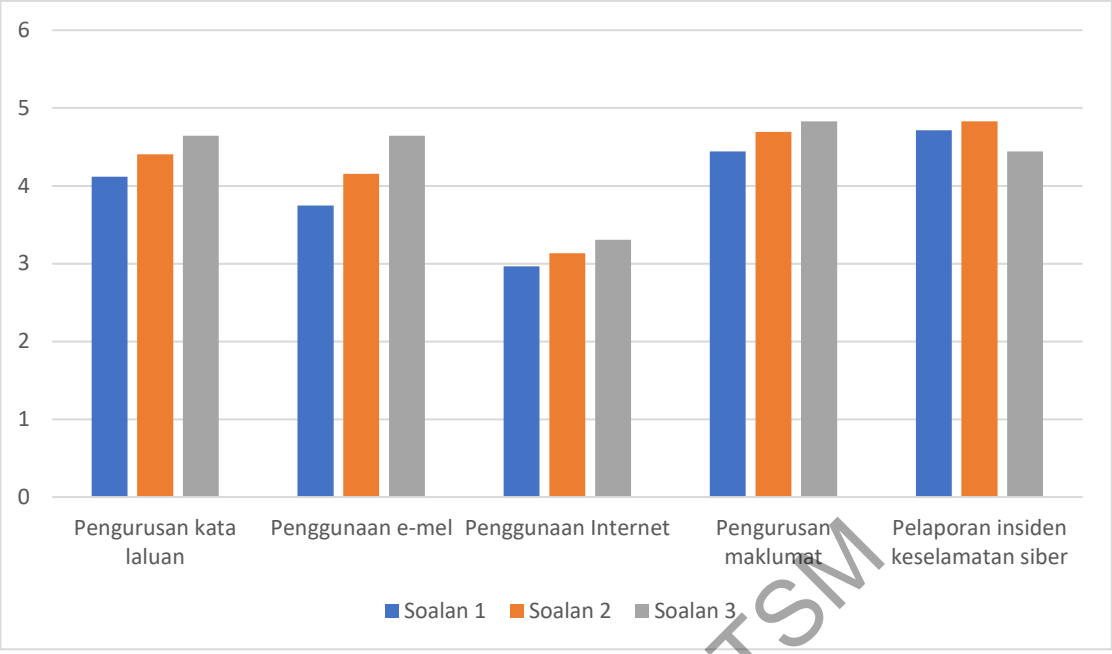
Analisis pada hasil soal selidik bagi pelaporan insiden keselamatan siber seperti di jadual 4.7 mendapati bahawa min purata bagi nilai semua komponen ialah 4.661017. Ini bermakna tahap kesedaran ahli farmasi komuniti berada pada tahap 5 iaitu sangat baik. Komponen F3 menunjukkan nilai min terendah (4.4407) berbanding komponen lain iaitu F1 (4.7119) dan F2 (4.8305) Komponen F2 merupakan komponen dengai nilai min tertinggi berbanding semua soalan di dalam soal selidik.

Jadual 4.7 Analisis pelaporan insiden keselamatan siber

Soalan	Pernyataan	1	2	3	4	5	Nilai Min	Penilaian
F1	Jika saya melihat seseorang yang mencurigakan di tempat kerja, saya akan lakukan sesuatu tentangnya	0 (0%)	0(0%)	2 (3.4%)	13 (22%)	44 (74.6%)	4.7119	Sangat Baik
F2 (RC)	Jika saya perhatikan kakitangan saya mengabaikan peraturan keselamatan, saya tidak mengambil sebarang tindakan	0 (0%)	0 (0%)	1 (1.7%)	8 (13.6%)	50 (84.7%)	4.8305	Sangat Baik
F3	Adalah wajib untuk melaporkan semua insiden keselamatan yang berlaku	0 (0%)	0 (0%)	5 (8.5%)	23 (39%)	31 (52.5%)	4.4407	Baik
						Purata	4.661017	Sangat Baik

4.3.7 Analisis Keseluruhan

Hasil analisis keseluruhan bagi semua komponen utama adalah seperti rajah 4.22 dan jadual 4.8 di bawah:



Rajah 4.22 Nilai min bagi setiap komponen soalan

Jadual 4.8 Analisis keseluruhan tahap kesedaran keselamatan siber

Item	Komponen utama	Komponen pecahan	Nilai min	Nilai Min purata	Tahap Kesedaran
B	Pengurusan kata laluan	Pengasingan kata laluan	4.1186	4.3898	4 (Baik)
		Perkongsian kata laluan	4.4068		
		Pemilihan kata laluan	4.6441		
C	Penggunaan e-mel	E-mel dari orang yang dikenali	3.7458	4.1808	4 (Baik)
		E-mel dari orang yang tidak dikenali	4.1525		
		E-mel yang mencurigakan	4.6441		
D	Penggunaan Internet	Muat turun fail	2.9661	3.1356	3 (Sederhana)
		Pelayaran laman sesawang	3.1356		
		Perkongsian maklumat di Internet	3.3051		

bersambung…

…sambungan

E	Pengurusan maklumat	Penghapusan dokumen sensitif	4.4407	4.6554	5 (Sangat baik)
		Pemacu pen USB	4.6949		
		Pengurusan dokumen sensitif	4.8305		
F	Pelaporan insiden keselamatan siber	Individu mencurigakan	4.7119	4.6610	5 (Sangat baik)
		Amalan buruk rakan sekerja	4.8305		
		Pelaporan semua insiden	4.4407		

Walaupun secara umumnya responden dianggap mempunyai tahap kesedaran keselamatan siber yang baik berkaitan pengurusan kata laluan, namun masih ada dikalangan ahli farmasi komuniti yang tidak mengambil berat berkaitan perkongsian kata laluan. Perkongsian kata laluan sesama rakan sekerja merupakan amalan berisiko tinggi yang boleh meningkatkan risiko ancaman keselamatan siber. Selain melemahkan keselamatan sesebuah organisasi, ia menyukarkan usaha mengesan punca pencerobohan kerana ramai individu menggunakan akaun dan kata laluan yang sama. Kombinasi huruf, nombor dan simbol bagi kata laluan telah menjadi fenomena biasa kerana banyak sistem yang telah mewajibkan penggunaannya bagi memastikan kata laluan lebih rumit dan selamat.

Pencerobohan sistem dan kecurian data melalui teknik pancingan data merupakan ancaman siber yang mempunyai tahap insiden yang tinggi di dalam sesebuah organisasi. Hasil kajian mendapati secara umumnya ahli farmasi komuniti adalah sangat berhati-hati ketika berinteraksi dengan pautan di dalam e-mel dari orang yang tidak dikenali, namun ramai yang kurang menyedari risiko ancaman keselamatan siber yang boleh juga hadir melalui pautan dari orang yang dikenali. Kandungan e-mel yang menarik juga boleh meningkatkan risiko sesetengah ahli farmasi komuniti untuk terdedah kepada ancaman siber seterusnya menjadi mangsa kepada pencerobohan sistem dan data.

Penggunaan Internet secara tidak selamat boleh mendedahkan pengguna kepada pelbagai risiko ancaman siber. Hasil kajian mendapati bahawa sejumlah besar ahli

farmasi komuniti tidak mengambil berat tentang risiko yang timbul hasil dari aktiviti memuat turun fail dari Internet. Ini menunjukkan bahawa kebanyakan mereka tidak risau tentang ancaman perisian hasad yang boleh terkandung di dalam pelbagai jenis fail yang dimuat turun. Membuka laman sesawang tanpa menilai risiko keselamatan siber juga boleh mendedahkan mereka dengan ancaman perisian hasad yang dihantar ke komputer yang digunakan tanpa sedar. Hasil kajian juga mendapati bahawa sebilangan besar ahli farmasi komuniti mempunyai risiko untuk menjadi mangsa kejuruteraan sosial dan kebocoran maklumat kerana tidak berhati-hati di dalam berkongsi maklumat di Internet.

Secara umumnya ahli farmasi komuniti mempunyai tahap kesedaran yang sangat baik berkaitan pengurusan maklumat. Ini berkemungkinan besar kerana mereka telah dilatih berkaitan pengurusan maklumat di dalam urusan pekerjaan mereka walaupun yang tidak berkaitan dengan keselamatan siber. Selain keperluan perundangan dan etika ahli farmasi yang perlu dipatuhi, ahli farmasi komuniti mempunyai tanggungjawab untuk mengikuti pelbagai garispanduan dan amalan terbaik yang merangkumi pengurusan rekod secara sistematik, selamat dan teratur.

Ahli farmasi komuniti juga mempunyai tahap kesedaran yang sangat baik dari sudut pelaporan insiden keselamatan siber. Sama seperti perbincangan berkaitan pengurusan maklumat sebelum ini, tahap kesedaran bagi komponen ini mungkin berkait rapat dengan latihan, peranan dan tugas ahli farmasi di dalam pelaporan insiden berkaitan dengan bidang kesihatan. Adalah menjadi kebiasaan untuk seseorang ahli farmasi melaporkan sebarang insiden berkaitan penggunaan ubat-ubatan dan sebarang kesan yang tidak diingini terhadap pesakit. Mereka telah dilatih untuk membuat pengumpulan data, dokumentasi, analisis ringkas, cadangan dan maklumbalas berkaitan sebarang insiden yang berlaku. Perkara ini mungkin turut menyumbang kepada tahap kesedaran mereka berkaitan pelaporan insiden.

4.4 KESIMPULAN

Berpandukan hasil analisis terhadap komponen demografi (komponen utama A) yang dijalankan di dalam bab ini, didapati bahawa majoriti ahli farmasi komuniti di negeri

Kelantan yang terlibat di dalam kajian ini adalah dari kalangan perempuan. Dari sudut umur, majoriti berumur 31-40 tahun. Hampir semua mempunyai sekurang-kurangnya ijazah sarjana muda, dan tidak pernah menerima latihan atau penerangan berkaitan keselamatan siber. Pecahan terbesar ahli farmasi komuniti yang terlibat di dalam kajian ini telah berkhidmat diantara 21-30 tahun sebagai ahli farmasi komuniti.

Tahap kesedaran ahli farmasi komuniti berada pada tahap 5 iaitu sangat baik bagi dua komponen utama iaitu E (pengurusan maklumat) dan F (pelaporan insiden keselamatan siber). Bagi komponen utama B (Pengurusan kata laluan) dan C pula (Penggunaan e-mel), tahap yang dicapai ialah 4 (baik) manakala tahap terendah iaitu 3 (sederhana) diperolehi bagi komponen utama C (Penggunaan Internet). Secara keseluruhannya, kesedaran ahli farmasi komuniti di negeri Kelantan terhadap keselamatan siber berada pada tahap yang baik.

BAB V

RUMUSAN DAN CADANGAN

5.1 PENGENALAN

Ringkasan kajian, dapatan kajian dan penemuan kajian akan dibincangkan dan dirumuskan di dalam bab ini. Analisis, implikasi dan kekangan kajian ini juga akan turut dibincangkan. Akhirnya, bab ini akan ditutup dengan cadangan penyelidikan pada masa akan datang.

5.2 RUMUSAN DAN PENEMUAN KAJIAN

Secara amnya, prinsip asas keselamatan siber iaitu kerahsiaan, integriti dan ketersediaan telah diterangkan di dalam kajian ini. Insiden-insiden keselamatan siber berskala besar yang berkait dengan faktor kelemahan manusia juga telah dibincangkan kerana ia berkait rapat dengan kepentingan menilai tahap keselamatan siber elemen manusia di dalam sesebuah organisasi. Kajian ini juga mendapati terdapat kepentingan untuk mengkaji tahap kesedaran keselamatan siber ahli farmasi komuniti kerana peranan penting mereka berkaitan dengan data kesihatan pesakit serta bertambahnya kebergantungan mereka terhadap sistem komputer.

Kajian ini juga telah berjaya mencapai 3 objektif yang ditetapkan di peringkat awal sepertimana yang dinyatakan di dalam Bab 1.

5.2.1 Objektif Kajian 1: Menentukan model dan petunjuk bagi penilaian tahap kesedaran keselamatan siber yang bersesuaian dengan kajian ini.

Di dalam kajian ini, model yang dipilih dan dianggap paling sesuai adalah model berasaskan pengetahuan, sikap dan tingkah laku (KAB Model) yang diterjemahkan kepada 5 topik tumpuan atau komponen utama iaitu pengurusan kata laluan, penggunaan e-mel, penggunaan Internet, pengurusan maklumat, dan pelaporan insiden

keselamatan siber sebagai petunjuk dan kriteria pengukuran tahap kesedaran keselamatan siber. Tahap kesedaran kemudiannya dinilai dan diukur berdasarkan nilai purata soalan-soalan di dalam 5 topik tumpuan tersebut.

5.2.2 Objektif Kajian 2: Menentukan instrumen yang bersesuaian dengan kajian ini.

Instrumen yang dibangunkan bagi kajian ini ialah instrumen dalam bentuk soal selidik menggunakan perisian “Google forms”. Skala Likert 5 poin digunakan bagi tujuan penilaian kepada jawapan responden. Soalan yang dibuat pula adalah berdasarkan petunjuk yang ditetapkan yang dipilih dan dihasilkan dari instrumen kajian yang telah disahkan oleh kajian sebelum ini iaitu HAIS-Q sebagai asas. Didapati model HAIS-Q adalah yang paling sesuai untuk kajian ini kerana lebih jelas dan sesuai untuk mengukur tahap kesedaran siber responden yang dipilih. Hasil instrumen soal selidik baharu yang dibuat pula kemudiannya dirujuk kepada pakar bagi tujuan pengesahan.

5.2.3 Objektif Kajian 3: Mengkaji tahap kesedaran keselamatan siber dikalangan ahli farmasi komuniti di negeri Kelantan

Melalui kajian ini, tahap kesedaran keselamatan siber dikalangan ahli farmasi komuniti di negeri Kelantan telah berjaya dikaji dan diukur. Seramai 59 orang responden memberi maklum balas melalui instrumen soal selidik yang diedarkan. Hasil kajian mendapati bahawa tahap kesedaran ahli farmasi komuniti di negeri Kelantan terhadap keselamatan siber berada pada tahap yang baik walaupun mereka tidak diberi latihan secara rasmi berkaitan keselamatan siber. Kajian lebih terperinci berdasarkan demografi responden seperti umur dan tahap pendidikan tidak dapat dibuat secara meyakinkan kerana jumlah sampel yang kecil dan taburan yang tidak seimbang.

5.3 ANALISIS, PERBINCANGAN DAN CADANGAN UNTUK MENINGKATKAN TAHAP KESEDARAN SIBER

Berdasarkan kepada hasil kajian yang diperolehi bagi 5 komponen utama di digunakan, didapati tahap kesedaran ahli farmasi komuniti berada pada tahap 5 iaitu sangat baik bagi dua komponen utama iaitu pengurusan maklumat dan pelaporan insiden keselamatan siber. Bagi komponen utama pengurusan kata laluan dan penggunaan e-mel pula, tahap yang dicapai ialah 4 (baik) manakala tahap terendah iaitu 3 (sederhana) diperolehi bagi komponen utama penggunaan Internet.

Berdasarkan kepada hasil kajian yang diperolehi, didapati sejumlah besar ahli farmasi komuniti tidak pernah menerima sebarang latihan berkaitan keselamatan siber. Walaupun dapatan tersebut adalah membimbangkan, namun hasil kajian menunjukkan tahap kesedaran keselamatan siber mereka secara umumnya berada di tahap yang baik. Ini memberi gambaran bahawa walaupun mereka tidak pernah menerima sebarang latihan secara rasmi, namun hasil pendidikan melalui kempen kesedaran, polisi dan hebahan media sedia ada mungkin telah menjadikan mereka lebih berhati-hati di dalam isu berkaitan keselamatan siber.

Analisis lanjutan berkaitan perbezaan tahap kesedaran keselamatan siber ahli farmasi komuniti di negeri Kelantan berdasarkan pecahan demografi tidak dapat dilakukan secara meyakinkan kerana kekurangan bilangan responden berdasarkan pecahan demografi yang boleh dikaji di dalam kajian ini. Jumlah responden yang lebih besar diperlukan bagi tujuan ini.

Dari sudut pendidikan, penggunaan internet perlu menjadi fokus di dalam latihan ataupun kempen kesedaran keselamatan siber yang disasarkan kepada golongan ahli farmasi komuniti. Masih terdapat diantara mereka yang tidak menyedari atau tidak mengambil peduli ancaman yang mungkin timbul dari aktiviti pelayaran Internet secara tidak selamat ketika pembukaan laman sesawang, memuat turun fail dan memuat naik maklumat di internet.

Dicadangkan juga penekanan diberi kepada topik penggunaan e-mel kerana komponen pecahan reaksi kepada e-mel dari orang yang dikenali memberi antara nilai min yang terendah di dalam hasil maklum balas responden. Pautan e-mel dari orang yang dikenali mungkin juga sama bahaya dengan pautan dari orang yang tidak dikenali jika tidak diselidiki terlebih dahulu oleh penerima e-mel tersebut kerana penjenayah siber mempunyai pelbagai taktik dan strategi bagi menjalankan aktiviti jenayah mereka.

Selain latihan tersebut, ahli farmasi komuniti juga boleh didedahkan dengan simulasi ancaman yang boleh berlaku akibat dari kegagalan mereka mengambil sikap berhati-hati dengan keselamatan siber. Simulasi ini boleh dibuat dalam bentuk pancingan melalui e-mel. Kaedah simulasi ini penting kerana program latihan yang dijalankan tanpa ujian mungkin tidak dapat membentuk sikap positif kerana mereka tidak didedahkan dengan risiko dan akibat dari perbuatan mereka.

Walaupun ahli farmasi komuniti dianggap mempunyai tahap kesedaran keselamatan siber yang baik dari sudut pengurusan maklumat dan pelaporan insiden keselamatan siber, mereka masih perlu diingatkan dan diberi latihan rasmi berkaitan kerahsiaan rekod perubatan dan data pesakit. Ini kerana perkara tersebut merupakan data dan aset paling berharga melibatkan pesakit yang disimpan di fasiliti mereka. Ahli farmasi komuniti juga perlu memiliki sikap berhati-hati ketika berurusan dengan pihak ketiga sepanjang perjalanan operasi farmasi komuniti mereka kerana kadang-kala pihak ketiga ini turut mempunyai capaian kepada komputer dan rekod perubatan contohnya juruteknik komputer yang ditugaskan untuk membaik pulih atau menaik taraf sistem komputer di farmasi komuniti tersebut.

Di dalam kajian ini, terdapat 2 lagi komponen utama kesedaran keselamatan siber yang tidak dikaji iaitu penggunaan telefon bimbit dan media sosial kerana didapati kurang sesuai berbanding komponen lain. Walaubagaimanapun, 2 komponen ini boleh dimasukkan di dalam program latihan kesedaran keselamatan siber kerana dijangka akan terdapat pertambahan ancaman dan risiko yang banyak berkait dengan komponen-komponen tersebut pada masa akan datang sesuai dengan perubahan cara hidup masyarakat.

5.4 SUMBANGAN KAJIAN

Kajian ini mempunyai beberapa sumbangan yang boleh dimanfaatkan iaitu:

1. Maklumat yang diperolehi dari hasil kajian ini boleh digunakan untuk menilai tahap kesedaran ahli farmasi komuniti khususnya di Kelantan terhadap keselamatan siber.

2. Topik atau skop tertentu yang perlu diberi perhatian khusus di dalam kempen pendidikan keselamatan siber berjaya dikenal pasti seterusnya memastikan kempen yang dijalankan akan lebih memberi kesan kepada ahli farmasi komuniti.

3. Model dan petunjuk yang digunakan di dalam kajian ini boleh dijadikan asas untuk digunakan di dalam kajian-kajian lain berkaitan tahap kesedaran keselamatan siber.

4. Kajian ini membantu pihak berwajib di dalam membuat penilaian kempen-kempen kesedaran dan pendidikan keselamatan siber yang dijalankan secara tidak rasmi kepada masyarakat umum.

5.5 LIMITASI KAJIAN

Limitasi bagi sesuatu kajian boleh berlaku disebabkan oleh pelbagai faktor. Bagi kajian ini, beberapa limitasi telah dikenal pasti iaitu seperti berikut:

Limitasi yang pertama ialah jumlah sampel. Di Kelantan dianggarkan terdapat 187 ahli farmasi komuniti, dan jumlah sampel minimum yang diperlukan ialah seramai 126 orang. Namun, hanya seramai 59 orang yang memberi maklum balas di dalam kajian ini. Perkara ini mungkin berlaku disebabkan oleh pelbagai faktor. Walaupun pelbagai perkara telah dilakukan seperti soal selidik dijalankan secara dalam talian dan soalan soal selidik telah diringkaskan untuk meningkatkan penglibatan responden, adalah didapati bahawa secara umumnya, responden pada masa kini semakin kurang memberi kerjasama untuk terlibat di dalam kajian berbanding tahun-tahun sebelumnya (Leeper 2019). Kekurangan sampel juga menyebabkan kajian lebih terperinci terhadap responden seperti perbezaan tahap kesedaran siber berdasarkan demografi tidak dapat dijalankan.

Limitasi yang kedua ialah data yang diperolehi melalui soal selidik yang dijalankan diberikan oleh responden secara pelaporan kendiri. Antara perkara yang dibimbangkan di dalam kaedah ini ialah situasi yang dikenali sebagai *socially desirable responding* iaitu responden cuba untuk menghasilkan imej yang lebih baik tentang diri mereka (Van 2008) ketika memberi maklum balas. samada secara sedar ataupun tidak. Perkara ini mungkin menyebabkan hasil kajian ini memberi kesimpulan yang lebih positif tentang tahap kesedaran ahli farmasi komuniti di negeri Kelantan lebih dari yang sepatutnya. Mewajibkan bakal responden memberi e-mel mereka sebagai syarat terlibat di dalam kajian ini juga mungkin menjadi faktor yang menghalang mereka melibatkan diri di dalam kajian yang dijalankan ini secara jujur disebabkan oleh kerisauan maklum balas yang diberikan boleh dikaitkan dengan mereka pada masa akan datang.

Limitasi yang ketiga ialah penggunaan perisian SPSS bagi tujuan analisis data. Perisian SPSS memerlukan latihan dan kemahiran yang cukup bagi memastikan ujian