STRATEGI PELAKSANAAN BYOD SELAMAT DI HOSPITAL PAKAR KPJ IPOH

VIKNAKARAN A/L GNANASEGAR

UNIVERSITI KEBANGSAAN MALAYSIA

STRATEGI PELAKSANAAN BYOD SELAMAT DI HOSPITAL PAKAR KPJ IPOH

VIKNAKARAN A/L GNANASEGAR

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

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT

UNIVERSITI KEBANGSAAN MALAYSIA

BANGI

2023

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nulikan dan ringkasan yang setiap satunya telah saya jelaskan sumbernya.

November 2023 VIKNAKARAN A/L GNANASEGAR

P1042356

PENGHARGAAN

Saya ingin merakamkan setinggi-tinggi penghargaan dan terima kasih atas bimbingan dan sokongan Dr. Rossilawati Sulaiman sepanjang kajian Strategi Pelaksanaan BYOD Selamat di Hospital Pakar KPJ Ipoh ini. Saya amat berterima kasih kerana anda telah meluangkan masa dan tenaga untuk membimbing dan memberi tunjuk ajar kepada saya dalam menjalankan kajian ini.

Dalam kajian ini, saya banyak belajar tentang aspek keselamatan siber dalam penggunaan peranti BYOD dan bagaimana ia boleh menjejaskan hospital dan pesakit. Kajian ini telah membantu saya memahami betapa pentingnya keselamatan siber dan keperluan untuk mempraktikkannya dalam setiap aspek kerja kami, terutamanya di hospital. Saya bersyukur kerana anda telah memberikan sokongan dan dorongan yang kuat kepada saya dalam kajian ini. Anda telah membantu saya melihat aspek keselamatan siber dengan perspektif yang lebih luas dan menarik. Saya menghargai kesabaran dan keikhlasan anda dalam membimbing dan menyokong saya sepanjang kajian ini.

Sekali lagi, saya ingin mengucapkan terima kasih di atas segala bimbingan dan sokongan yang diberikan. Saya berharap untuk terus belajar daripada anda dan bekerjasama dalam pengajian akan datang. Semoga kajian ini dapat memberi manfaat dan sumbangan yang berguna untuk Hospital Pakar KPJ Ipoh.

ABSTRAK

Konsep "Bawa Peranti Anda Sendiri" atau Bring Your Own Device (BYOD) membolehkan pengguna menggunakan peranti mudah alih peribadi seperti telefon pintar, tablet atau komputer riba mereka untuk melaksanakan tugas kerja dan mengakses sumber organisasi. Trend BYOD telah meningkat dengan pesat dalam beberapa tahun kebelakangan ini sejajar dengan kemajuan teknologi dan peningkatan pergantungan pada peranti mudah alih. Kajian ini memfokus kepada pelaksanaan selamat BYOD di Hospital Pakar KPJ Ipoh yang merupakan sebahagian daripada rangkaian KPJ Healthcare Berhad dan menawarkan pelbagai perkhidmatan kesihatan. Di Hospital Pakar KPJ Ipoh, amalan semasa adalah memberikan peranti milik hospital kepada pengguna seperti doktor, jururawat dan kakitangan kewangan. Peranti ini disambungkan ke rangkaian Internet dalaman hospital untuk mengakses sistem hospital. Bagaimanapun terdapat beberapa kelemahan dalam proses semasa, termasuk pergantungan tinggi pada peranti mudah alih milik hospital dan rangkaian Internet dalaman. Di samping itu, amalan semasa tidak menyediakan akses mudah kepada maklumat pesakit untuk kakitangan di luar hospital, menyebabkan kesukaran dalam situasi kecemasan. Keselamatan data dan privasi pesakit juga merupakan isu penting, terutamanya risiko kecurian data atau pelanggaran privasi. Pergantungan kepada teknologi juga boleh menghadapi cabaran jika kakitangan tidak mempunyai kecekapan yang mencukupi dalam penggunaan sistem hospital. Ketersediaan peranti dan kos biayaan juga merupakan aspek kritikal yang perlu diatasi. Kajian ini dijalankan untuk mengenal pasti faktor-faktor yang mempengaruhi pelaksanaan BYOD yang selamat, mengenal pasti proses kerja yang bermasalah serta mencadangkan garis panduan yang sesuai. Evaluasi terhadap faktor teknologi, keselamatan, organisasi dan manusia secara kuantitatif melalui tinjauan soal selidik yang diedarkan secara dalam talian. Pengumpulan data turut dilaksanakan menerusi temu bual pakar dalam bidang teknologi maklumat dan keselamatan siber. Hasil analisis kajian menunjukkan terdapat hubung kait antara faktor teknologi, keselamatan, organisasi dan manusia dalam pelaksanaan BYOD yang selamat di Hospital Pakar KPJ Ipoh. Hasil kajian ini akan digunakan untuk menyusun garis panduan yang sesuai dan berkesan dalam penggunaan peranti BYOD. Kajian lanjutan boleh dijalankan untuk menilai keberkesanan garis panduan yang ditetapkan dan memberi tumpuan kepada penggunaan Pengurusan Peranti Mudah Alih (MDM) untuk meningkatkan keselamatan BYOD. Pengemaskinian garis panduan secara berkala juga boleh dicadangkan untuk mengikuti perubahan teknologi dan trend keselamatan yang berlaku selepas 2023.

BYOD SECURITY STRATEGY ANALYSIS
KPJ SPECIALIST HOSPITAL IPOH

ABSTRACT

The concept of "Bring Your Own Device" or BYOD allows users to use personal mobile devices such as their smartphones, tablets or laptops to perform work tasks and access organizational resources. The BYOD trend has increased rapidly in recent years in line with technological advances and increased reliance on mobile devices. This study focuses on the safe implementation of BYOD at KPJ Specialist Hospital Ipoh which is part of the KPJ Healthcare Berhad network and offers various health services. At KPJ Ipoh Specialist Hospital, the current practice is to provide hospital-owned devices to users such as doctors, nurses and financial staff. These devices are connected to the hospital's internal Internet network to access the hospital system. However, there are several weaknesses in the current process, including a high reliance on hospital-owned mobile devices and internal Internet networks. In addition, current practice does not provide easy access to patient information for staff outside the hospital, causing difficulties in emergency situations. Data security and patient privacy are also important issues, especially the risk of data theft or privacy breaches. Reliance on technology can also face challenges if staff do not have sufficient competence in the use of hospital systems. Device availability and cost are also critical aspects that need to be addressed. This study was conducted to identify the factors that influence the safe implementation of BYOD, identify problematic work processes and propose appropriate guidelines. Evaluation of technological, security, organizational and human factors quantitatively through a questionnaire survey distributed online. Data collection was also carried out through interviews with experts in the field of information technology and cyber security. The results of the study analysis show that there is a link between technology, security, organization and human factors in the safe implementation of BYOD at KPJ Specialist Hospital Ipoh. The results of this study will be used to compile appropriate and effective guidelines in the use of BYOD devices. Further studies can be conducted to evaluate the effectiveness of established guidelines and focus on the use of Mobile Device Management (MDM) to improve BYOD security. Regular updating of the guidelines may also be proposed to follow technological changes and safety trends that occur after 2023.

KANDUNGAN

SENARAI JADUAL

SENARAI ILUSTRASI

SENARAI SINGKATAN

BYOD	*Bring Your Own Device*
MDM	*Mobile Device Management*
IT	*Information Technology*
QoS	*Quality of Service*
VPN	*Virtual Private Network*
KPJ	*Kumpulan Perubatan Johor*
KCIS	*KPJ Clinical Information System*
HITS	*Health Information System*
BMS	*Bed Management System*
Wi-Fi	*Wireless Fidelity*
LAN	*Local Area Network*
DDoS	*Distributed Denial-of-Service*
UAS	*User Access System*
PPT	*People, Policy, Technology*
AD	*Active Directory*

BAB I

PENDAHULUAN

1.1 PENGENALAN

Bawa Peranti Anda Sendiri atau Bring Your Own Device (BYOD) merangkumi peranti mudah alih seperti telefon pintar, komputer riba atau tablet. Peranti BYOD dan peranti mudah alih, kedua-dua istilah ini merujuk kepada perkara yang sama iaitu peranti yang dimiliki oleh individu dan digunakan untuk tujuan peribadi atau profesional. Secara umum, kedua-dua istilah ini dapat digunakan secara bergantian. Bagaimanapun, istilah "peranti mudah alih" adalah lebih umum dan meliputi semua jenis peranti yang boleh dibawa bersama, manakala istilah “BYOD” lebih spesifik merujuk kepada amalan membawa peranti peribadi ke tempat kerja dan menggunakannya untuk tujuan kerja. Pengunaan peranti BYOD di tempat kerja telah meningkat dalam beberapa tahun lalu. Salah satu sebab juga adalah kerana penularan pandemik Covid-19 yang melanda negara baru-baru ini.

Amalan BYOD memberikan kelebihan seperti meningkatkan produktiviti dan fleksibiliti pekerja. Pekerja boleh mengakses maklumat dan dokumen yang diperlukan pada bila-bila masa dan di mana-mana sahaja. Ini dapat meningkatkan produktiviti dan mempercepat proses kerja. Selain itu, organisasi juga dapat menjimat kos pembiayaan. Dengan membenarkan pekerja menggunakan peranti BYOD, organisasi tidak perlu melabur banyak dalam peralatan teknologi. Ini dapat membantu organisasi mengurangkan kos yang berkaitan dengan pembelian, penyelenggaraan, dan penggantian peralatan.

Bagaimanapun, pendekatan ini juga memberikan pelbagai cabaran kepada industri. Salah satu cabaran terbesar BYOD ialah potensi risiko keselamatan. Pekerja yang menggunakan peranti peribadi untuk mengakses data korporat meningkatkan risiko pelanggaran data, pencerobohan perisian hasad dan akses tanpa kebenaran kepada maklumat sensitif. Ini boleh menjadi masalah khusus bagi organisasi yang

mengendalikan data sensitif, seperti perubatan, perkhidmatan kewangan dan agensi kerajaan. Satu contoh kajian yang menunjukkan penggunaan peranti IT di tempat kerja sebagai penyebab penipuan siber ialah kajian yang dilakukan oleh Perisian Keselamatan Kaspersky pada tahun 2020 (Kaspersky, 2020). Kajian ini melibatkan lebih daripada 8,000 kakitangan dari pelbagai sektor, termasuk sektor kesihatan. Hasil kajian menunjukkan bahawa sebanyak 52% daripada kesemua kes ancaman siber dalam tempoh satu tahun adalah disebabkan oleh tindakan pengguna peranti IT di tempat kerja yang tidak selamat. Ini termasuk tindakan seperti mengklik pada pautan yang mencurigakan atau memasukkan kelayakan log masuk (*log in credentials*) ke laman web palsu. Kajian ini menunjukkan bahawa penggunaan peranti di tempat kerja boleh menjadi faktor risiko yang tinggi dalam penipuan siber dan menekankan keperluan untuk meningkatkan kesedaran keselamatan siber dalam kalangan kakitangan.

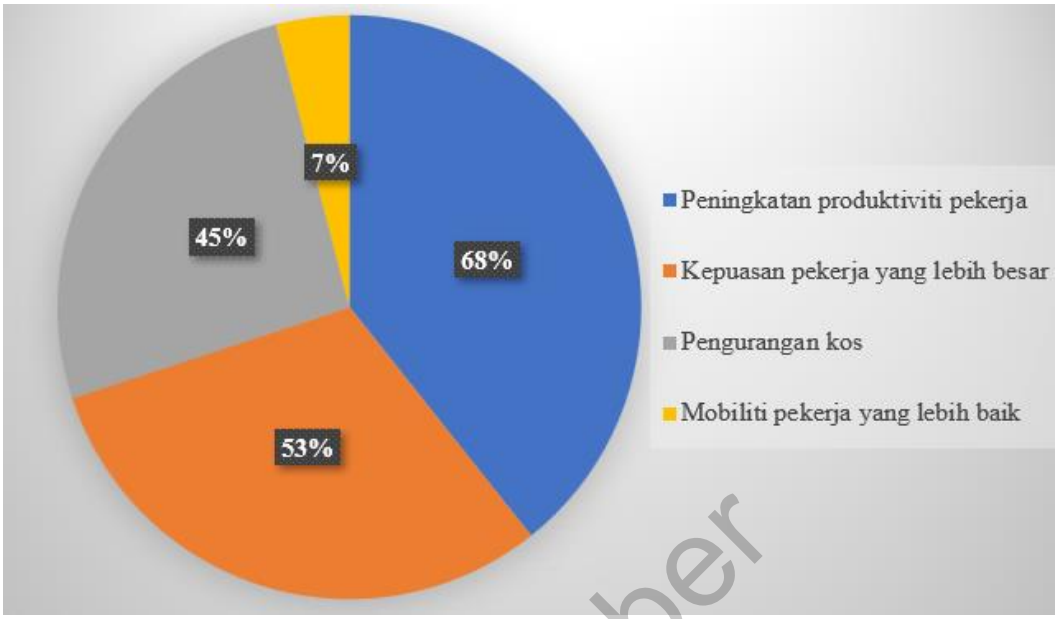
Selain itu, mengurus dan menyelenggara pelbagai peranti yang digunakan oleh pekerja menyukarkan bagi jabatan IT. Mereka mungkin tidak mempunyai kawalan ke atas perkakasan dan perisian pada peranti peribadi pekerja, menjadikannya sukar untuk memastikan peranti dikonfigurasi dengan betul dan memenuhi piawaian keselamatan. Ini boleh menyebabkan kelewatan mendapatkan maklumat penting dan boleh menyukarkan untuk mengesan dan bertindak balas terhadap insiden keselamatan. Cabaran lain dengan BYOD ialah kesukaran untuk membangunkan garis panduan yang mengimbangi keperluan pekerja untuk fleksibiliti dan keselesaan dengan keperluan mereka untuk keselamatan dan kawalan. Ini boleh menyukarkan syarikat untuk memastikan pematuhan terhadap peraturan, seperti yang berkaitan dengan kerahsiaan dan keselamatan data.

Pelanggaran pematuhan yang disebabkan peranti peribadi tidak mematuhi peraturan industri, boleh menyebabkan denda atau hukuman bagi syarikat. Kehilangan atau kecurian peranti juga merupakan salah satu cabaran jika peranti peribadi seseorang pekerja hilang atau dicuri, ia boleh menjejaskan data syarikat. Salah satu industri yang menghadapi cabaran keselamatan BYOD adalah industri kewangan. Bank dan institusi kewangan lain mesti mematuhi peraturan yang ketat dan melindungi data sensitif pelanggan. Industri undang-undang seperti firma guaman juga mengendalikan maklumat rahsia dan mesti memastikan ia dilindungi. Selain itu, industri peruncitan perlu melindungi data pelanggan, seperti maklumat kad kredit daripada dicuri. Dalam

perkhidmatan teknologi juga mesti kerap mengendalikan maklumat sensitif dan harta intelek yang perlu dilindungi daripada ancaman siber.

Selain daripada bidang industri yang dinyatakan, trend membawa peranti peribadi (BYOD) juga semakin terkenal dalam industri kesihatan. Profesional perubatan menggunakan peranti peribadi mereka untuk mengakses maklumat pesakit dan melakukan tugas-tugas berkaitan dengan rawatan pesakit. Namun, penggunaan peranti peribadi dalam persekitaran hospital menimbulkan kebimbangan tentang keselamatan data pesakit yang sensitif dan juga hospital. Kajian sebelum ini telah menunjukkan bahawa BYOD dalam kesihatan boleh meningkatkan risiko kebocoran data dan insiden keselamatan. Kajian ini juga menyatakan bahawa hospital tidak mempunyai langkah-langkah keselamatan yang memadai untuk melindungi data pesakit pada peranti peribadi (Tafheem et al., 2020).

Selain itu, terdapat kekurangan kajian tentang strategi keselamatan yang spesifik untuk hospital melaksanakan BYOD dan keberkesanannya. Projek yang dibangunkan ini bertujuan mengisi jurang kajian ini dengan mengkaji strategi pelaksanaan BYOD yang selamat dalam persekitaran Hospital Pakar KPJ Ipoh. Hipotesis dari kajian ini mendapati amalan semasa yang digunakan di hospital tidak bersesuaian dengan trend masa kini. Kajian ini akan mengenal pasti potensi kerentanan dan mencadangkan garis panduan untuk meningkatkan kesedaran pengguna BYOD dan meningkatkan keselamatan data pesakit dan hospital. Motivasi bagi kajian ini adalah untuk menangani kebimbangan yang semakin meningkat tentang kebocoran data dalam industri kesihatan dan untuk menyediakan penyelesaian praktikal bagi memastikan perlindungan maklumat pesakit yang sensitif. Keputusan kajian ini boleh mempunyai implikasi yang penting untuk industri kesihatan dan memberi sumbangan yang berkesan kepada pembangunan dasar keselamatan BYOD. Selain itu, kajian ini akan bermanfaat bagi golongan profesional dalam bidang kesihatan, pentadbir hospital dan pembuat dasar untuk memahami ancaman keselamatan BYOD dan bagaimana untuk mengatasinya. Rajah 1.1 menunjukkan kelebihan penggunaan BYOD.



Rajah 1.1 Faedah Penggunaan BYOD

Sumber: Cybersecurity Insiders, 2021

1.2 LATAR BELAKANG KAJIAN

Hospital Pakar KPJ Ipoh merupakan sebuah hospital swasta yang terletak di Ipoh, Perak. Hospital ini merupakan salah satu dari rangkaian hospital milik KPJ Healthcare Berhad, syarikat swasta terkemuka dalam sektor kesihatan di Malaysia. Hospital Pakar KPJ Ipoh menyediakan pelbagai perkhidmatan perubatan termasuk pembedahan, obstetrik dan ginekologi, pediatrik, onkologi, dan perkhidmatan rawatan kesihatan mental. Hospital Pakar KPJ Ipoh mempunyai lebih kurang 800 kakitangan dan dibahagikan kepada dua bahagian utama iaitu bahagian Perubatan dan Bukan Perubatan. Kakitangan bahagian Perubatan terdiri daripada doktor, jururawat, ahli farmasi, x-ray, fisiologi dan makmal. Manakala, bahagian Bukan Perubatan terdiri daripada jabatan perkhidmatan pesakit, kejuruteraan, kewangan, pengurusan rekod kesihatan dan stor. Jabatan IT juga terdapat di Hospital Pakar KPJ Ipoh untuk menguruskan sistem dan rangkaian hospital. Jabatan IT bertanggungjawab untuk memastikan bahawa sistem teknologi maklumat dan komunikasi di hospital berfungsi dengan baik dan terus berkembang mengikut keperluan semasa. Selain itu, jabatan ini

juga memastikan keselamatan dan privasi data pesakit dan maklumat hospital dijaga dengan baik.

Amalan semasa di Hospital Pakar KPJ Ipoh adalah pengguna diberi peranti milik hospital yang disambung kepada rangkaian Internet dalaman hospital untuk mencapai sistem hospital. Pengguna yang terlibat adalah seperti doktor, jururawat, pembantu makmal dan kerani kewangan. Ini bermakna bahawa setiap kakitangan perlu menggunakan peranti yang diberikan oleh hospital untuk melakukan tugasan harian mereka dan mengakses sistem hospital. Contohnya, doktor menggunakan peranti ini untuk melihat rekod pesakit, memeriksa ujian makmal dan radiologi, serta memasukkan maklumat mengenai diagnosis dan rawatan pesakit ke dalam sistem hospital. Jururawat pula menggunakan peranti ini untuk merekod tindakan dan ubat yang diberikan kepada pesakit, serta mengemaskini status pesakit dalam sistem hospital. Pembantu makmal dan kerani kewangan pula menggunakan peranti ini untuk mengemaskini rekod pembayaran pesakit dan membuat pembayaran terus melalui sistem hospital. Setiap peranti milik hospital ini disediakan dengan konfigurasi dan perisian yang telah dipasang oleh Jabatan IT Hospital Pakar KPJ Ipoh untuk memastikan kebolehpercayaan dan keselamatan data yang disimpan dalam sistem hospital.

1.3 PROSES KERJA

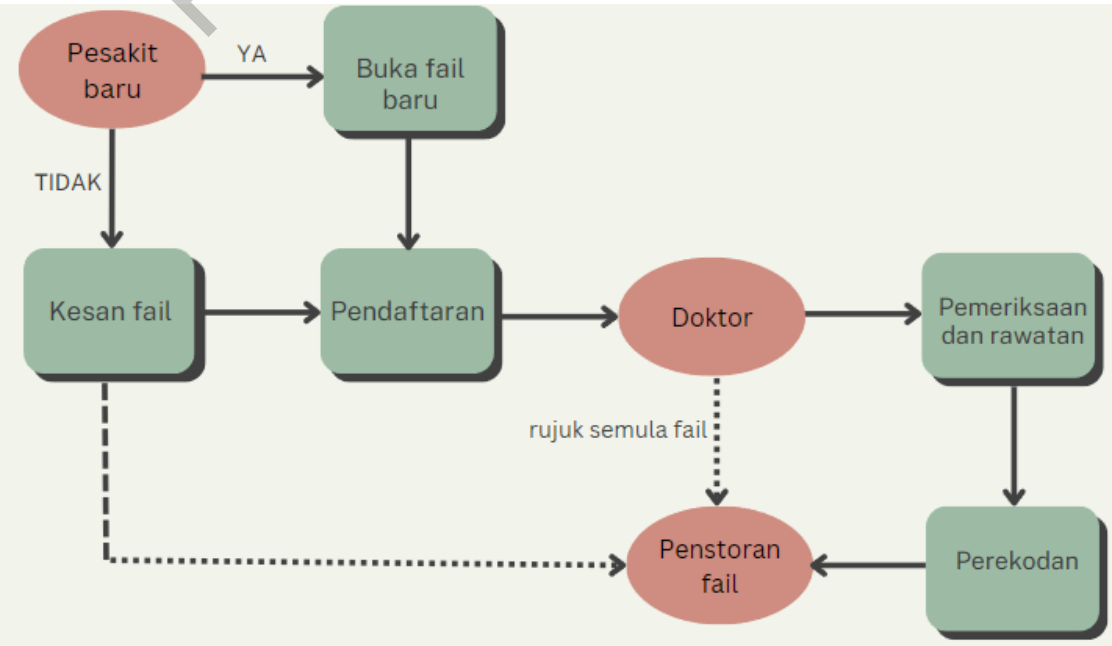
1.3.1 Proses Kerja Tradisional

Proses kerja tradisional di Hospital Pakar KPJ Ipoh sebelum ini melibatkan penggunaan kertas manual dan penciptaan fail bagi setiap pesakit, serta merekod data pesakit dalam peranti IT yang disediakan hospital. Walaupun peranti IT digunakan, proses ini tidak melibatkan penggunaan sistem maklumat klinikal untuk memasukkan data pesakit. Dalam proses ini, setiap pesakit akan mempunyai fail kertas yang disediakan oleh pihak hospital. Fail pesakit berfungsi sebagai rekod utama yang menyimpan maklumat penting seperti butiran peribadi, sejarah perubatan, keputusan ujian, diagnosis dan rawatan yang telah diberikan. Kakitangan kesihatan akan merekod maklumat ini secara manual dalam fail. Selain merekod di atas kertas, hospital juga menyediakan peranti IT kepada kakitangan sebagai alat untuk merekod dan mengakses data pesakit. Peranti IT seperti komputer, tablet dan komputer riba yang membolehkan pengguna memasukkan

dan mengemas kini maklumat pesakit. Bagaimanapun, proses ini masih melibatkan rakaman manual yang kemudiannya dimasukkan ke dalam peranti IT, tanpa sistem maklumat klinikal.

Kelemahan proses kerja tradisional ini ialah kebergantungan pada rakaman manual dan fail kertas. Ini boleh menyebabkan masalah seperti kesilapan menulis, kesukaran mencari dan mengakses maklumat pesakit dengan cepat, dan risiko kehilangan atau merosakkan fail kertas. Selain itu, proses pemindahan data dari kertas ke peranti IT juga boleh memakan masa dan meningkatkan risiko ralat dalam pemindahan maklumat. Selain itu, tanpa sistem maklumat klinikal, keupayaan untuk berkongsi dan mengakses data pesakit dengan cekap antara pasukan perubatan juga terhad. Maklumat pesakit mungkin tidak boleh diakses dalam masa nyata oleh semua ahli pasukan yang terlibat dalam rawatan, yang mungkin memerlukan kerjasama dan penyelarasan yang berkesan.

Kesimpulannya, penggunaan kertas manual dan penciptaan fail bagi setiap pesakit, serta rakaman data pesakit dalam peranti IT tanpa sistem maklumat klinikal di Hospital Pakar KPJ Ipoh sebelum ini mempunyai kelemahan tertentu. Peralihan kepada sistem maklumat klinikal akan memudahkan rakaman dan akses data pesakit yang lebih cekap, kerjasama pasukan perubatan yang lebih baik, mengurangkan risiko ralat, dan meningkatkan kebolehpercayaan dan keselamatan data. Rajah 1.2 menunjukkan aliran proses jika seorang pesakit datang merawat di Hospital Pakar KPJ Ipoh.



Rajah 1.2 Aliran proses kerja tradisional

1. **Pendaftaran**: Pesakit yang datang ke Hospital Pakar KPJ Ipoh akan mendaftar di kaunter pendaftaran. Kerani akan menyemak sama ada individu tersebut adalah pesakit baru atau yang pernah datang sebelum ini.
2. **Pembukaan fail**: Jika pesakit baru, fail akan dibuka untuk menyimpan rekod keseluruhan pesakit. Fail ini biasanya berasaskan kertas dan diberi nombor rujukan yang unik.
3. **Pengesanan fail**: Jika pesakit lama, fail akan dikesan dari rak fail.
4. **Pemeriksaan dan rawatan**: Pesakit kemudiannya akan dipanggil oleh doktor untuk pemeriksaan. Doktor akan mencatat simptom, diagnosis, dan cadangan rawatan dalam fail pesakit.
5. **Perekodan**: Doktor atau kakitangan kesihatan lain akan menggunakan fail pesakit untuk merekodkan tindakan yang dilakukan, ubat-ubatan yang diberikan dan maklumat penting lain seperti keputusan ujian dan keputusan radiologi.
6. **Penstoran fail**: Fail pesakit akan disimpan dalam sistem rak fail di hospital. Biasanya, fail ini disimpan secara fizikal dalam bentuk kertas dan disusun dalam susunan tertentu untuk memudahkan carian semasa.
7. **Rujuk semula fail**: Doktor atau kakitangan kesihatan lain boleh merujuk fail semula pesakit untuk mengemas kini maklumat. Ini termasuk merekodkan perubahan dalam status pesakit, maklumat rawatan terkini dan rekod lain yang berkaitan dengan kesihatan pesakit.

1.3.2 Proses Kerja Semasa

Proses kerja semasa di Hospital Pakar KPJ Ipoh telah mengalami perubahan daripada proses kerja tradisional yang menggunakan kertas manual dan fail kertas. Dengan pengenalan kepada sistem maklumat klinikal (*KCIS*), proses pengurusan data pesakit menjadi lebih teratur, cekap dan membolehkan maklumat pesakit diperoleh dengan mudah dan tepat pada masanya. Rajah 1.3 menerangkan tentang rajah proses kerja semasa menggunakan sistem ini. Kini, setiap pesakit di Hospital Pakar KPJ Ipoh akan mempunyai rekod elektronik yang disimpan dalam *KCIS*. Rekod elektronik ini menggantikan penggunaan fail kertas sebagai rekod utama. Maklumat penting seperti butiran peribadi, sejarah perubatan, keputusan ujian, diagnosis dan rawatan pesakit direkodkan secara elektronik. Rekod ini boleh diakses oleh kakitangan kesihatan yang

berkenaan dengan peranti IT seperti komputer, tablet atau komputer riba. Proses kerja semasa juga melibatkan penggunaan sistem klinikal untuk memasukkan data pesakit terus ke dalam sistem. Kakitangan kesihatan boleh merekod maklumat pesakit secara elektronik menggunakan antara muka yang disediakan oleh sistem. Ini mengurangkan kebergantungan pada rakaman manual dan mengurangkan risiko kesilapan menulis.

Kelebihan utama *KCIS* ialah keupayaannya untuk menyimpan dan mengurus data pesakit secara berpusat. Maklumat pesakit tersedia dalam masa nyata kepada semua ahli pasukan perubatan yang berkaitan, termasuk doktor, jururawat, ahli farmasi dan pakar lain yang terlibat dalam penjagaan pesakit. Ini memudahkan kerjasama antara ahli pasukan perubatan dan membolehkan penyelarasan yang lebih baik dalam menyediakan rawatan yang tepat dan berkesan. Dalam proses kerja semasa, akses kepada maklumat pesakit juga boleh ditingkatkan. Pasukan perubatan boleh mencari dan mengakses maklumat yang mereka perlukan dengan mudah tanpa perlu mencari fail kertas secara manual. Ini mempercepatkan proses membuat keputusan, mengurangkan risiko kehilangan atau kerosakan kertas, dan meningkatkan kelajuan tindak balas terhadap keadaan pesakit. Selain itu, *KCIS* juga membolehkan pengurangan risiko ralat dalam pemindahan data. Data pesakit yang direkod secara elektronik tidak perlu dipindahkan dari kertas ke peranti IT secara manual, sekali gus mengurangkan kemungkinan ralat atau kehilangan data dalam proses. Rajah 1.3 menunjukkan aliran proses kerja semasa di Hospital Pakar KPJ Ipoh.

Rajah 1.3 Aliran proses kerja semasa

Dalam sistem maklumat klinikal yang berkaitan, terdapat beberapa entiti yang terlibat iaitu Jabatan IT, doktor, kakitangan dan pesakit. Jabatan IT bertanggungjawab ke atas pengurusan sistem maklumat klinikal. Mereka menyelia pemasangan, konfigurasi, penyelenggaraan dan pemulihan sistem. Jabatan IT juga bertanggungjawab untuk memastikan keselamatan dan keselamatan data pesakit, menjalankan pemantauan, mengurus sandaran dan pemulihan data, serta menangani isu dan masalah teknikal dalam sistem. Mereka juga melaksanakan pelaporan daripada sistem maklumat klinikal untuk membantu dalam membuat keputusan dan pengurusan hospital secara keseluruhan.

Manakala, doktor menggunakan sistem maklumat klinikal untuk melakukan pemeriksaan perubatan, mendiagnosis penyakit, menyediakan rawatan dan merekod maklumat pesakit. Mereka boleh mengakses sejarah perubatan pesakit, keputusan ujian, diagnosis terdahulu dan maklumat penting lain yang diperlukan untuk menentukan diagnosis dan merancang rawatan. Doktor juga boleh menggunakan sistem untuk memeriksa keadaan keseluruhan pesakit dan membuat nota serta kemaskini tentang penjagaan yang diberikan.

Ini memudahkan kerjasama dan perkongsian maklumat antara doktor yang merawat pesakit.

Sementara itu, kakitangan hospital seperti jururawat dan pendaftar juga menggunakan sistem maklumat klinikal untuk merekod dan melaporkan data berkaitan pesakit. Mereka boleh memasukkan maklumat seperti data peribadi pesakit, sejarah perubatan, prosedur dan tindakan yang dilakukan, serta rekod pemerhatian dan rawatan lain. Kakitangan juga boleh menghasilkan laporan hospital yang diperlukan untuk pentadbiran dan pemantauan prestasi. Pesakit pula mendapat bil rawatan dan membuat bayaran kepada kakitangan hospital yang menggunakan sistem maklumat klinikal. Pesakit tidak mempunyai akses kepada sistem dan hanya kakitangan yang boleh memberi maklumat bayaran kepada pesakit.

Walaupun penggunaan *KCIS* membawa banyak kelebihan, terdapat beberapa batasan dan kelemahan dari segi keselamatan. Satu cara untuk menambah baik pengenalan teknologi adalah dengan menggalakkan penggunaan BYOD.

1.3.3 Proses Kerja Gabungan

Selain itu, terdapat juga kakitangan hospital yang menggunakan kedua-dua proses kerja. Ada juga kakitangan yang masih menulis dalam kertas manual dan fail kertas dahulu dan kemudian merekod semula ke dalam sistem maklumat klinikal (*KCIS*). Ketidaksediaan peranti IT mungkin menjadi salah satu faktor utama yang menyebabkan kakitangan menggunakan proses manual terlebih dahulu. Peranti IT terhad atau tidak mencukupi untuk semua kakitangan. Kakitangan yang menggunakan proses manual mungkin melibatkan situasi di mana peranti IT tidak segera tersedia atau digunakan oleh kakitangan lain. Selain itu, kakitangan yang menggunakan kedua-dua proses mungkin menyesuaikan diri dengan perubahan yang berlaku dalam keseluruhan sistem. Ini termasuk membiasakan diri dengan penggunaan peranti IT dan mengenali manfaat menggunakan sistem maklumat klinikal. Namun demikian, proses kerja ini juga mempunyai beberapa kelemahan.

1.4 PENYATAAN MASALAH

Amalan kerja di Hospital Pakar KPJ Ipoh mempunyai beberapa kelemahan yang perlu diberi perhatian dan diperbaiki. Kewujudan kelemahan-kelemahan ini boleh memberi kesan terhadap kecekapan dan keberkesanan operasi hospital.

Kebergantungan yang tinggi pada peranti milik hospital dan rangkaian internet hospital dalaman menimbulkan risiko, terutamanya jika terdapat gangguan dalam rangkaian atau kegagalan peranti, kakitangan tidak dapat mengakses sistem hospital dengan mudah. Ini boleh menyebabkan gangguan dalam penyampaian rawatan dan perkhidmatan kepada pesakit. Peranti milik hospital hanya menggunakan jaringan WiFi dalaman hospital. Pembatasan penggunaan jaringan WiFi hanya kepada rangkaian dalaman hospital bertujuan untuk memastikan bahawa peranti milik hospital hanya terhubung ke rangkaian yang terkawal dan selamat. Pembatasan penggunaan jaringan WiFi hanya kepada rangkaian dalaman hospital mempunyai tujuan yang baik, iaitu memastikan bahawa peranti IT milik hospital hanya terhubung ke rangkaian yang terkawal dan selamat. Namun, ia juga mempunyai kelemahan dalam situasi kecemasan yang mana seorang doktor berada di luar hospital dan memerlukan akses kepada maklumat pesakit secara cepat dan tepat. Keadaan ini boleh menyebabkan pembaziran masa dan tenaga dalam situasi di mana masa adalah faktor yang sangat penting dalam menyelamatkan nyawa pesakit. Selain itu, doktor tidak mempunyai akses ke maklumat pesakit yang diperlukan untuk membuat keputusan klinikal yang tepat dan segera dalam situasi kecemasan. Situasi ini juga boleh mempengaruhi kepercayaan pesakit terhadap sistem kesihatan dan hospital. Jika pesakit merasa bahawa doktor tidak mempunyai akses yang mencukupi ke maklumat pesakit dan tidak dapat memberikan rawatan yang tepat pada masanya, ini boleh menyebabkan ketidakpercayaan terhadap sistem kesihatan. Masalah ketersediaan juga timbul apabila kakitangan hospital mengalami kesukaran untuk mengakses peranti-peranti hospital yang digunakan secara bersama. Ini berlaku apabila peranti-peranti itu digunakan oleh kakitangan yang ramai, dan terdapat persaingan untuk mengakses peranti-peranti tersebut. Kesukaran untuk mengakses peranti-peranti tersebut boleh mengurangkan kecekapan dan keberkesanan kerja kakitangan hospital, terutamanya dalam situasi kecemasan di mana kakitangan memerlukan akses segera kepada maklumat penting pesakit. Selain itu, pengurusan peranti hospital dan pemantauan aktiviti penggunaan peranti-peranti tersebut juga mungkin menjadi sukar, terutamanya jika hospital mempunyai kakitangan yang ramai

dan peranti yang banyak. Di samping itu, keselamatan data dan privasi pesakit mungkin menjadi isu. Walaupun perisian dan konfigurasi telah dipasang untuk memastikan kebolehpercayaan dan keselamatan data, risiko kecurian data atau pelanggaran privasi masih wujud. Hospital perlu mengambil langkah tambahan untuk memastikan perlindungan yang kukuh bagi maklumat pesakit dan menguatkuasakan amalan keselamatan data yang ketat. Seterusnya, pergantungan kepada teknologi boleh menghadapi cabaran jika kakitangan tidak mempunyai kecekapan yang mencukupi dalam menggunakan sistem hospital. Kekurangan latihan dan kesedaran mengenai penggunaan peranti dan aplikasi hospital boleh menyebabkan kelewatan atau kesilapan dalam melaksanakan tugas harian. Ini boleh mengurangkan kecekapan dan kualiti penyampaian perkhidmatan. Masalah pematuhan adalah satu lagi isu yang penting dalam penggunaan peranti hospital oleh kakitangan hospital. Pematuhan terhadap peraturan keselamatan dan privasi data adalah penting untuk memastikan bahawa data kesihatan sensitif yang dikumpulkan dan disimpan oleh hospital dijaga dengan baik dan tidak didedahkan secara tidak sengaja atau tidak sah. Bagaimanapun, kakitangan hospital tidak mematuhi peraturan keselamatan dan privasi data yang berkaitan dengan penggunaan peranti IT. Salah satu sebabnya ialah tidak semua kakitangan hospital mempunyai pengetahuan yang mencukupi tentang peraturan-peraturan ini, atau kerana mereka mungkin tidak memahami risiko yang terlibat dalam penggunaan peranti IT yang tidak selamat. Membawa peranti milik hospital ke luar hospital juga boleh membuka peluang untuk penggunaan peranti secara tidak selamat atau tidak sah oleh kakitangan hospital. Misalnya, mereka mungkin menggunakannya untuk melayari laman web yang tidak selamat atau tidak patuh kepada polisi hospital. Hal ini boleh menyebabkan perisian hasad atau virus berada dalam peranti tersebut dan menyebarkan ke dalam rangkaian hospital ketika peranti tersebut dihubungkan semula ke dalam rangkaian hospital. Keadaan ini boleh menyebabkan risiko keselamatan yang serius, seperti kehilangan data kesihatan yang sensitif atau gangguan sistem hospital. Selain itu, kos yang tinggi diperlukan untuk membeli dan menyelenggarakan peranti dimiliki hospital. Selain kos pembelian, hospital juga perlu memikirkan kos penyelenggaraan dan pengurusan peranti-peranti tersebut. Kos ini meliputi kos untuk mengubahsuai, memasang dan menyelenggarakan peranti-peranti baru, membeli perisian keselamatan, memastikan peranti-peranti itu sentiasa dikemas kini dengan perisian dan peralatan terkini. Tambahan pula, hospital juga perlu memperbaharui dan membaiki peranti yang

rosak, dan kos ini mungkin menjadi lebih tinggi jika peranti-peranti tersebut digunakan secara meluas oleh kakitangan hospital. Hospital juga perlu mempertimbangkan kos untuk menggantikan peranti-peranti yang telah mencapai tempoh hayat atau tidak dapat diselenggarakan lagi, dan kos ini mungkin menjadi sangat tinggi jika hospital mengambil pendekatan untuk membeli peranti-peranti berkualiti tinggi dan canggih. Kos yang tinggi ini boleh mempengaruhi bajet hospital dan menjejaskan kemampuan hospital untuk menyediakan perkhidmatan kesihatan yang berkualiti tinggi.

Di samping itu, terdapat juga beberapa proses kerja yang bermasalah. Kakitangan yang mengamalkan proses kerja gabungan mungkin boleh mewujudkan konflik dalam data pesakit. Salah satu kelemahan ketara yang timbul ialah ketidaksepadanan maklumat antara rekod manual dan sistem maklumat klinikal. Ini boleh menyebabkan kekeliruan dalam diagnosis, rawatan atau keputusan lain yang berkaitan dengan pesakit. Selain itu, proses gabungan juga melibatkan penggunaan masa dan tenaga yang lebih besar. Kakitangan perlu meluangkan masa menyalin maklumat daripada fail kertas ke dalam sistem. Ini boleh mengurangkan produktiviti dan sumber pembaziran yang boleh digunakan untuk tugas lain. Tambahan pula, proses kerja kini turut melibatkan menunggu giliran untuk menggunakan peranti yang boleh memakan masa dan menyebabkan ketidakcekapan dalam operasi harian.

Selain daripada isu-isu yang telah dibincangkan sebelum ini, penerapan dan pelaksanaan BYOD di Hospital Pakar KPJ Ipoh diarahkan oleh Ibu Pejabat KPJ di Kuala Lumpur. Menurut Ketua Pengawai Digital KPJ, En. Nanda Kumar A/L Subramanian, ini adalah satu langkah penting dalam memperkukuhkan penggunaan teknologi dalam penyampaian perkhidmatan kesihatan di hospital tersebut. Selain itu, langkah ini diharapkan dapat membantu meningkatkan kecekapan, produktiviti dan kepuasan pengguna dalam hospital. Bagaimanapun, perlu ditegaskan bahawa pelaksanaan BYOD mesti disertakan dengan strategi keselamatan yang ketat untuk memastikan keselamatan data dan maklumat kesihatan yang sensitif. Oleh itu, hasil kajian ini bertujuan untuk membentuk garis panduan yang akan menjadi asas kepada penggunaan BYOD yang selamat dan terkawal di Hospital Pakar KPJ Ipoh. Garis panduan BYOD akan memberikan panduan yang jelas dan terperinci tentang dasar, prosedur dan langkah keselamatan yang mesti dipatuhi oleh pengguna peranti mudah alih BYOD di hospital. Tujuan utamanya adalah untuk melindungi keselamatan data dan maklumat kesihatan yang sensitif, mengekalkan privasi, dan mengurangkan risiko

yang berkaitan dengan penggunaan BYOD. Di samping itu, garis panduan ini akan memastikan hospital mematuhi peraturan dan piawaian yang digunakan dalam industri kesihatan. Justeru, garis panduan BYOD menjadi garis panduan penting bagi Hospital Pakar KPJ Ipoh dalam melaksanakan BYOD dengan selamat, cekap, dan mengikut peraturan yang berkuat kuasa. Melalui garis panduan ini, pengguna peranti mudah alih BYOD akan mempunyai pemahaman yang jelas tentang tanggungjawab, kewajipan dan langkah yang mesti mereka ambil untuk memastikan penggunaan BYOD yang selamat dan terkawal. Di samping itu, garis panduan itu juga akan menjadi rujukan kepada pasukan pengurusan IT dan keselamatan untuk mengatur infrastruktur teknologi, pemantauan keselamatan, dan menerima pakai pencegahan dan langkah balas yang sesuai. Dengan garis panduan BYOD yang komprehensif dan tersusun, Hospital Pakar KPJ Ipoh boleh melaksanakan BYOD dengan yakin, menjamin keselamatan data dan maklumat kesihatan yang sensitif, serta mengekalkan reputasi dan kepercayaan pesakit.

1.5 OBJEKTIF KAJIAN

Objektif kajian ini adalah untuk:

1. Mengenal pasti faktor yang mempengaruhi pelaksanaan BYOD yang selamat di Hospital Pakar KPJ Ipoh
2. Mengenal pasti proses kerja yang bermasalah
3. Mencadangkan garis panduan yang sesuai untuk diimplementasi dalam penggunaan peranti BYOD

1.6 PERSOALAN KAJIAN

Bagi menggambarkan keperluan dalam mengenal pasti kesediaan Hospital Pakar KPJ Ipoh mengimplementasikan konsep BYOD di dalam hospital, beberapa persoalan kajian akan difokuskan dalam kajian ini, iaitu:

1. Apakah strategi pelaksanaan BYOD yang boleh dicadangkan untuk Hospital Pakar KPJ Ipoh?
2. Apakah kelemahan-kelemahan yang perlu diberi perhatian?
3. Apakah prosedur yang boleh diikuti oleh pengguna di hospital bagi memastikan pelaksanaan BYOD yang selamat?

1.7 KEPENTINGAN KAJIAN

Kajian ini penting kerana ia dapat memberi pandangan yang lebih jelas tentang kesediaan dan keperluan Hospital Pakar KPJ Ipoh untuk melaksanakan konsep BYOD dalam persekitaran hospital. Kajian ini juga akan membantu hospital untuk memahami tahap kesedaran di kalangan kakitangan hospital berkenaan dengan dasar dan prosedur keselamatan BYOD. Kajian ini juga dapat membantu untuk mengenal pasti potensi kelemahan dan cabaran dalam melaksanakan strategi keselamatan BYOD yang berkesan di hospital. Selain itu, hasil kajian ini dapat memberi sumbangan kepada peningkatan kesedaran dan pengetahuan kakitangan hospital mengenai dasar dan prosedur keselamatan BYOD, sekali gus dapat membantu meningkatkan keselamatan data pesakit dan menjaga integriti hospital secara keseluruhan.

1.8 SKOP KAJIAN

Kajian ini bertujuan mengkaji strategi pelaksanaan BYOD yang selamat di Hospital Pakar KPJ Ipoh dengan fokus pada pengenalan penggunaan BYOD dan pembinaan garis panduan serta model keselamatan yang sesuai. Skop kajian meliputi penilaian keadaan semasa, kajian susastera, pengumpulan data melalui temu bual, analisis data, dan pembinaan garis panduan dan model keselamatan BYOD yang bersesuaian dengan Hospital Pakar KPJ Ipoh.

1.9 PENDEKATAN PENYELIDIKAN

Kajian ini menggunakan gabungan kaedah kuantitatif dan kualitatif. Kaedah kuantitatif digunakan untuk mengumpul data kuantitatif seperti nombor dan statistik yang diukur dan dianalisis secara kuantitatif. Contohnya, kajian ini dapat menggunakan kaedah kuantitatif untuk mengukur tahap kesedaran kakitangan hospital terhadap keselamatan BYOD dengan memberikan soal selidik dan menghitung skor dan statistik yang berkaitan. Kaedah kualitatif pula digunakan untuk mengumpul data kualitatif seperti pandangan, persepsi, dan maklum balas yang diungkapkan secara naratif atau deskriptif. Contohnya, kajian ini dapat menggunakan kaedah kualitatif untuk mengkaji pengalaman dan pandangan kakitangan hospital tentang pelaksanaan BYOD di hospital melalui temu bual atau kajian kes. Gabungan kedua-dua kaedah ini dapat memberikan

gambaran yang lebih menyeluruh tentang isu yang dikaji, membolehkan penyelidik untuk meneliti lebih terperinci aspek-aspek tertentu yang berkaitan dengan kajian, dan memberikan maklumat yang lebih bermakna tentang perkara yang dikaji.

1.10 PENYUSUNAN PROJEK

Bab I merangkumi pengenalan dan latar belakang kajian mengenai BYOD di Hospital Pakar KPJ Ipoh. Selain itu, objektif kajian iaitu mengkaji dan melaksanakan strategi keselamatan BYOD di hospital. Seterusnya, Bab II akan mengulas kajian-kajian lepas yang berkaitan dengan kajian ini dan penggunaan kajian susastera yang lepas akan membantu dalam memahami kajian dengan lebih baik. Bab III akan menerangkan kaedah yang digunakan sepanjang kajian dilaksanakan secara terperinci dan mengikut turutan. Bab IV pula akan membincangkan hasil penemuan kajian yang merujuk kepada analisis berdasarkan objektif yang telah ditetapkan. Bab V akan merumuskan kesimpulan, membincangkan penemuan kajian dan menyediakan cadangan untuk kajian seterusnya.

1.11 RUMUSAN

Kajian ini bertujuan mengkaji kesediaan Hospital Pakar KPJ Ipoh dalam melaksanakan konsep BYOD dengan memberi tumpuan kepada aspek keselamatan. Gabungan kaedah kuantitatif dan kualitatif digunakan untuk mengumpulkan data melalui soal selidik dan temu bual. Penemuan kajian menunjukkan bahawa kebanyakan kakitangan hospital mempunyai pengalaman menggunakan peranti BYOD untuk urusan peribadi, namun kebanyakan tidak mempunyai pengetahuan yang mencukupi tentang risiko keselamatan yang terlibat dalam penggunaan peranti ini dalam persekitaran hospital. Polisi dan peraturan BYOD yang jelas dan mantap sangat penting dalam merancang dan melaksanakan strategi keselamatan BYOD di hospital. Penemuan kajian ini memberikan kesimpulan bahawa Hospital Pakar KPJ Ipoh perlu meningkatkan kesedaran kakitangan hospital tentang risiko keselamatan yang terlibat dalam penggunaan peranti mudah alih peribadi di dalam hospital. Hospital ini juga perlu memperkuatkan polisi dan peraturan BYOD untuk memastikan keselamatan data dan

maklumat peribadi pesakit terjamin. Oleh itu, kajian ini memberi panduan dan cadangan untuk Hospital Pakar KPJ Ipoh dalam merancang dan melaksanakan garis panduan BYOD yang efektif dan selamat.

BAB II

KAJIAN SUSASTERA

2.1 PENGENALAN

Penggunaan peranti BYOD kini semakin berkembang pesat dan menjadi pilihan utama pelbagai organisasi dengan fokus utama pada aplikasi untuk peranti BYOD dan pemantauan yang sesuai. Konsep menyediakan pekerja dengan komputer, komputer riba dan tablet telah berubah dengan organisasi sekarang membenarkan pekerja untuk menggunakan peranti mudah alih sendiri untuk melaksanakan tugasan kerja dan memberikan akses kepada sistem organisasi.

Menurut kajian oleh MarketsandMarkets (2016), saiz pasaran BYOD dianggarkan bernilai USD 366.95 bilion menjelang 2022. Selain itu, menurut kajian oleh Strategy Analytics (2021), separuh daripada seluruh penduduk dunia kini memiliki telefon pintar sehingga bulan Jun 2021. Kira-kira empat bilion orang menggunakan telefon pintar hari ini. Di samping itu, Samsung (2018) menyimpulkan bahawa 82% pekerja yang ditinjau berkata peranti mudah alih meningkatkan produktiviti dan kelajuan membuat keputusan mereka di tempat kerja. 76% berkata telefon bimbit mempunyai kesan positif terhadap perkhidmatan dan kepuasan pelanggan. Sementara kajian oleh Gartner (2020) meramalkan bahawa menjelang 2023, 30% daripada semua organisasi IT akan mengembangkan dasar BYOD mereka untuk menyertakan Bring Your Own Enhancement (BYOE) untuk menangani peranan teknologi dalam perkembangan manusia di tempat kerja. Statistik ini menunjukkan bahawa penggunaan BYOD semakin popular dalam kalangan organisasi, tetapi kebanyakan organisasi perlu memastikan polisi keselamatan BYOD yang kukuh untuk mengelakkan risiko keselamatan yang besar. Penggunaan peranti BYOD di hospital juga semakin popular dengan memudahkan pekerja di hospital untuk mengakses data dan sistem maklumat kesihatan di mana sahaja dan pada bila-bila masa, mengurangkan kebergantungan pada

peranti yang diberikan oleh hospital.

Bagaimanapun, penggunaan BYOD di hospital juga mempunyai risiko keselamatan yang tinggi seperti penyebaran jangkitan, kebocoran maklumat kesihatan sensitif dan masalah keterasingan data yang boleh menjejaskan operasi hospital dan kesihatan pesakit. Oleh itu, hospital perlu mengambil kira risiko keselamatan tersebut dan memastikan strategi keselamatan yang sesuai dilaksanakan untuk mengurangkan risiko tersebut.

Menurut Tafheem et al. (2020), didapati bahawa hospital tidak mempunyai langkah keselamatan yang mencukupi untuk melindungi data pesakit pada peranti peribadi. Beliau menekankan keperluan untuk hospital menjalankan dasar dan prosedur untuk BYOD untuk memastikan keselamatan dan privasi data. Beliau juga mencadangkan penggunaan penyelesaian pengurusan peranti mudah alih (MDM) untuk mengurus dan melindungi peranti peribadi yang digunakan di hospital. Satu kajian yang dijalankan oleh Mike K. (2018) mencadangkan suatu rangka kerja untuk penggunaan BYOD di hospital. Rangka kerja tersebut memberi tumpuan kepada empat kawasan utama: dasar dan tadbir urus, teknologi dan infrastruktur, perlindungan data dan privasi, dan pengurusan risiko. Selanjutnya, Moh. Idris (2019) mencadangkan kepentingan pemilihan penyelesaian BYOD berdasarkan kawalan keselamatannya. Kajian tersebut mencadangkan suatu rangka kerja untuk memilih penyelesaian BYOD yang mengambil kira kawalan keselamatan seperti kawalan akses, pengesahan, penyulitan, dan pencegahan kebocoran data. Pelaksanaan polisi BYOD yang ketat sangat penting dalam mengurangkan risiko keselamatan dalam penggunaan BYOD di organisasi seperti mana yang telah dijelaskan oleh Marziana (2017). Di samping itu, Bilquis (2022) mengkaji risiko keselamatan siber yang terlibat dalam penggunaan BYOD di tempat kerja dan strategi untuk mengatasinya. Walaupun kajian ini tidak terfokus pada penggunaan BYOD di hospital, ia memberikan pemahaman yang penting mengenai risiko keselamatan yang perlu diambil kira dalam penerapan BYOD.

2.2 MEKANISME PROSES SEDIA ADA DI HOSPITAL PAKAR KPJ IPOH

Hospital Pakar KPJ Ipoh menyediakan peranti IT kepada kakitangan dalam bentuk komputer riba, telefon pintar dan tablet. Peranti ini disediakan untuk digunakan dalam

persekitaran hospital. Selanjutnya, hospital mempunyai mekanisme untuk penyelenggaraan dan pembaikan peranti IT. Jika terdapat masalah teknikal, kakitangan melaporkannya kepada jabatan penyelenggaraan IT untuk membaiki peranti. Setiap kakitangan yang menerima peranti IT akan diberikan ID pengguna dengan kelayakan akses yang ditentukan. Ini memastikan bahawa hanya kakitangan yang diberi kuasa boleh menggunakan peranti tersebut. Selain itu, hospital melaksanakan kawalan keselamatan untuk mengelakkan kehilangan peranti IT atau penggunaan tanpa kebenaran. Peranti IT diberikan tanda unik seperti nombor siri untuk memudahkan pengurusan penjejakan dan inventori. Hospital Pakar KPJ Ipoh juga mempunyai dasar privasi dan keselamatan maklumat yang menggariskan amalan yang perlu dipatuhi oleh kakitangan. Ini termasuk kewajipan untuk mengekalkan kerahsiaan maklumat dan mengambil langkah keselamatan yang sesuai apabila menggunakan peranti IT. Dalam usaha untuk meningkatkan pemahaman dan kesedaran kakitangan, hospital menyediakan latihan tentang penggunaan peranti IT yang betul. Latihan ini merangkumi aspek keselamatan, kepentingan melindungi maklumat sensitif, dan pemahaman tentang risiko yang terlibat dalam pengendalian peranti IT. Pemantauan aktiviti penggunaan peranti IT dilakukan oleh hospital untuk memastikan pematuhan kepada polisi dan prosedur yang ditetapkan. Ini boleh membantu mengesan dan memantau penggunaan yang tidak dibenarkan atau pelanggaran dasar keselamatan, membolehkan langkah pembetulan diambil jika perlu. Walaupun terdapat beberapa langkah dalam pengendalian peranti IT, masih terdapat kelemahan seperti tidak ada garis panduan khusus untuk pengendalian BYOD dan pengurusan kebolehcapaian peranti BYOD, dan risiko kehilangan atau kecurian peranti yang lebih tinggi. Dalam usaha untuk meningkatkan kecekapan dan keselamatan pengendalian peranti IT, adalah penting bagi Hospital Pakar KPJ Ipoh mengkaji strategi keselamatan BYOD yang sesuai dan memperkenalkannya ke dalam mekanisme proses.

2.2.1 Rangkaian Internet

Hospital Pakar KPJ Ipoh menggunakan rangkaian LAN atau *Local Area Network*. Rangkaian ini menghubungkan peranti-peranti seperti komputer, pencetak, dan peralatan perubatan lain di dalam hospital. Rangkaian LAN ini biasanya digunakan untuk menghantar data yang memerlukan kecepatan dan keselamatan yang tinggi,

seperti maklumat pesakit dan data perubatan yang sensitif. Rangkaian LAN di Hospital Pakar KPJ Ipoh biasanya menggunakan teknologi kabel Ethernet yang memberikan kelajuan tinggi dan kebolehpercayaan yang tinggi. Kabel Ethernet ini biasanya terletak di dalam dinding atau di dalam siling, dan dihubungkan ke soket pada setiap stesen kerja atau peranti lain di hospital.

Rangkaian LAN di Hospital Pakar KPJ Ipoh juga biasanya dilindungi dengan perisian tembok api (*firewall*) dan peralatan keselamatan lain untuk melindungi data sensitif dan memastikan akses hanya dibenarkan oleh kakitangan yang dibenarkan sahaja. Dengan menggunakan rangkaian LAN, hospital dapat menyediakan perkhidmatan perubatan yang lebih cepat dan lebih efisien, serta memastikan data dan maklumat sensitif pesakit selamat dan terlindung.

Selain itu, terdapat tiga jenis rangkaian WiFi di Hospital Pakar KPJ Ipoh iaitu CITRIXISH, KPJEMED dan KPJPUBLIC. CITRIXISH adalah jenis rangkaian WiFi yang digunakan untuk tujuan dalaman, di mana rangkaian ini membolehkan pengguna untuk mengakses sistem hospital. Oleh itu, rangkaian ini hanya boleh diakses oleh doktor dan kakitangan hospital yang telah mendapat kebenaran dan kelayakan untuk mengakses sistem hospital. KPJEMED dan KPJPUBLIC adalah jenis rangkaian WiFi yang digunakan untuk tujuan akses ke rangkaian luar hospital. KPJEMED adalah jaringan WiFi yang terhad kepada doktor sahaja, manakala KPJPUBLIC adalah jaringan WiFi yang boleh diakses oleh semua orang. Oleh itu, pengguna yang terhubung ke rangkaian ini hanya akan mempunyai akses ke Internet dan tidak boleh mengakses sistem hospital.

Penggunaan tiga jaringan WiFi yang berbeza ini membolehkan pengurusan keselamatan maklumat yang lebih baik di hospital. Ia membolehkan doktor dan kakitangan hospital mempunyai akses kepada sumber maklumat yang sensitif dan kritikal secara selamat melalui jaringan yang terhad, manakala penggunaan KPJPUBLIC sebagai jaringan WiFi untuk orang awam dapat memastikan bahawa akses ke rangkaian WiFi hospital terhad kepada pengguna yang memerlukan sahaja.

2.2.2 Mekanisme Keselamatan

Hospital Pakar KPJ Ipoh menggunakan pelbagai mekanisme keselamatan untuk

memastikan maklumat dan data yang disimpan dan diproses di hospital itu selamat dan dilindungi daripada ancaman luar. Antara mekanisme keselamatan yang digunakan adalah seperti berikut:

1. Tembok api: Hospital Pakar KPJ Ipoh menggunakan tembok api untuk mengawal trafik rangkaian yang masuk dan keluar dari hospital. tembok api ini berfungsi untuk melindungi sistem hospital daripada serangan luar seperti serangan nafi khidmat teragih (DDoS), virus, perisian hasad, dan sebagainya. Selain daripada melindungi sistem hospital daripada serangan luar, tembok api juga membantu mengawal akses penggunaan rangkaian dalam hospital. Dengan mengawal trafik rangkaian, ia dapat memastikan hanya pengguna yang dibenarkan sahaja yang boleh mengakses rangkaian hospital dan mengelakkan pengguna yang tidak sah daripada mengakses data sensitif hospital. Tembok api juga mempunyai keupayaan untuk menyekat akses terhadap laman web yang tidak diingini dan memastikan penggunaan Internet yang selamat dan selaras dengan polisi hospital. Sebagai contoh, hospital boleh menetapkan polisi untuk menghalang akses ke laman web yang berkaitan dengan perjudian, pornografi, atau aktiviti tidak bermoral lain yang tidak sesuai dengan nilai dan etika hospital. Penggunaan tembok api adalah penting dalam menjaga keselamatan dan kebolehpercayaan sistem rangkaian hospital. Dengan mengawal trafik rangkaian, tembok api dapat mengurangkan risiko serangan siber dan memastikan penggunaan rangkaian hospital yang selamat. Tembok api yang dipasang di hospital ialah *Sangfor*.

2. Anti-virus: TrendMicro (https://www.trendmicro.com/en_my/business.html) adalah perisian antivirus yang digunakan oleh Hospital Pakar KPJ Ipoh untuk melindungi sistem daripada serangan virus dan perisian hasad. TrendMicro menawarkan pelbagai ciri keselamatan siber seperti perlindungan terhadap ancaman siber yang semakin berkembang, mengesan dan menghapuskan perisian hasad dan virus, perlindungan privasi untuk data sensitif, perlindungan terhadap ancaman luar seperti serangan perisian tebusan, dan banyak lagi. TrendMicro juga menyediakan pengurusan terpusat yang membolehkan pentadbir rangkaian untuk menguruskan perlindungan keselamatan siber untuk

setiap peranti dalam hospital. Perisian ini mempunyai ciri keselamatan tambahan seperti pemantauan dan pengesan ancaman jaringan, menghalang serangan berdasarkan *file signature*, memastikan keselamatan rangkaian dengan pengesanan peranti yang tidak sah, dan banyak lagi. TrendMicro juga digunakan di Hospital Pakar KPJ Ipoh untuk memastikan keselamatan dan kebolehpercayaan sistem dalam menghadapi ancaman siber yang semakin berkembang.

3. Pengesahan pengguna: Sistem pengesahan pengguna adalah proses di mana pengguna perlu membuktikan identiti mereka sebelum diberikan akses ke sistem hospital. Proses pengesahan pengguna ini membantu menghalang pengguna tidak sah daripada mengakses sistem hospital dan mengurangkan risiko keselamatan siber. Dengan menghalang akses pengguna yang tidak dibenarkan, sistem hospital dapat melindungi data sensitif dan mengurangkan risiko jangkitan virus atau perisian hasad yang mungkin disebabkan oleh tindakan pengguna tidak bertanggungjawab. Pengesahan pengguna juga membolehkan hospital memantau akses pengguna dan mengesan sebarang aktiviti yang mencurigakan atau tidak sah. Sistem pengesahan ini dikenali sebagai *User Access System* (UAS) KPJ Ipoh.

4. Pengurusan log: Pengurusan log adalah proses memantau, merekod, dan menganalisis aktiviti sistem, rangkaian dan aplikasi yang berlaku dalam sistem IT dalam sesuatu organisasi. Hospital Pakar KPJ Ipoh menggunakan pengurusan log untuk merekod setiap aktiviti di dalam sistem hospital dan rangkaian untuk mengesan sebarang ancaman keselamatan siber dan juga untuk memenuhi syarat undang-undang dan peraturan yang berkaitan dengan pemantauan dan rekod aktiviti pengguna. Log aktiviti ini termasuk log maklumat masuk, log aplikasi, log sistem, log keselamatan, dan sebagainya. Hospital Pakar KPJ Ipoh menggunakan sistem pengurusan log yang berkesan dan mempunyai kemampuan untuk menganalisis log aktiviti untuk mengesan aktiviti yang mencurigakan dan memulakan tindakan sewajarnya untuk mengurangkan risiko keselamatan siber. Selain itu, Hospital Pakar KPJ Ipoh juga mengamalkan prinsip *least privilege* di mana hanya pengguna yang mempunyai keperluan

kerja sahaja yang diberikan akses ke sistem hospital dan rangkaian. Setiap aktiviti yang dilakukan oleh pengguna yang mempunyai akses ke sistem hospital akan direkodkan dalam log aktiviti dan akan disemak oleh pasukan keselamatan siber untuk memastikan bahawa tiada aktiviti yang mencurigakan atau mencemarkan keselamatan sistem hospital.

Secara keseluruhannya, Hospital Pakar KPJ Ipoh mengambil langkah-langkah keselamatan yang serius untuk melindungi maklumat dan data yang diuruskan oleh hospital itu. Ini termasuk penggunaan teknologi terkini dan pemantauan keselamatan yang berterusan untuk mengesan dan menangani sebarang ancaman keselamatan.

2.2.3 Penggunaan Citrix Workspace

Komputer yang dipasang dengan rangkaian LAN adalah peranti yang terhubung secara langsung dengan rangkaian kabel dan mempunyai akses terus ke sistem hospital seperti Sistem Maklumat Klinikal (*KCIS)*, Sistem Perakaunan dan Inventori (*HITS*), Sistem Pengurusan Katil (*BMS*) dan lain-lain. Penggunaan LAN membolehkan komunikasi antara peranti berlaku dengan cepat dan stabil kerana tidak bergantung pada isyarat gelombang seperti pada rangkaian WiFi. Bagaimanapun, peranti yang menggunakan rangkaian WiFi CITRIXISH tidak dapat mengakses sistem hospital secara langsung. Sebaliknya, pengguna perlu log masuk ke *Citrix Workspace* terlebih dahulu untuk mendapatkan akses ke sistem hospital. *Citrix Workspace* adalah platform perisian yang digunakan untuk menyediakan akses yang selamat dan mudah kepada aplikasi dan data dari peranti mudah alih.

Kelebihan *Citrix Workspace* termasuk:

1. Keselamatan yang lebih baik: menawarkan kawalan keselamatan yang lebih ketat, termasuk akses dengan pelbagai faktor, penyulitan saluran komunikasi, dan mengawal aplikasi serta data. Ini membantu menjaga data sensitif hospital dan privasi pesakit supaya selamat dan terlindung dari ancaman.
2. Mudah diakses: memudahkan pengguna untuk mengakses aplikasi dan fail dari mana-mana peranti, termasuk telefon pintar dan tablet, dari mana-mana lokasi.

Ini membolehkan kakitangan hospital untuk mengakses aplikasi dan data yang diperlukan dengan mudah dan cekap.

3. Meningkatkan produktiviti: membolehkan pengguna untuk mengakses aplikasi dan data dari mana-mana peranti dengan cepat dan mudah. Ini membolehkan kakitangan hospital untuk bekerja lebih cekap dan meningkatkan produktiviti.

Manakala, kelemahan *Citrix Workspace* termasuk:

1. Bergantung pada talian Internet: Pengguna perlu akses Internet yang baik untuk mengakses aplikasi dan data melalui *Citrix Workspace*. Jika sambungan Internet bermasalah atau terputus, pengguna tidak dapat mengakses aplikasi atau data tersebut.
2. Pengurusan dan penyelenggaraan: Pentadbir hospital perlu menyediakan dan menyelenggarakan infrastruktur yang diperlukan untuk menjalankan *Citrix Workspace,* yang melibatkan kos dan kerumitan penyelenggaraan. Pentadbir juga perlu menguruskan hak pengguna dan akses untuk memastikan keselamatan data dan privasi.
3. Kepentingan privasi: Walaupun *Citrix Workspace* menawarkan kawalan keselamatan yang ketat, ia masih boleh menjadi titik kelemahan untuk keselamatan dan privasi data. Oleh itu, pentadbir perlu memastikan bahawa pengguna memahami risiko dan mematuhi dasar keselamatan dan privasi hospital.

Ini bermakna setiap peranti mudah alih perlu memasang aplikasi Citrix Workspace dan log masuk menggunakan perakuan kelulusan (*credential)* yang telah diberikan oleh hospital sebelum penggunaan rangkaian WiFi. Ini adalah langkah keselamatan yang diambil oleh hospital untuk memastikan hanya pengguna yang dibenarkan sahaja yang mempunyai akses ke sistem hospital. Bagaimanapun, penggunaan peranti mudah alih hanya terhad di dalam hospital. Ini disebabkan peranti-peranti ini milik hospital dan disambung ke rangkaian WiFi dalaman CITRIXISH. Oleh itu, doktor atau kakitangan hospital tidak boleh membawa pulang peranti mudah alih ini.

2.3 ANCAMAN SEMASA PERANTI MUDAH ALIH

Ancaman terhadap keselamatan peranti mudah alih merujuk kepada risiko atau bahaya yang boleh membahayakan integriti, kerahsiaan dan ketersediaan peranti mudah alih tersebut. Peranti mudah alih Hospital Pakar KPJ Ipoh terdedah kepada beberapa kategori ancaman.

Ancaman daripada aplikasi adalah risiko yang timbul daripada aplikasi yang dipasang pada peranti mudah alih. Terdapat aplikasi yang mungkin mempunyai kelemahan keselamatan yang tidak diketahui, termasuk aplikasi yang dimuat turun daripada sumber yang tidak dipercayai atau aplikasi yang telah diubah suai. Aplikasi ini mungkin mengandungi perisian hasad, perisian pengintip atau perisian hasad lain yang boleh mencuri maklumat peribadi atau merosakkan peranti.

Ancaman daripada laman web adalah ancaman yang timbul daripada laman web yang tidak selamat atau direka untuk menyebabkannya tidak selamat. Pengguna peranti mudah alih mungkin terdedah kepada laman web pancingan data, laman web palsu atau laman web yang mempunyai skrip berniat jahat (*malicious script*). Apabila pengguna mengakses laman web ini, data peribadi mereka boleh dicuri dan peranti mudah alih boleh dijangkiti perisian hasad.

Ancaman rangkaian merujuk kepada risiko keselamatan yang berkaitan dengan penggunaan rangkaian tanpa wayar (Wi-Fi) atau sambungan rangkaian di hospital. Sambungan Wi-Fi awam yang tidak selamat boleh menjadi pintu masuk mudah bagi pihak yang tidak bertanggungjawab untuk mencuri data atau melancarkan serangan terhadap peranti mudah alih.

Yang terakhir ialah ancaman fizikal yang merujuk kepada risiko fizikal yang mungkin menimpa peranti mudah alih di hospital. Ini termasuk kehilangan atau kecurian peranti mudah alih, yang boleh mengakibatkan kebocoran data sensitif dan akses tanpa kebenaran.

Ancaman-ancaman ini boleh memberi kesan serius kepada Hospital Pakar KPJ Ipoh dari segi privasi dan keselamatan maklumat, reputasi hospital, kepercayaan pesakit, serta operasi harian. Oleh itu, adalah penting bagi hospital untuk mengambil langkah keselamatan yang sesuai untuk melindungi peranti mudah alih dan data yang mereka kendalikan. Ini termasuk pelaksanaan keselamatan yang ketat, penyediaan latihan kesedaran kepada pengguna, pengurusan aplikasi dan tapak web selamat, dan

perlindungan dasar peranti mudah alih untuk mengurangkan risiko ancaman tersebut Martin G. (2021).

2.4 PENGENALAN KEPADA PERANTI BYOD

Peranti BYOD merujuk kepada peranti mudah alih atau peribadi seperti telefon pintar, tablet, dan komputer riba yang dimiliki oleh individu dan digunakan untuk tujuan perniagaan atau kerja di dalam organisasi. Dalam konsep BYOD, pekerja diberikan kebebasan untuk menggunakan peranti mudah alih milik sendiri untuk melaksanakan tugas mereka di tempat kerja, bukan hanya bergantung pada peranti yang disediakan oleh majikan. Oleh kerana peranti BYOD adalah milik individu, ia membolehkan pengguna untuk lebih terbiasa dan produktif dengan peranti yang mereka gunakan secara peribadi, memungkinkan mereka untuk bekerja di luar tempat kerja dan memudahkan akses ke sistem dan data organisasi dari mana-mana sahaja dan pada bila-bila masa.

2.4.1 Insiden Keselamatan BYOD

Insiden keselamatan BYOD adalah situasi atau kejadian di mana keselamatan atau privasi peranti peribadi yang digunakan oleh seseorang dalam persekitaran perniagaan atau organisasi diabaikan atau terancam yang boleh mengakibatkan kerugian dan implikasi negatif yang serius. Ancaman ini boleh menyebabkan kerugian kepada perniagaan atau organisasi dalam bentuk kehilangan data sensitif, reputasi terjejas dan penalti undang-undang. Oleh itu, adalah penting bagi organisasi untuk mengambil langkah-langkah pengendalian risiko yang sesuai dan melaksanakan strategi keselamatan BYOD yang efektif untuk meminimumkan risiko insiden keselamatan BYOD. Beberapa insiden keselamatan yang terkait dengan penggunaan BYOD adalah *(Tafheem et al., 2020; Ezer Osei et al.,2016; Obinna et al.,2018)*:

1. Kehilangan atau pencurian peranti BYOD. Ia merupakan salah satu insiden keselamatan BYOD yang paling sering berlaku kerana peranti yang kecil dan mudah dibawa ini mudah hilang atau dicuri. Apabila peranti yang mengandungi data sensitif atau rahsia syarikat diambil oleh orang yang tidak bertanggungjawab, ia boleh membawa kepada ancaman keselamatan data yang

serius. Jika peranti tersebut tidak dilindungi dengan betul, pihak yang mengambilnya boleh memperoleh akses kepada data sensitif atau maklumat rahsia seperti katalaluan, nombor akaun, dan maklumat penting lain yang disimpan dalam peranti. Dalam senario kes terburuk, data ini boleh digunakan untuk tujuan jenayah seperti penipuan, pencurian identiti, atau jangkitan perisian hasad yang membawa kepada ancaman keselamatan yang lebih besar lagi. Selain itu, kehilangan atau pencurian peranti BYOD juga boleh membawa kesan buruk kepada reputasi organisasi dan kepercayaan pelanggan. Sekiranya maklumat sensitif atau data pelanggan diketahui telah hilang atau dicuri, ia boleh mengakibatkan penurunan keyakinan pelanggan dan mungkin mempengaruhi keputusan mereka untuk berurusan dengan organisasi tersebut pada masa depan.

2. Serangan perisian hasad – Ia adalah ancaman yang serius bagi keselamatan BYOD. Perisian hasad merujuk kepada sebarang perisian yang dicipta dengan tujuan jahat untuk merosakkan atau mengganggu peranti komputer, rangkaian atau data pengguna. Contohnya termasuk virus komputer, *worm*, trojan, perisian hasad, *spyware*, *adware*, dan sebagainya. Ia dapat merosakkan sistem operasi, mengambil alih kawalan sistem, mencuri data, mengganggu prestasi peranti, dan menyebar ke peranti lain melalui jaringan atau media penyimpanan bersama. Peranti BYOD yang terhubung ke jaringan organisasi dapat menjadi sasaran utama serangan perisian hasad jika tidak memiliki kawalan keselamatan yang mencukupi. Serangan perisian hasad dapat merosakkan sistem operasi dan aplikasi pada peranti BYOD, yang pada akhirnya dapat menyebabkan kerugian kewangan dan menyebabkan reputasi buruk bagi organisasi.
3. Akses tidak sah - Akses tidak sah adalah insiden di mana data atau sistem telah diakses oleh pengguna yang tidak sah, yang seharusnya hanya dapat diakses oleh pengguna yang diberi kuasa. Dalam konteks BYOD, ini terjadi apabila peranti yang tidak berdaftar terhubung ke jaringan organisasi atau ketika pengguna BYOD tidak memiliki izin untuk mengakses data atau sistem tertentu. Hal ini dapat menyebabkan kebocoran data sensitif, penggunaan data yang tidak sah, dan pelanggaran privasi pengguna lainnya. Contohnya, jika seorang pengguna menggunakan peranti BYOD yang tidak disetujui atau didaftar oleh

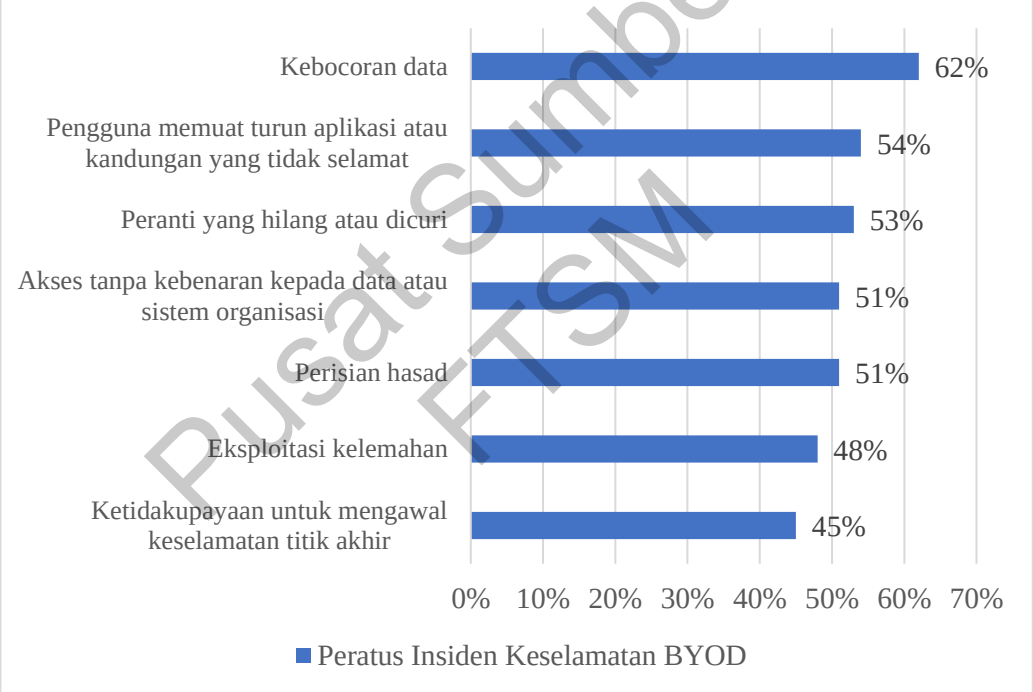
organisasi untuk mengakses sistem organisasi dan mengakses data sensitif, maka perkara ini menyebabkan akses tidak sah.

4. Penyalahgunaan akses - Penyalahgunaan akses dalam konteks penggunaan BYOD merujuk kepada tindakan pengguna yang secara tidak sah menggunakan akses yang diberikan ke peranti mereka untuk tujuan yang tidak berkaitan dengan pekerjaan atau tugas perusahaan. Contohnya, seorang pekerja mungkin memanfaatkan akses yang diberikan untuk mengakses maklumat rahsia organisasi untuk kepentingan peribadi mereka, atau mungkin menyalin data organisasi ke peranti mereka untuk tujuan yang tidak sah. Tindakan seperti ini dapat menyebabkan kebocoran data dan menjejaskan organisasi dari segi kewangan dan reputasi. Penyalahgunaan akses juga dapat terjadi ketika seorang pekerja mengizinkan orang lain untuk menggunakan peranti mudah alih mereka untuk mengakses sistem organisasi atau maklumat penting yang mereka miliki. Tindakan ini dapat mengakibatkan akses tidak sah ke maklumat penting dan membahayakan keselamatan dan keamanan organisasi.
5. Pelanggaran polisi BYOD - Pelanggaran polisi BYOD merujuk kepada pelanggaran terhadap peraturan atau polisi yang ditetapkan oleh organisasi berkaitan penggunaan peranti BYOD. Ini melibatkan penggunaan peranti yang tidak disetujui, memasang aplikasi yang tidak diizinkan, atau melakukan tindakan yang melanggar privasi atau keselamatan data organisasi. Contoh pelanggaran polisi BYOD termasuk:
    a. Menggunakan peranti yang tidak didaftar oleh organisasi: Organisasi mendaftar peranti yang disetujui dan memiliki ciri-ciri keselamatan tertentu yang harus dipenuhi sebelum peranti dapat digunakan untuk akses ke sistem organisasi. Jika seorang pengguna menggunakan peranti yang tidak disetujui, maka ini dapat membuka risiko keselamatan untuk organisasi.
    b. Memasang aplikasi yang tidak diizinkan: Organisasi memasang aplikasi yang diizinkan untuk digunakan pada peranti BYOD. Jika pengguna memasang aplikasi yang tidak diizinkan, aplikasi tersebut dapat menyebarkan perisian hasad yang boleh menyebabkan kebocoran dan kecurian ataupun kerosakan data organisasi.
    c. Melanggar privasi atau keselamatan data organisasi: Pengguna memilih

untuk menggunakan peranti BYOD untuk tujuan peribadi atau menyebarkan data sensitif organisasi melalui media sosial tanpa izin. Perkara ini dapat membahayakan privasi dan keselamatan data organisasi.

d. Tidak mematuhi prosedur pelaporan pelanggaran: Jika seorang pengguna mengetahui tentang pelanggaran keselamatan atau privasi yang berkaitan dengan BYOD, mereka harus melaporkannya kepada pihak berkuasa atau IT dengan segera. Tidak melaporkan pelanggaran dapat mengakibatkan risiko keselamatan yang lebih besar untuk organisasi.

2.4.2 Kebimbangan Keselamatan Utama BYOD



Rajah 2.1 Insiden Keselamatan BYOD

Sumber: Cybersecurity Insiders (2021)

Berdasarkan hasil laporan Cybersecurity Insiders seperti yang ditunjukkan dalam rajah 2.1, terdapat beberapa kebimbangan utama mengenai keselamatan BYOD. Dalam laporan itu, beberapa insiden keselamatan BYOD yang ketara telah dikenal pasti. sensitif yang disimpan dalam peranti mudah alih. Kebocoran data boleh mengakibatkan

Antaranya ialah kebocoran data adalah kebimbangan utama dengan peratusan sebanyak 62%. Ini menunjukkan bahawa terdapat risiko tinggi kebocoran atau penyebaran data kerugian serius bagi organisasi, seperti kehilangan maklumat sulit atau penyalahgunaan data oleh pihak yang tidak dibenarkan.

Selain itu, sebanyak 54% responden menyatakan kebimbangan mengenai penggunaan aplikasi atau kandungan yang tidak selamat yang dimuat turun oleh pengguna BYOD. Memuat turun aplikasi atau kandungan yang tidak dipercayai atau tidak selamat boleh membuka pintu kepada serangan siber, seperti perisian hasad atau perisian tebusan, yang boleh membahayakan peranti dan data di dalamnya. Sebanyak 53% responden pula bimbang tentang kehilangan atau kecurian peranti mudah alih BYOD. Kehilangan atau kecurian peranti boleh mengakibatkan akses tanpa kebenaran kepada data dan maklumat sensitif, serta mempertaruhkan kerahsiaan dan integriti data yang disimpan dalam peranti.

Di samping itu, 51% responden menyatakan kebimbangan mengenai akses tanpa kebenaran kepada data atau sistem organisasi. Capaian tanpa kebenaran boleh membahayakan keselamatan dan privasi maklumat, serta mengancam kesinambungan operasi organisasi. Peratusan yang sama iaitu 51% juga menunjukkan kebimbangan tentang kewujudan perisian hasad yang boleh membahayakan peranti dan data pengguna. Perisian hasad boleh mencuri maklumat peribadi atau mengakses data secara haram, membahayakan integriti dan kerahsiaan maklumat.

Tambahan pula, 48% responden menyatakan kebimbangan mengenai eksploitasi kelemahan dalam peranti mudah alih BYOD. Eksploitasi kelemahan sedemikian boleh dimanfaatkan oleh penyerang untuk mendapatkan akses tanpa kebenaran kepada data dan sistem yang terdedah, menyebabkan kerugian besar kepada organisasi.

Akhir sekali, sebanyak 45% responden menyerlahkan kekurangan keupayaan untuk mengawal keselamatan titik akhir *(endpoint security)* peranti BYOD. Ketidakupayaan untuk melaksanakan langkah keselamatan yang berkesan pada peranti boleh meningkatkan risiko serangan dan mengancam keselamatan secara keseluruhan.

2.5 PENGGUNAAN PERANTI BYOD DALAM PERSEKITARAN SELAMAT: KAJIAN LEPAS

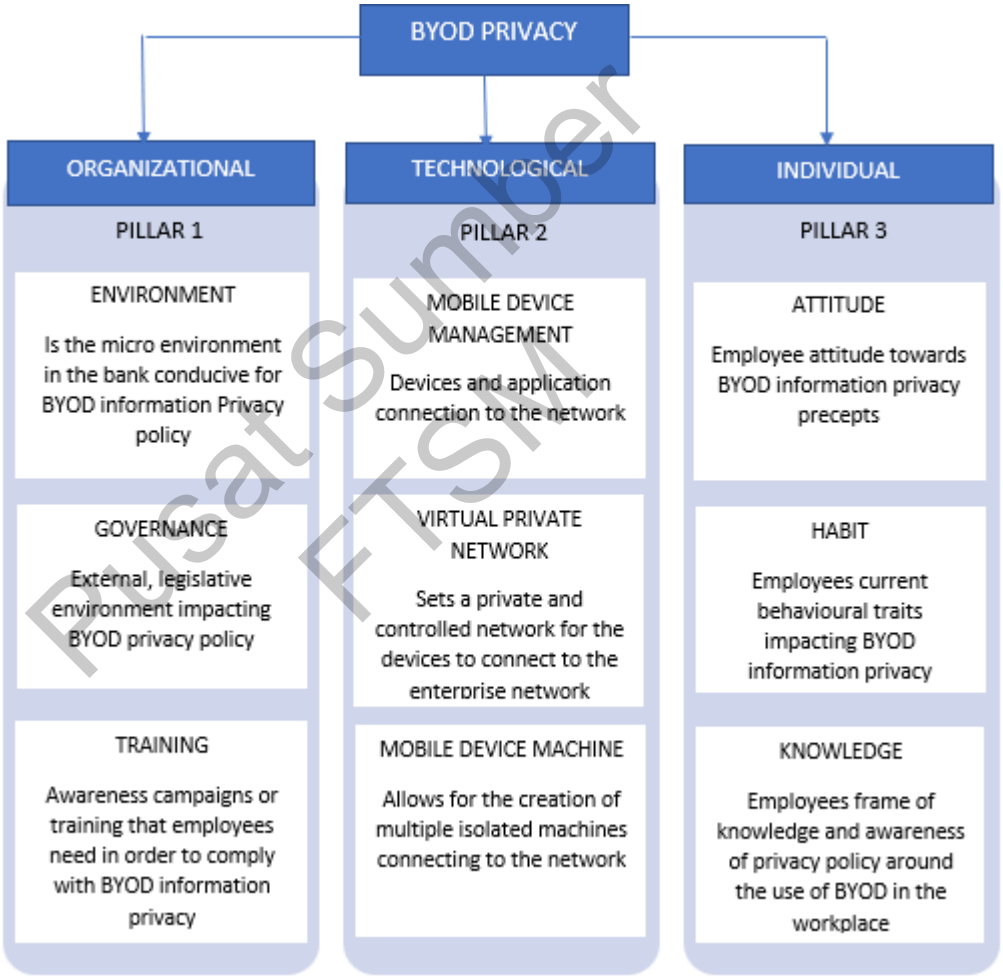
Mike K. (2018) telah membentangkan satu rangka kerja yang komprehensif untuk membantu hospital dalam melaksanakan BYOD dengan jayanya. Beliau telah mengenal pasti empat model yang relevan dalam penggunaan BYOD iaitu Model Teknologi, Model Organisasi, Model Pihak Berkepentingan dan Model Keselamatan seperti yang diterangkan dalam rajah 2.2. Model Teknologi yang berkaitan dengan infrastruktur WIFI, seni bina sistem dan seni bina aplikasi untuk dipertimbangkan untuk menyokong penggunaan peranti peribadi di hospital. Model Organisasi membincangkan pengaturan tadbir urus dalaman, polisi, piawaian kualiti dan perolehan yang diperlukan dalam penerimaan BYOD. Model Pihak Berkepentingan memberi tumpuan kepada penglibatan pihak berkepentingan, latihan, panduan pengguna dan dokumentasi yang berkaitan dengan penggunaan peranti peribadi. Sementara itu, Model Keselamatan membincangkan perlindungan data, dasar BYOD dan penilaian risiko yang harus digunakan dalam persekitaran BYOD. Rangka kerja yang dicadangkan dalam kajian ini telah diuji di beberapa hospital di Switzerland dengan keputusan yang positif. Kajian ini menunjukkan bahawa dengan mengikuti langkah dan garis panduan yang dibentangkan dalam rangka kerja, hospital boleh mengguna pakai BYOD dengan berkesan dan cekap. Rangka kerja ini mempertimbangkan aspek teknikal, organisasi, penglibatan pihak berkepentingan dan keselamatan data penggunaan BYOD. Secara keseluruhan, kajian ini memberikan pandangan yang berharga untuk hospital yang ingin menerima pakai BYOD. Rangka kerja yang dicadangkan boleh menjadi panduan praktikal untuk memperkenalkan dan menyepadukan BYOD dalam persekitaran hospital dengan memberi perhatian kepada keperluan individu dan cabaran sedia ad

Rajah 2.2 Dimensi BYOD

Sumber: Mike K. (2018)

Alfred M. dan Stephen F. (2019) telah membincangkan isu privasi maklumat dalam konteks BYOD. Mereka mengenal pasti keperluan untuk strategi yang betul untuk menerima pakai BYOD tanpa mengorbankan privasi data untuk organisasi dan keselamatan maklumat. Sebelum penggunaan BYOD menjadi relevan, isu privasi maklumat lebih menjadi tanggungjawab Jabatan Teknologi Maklumat (IT) dan Pengurusan Risiko dalam sesebuah organisasi. Bagaimanapun, dengan BYOD, tanggungjawab ini diperluaskan kepada semua pekerja dalam organisasi. Kajian ini menyediakan rangka kerja untuk meningkatkan privasi maklumat dalam BYOD berdasarkan tinjauan yang dijalankan di sebuah bank di Zimbabwe serta kajian susastera tentang kesan Peraturan Perlindungan Data Am (GDPR) terhadap privasi maklumat. Tinjauan itu melibatkan penyertaan 205 pekerja, dengan 179 daripada mereka memberikan keputusan lengkap. Hasil tinjauan kemudiannya dianalisis secara kualitatif dan digabungkan dengan penemuan daripada kajian susastera. Kesimpulan dan cadangan daripada kajian ini menyatakan keperluan rangka kerja privasi data dalam fenomena BYOD. Rangka kerja ini berdasarkan tiga faktor utama, iaitu privasi organisasi, privasi individu, dan teknologi yang digunakan (rajah 2.3). Rangka kerja

ini menyediakan panduan praktikal untuk organisasi dalam menghadapi cabaran privasi maklumat dalam BYOD. Secara keseluruhan, kajian ini memberikan pandangan penting tentang isu privasi maklumat dalam BYOD. Dengan mengguna pakai rangka kerja yang dicadangkan, organisasi boleh melindungi privasi data mereka dengan lebih baik dalam persekitaran BYOD. Kajian ini juga menekankan keperluan untuk pemahaman kolektif dan kesedaran tentang dasar privasi dan pelaksanaan GDPR dalam konteks BYOD.



Rajah 2.3 Rangka Kerja Privasi BYOD

Sumber: Alfred M. et al. (2019)

Dalam tahun 2020, Nirusha R. telah mengkaji keadaan, masalah dan penyelesaian sedia ada yang berkaitan dengan BYOD. Penulis menyiasat penggunaan

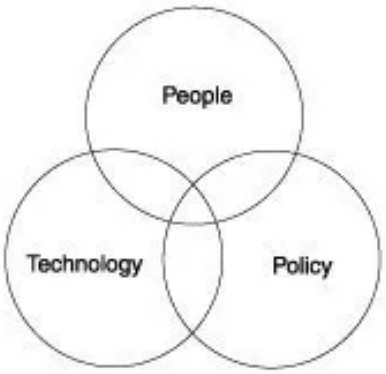
BYOD dalam persekitaran kerja dan mengenalpasti masalah yang mungkin timbul serta menyediakan penyelesaian untuk mengatasinya. Dalam kajian ini, penulis menjelaskan bahawa BYOD telah menjadi trend biasa dalam persekitaran kerja hari ini, di mana pekerja menggunakan peranti peribadi mereka untuk keperluan kerja. Namun begitu, penggunaan BYOD juga menyebabkan masalah yang perlu diatasi. Beberapa isu yang dibincangkan termasuk keselamatan data, privasi maklumat, pengurusan peranti dan dasar BYOD. Hasil daripada analisis kajian sedia ada adalah seperti yang ditunjukkan dalam rajah 2.4. Salah satunya ialah mengamalkan dasar BYOD yang jelas, termasuk dasar keselamatan yang ketat untuk melindungi data organisasi. Selain itu, penulis mengesyorkan penggunaan teknologi pengurusan peranti mudah alih (MDM) untuk mengurus peranti yang digunakan dalam BYOD. Pendidikan dan latihan pekerja juga dianggap penting supaya mereka memahami risiko dan dasar yang berkaitan dengan penggunaan BYOD. Kajian ini memberikan pemahaman yang mendalam tentang situasi BYOD, masalah yang timbul, dan penyelesaian yang boleh digunakan. Dengan mengguna pakai penyelesaian yang dicadangkan, organisasi boleh memanfaatkan potensi BYOD sambil mengekalkan keselamatan dan privasi data. Kajian ini merupakan sumber maklumat yang berharga untuk organisasi yang ingin berjaya melaksanakan BYOD dan mengatasi cabaran yang berkaitan.

Category	Security issue	Research
Deployment	To whom, where, and how to implement BYOD security into an existing network	[2]
Technical	Executing security methods to protect all devices	[2]
	Providing 24/7 support	[4]
	Protecting cloud storage facilities.	[5]
Policies and Regulations	Local government laws and regulations	[3]
Human Aspect	Employee education and training of BYOD security.	[2] [6]

Rajah 2.4 Faktor Keselamatan BYOD

Sumber: Nirusha R. (2020)

Richard N., Annabella E. dan Fred K. (2021) telah meneliti cabaran keselamatan yang dihadapi oleh institusi pendidikan dalam melaksanakan BYOD dan menyediakan penyelesaian untuk meningkatkan keselamatan dalam persekitaran BYOD. Penulis menggunakan pendekatan PPT (*People, Policy and Technology*) seperti dalam rajah 2.5. Pendekatan PPT digunakan untuk mengenalpasti cabaran daripada kajian susastera dengan menghimpunkannya kepada cabaran Teknologi, cabaran Pengguna dan cabaran Polisi. Cabaran Teknologi termasuk isu keselamatan peranti, kelemahan rangkaian dan keperluan untuk langkah keselamatan yang kukuh seperti tembok api, antivirus dan enkripsi data. Cabaran dari sudut pandangan Pengguna memberi tumpuan kepada aspek manusia pelaksanaan BYOD. Ini termasuk keperluan untuk kesedaran dan latihan pengguna tentang amalan keselamatan yang baik, serta mengurus akses pengguna untuk memastikan bahawa hanya individu yang diberi kuasa boleh mengakses maklumat sensitif. Cabaran Polisi menyerlahkan kepentingan mewujudkan dasar yang jelas dan komprehensif yang mengawal selia penggunaan peranti peribadi dalam persekitaran pendidikan. Ini termasuk pembangunan dasar penggunaan yang boleh diterima, dasar perlindungan data dan garis panduan untuk mengendalikan insiden dan pelanggaran keselamatan. Dengan menggunakan pendekatan PPT, kajian ini memberikan pemahaman yang menyeluruh tentang cabaran yang berkaitan dengan pelaksanaan BYOD dalam pendidikan, baik dari segi teknologi, manusia dan dasar. Pendekatan ini membolehkan pemahaman holistik tentang kerumitan yang terlibat dan memudahkan pembangunan strategi dan penyelesaian yang berkesan untuk meningkatkan keselamatan BYOD dalam persekitaran pendidikan.



Rajah 2.5 Model PPT

Sumber: Richard N. et al. (2021)

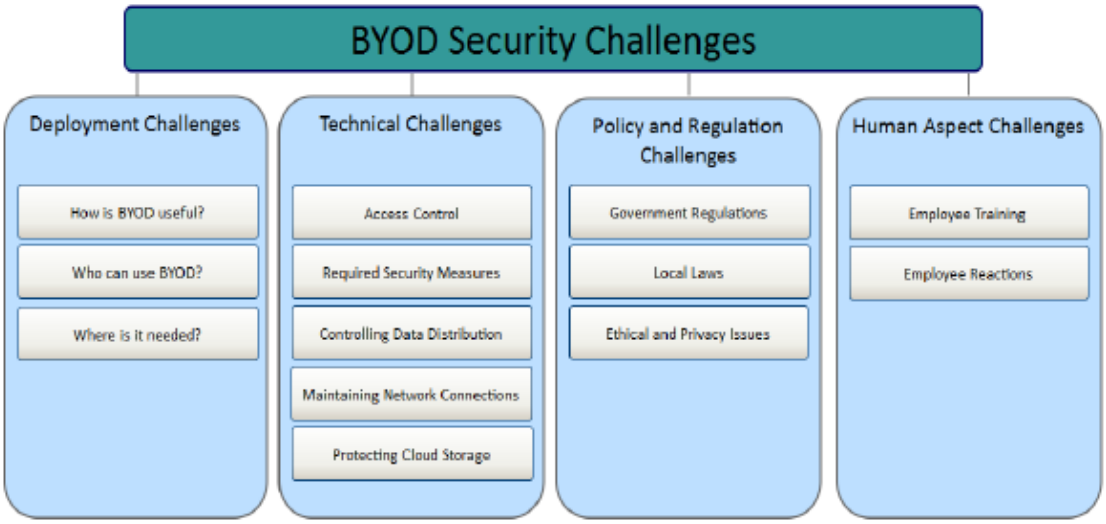
Ivan V. dan Adheesh B. (2019) telah membincangkan pembangunan model pengurusan risiko BYOD berdasarkan kajian kes dari sebuah organisasi di Afrika Selatan. Kajian ini bertujuan untuk menyediakan panduan praktikal untuk organisasi dalam menguruskan risiko yang berkaitan dengan penggunaan BYOD. Dalam kajian ini, mereka mengenal pasti cabaran yang dihadapi oleh organisasi dalam melaksanakan BYOD, termasuk keselamatan data, privasi pengguna, dasar penggunaan peranti peribadi dan pematuhan kepada peraturan dan undang-undang yang berkenaan (Rajah 2.6). Mereka kemudiannya mencadangkan model pengurusan risiko BYOD yang terdiri daripada beberapa peringkat iaitu pengenalpastian risiko, penilaian risiko, pembangunan strategi pengurusan risiko, pelaksanaan tindakan mitigasi, dan pemantauan dan penilaian berterusan. Kajian kes yang digunakan melibatkan sebuah organisasi di Afrika Selatan, di mana model pengurusan risiko BYOD dilaksanakan. Mereka berkongsi hasil dan pengalaman daripada pelaksanaan model ini, termasuk langkah-langkah yang diambil untuk mengatasi risiko BYOD khusus untuk konteks organisasi. Kajian ini memberikan pandangan yang berharga untuk organisasi yang ingin menerima pakai BYOD dengan menguruskan risiko yang berkaitan. Model pengurusan risiko BYOD yang dicadangkan boleh membantu organisasi dalam mengenal pasti, menilai dan mengurangkan risiko yang timbul daripada penggunaan peranti peribadi dalam persekitaran kerja. Dengan menggunakan model ini, organisasi boleh mengoptimumkan faedah BYOD sambil mengekalkan keselamatan, privasi dan pematuhan terhadap peraturan yang berkenaan.

PRIMARY RISK CATEGORY	BYOD RISK
Implementational	Protecting data, ensuring security, providing support
Technological	Malware
	Risks and vulnerabilities due to the installation of malicious software
	Cross-over threats
	Contamination of data in cloud storage
	Jailbreaking
	Compromised user accounts
	Phishing and social engineering
	Compromised network
Human aspects	Lack of control over data and devices
	Stolen or lost devices
	Identity theft
Organisational	Inadequate user education / Organisational security culture
	Lack of organisational policies (e.g. security, governance, etc.)
Legislation, regulation and privacy	POPI, ethical issues, tracking of data, breach of normal working hours, liability due to loss of organisational data, etc.

Rajah 2.6 Model Pengurusan Risiko BYOD

Sumber: Ivan V. et al. (2019)

Menurut Kathleen D. dan Maumita B. (2015), penggunaan BYOD memberikan faedah seperti fleksibiliti dan produktiviti yang lebih tinggi, tetapi juga membawa risiko keselamatan yang serius. Cabaran keselamatan yang timbul perlu diatasi melalui pendekatan holistik yang merangkumi aspek pelaksanaan, teknikal, dasar dan manusia (Rajah 2.7). Cabaran pelaksanaan melibatkan cara menggunakan dan mengurus peranti BYOD dengan selamat dan mematuhi dasar keselamatan organisasi. Cabaran teknikal memberi tumpuan kepada penggunaan teknologi keselamatan yang betul untuk melindungi peranti dan data daripada ancaman siber. Cabaran dasar dan kawal selia menekankan kepentingan mempunyai dasar BYOD yang jelas dan komprehensif dengan langkah keselamatan yang ketat. Cabaran aspek manusia menggariskan keperluan untuk kesedaran dan latihan untuk pekerja untuk mengelakkan tingkah laku berisiko dan menghargai kepentingan keselamatan dalam penggunaan peranti BYOD. Penulis menekankan bahawa dengan menghadapi cabaran ini melalui penggunaan rangka kerja keselamatan yang betul dan fokus penyelesaian yang betul, organisasi boleh melaksanakan BYOD dengan lebih selamat dan berkesan, seterusnya dapat menjaga keselamatan data dan maklumat organisasi.

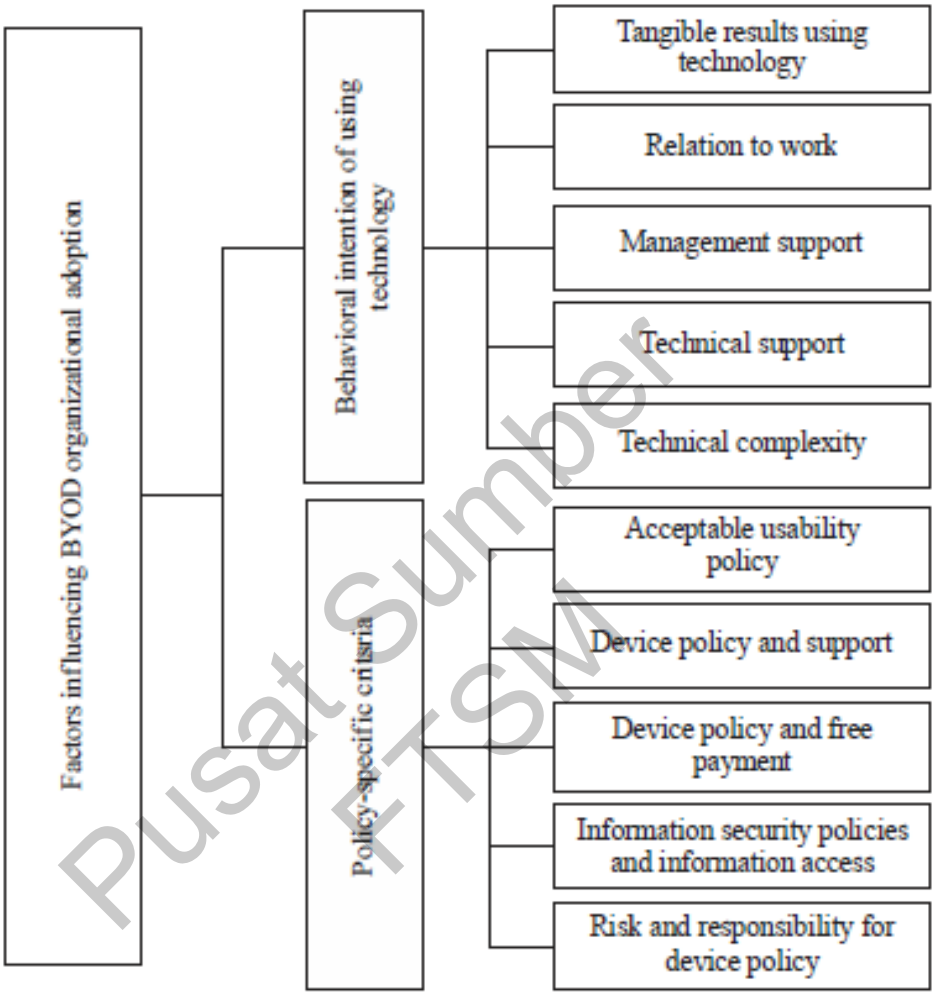


Rajah 2.7 Rangka Kerja Keselamatan dan Fokus Penyelesaian

Sumber: Kathleen D. et al. (2015)

Zainab et. al (2017) telah menerangkan dengan terperinci penggunaan Bring Your Own Device (BYOD) dalam organisasi dan mencadangkan model konsep yang menggunakan Hierarki Analitik Fuzzy daripada Proses (FAHP) seperti Rajah 2.8 untuk memahami faktor teknologi dan polisi yang mempengaruhi penggunaan BYOD. Dalam kajian ini, penulis menjelaskan bahawa penggunaan BYOD dalam organisasi memerlukan pemahaman yang mendalam tentang teknologi dan faktor polisi yang berkaitan. Untuk itu, penulis menggunakan FAHP sebagai kaedah untuk mengenalpasti, menilai, dan memberi timbangan kepada faktor-faktor tersebut. Model konseptual yang dicadangkan terdiri daripada dua faktor utama iaitu faktor teknologi dan faktor polisi. Faktor teknologi melibatkan aspek seperti kebolehpercayaan peranti, keselamatan data dan keserasian dengan infrastruktur organisasi. Faktor polisi termasuk perkara seperti dasar BYOD, pematuhan undang-undang dan tadbir urus keselamatan. Dengan menggunakan FAHP, penulis boleh memberikan pemberat relatif kepada setiap faktor dan sub-faktor dalam model konseptual. Ini membantu dalam memahami keutamaan dan hubungan antara faktor yang mempengaruhi penggunaan BYOD. Kajian ini memberikan pemahaman yang lebih baik tentang faktor teknologi dan polisi yang perlu dipertimbangkan dalam penggunaan BYOD dalam organisasi. Model konseptual yang dicadangkan boleh menjadi rangka kerja yang berguna dalam mengenalpasti, menilai, dan mengutamakan faktor-faktor ini. Dengan mempertimbangkan faktor-faktor ini,

organisasi boleh membuat keputusan yang lebih baik dalam menerima pakai BYOD dan memastikan pelaksanaan yang berjaya.



Rajah 2.8 Model Konseptual (Fuzzy Analytic Hierarchy Process)

Sumber: Zainab A. et al. (2017)

2.6 ANALISIS KAJIAN SUSASTERA

Berdasarkan carian susastera, tujuh model telah dikenal pasti yang boleh digunakan dalam kajian ini untuk mencapai objektif utama dan menjawab persoalan kajian, iaitu mengenal pasti faktor-faktor yang mempengaruhi keselamatan BYOD di Hospital Pakar KPJ Ipoh. Tujuh model yang dikenal pasti diringkaskan dalam jadual 2.3.

Jadual 2.1: Analisis Model Kajian Susastera

BIL.	MODEL	FAKTOR	SUMBER	TAHUN KAJIAN
1.	Dimensi BYOD	Teknologi, Keselamatan, Organisasi dan Pihak Berkepentingan	A Framework for the Adoption of Bring Your Own Device (BYOD) in the Hospital Environment: *Mike Krey*	2018
2.	Rangka Kerja Privasi BYOD	Teknologi, Organisasi dan Individu	Information Privacy in the BYOD: *Alfred Musarurwa; Stephen Flowerday et al.*	2019
3.	Model Keselamatan BYOD	Pelaksanaan, Teknikal, Polisi, Manusia	Bring Your Own Device (BYOD): Existent State, Issues, and Solutions: *Nirusha Rajapaksha*	2020
4.	Model PPT	Teknologi, Polisi dan Manusia	Enhancing Bring Your Own Device Security in Education: *Richard Ntwari; Fred Kaggwa; Annabella Habinka et al.*	2021
5.	Model Pengurusan Risiko BYOD	Pelaksanaan, Teknologi, Manusia, Organisasi, Perundangan, peraturan dan privasi	Development of Bring-Your-Own-Device Risk Management Model: Case Study from a South African Organisation: *Ivan Veljkovic; Adheesh Budree et al.*	2019
6.	Rangka Kerja Keselamatan dan Fokus Penyelesaian	Pelaksanaan, Teknologi, Polisi, Manusia	BYOD Security: A New Business Challenge: *Kathleen Downer; Maumita Bhattacharya et al.*	2015
7.	Model Konseptual menggunakan Fuzzy Analytic Hierarchy Process	Teknologi, Polisi	A New Conceptual Model for BYOD Organizational Adoption: *Zainab Alansari; Safeeullah Soomro; Mohammad Riyaz Belgaum et al.*	2017

2.6.1 Faktor Yang Mempengaruhi Implementasi BYOD

Berikut adalah faktor atau faktor yang telah dikenal pasti melalui analisis kajian-kajian susastera:

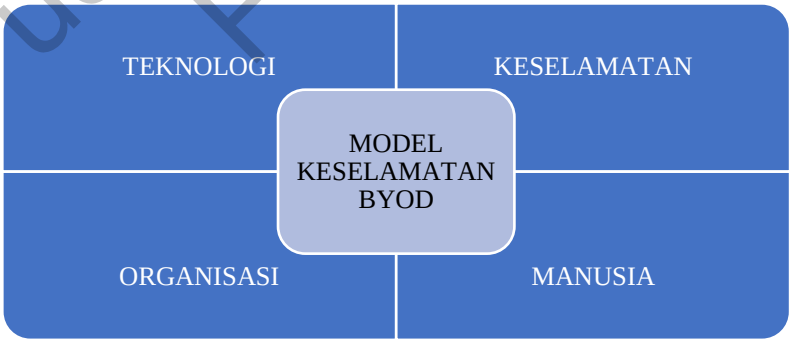
a. **Teknologi**: Faktor ini merujuk kepada komponen peranti mudah alih dan infrastruktur teknologi yang digunakan dalam persekitaran BYOD. Ini termasuk sistem pengendalian, aplikasi, keselamatan data, penyulitan, pengesanan ancaman, pemantauan rangkaian dan teknologi lain yang digunakan untuk melindungi peranti mudah alih dan data sensitif daripada serangan dan penyalahgunaan.
b. **Keselamatan**: Faktor ini berkaitan dengan langkah keselamatan yang diperlukan untuk melindungi data dan sistem daripada ancaman dan serangan. Ini termasuk penggunaan penyulitan, keselamatan rangkaian, tetapan katalaluan yang kukuh dan pemantauan aktiviti yang mencurigakan.
c. **Organisasi**: Faktor ini melibatkan struktur organisasi dan peranan yang ditentukan dalam konteks BYOD. Ini termasuk mewujudkan dasar dan prosedur BYOD, pengurusan risiko, pengasingan tugas dan melaporkan kepada pihak atasan.
d. **Manusia**: Faktor Manusia merujuk kepada pengguna peranti mudah alih BYOD dan individu yang terlibat dalam pengurusan, pematuhan dasar dan amalan keselamatan BYOD. Ini termasuk pengguna peranti mudah alih, pengurus IT, kakitangan keselamatan dan pihak berkepentingan lain yang terlibat dalam penggunaan peranti mudah alih BYOD. Kesedaran keselamatan, latihan pengguna, pematuhan dasar dan perlindungan privasi adalah aspek penting untuk dipertimbangkan dalam faktor Manusia.
e. **Pelaksanaan**: Faktor Pelaksanaan adalah cara melaksanakan langkah keselamatan BYOD ke dalam rangkaian sedia ada. Mengenal pasti siapa dalam organisasi memerlukan BYOD dan mengenal pasti tempat atau situasi di mana penggunaan BYOD memberikan manfaat yang ketara. Ini termasuk memilih peranti mudah alih yang sesuai, menyediakan akses selamat, menetapkan dasar penggunaan peranti dan memantau pematuhan pengguna.

   Polisi / Perundangan, peraturan dan privasi: Faktor Polisi merujuk kepada peraturan dan arahan yang ditetapkan untuk mengawal selia penggunaan peranti mudah alih BYOD. Ini termasuk dasar, piawaian, prosedur dan tindakan penguatkuasaan yang memastikan pematuhan dan perlindungan keselamatan

dalam penggunaan peranti mudah alih BYOD. Polisi ini juga melibatkan isu penting seperti perlindungan privasi, pematuhan undang-undang, pengurusan risiko dan tindak balas terhadap pelanggaran keselamatan. Faktor Polisi berbeza dengan Faktor Organisasi. Faktor Organisasi menumpu kepada struktur organisasi dan proses dalaman dalam mengurus keselamatan BYOD, manakala faktor Polisi memberi tumpuan kepada dasar dan prosedur yang ditetapkan untuk mengawal dan melindungi penggunaan BYOD dalam organisasi. Walaupun kedua-duanya berkaitan dengan pengurusan keselamatan BYOD, fokus dan peranan mereka berbeza dalam konteks pengaturcaraan dan pelaksanaan langkah keselamatan BYOD.

2.7 MODEL KESELAMATAN BYOD YANG DICADANGKAN

Rajah 2.9 ialah model keselamatan yang disediakan hasil daripada kajian susastera yang telah dilaksanakan. Secara kesimpulannya, pembinaan model keselamatan ini mampu dijadikan panduan untuk memastikan kajian ini dapat menjawab persoalan kajian yang telah ditimbulkan dalam Bab I. Model kajian ini juga memastikan objektif utama kajian ini tercapai.



Rajah 2.9: Model Keselamatan BYOD

Garis panduan keselamatan BYOD di Hospital Pakar KPJ Ipoh perlu mempertimbangkan beberapa faktor penting bagi memastikan penggunaan BYOD mematuhi dasar dan peraturan yang ditetapkan. Faktor-faktor yang dicadangkan ialah Teknologi, Keselamatan, Organisasi dan Manusia.

Faktor Teknologi dipilih kerana ia merupakan asas pelaksanaan BYOD. Dalam garis panduan, penekanan harus diberikan pada teknologi yang digunakan untuk mengurus peranti mudah alih BYOD di hospital. Ini termasuk pengenalan perisian keselamatan yang canggih, sistem pengesanan ancaman, penyulitan data, pengurusan identiti dan alatan keselamatan lain yang berkaitan. Langkah-langkah ini adalah perlu untuk melindungi maklumat sensitif serta melaksanakan kawalan teknikal yang diperlukan dalam penggunaan BYOD.

Keselamatan adalah aspek kritikal menggunakan BYOD di hospital. Oleh itu, garis panduan keselamatan BYOD harus menekankan langkah keselamatan yang perlu diambil untuk melindungi data dan sistem di hospital daripada ancaman keselamatan dan risiko yang berkaitan dengan penggunaan peranti mudah alih BYOD. Ini termasuk menggunakan mekanisma penyulitan, keselamatan rangkaian, penetapan katalaluan selamat dan pemantauan aktiviti yang mencurigakan.

Aspek organisasi juga perlu dipertimbangkan dalam garis panduan keselamatan BYOD. Garis panduan perlu mengambil kira struktur organisasi hospital, serta tanggungjawab dan peranan yang berkaitan dengan penggunaan BYOD. Ini melibatkan pengenalpastian pelbagai jabatan dan keperluan mereka dalam penggunaan BYOD. Di samping itu, garis panduan harus menjelaskan peraturan dan prosedur yang berkaitan dengan penggunaan peranti mudah alih BYOD di hospital. Pemantauan dan pematuhan garis panduan organisasi yang ditetapkan juga perlu dititikberatkan.

Faktor Manusia merupakan faktor penting dalam penggunaan BYOD di Hospital Pakar KPJ Ipoh. Oleh itu, garis panduan keselamatan BYOD perlu menyediakan latihan dan kesedaran kepada pengguna BYOD tentang isu keselamatan, amalan terbaik dalam penggunaan BYOD, serta tanggungjawab individu dalam mengekalkan keselamatan dan melindungi data sensitif apabila menggunakan peranti mudah alih BYOD. Faktor manusia juga merujuk kepada pemantauan dan tindakan yang diambil terhadap aktiviti pengguna yang melanggar dasar atau mendapat akses tanpa kebenaran. Pengguna BYOD perlu memahami kepentingan keselamatan dan peranan mereka dalam melindungi maklumat sensitif di hospital.

Gabungan faktor Teknologi, Keselamatan, Organisasi dan Manusia dalam garis panduan keselamatan BYOD di Hospital Pakar KPJ Ipoh akan membantu memastikan keberkesanan dan kemampanan penggunaan BYOD sambil mengekalkan keselamatan dan melindungi maklumat sensitif. Dalam merumuskan garis panduan ini, perlu ada

penekanan terhadap penggunaan teknologi canggih, pelaksanaan langkah keselamatan yang ketat, pengaturan organisasi yang betul, dan pendidikan serta kesedaran pengguna BYOD. Hanya dengan mengintegrasikan kesemua faktor ini, Hospital Pakar KPJ Ipoh boleh mengamalkan penggunaan BYOD dengan selamat dan berkesan.

Faktor Pelaksanaan dan faktor Polisi tidak dipertimbangkan kerana kedua-dua faktor boleh diterapkan dan digabungkan dalam faktor Organisasi. Faktor Organisasi merangkumi pelbagai aspek berkaitan struktur, tadbir urus, peraturan, dan peranan yang berkaitan dengan penggunaan BYOD di hospital. Dalam konteks ini, kedua-dua pelaksanaan dan polisi adalah sebahagian daripada penyusunan organisasi yang berkesan.

2.8 RUMUSAN

Berdasarkan kajian susastera yang telah dijalankan, kajian ini akan membangunkan satu garis panduan BYOD di Hospital Pakar KPJ Ipoh berdasarkan model keselamatan yang telah dibentuk. Setiap faktor dalam model keselamatan akan dikaji dengan mendapatkan pendapat dan semakan pakar di dalam bidang keselamatan teknologi maklumat dalam bentuk soalan temu bual yang akan digunakan sebagai instrumen kajian. Hasil analisis dan semakan pakar akan dibincangkan secara terperinci di dalam Bab IV.

BAB III

METODOLOGI

3.1 PENGENALAN

Dalam kajian ini, metodologi yang digunakan merangkumi reka bentuk kajian untuk membina rangka kerja kajian, pemilihan sampel kajian yang melibatkan kakitangan yang terlibat dalam pengurusan dan penggunaan peranti mudah-alih di hospital, dan pengumpulan data melalui tinjauan soal selidik atau temu bual. Instrumen kajian seperti soal selidik disediakan untuk mendapatkan maklum balas mengenai strategi keselamatan BYOD yang akan dilaksanakan, cabaran yang dihadapi, dan persepsi kakitangan terhadap keberkesanan strategi tersebut. Proses pengumpulan data akan melibatkan protokol dan prosedur yang ditetapkan untuk memastikan data yang diperoleh adalah relevan dan sahih. Data yang dikumpul kemudiannya akan dianalisis menggunakan kaedah analisis yang sesuai seperti analisis kualitatif atau kuantitatif, bergantung kepada jenis data yang dikumpul. Akhir sekali, hasil kajian akan digubal dan dibentangkan dalam bentuk laporan yang merangkumi penemuan, rumusan, dan cadangan untuk menambah baik strategi keselamatan BYOD di Hospital Pakar KPJ Ipoh.

3.2 REKA BENTUK KAJIAN

Kajian ini menggunakan pendekatan kaedah campuran yang menggabungkan kaedah kualitatif dan kuantitatif. Pendekatan ini akan memberikan pemahaman holistik tentang strategi keselamatan BYOD yang akan dilaksanakan di hospital. Untuk kaedah kualitatif, langkah pertama ialah menjalankan analisis semakan susastera yang berkaitan tentang keselamatan BYOD, termasuk peraturan, amalan terbaik dan isu keselamatan yang berkaitan. Melalui analisis kajian susastera ini, faktor penting yang mempengaruhi strategi keselamatan BYOD dapat dikenalpasti.

Selain itu, sesi temu bual akan dijalankan bersama pakar dalam bidang keselamatan maklumat atau IT yang mempunyai pengetahuan dan pengalaman dalam pengurusan BYOD. Temu bual ini akan membantu mendapatkan pandangan pakar dan perspektif tambahan tentang pembentukan garis panduan keselamatan BYOD yang akan dilaksanakan di Hospital Pakar KPJ Ipoh. Bagi kaedah kuantitatif, analisis tinjauan soal selidik akan dilakukan kepada kakitangan yang menggunakan peranti mudah-alih di Hospital Pakar KPJ Ipoh. Soal selidik ini akan mengumpulkan data tentang persepsi pengguna dan pengetahuan mengenai konsep BYOD yang akan dilaksanakan. Soal selidik ini juga akan melibatkan soalan yang memfokuskan kepada aspek teknikal, seperti penggunaan perisian keselamatan, amalan penyulitan data, dan pemahaman tentang langkah-langkah keselamatan yang perlu diambil. Melalui gabungan analisis kualitatif dan kuantitatif, hasil kajian akan dapat memberikan gambaran menyeluruh tentang keberkesanan strategi keselamatan BYOD di Hospital Pakar KPJ Ipoh. Data yang diperoleh melalui analisis kuantitatif akan memberikan pemahaman tentang persepsi dan amalan pengguna, manakala penemuan daripada analisis kualitatif akan memberikan gambaran yang lebih mendalam tentang faktor-faktor yang mempengaruhi pelaksanaan dan keberkesanan garis panduan keselamatan BYOD.

Selain itu, dalam reka bentuk kajian ini juga penting untuk memastikan skop kajian tertumpu kepada kakitangan di Hospital Pakar KPJ Ipoh yang terlibat secara langsung dalam penggunaan dan pengurusan peranti mudah alih. Ini akan memastikan bahawa data yang diperoleh adalah relevan dan dapat memberikan pandangan menyeluruh tentang strategi keselamatan BYOD dalam persekitaran.

3.3 SAMPEL KAJIAN

Berdasarkan maklumat yang diberikan oleh Bahagian Sumber Manusia hospital, jumlah keseluruhan kakitangan adalah 790 orang, dibahagikan kepada kakitangan daripada bahagian Perubatan dan Bukan Perubatan. Daripada jumlah tersebut, 40 orang telah dikenal pasti yang relevan untuk skop kajian serta mempunyai keperluan menggunakan peranti mudah-alih dalam kerja harian. Perincian data kakitangan hospital ditunjukkan dalam Jadual 3.1.

Jadual 3.1 Jumlah kakitangan hospital dan jumlah terlibat dalam skop kajian

Bahagian	Jumlah kakitangan	Jumlah terlibat dalam skop kajian
Perubatan	583	30
Bukan Perubatan	207	10
Jumlah Keseluruhan	790	40

Tujuan sampel adalah untuk mewakili populasi. Smith (2008) berpendapat bahawa saiz sampel minimum harus mempertimbangkan peratusan populasi, tetapi mengakui bahawa menggunakan 10% daripada populasi seperti yang dicadangkan oleh Cates (1990) mungkin terlalu besar dalam kebanyakan situasi. Sebaliknya, Smith mengesyorkan menggunakan peratusan yang lebih rendah, seperti 5-8% daripada populasi, untuk memastikan saiz sampel yang munasabah tanpa menanggung kekangan masa dan kos yang tinggi. Bagi populasi yang lebih kecil, Smith menekankan kepentingan memilih saiz sampel yang mencukupi untuk mencapai kebolehpercayaan yang mencukupi. Walaupun saiz sampel yang kecil boleh memberikan ketidakpastian dalam keyakinan penyelidik, Smith mencadangkan bahawa dengan menggunakan teknik persampelan yang baik dan analisis yang tepat, kelemahan ini dapat dikurangkan. Smith juga menekankan penggunaan kaedah statistik dalam menentukan saiz sampel yang sesuai. Dengan menggunakan formula statistik yang berkaitan, seperti formula Slovin atau pendekatan lain yang mempertimbangkan kebolehubahan dalam populasi, penyelidik boleh memilih saiz sampel yang menggambarkan populasi dengan tepat. Pendekatan Smith menyediakan alternatif kepada pandangan sebelumnya dengan menekankan kepentingan peratusan populasi, mempertimbangkan kebolehpercayaan dan ketepatan, dan menggunakan kaedah statistik yang sesuai untuk menentukan saiz sampel yang mencukupi. Tumpuan responden untuk kajian ialah doktor, jururawat dan kakitangan dari bahagian kewangan di Hospital Pakar KPJ Ipoh.

3.4 KAJIAN RINTIS

Sebelum kajian sebenar dijalankan, satu siri soal selidik telah diedarkan kepada tiga orang pengawai dalam bidang IT bagi menyokong kajian rintis dan menentukan jenis dan tahap soalan yang sesuai untuk diedarkan kepada responden. Set pertama soal selidik ini mempunyai empat seksyen utama bagi mendapatkan kajian faktor Teknologi, faktor Keselamatan, faktor Organisasi dan faktor Manusia. Tiga pegawai ini diberikan masa selama dua jam untuk menilai set pertama soal selidik ini dan memberikan sebarang pendapat dan cadangan penambahbaikan sekiranya perlu. Jadual 3.2 meringkaskan hasil penilaian soalan tinjauan. Ini menunjukkan keperluan untuk penambahbaikan soalan tinjauan dalam kajian ini.

Jadual 3.2 Penilaian Kajian Rintis Soal Selidik Peringkat Pertama

Bil.	Kriteria Penilaian	Seksyen A	Seksyen B	Seksyen C	Seksyen D
1.	**Tahap soalan**	Mudah	Sederhana	Sukar	Sederhana
2.	**Tahap kesesuaian soalan**	Sesuai	Kurang sesuai	Kurang sesuai	Sesuai
3.	**Jenis soalan**	Pilihan objektif	Pilihan objektif	Pilihan objektif	Pilihan objektif
4.	**Bilangan soalan**	Kekal	Perlu tambah	Perlu tambah	Perlu tambah
5.	**Cadangan Penambahbaikan**	Gunakan skala Likert	Gunakan skala Likert	Gunakan skala Likert	Gunakan skala Likert

3.5 INSTRUMEN KAJIAN

Dua kaedah pengumpulan data akan digunakan untuk menjalankan kajian ini. Kaedah kuantitatif melalui tinjauan soal selidik dan kaedah kualitatif dengan menemu bual pakar.

3.5.1 Tinjauan Soal Selidik

Kajian kuantitatif telah dilakukan dengan menjalankan soal selidik yang diedarkan secara atas talian kepada kakitangan hospital yang terlibat dalam skop kajian. Soal selidik ini meneroka ketersediaan kakitangan dalam pelaksanaan BYOD di hospital, serta mengkaji strategi keselamatan penggunaan BYOD. Soal selidik ini mempunyai 30 soalan dibahagikan kepada Bahagian 1 dan 2. Bahagian 2 dipecahkan kepada empat seksyen seperti yang ditunjukkan dalam jadual 3.3.

Jadual 3.3 Bahagian Soal Selidik

Bahagian	Perkara yang ingin dikaji
1	Latar belakang responden
2	A. Faktor Teknologi
	B. Faktor Keselamatan
	C. Faktor Organisasi
	D. Faktor Manusia

Responden diberi masa seminggu untuk menjawab dan melengkapkan soal selidik. Data tinjauan ini disimpan dalam talian menggunakan Borang Google dan perisian Microsoft Excel. Bahagian 1 akan merangkumi soalan yang berkaitan dengan latar belakang responden seperti jantina, umur, tempoh perkhidmatan dan bidang tugas semasa di Hospital Pakar KPJ Ipoh. Sementara itu, Bahagian 2 akan memfokus kepada empat faktor yang akan dikaji berdasarkan model keselamatan yang telah dibangunkan di akhir Bab II. Kaedah pengukuran yang digunakan adalah menggunakan skala Likert.

Skala Likert terdiri dari pilihan jawapan tetap yang digunakan untuk mengukur sikap atau pendapat responden. Skala ini bersifat ordinal dan digunakan untuk mengukur tahap persetujuan pendapat responden. Skala Likert yang digunakan dalam kajian ini terdiri dari empat pilihan jawapan. Nilai 1 mewakili pendapat "Tidak Setuju" dan nilai 5 mewakili pendapat "Sangat Setuju". Setiap pilihan jawapan diberikan nombor untuk memudahkan responden dalam menjawab tanpa perlu merujuk kepada jadual. Responden hanya perlu memilih satu pilihan jawapan yang paling sesuai. Jadual 3.4 memberikan gambaran ringkas tentang kandungan dan struktur soal selidik.

Jadual 3.4 Kandungan dan struktur soal selidik

Bahagian	Kajian	Fokus kajian	No. Soalan	Jumlah soalan
1	Latar belakang responden	Jantina, umur, tempoh perkhidmatan dan bidang tugas semasa	R1 - R6	6
2	Faktor Teknologi	Pembangunan komponen teknologi	A1 - A6	6
	Faktor Keselamatan	Penilaian aspek keselamatan	B1 - B6	6
	Faktor Organisasi	Pengurusan dan pembentukan dasar	C1 - C6	6
	Faktor Manusia	Pematuhan dasar dan amalan keselamatan	D1 - D6	6
			JUMLAH	**30**

3.5.2 Soalan Temu Bual

Bagi mengukuhkan data yang diperoleh dalam kajian ini secara kualitatif, maklumat daripada seorang pakar melalui sesi temu bual juga dikaji. Pakar yang telah dipilih mempunyai pengalaman bekerja dalam bidang IT lebih daripada 20 tahun. Beliau mempunyai kepakaran dalam bidang pengurusan infrastruktur teknologi, keselamatan siber dan transformasi digital dalam organisasi. Berikut adalah soalan-soalan yang dikemukakan:

S1. Pendapat tentang perkembangan dan penggunaan BYOD di tempat kerja pada masa sekarang.
S2. Kelebihan dan kelemahan yang dilihat dalam pelaksanaan BYOD di Hospital Pakar KPJ Ipoh
S3. Faktor-faktor yang mempengaruhi pelaksanaan BYOD yang selamat
S4. Pengendalian isu pengurusan peranti mudah-alih dan aplikasi yang tidak selamat atau tidak dipercayai.
S5. Cadangan strategi keselamatan untuk memastikan penggunaan BYOD berlaku dengan selamat.

3.5.3 Pemerhatian

Kakitangan hospital yang terlibat dalam skop kajian akan diberikan masa seminggu untuk menjawab soal selidik secara dalam talian menggunakan Borang Google sebelum data dikumpul untuk dianalisis. Kelebihan Borang Google adalah ia menjimatkan masa mengumpul data kajian dan membolehkan responden menjawab dengan mudah dan cepat. Hasil temu bual dengan pakar akan digunakan sebagai bahan rujukan tambahan dalam analisis kajian untuk menyokong dan mengukuhkan data yang diperoleh.

3.6 PROTOKOL DAN PROSEDUR PENGUMPULAN DATA

Proses pengumpulan data dalam kajian ini terbahagi kepada dua fasa. Fasa pertama ialah penyediaan dan penentuan skop kajian. Dalam fasa ini, objektif kajian ditetapkan secara terperinci termasuk isu atau topik yang akan disiasat berkenaan keselamatan BYOD di Hospital Pakar KPJ Ipoh. Persoalan kajian berkaitan objektif juga ditentukan. Selain itu, responden yang diperlukan untuk kajian ini seperti doktor dan kakitangan hospital yang terlibat dalam penggunaan BYOD di Hospital Pakar KPJ Ipoh dikenal pasti dan senarai responden disusun berdasarkan jabatan dan tahap pengalaman. Oleh kerana para responden adalah dari tempat yang sama, proses temu janji menjadi lebih mudah dan efisien.

Fasa kedua pula melibatkan aktiviti pengumpulan data melalui tinjauan soal selidik dalam talian menggunakan Borang Google. Platform Borang Google digunakan untuk membuat soal selidik yang mengandungi soalan yang sepadan dengan objektif kajian. Soal selidik ini kemudiannya diedarkan kepada responden melalui saluran komunikasi yang sesuai, seperti melalui e-mel atau aplikasi komunikasi dalaman hospital. Responden diberi masa yang mencukupi untuk menjawab soal selidik dalam tempoh yang ditetapkan selama seminggu. Proses pengumpulan data dipantau untuk memastikan tindak balas yang mencukupi diperoleh.

Sejajar dengan itu, penyelarasan dan kawalan kualiti data juga penting dalam protokol pengumpulan data ini. Data yang diterima daripada soal selidik akan disemak dan dinilai untuk memastikan kesesuaian, kebolehpercayaan dan kualiti. Setelah proses pengumpulan data selesai, data yang dikumpul akan digunakan untuk analisis dalam langkah kajian seterusnya.

Adalah penting untuk memastikan bahawa semua langkah dalam protokol dan prosedur pengumpulan data dipatuhi dengan teliti untuk memastikan kualiti dan ketepatan data yang dikumpul. Dengan mengikut protokol dan prosedur yang telah ditetapkan, data yang diperoleh akan lebih relevan dan dapat memberikan maklumat yang berguna untuk menjawab persoalan kajian. Berikut adalah proses dan prosedur dalam pengumpulan data secara ringkas.

1. Mendapatkan Kebenaran dan Persetujuan:
    a. Hubungi responden secara peribadi melalui emel, panggilan telefon, atau pertemuan langsung untuk menjelaskan tujuan kajian dan kepentingan penyertaan mereka.
    b. Pastikan responden memberikan kebenaran atau persetujuan mereka untuk menyertai kajian dan menyumbangkan data.
    c. Jelaskan bahawa penyertaan mereka adalah sukarela dan privasi mereka akan dijaga.

2. Penjadualan Temu Janji
    a. Mengatur temu janji dengan responden
    b. Tetapkan masa yang sesuai untuk bertemu dengan responden.
    c. Berikan kefahaman yang jelas mengenai jangka masa yang diperlukan untuk sesi temu bual

3. Penyampaian Soal Selidik:
    a. Kongsi pautan tinjauan melalui platform Borang Google
    b. Pastikan pautan mudah diakses dan boleh diakses daripada peranti mudah alih atau komputer.
    c. Jelaskan bahawa responden dikehendaki mengisi semua bahagian soal selidik dengan jujur dan teliti.
    d. Berikan bantuan dan penjelasan untuk membantu responden memahami soal selidik dengan lebih baik.

4. Pengumpulan data

a. Beri masa yang mencukupi kepada responden untuk menjawab soal selidik dalam tempoh yang ditetapkan.
b. Pantau dan rekod bilangan maklum balas yang diterima daripada doktor dan kakitangan hospital.
c. Pastikan data yang dikumpul dikemas kini dalam talian dan disimpan dengan selamat.

3.7 ANALISIS DATA

Penyediaan data untuk proses analisis diperoleh daripada dua sumber iaitu data kuantitatif dan data kualitatif. Data kuantitatif diperoleh daripada soal selidik yang diberikan kepada doktor dan kakitangan hospital dalam skop kajian, manakala data kualitatif daripada analisis soalan temu bual pakar. Data kuantitatif yang diperoleh dianalisis menggunakan perisian Microsoft Excel dan *Social Science Statistical Package* (SPSS) untuk pengesahan data dan pengemaskinian data. Data yang diperoleh daripada penyelidikan ini direkod dan diteliti untuk menghasilkan pola dan kelas yang boleh diproses untuk menjawab objektif kajian. Data kualitatif pula mengandungi unsur subjektif kerana ia bergantung pada pandangan, tafsiran dan pengalaman pakar. Pakar memberikan pandangan peribadi dan memberi persepsi yang tidak boleh diukur secara kuantitatif.

3.7.1 Analisis Dan Interpretasi Data Kuantitatif

Data yang diperoleh daripada tinjauan ini akan dianalisis menggunakan statistik deskriptif. Dalam analisis ini, data akan diringkaskan untuk mengenal pasti pola dan menghasilkan nilai Min, peratusan dan frekuensi untuk faktor Teknologi, Keselamatan, Organisasi dan Manusia. Penilaian soalan dalam soal selidik menggunakan skala Likert dengan nilai 1 (Sangat Tidak Setuju), 2 (Tidak Setuju), 3 (Tidak Pasti), 4 (Setuju), dan 5 (Sangat Setuju). Bagi data Bahagian 1 berkaitan latar belakang responden, frekuensi dan peratusan akan dikira bagi setiap pilihan jawapan yang disediakan oleh responden. Bagi data di Bahagian 2, frekuensi, peratusan, nilai purata (Min) dan persepsi akan

dianalisis berdasarkan pilihan jawapan responden. Pengiraan nilai purata (Min) bagi setiap soalan akan mempengaruhi persepsi sama ada ia menghasilkan persepsi Positif (Min > 3.5) atau persepsi Negatif (Min < 3.5). Soalan yang memberi persepsi Positif akan dibincangkan sebagai faktor yang mempengaruhi pelaksanaan garis panduan keselamatan BYOD manakala soalan yang menghasilkan persepsi Negatif akan menjadi fokus penambahbaikan dalam keselamatan BYOD. Jadual 3.5 menunjukkan penentuan persepsi berdasarkan Min.

Jadual 3.5 Persepsi berdasarkan nilai min

Persepsi	**Min**
Positif	>= 3.5
Negatif	< 3.5

3.7.2 Pengesahan Data Kuantitatif

Dalam kajian ini, saiz sampel sasaran yang diperlukan ialah 40 daripada jumlah keseluruhan kakitangan iaitu 790 orang yang terdiri daripada dua bahagian utama iaitu bahagian perubatan dan bukan perubatan. 40 sampel ini telah dikenal pasti sebagai responden yang terlibat dalam skop kajian iaitu mereka yang terlibat penggunaan peranti IT untuk tugasan harian. Sekiranya terdapat data yang melebihi bilangan sampel yang diperlukan, data tersebut tetap akan diambil kira sebagai data tambahan yang boleh membantu dalam membuat keputusan akhir kajian. Data yang diperoleh akan dikemaskini untuk mengesan sebarang kesilapan yang mungkin berlaku semasa responden mengisi tinjauan soal selidik. Sekiranya terdapat ralat seperti ruangan yang dibiarkan kosong oleh responden, ruangan tersebut akan diisi dengan data yang mempunyai skala 3 - Tidak Pasti. Langkah ini diambil untuk memastikan tiada medan dibiarkan kosong yang boleh menyebabkan ralat dalam pengesahan data.

3.8 RUMUSAN

Kajian ini melibatkan penggunaan dua kaedah kajian iaitu kuantitatif dan kualitatif. Bagi kaedah kuantitatif, tinjauan soal selidik telah dijalankan secara dalam talian menggunakan platform Borang Google dan diedarkan kepada responden dalam skop kajian. Manakala bagi kaedah kualitatif, soalan temu bual diedarkan kepada pakar dalam bidang IT. Tujuan kaedah ini adalah untuk mendapatkan pendapat pakar tentang pelaksanaan BYOD di Hospital Pakar KPJ Ipoh. Data yang diperoleh daripada kedua-dua kaedah ini akan dianalisis menggunakan perisian Microsoft Excel dan SPSS untuk mendapatkan peratusan, frekuensi dan nilai purata (Min) faktor Teknologi, Keselamatan, Organisasi dan Manusia yang digunakan dalam model keselamatan BYOD. Penggunaan kedua-dua kaedah ini dipilih untuk memenuhi objektif kajian dan menjawab persoalan kajian yang telah ditetapkan sebelum ini.

BAB IV

ANALISIS DAN PERBINCANGAN

4.1 PENGENALAN

Bab ini membentangkan hasil kajian berdasarkan keputusan ujian dan maklum balas yang diterima daripada responden yang telah dikenal pasti sebagai peserta dalam skop kajian. Selain itu, analisis data juga telah dilakukan untuk menghasilkan penemuan kajian yang signifikan. Dalam kajian ini, perisian SPSS, versi 29.0.1.0 (171) telah digunakan untuk melakukan analisis data terperinci. Hasil kajian ini dipersembahkan dalam bentuk jadual, carta pai, dan graf untuk memudahkan pemahaman dan visualisasi penemuan. Dalam bab ini, hasil kajian dibentangkan bertujuan untuk menjelaskan jawapan kepada persoalan kajian iaitu mengenal pasti faktor-faktor yang mempengaruhi pelaksanaan peranti BYOD selamat di Hospital Pakar KPJ Ipoh. Selain itu, bab ini juga mencadangkan garis panduan yang sesuai untuk dilaksanakan dalam penggunaan peranti BYOD di hospital. Hasil kajian yang dibentangkan dalam bab ini diharapkan dapat memberi panduan dan maklumat yang relevan kepada pihak berkepentingan dalam melaksanakan penggunaan peranti BYOD yang selamat di Hospital Pakar KPJ Ipoh. Pemahaman tentang pemilihan faktor dan garis panduan yang dicadangkan akan membantu dalam memastikan kejayaan pelaksanaan dan keselamatan yang tinggi dalam penggunaan peranti BYOD di hospital.

4.2 HASIL SOAL SELIDIK

Statistik deskriptif digunakan untuk menganalisis latar belakang responden dalam kajian ini. Dengan menggunakan statistik deskriptif, data latar belakang responden

boleh diringkaskan kepada nilai purata dan peratusan bagi setiap pembolehubah yang terlibat. Analisis ini memberikan gambaran yang jelas tentang ciri-ciri responden dalam kajian ini. Selain itu, statistik deskriptif juga digunakan untuk menghasilkan pengiraan nilai Min bagi setiap faktor yang dikaji, termasuk teknologi, keselamatan, organisasi dan manusia. Nilai Min ini digunakan untuk menilai persepsi responden sama ada positif atau negatif terhadap empat faktor tersebut. Hasil analisis ini membantu dalam membentuk garis panduan pelaksanaan BYOD yang selamat di Hospital Pakar KPJ Ipoh.

Bagi menjalankan kajian ini, soalan tinjauan telah diedarkan secara dalam talian melalui Borang Google kepada responden yang telah dikenal pasti terlibat dalam skop kajian. Seramai 40 orang responden telah mengambil bahagian dalam menjawab soal selidik ini, memberikan maklum balas penting dalam menganalisis data dan menjalankan analisis statistik yang diperlukan.

4.2.1 Latar Belakang Responden

Analisis data latar belakang responden untuk tinjauan soal selidik ini telah ditunjukkan dalam bentuk jadual yang memaparkan frekuensi dan peratusan bagi setiap item soalan 1 hingga 4. Jadual 4.1 menunjukkan hasil analisis tersebut.

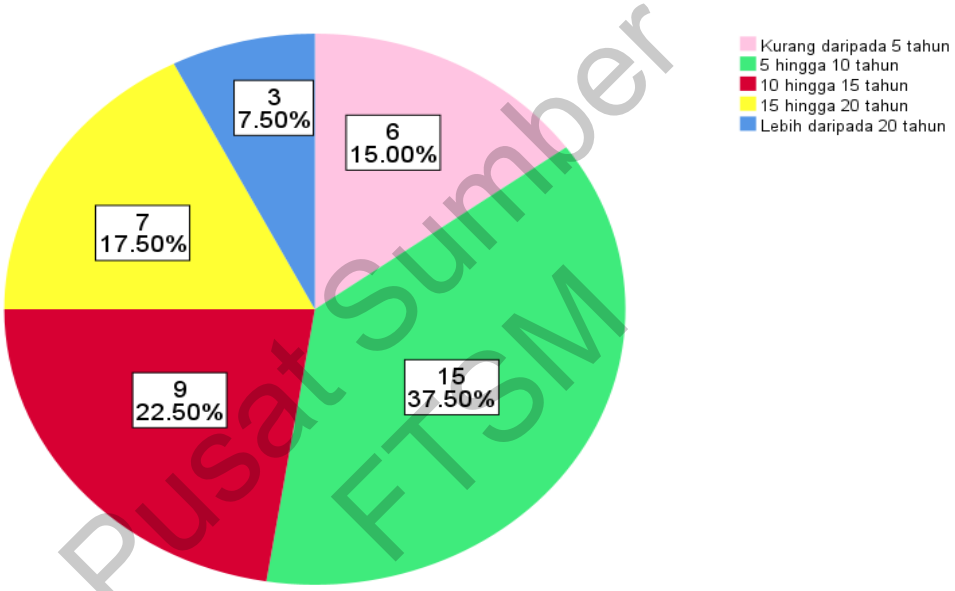
Jadual 4.1 Analisis Data Latar Belakang Responden

Bil.		Kategori	Frekuensi	Peratus (%)
1	Jantina			
	1.1	Lelaki	14	35
	1.2	Perempuan	26	65
2	Umur			
	2.1	< 21 tahun	1	2.5
	2.2	21 hingga 30 tahun	6	15
	2.3	31 hingga 40 tahun	19	47.5
	2.4	41 hingga 50 tahun	9	22.5
	2.5	> 50 tahun	5	12.5
3	Tempoh perkhidmatan			
	3.1	< 5 tahun	6	15
	3.2	5 hingga 10 tahun	15	37.5
	3.3	10 hingga 15 tahun	9	22.5
	3.4	15 hingga 20 tahun	7	17.5
	3.5	> 20 tahun	3	7.5
4	Bidang tugas			
	4.1	Doktor	24	60
	4.2	Ketua Jururawat	5	12.5
	4.3	Pengawai kewangan	10	25
	4.4	Lain-lain	1	2.5
5	Mekanisme proses dan keselamatan IT sedia ada di Hospital Pakar KPJ Ipoh adalah memadai.	Sangat tidak setuju	0	0
		Tidak setuju	0	0
		Kurang setuju	2	5
		Setuju	31	77.5
		Sangat setuju	7	17.5
6	Memahami konsep BYOD	Ya	36	90
		Tidak	4	10

Kajian ini melibatkan 40 orang responden yang terdiri daripada 65% (26 orang) responden perempuan dan 35% (14 orang) responden lelaki. Daripada analisis jantina responden menunjukkan bilangan responden perempuan adalah lebih ramai berbanding responden lelaki. Ini berikutan bilangan kakitangan wanita di tiga bidang tugas terbabit adalah lebih ramai berbanding kakitangan lelaki.

Selain itu, analisis tinjauan soal selidik juga mendapati terdapat enam orang responden yang telah berkhidmat kurang daripada lima tahun iaitu sebanyak 15% daripada jumlah

keseluruhan responden. Seramai 15 orang responden berada dalam kategori tempoh perkhidmatan antara lima hingga 10 tahun iaitu sebanyak 37.5% daripada jumlah keseluruhan responden. Terdapat juga sembilan orang responden dalam kategori tempoh perkhidmatan antara 10 hingga 15 tahun iaitu 22.5%. Tambahan pula, tujuh orang responden berada dalam kategori tempoh perkhidmatan antara 15 hingga 20 tahun iaitu sebanyak 17.5%. Manakala terdapat tiga orang responden yang telah berkhidmat melebihi 20 tahun iaitu 7.5% daripada jumlah keseluruhan responden. Rajah 4.1 menunjukkan ringkasan peratusan tahun perkhidmatan responden.



Rajah 4.1 Carta pai tempoh perkhidmatan responden

Terdapat seorang responden yang berumur kurang daripada 21 tahun iaitu 2.5% daripada jumlah keseluruhan responden. Terdapat juga enam orang responden dalam kategori umur antara 21 hingga 30 tahun iaitu sebanyak 15% daripada jumlah keseluruhan responden. Responden dalam lingkungan umur 31 hingga 40 tahun adalah penyumbang tertinggi sebanyak 19 orang iaitu 47.5%. Manakala kategori umur 41 hingga 50 tahun sebanyak 22.5% dan 12.5% adalah responden dari linkungan umur lebih daripada 50 tahun.

Responden juga dikategorikan berdasarkan bidang tugas semasa mereka. Terdapat 24 orang responden yang berada dalam bidang tugas doktor iaitu sebanyak 60% daripada jumlah keseluruhan responden. Seterusnya, terdapat enam orang responden sebagai

Ketua Jururawat iaitu sebanyak 15% daripada jumlah keseluruhan responden. Manakala, terdapat juga 10 orang responden dalam bidang tugas Pegawai Kewangan iaitu 25%. Statistik menunjukkan responden daripada kategori umur antara 31 hingga 40 tahun adalah tinggi untuk setiap bidang tugas yang dikaji. Individu dalam kategori umur ini selalunya berada dalam fasa kehidupan di mana mereka terdedah kepada perkembangan teknologi yang pesat. Mereka mungkin lebih terbuka dan boleh menyesuaikan diri dengan perubahan teknologi baharu, dan mempunyai minat yang tinggi untuk meneroka dan menggunakan alatan dan aplikasi digital baharu. Ini merupakan salah satu sebab responden dari kategori ini dipilih untuk tinjauan soal selidik kajian ini. Rajah 4.2 menunjukkan statistik umur dan bidang tugas responden.

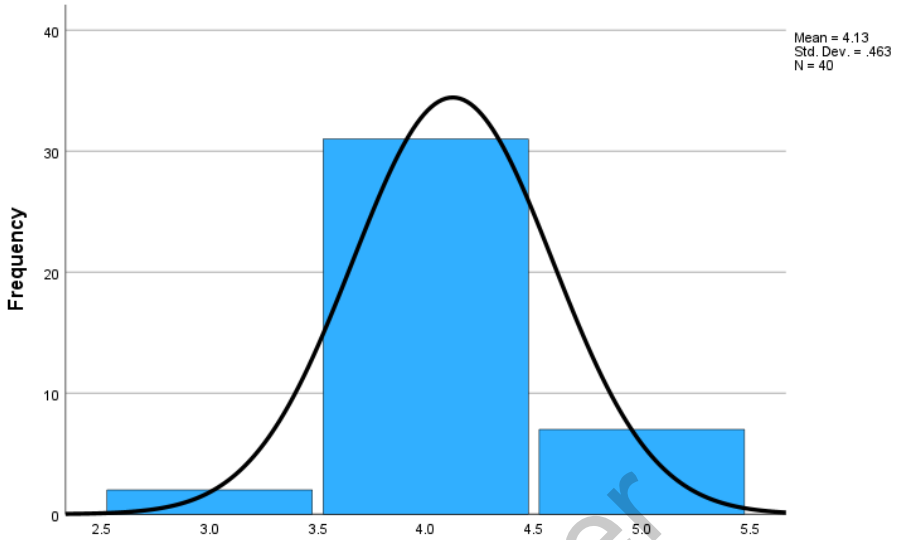
UMUR * BIDANG TUGAS Crosstabulation

Count

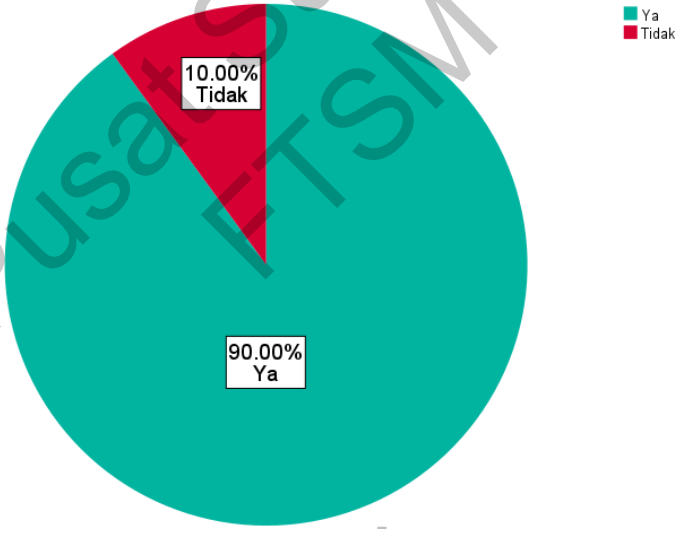
		BIDANG TUGAS			
		Doktor	Ketua Jururawat	Pengawai Kewangan	Total
UMUR	Kurang daripada 21 tahun	0	0	1	1
	21 hingga 30 tahun	2	2	2	6
	31 hingga 40 tahun	11	2	6	19
	41 hingga 50 tahun	7	1	1	9
	Lebih daripada 50 tahun	4	1	0	5
Total		24	6	10	40

Rajah 4.2 Statistik umur dan bidang tugas

Soalan 5 adalah dalam bentuk skala Likert yang mengukur pandangan responden terhadap mekanisme keselamatan dan proses IT sedia ada di Hospital Pakar KPJ Ipoh. Berdasarkan data yang diberikan (Rajah 4.3), terdapat dua orang responden (5%) yang menyatakan tidak bersetuju dengan penyataan tersebut. Seramai 31 orang responden (77.5%) menyatakan setuju dengan penyataan tersebut, manakala tujuh orang responden (17.5%) menyatakan sangat setuju. Keputusan ini menunjukkan majoriti responden cenderung menyokong pandangan bahawa mekanisme keselamatan dan proses IT sedia ada di Hospital Pakar KPJ Ipoh adalah mencukupi. Dengan hanya sebilangan kecil responden yang tidak bersetuju, keputusan ini menggambarkan keyakinan responden terhadap keselamatan IT dan perlindungan data di hospital.



Rajah 4.3 Mekanisme proses dan keselamatan IT sedia ada



Rajah 4.4 Memahami konsep BYOD

Soalan akhir dalam bahagian ini adalah binari, di mana responden perlu memilih antara Ya atau Tidak sebagai jawapan (Rajah 4.4). Berdasarkan data yang diberikan, terdapat 36 responden (90%) yang memilih Ya, menunjukkan bahawa mereka memahami konsep BYOD. Hanya sebilangan kecil responden yang memilih Tidak, menunjukkan kurangnya pemahaman tentang konsep BYOD.

4.2.2 Seksyen A: Kajian Faktor Teknologi

Seksyen ini bertujuan untuk menganalisis enam soalan yang menilai faktor teknologi yang penting dalam pelaksanaan selamat BYOD di Hospital Pakar KPJ Ipoh. Soalan ini dinilai menggunakan skala Likert 5 mata, di mana responden memberikan penilaian dari 1 hingga 5, dengan 1 mewakili "Sangat Tidak Setuju" dan 5 mewakili "Sangat Setuju". Melalui soalan-soalan ini, persepsi responden berkaitan faktor teknologi yang mempengaruhi keselamatan peranti mudah alih dalam persekitaran dapat diketahui. Jadual 4.2 menunjukkan hasil analisis berdasarkan jawapan yang diberikan oleh responden.

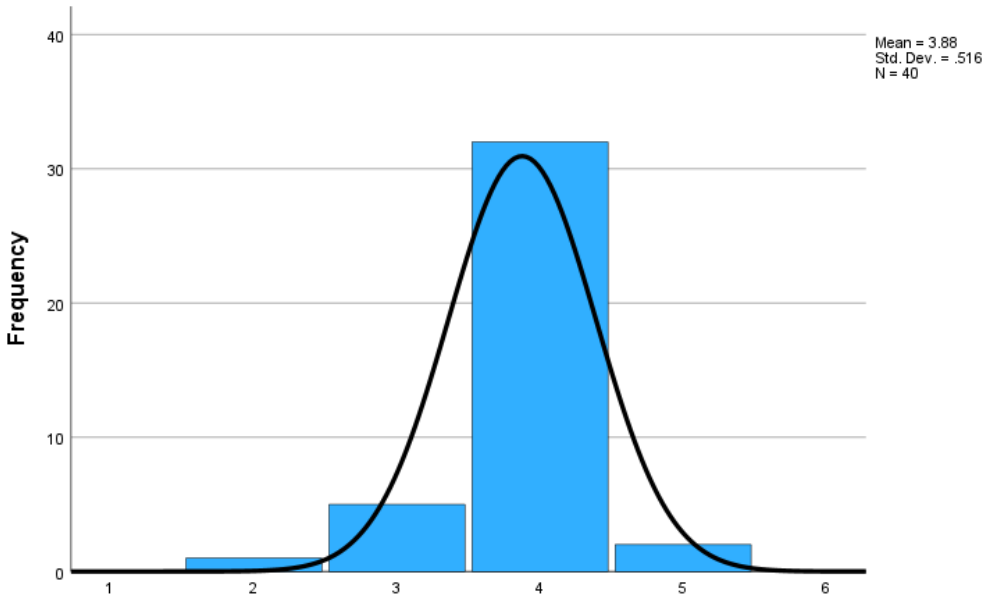
Jadual 4.2 Analisis data bagi Faktor Teknologi

Bil.	Soalan	Skala					Min	Persepsi
		1	2	3	4	5		
1	Ketersediaan rangkaian Wi-Fi yang disediakan di Hospital Pakar KPJ Ipoh memadai untuk mengalakkan penggunaan peranti BYOD.	-	1 (2.5%)	5 (12.5%)	32 (80%)	2 (5%)	3.88	Positif
2	Sambungan ke rangkaian Wi-Fi KPJEMED dan KPJPUBLIC adalah stabil dan jarang mengalami gangguan.	-	-	6 (15%)	31 (77.5%)	3 (7.5%)	3.93	Positif
3	Penggunaan VPN memastikan data yang dikirim antara peranti dan rangkaian Wi-Fi terlindungi dari ancaman pencerobohan atau penggodaman.	-	-	-	35 (87.5%)	5 (12.5%)	4.13	Positif
4	Kebolehgunaan aplikasi Citrix Workspace memudahkan pengguna untuk mengakses sistem hospital dengan mudah dan selamat.	-	-	-	27 (67.5%)	13 (32.5%)	4.33	Positif

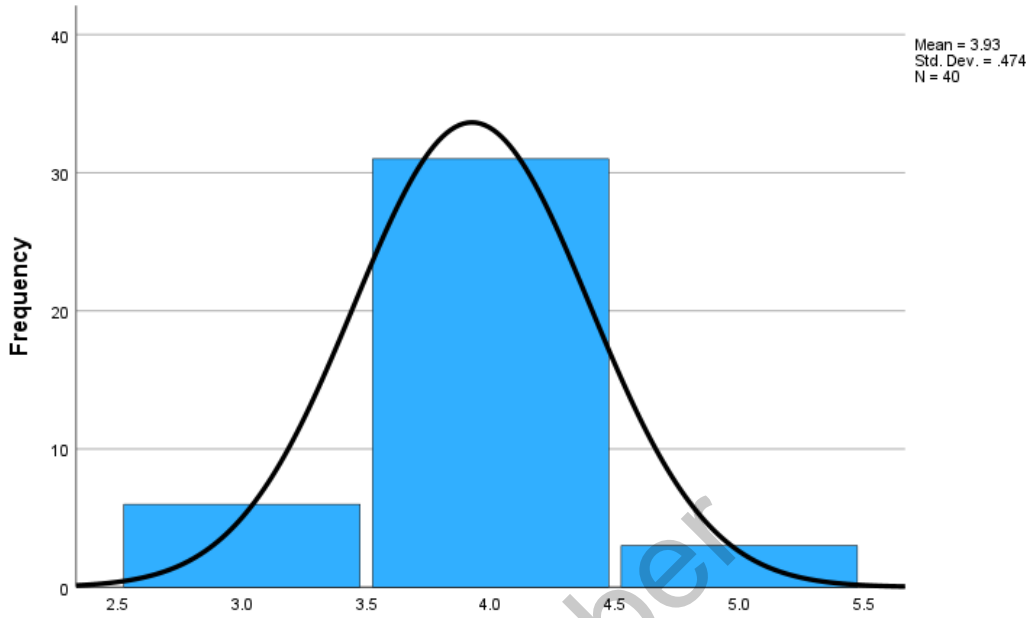
bersambung..

5	Semua perisian dalam peranti diperbaharui dengan versi terkini membantu mengurangkan kerentanan terhadap ancaman keselamatan.	-	-	7 (17.5%)	31 (77.5%)	2 (5%)	3.88	Positif
6	Maklumat peranti seperti nombor siri, versi sistem operasi dan perisian keselamatan yang digunakan adalah penting untuk pengurusan BYOD	-	-	-	15 (37.5%)	25 (62.5%)	4.63	Positif

Dalam soalan pertama, responden diminta menilai ketersediaan rangkaian Wi-Fi yang disediakan di Hospital Pakar KPJ Ipoh. Keputusan menunjukkan bahawa sebanyak 80% iaitu 32 responden bersetuju bahawa ketersediaan rangkaian Wi-Fi adalah mencukupi untuk menggalakkan penggunaan peranti BYOD (Rajah 4.5). Manakala, dua responden sangat bersetuju. Terdapat seorang responden yang tidak bersetuju dan lima lagi yang kurang setuju terhadap penyataan tersebut. Ini berkemungkinan jika ramai pengguna menggunakan rangkaian Wi-Fi pada masa yang sama, terutamanya semasa waktu sibuk, ini boleh menyebabkan had lebar jalur (*bandwidth*) yang menyebabkan sambungan menjadi perlahan. Ini mungkin mengurangkan daya tarikan responden untuk bergantung pada Wi-Fi untuk penggunaan peranti BYOD. Purata skor 3.88 menunjukkan persepsi positif terhadap ketersediaan rangkaian Wi-Fi.



Rajah 4.5 Ketersediaan rangkaian Wi-Fi yang disediakan di Hospital Pakar KPJ Ipoh



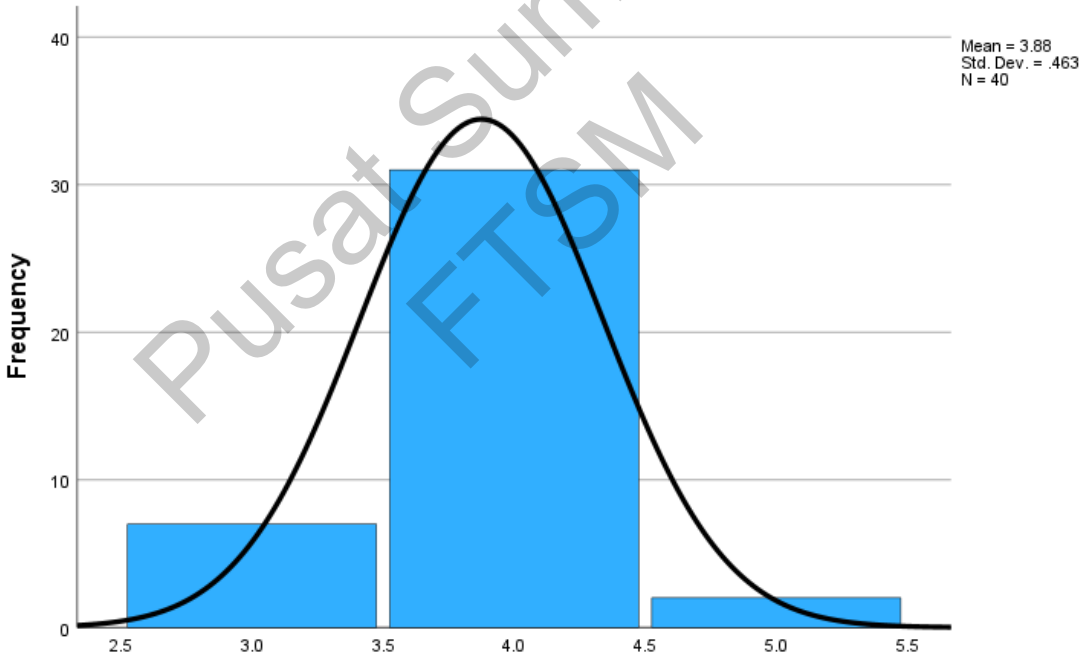
Rajah 4.6 Sambungan ke rangkaian Wi-Fi KPJEMED dan KPJPUBLIC

Soalan kedua berkaitan dengan kestabilan sambungan ke rangkaian Wi-Fi KPJEMED dan KPJPUBLIC. Seramai 31 responden (77.5%) bersetuju bahawa sambungan adalah stabil dan jarang mengalami gangguan. Ini menunjukkan kualiti infrastruktur rangkaian Wi-Fi yang baik di hospital. Tiga responden menyatakan sangat bersetuju. Manakala, terdapat enam responden yang kurang bersetuju. Responden mungkin mengalami masalah dengan kualiti isyarat Wi-Fi di sesetengah kawasan hospital, seperti isyarat lemah atau gangguan yang kerap. Ini boleh menyebabkan pengalaman menggunakan peranti menjadi tidak selesa dan mengganggu produktiviti. Purata skor 3.93 juga mengukuhkan persepsi positif seperti yang ditunjukkan dalam rajah 4.6.

Penggunaan VPN menjadi tumpuan dalam soalan ketiga. Responden diminta menilai kepentingan penggunaan VPN dalam melindungi data yang dihantar antara peranti dan rangkaian Wi-Fi. Seramai 35 responden (87.5%) bersetuju bahawa penggunaan VPN adalah penting untuk memastikan keselamatan data. Manakala, selebihnya sangat bersetuju. Purata skor 4.13 menunjukkan persepsi positif terhadap penggunaan VPN di Hospital Pakar KPJ Ipoh.

Soalan keempat berkaitan dengan kebolehgunaan aplikasi Citrix Workspace. 27 responden iaitu sebanyak 67.5% bersetuju bahawa aplikasi ini memudahkan pengguna mengakses sistem hospital dengan mudah dan selamat. Manakala selebihnya seramai

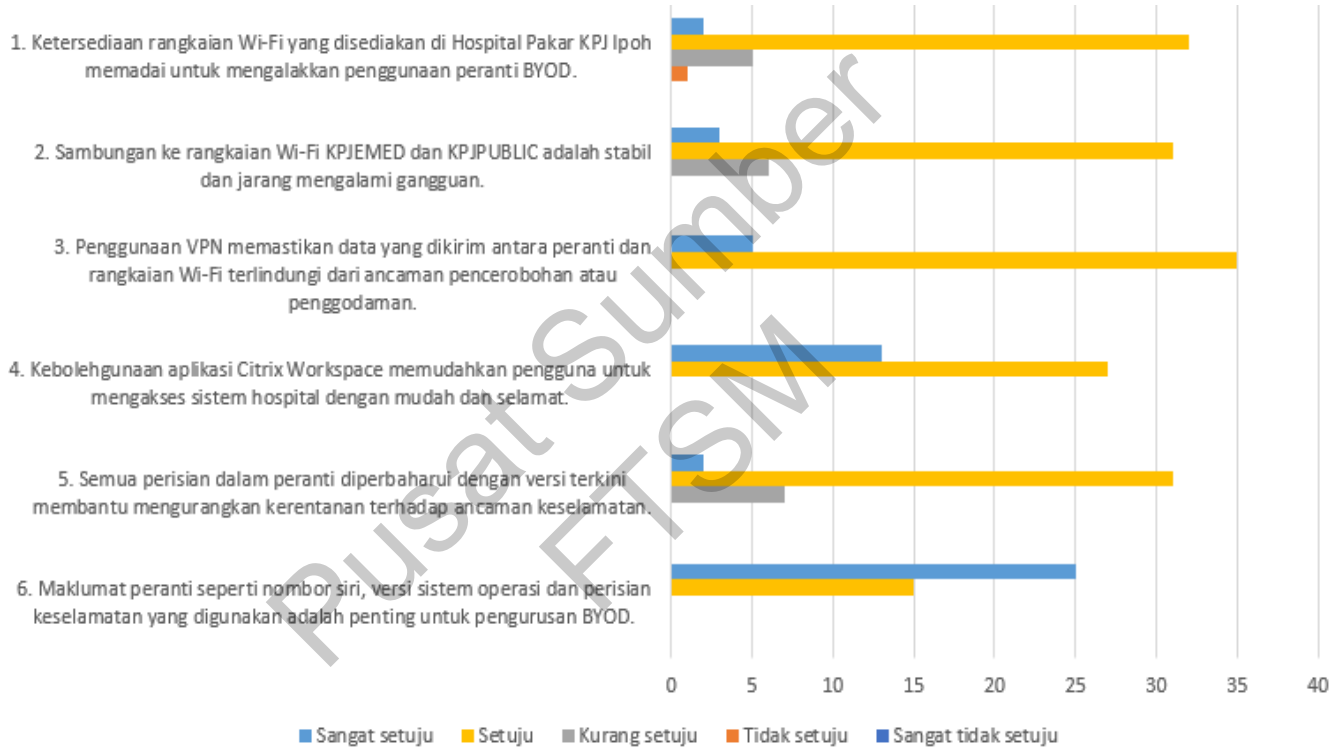
13 responden sangat bersetuju. Nilai skor purata 4.33 menunjukkan persepsi yang positif terhadap kebolehgunaan aplikasi Citrix Workspace di Hospital Pakar KPJ Ipoh. Soalan kelima melibatkan pengemaskinian perisian dalam peranti. Seramai 31 responden (77.5%) bersetuju bahawa mengemas kini perisian dengan versi terkini membantu mengurangkan kerentanan kepada ancaman keselamatan, dengan dua responden memberi jawapan sangat bersetuju. Terdapat tujuh responden yang kurang setuju, mungkin kerana mereka teragak-agak untuk mengemas kini perisian kerana bimbang kemas kini boleh menjejaskan fungsi atau prestasi peranti. Mereka mungkin lebih suka menggunakan versi lama perisian yang telah terbukti stabil, walaupun ini bermakna mengorbankan keselamatan. Nilai skor purata 3.88 menunjukkan persepsi positif terhadap kemas kini perisian dalam peranti BYOD seperti yang ditunjukkan dalam rajah 4.7.



Rajah 4.7 Langkah untuk mengurangkan kerentanan terhadap ancaman keselamatan

Akhir sekali, soalan keenam menyerlahkan kepentingan maklumat peranti seperti nombor siri, versi sistem pengendalian dan perisian keselamatan yang digunakan. Seramai 25 responden (62.5%) sangat bersetuju bahawa maklumat ini penting dalam pengurusan BYOD. Manakala, 15 responden lagi menjawab setuju. Purata skor tertinggi iaitu 4.63 menunjukkan persepsi positif yang tinggi terhadap kepentingan

maklumat peranti ini. Kesimpulannya, Faktor Teknologi memainkan peranan penting dalam pelaksanaan selamat BYOD di Hospital Pakar KPJ Ipoh. Ketersediaan rangkaian Wi-Fi yang mencukupi, sambungan yang stabil, penggunaan VPN, kebolehgunaan aplikasi, kemas kini perisian dan kepentingan maklumat peranti adalah faktor yang memberi keyakinan dalam menggunakan peranti BYOD di hospital (Rajah 4.8). Hasil kajian ini boleh digunakan sebagai panduan dalam menambah baik infrastruktur teknologi dan memberikan sokongan yang lebih baik untuk penggunaan peranti BYOD yang selamat pada masa hadapan.



Rajah 4.8 Taburan skala Faktor Teknologi

4.2.3 Seksyen B: Kajian Faktor Keselamatan

Seksyen B memfokuskan kepada analisis faktor keselamatan dalam pelaksanaan selamat BYOD di Hospital Pakar KPJ Ipoh. Terdapat enam soalan yang direka untuk menilai faktor keselamatan penting dalam penggunaan peranti mudah alih di hospital ini. Soalan-soalan ini membantu dalam menilai persepsi dan tindak balas responden terhadap langkah keselamatan yang dilaksanakan.

Analisis jawapan kepada soalan ini memberikan gambaran tentang sejauh mana keselamatan BYOD difahami dan dianggap penting oleh responden. Dengan memerhatikan hasil analisis ini, langkah keselamatan yang sesuai boleh dirumuskan untuk memastikan pelaksanaan BYOD yang selamat dan melindungi maklumat sensitif di Hospital Pakar KPJ Ipoh. Jadual 4.3 adalah hasil analisis berdasarkan maklum balas yang diberikan oleh responden.

Jadual 4.3 Analisis data bagi Faktor Keselamatan

Bil.	**Soalan**	**Skala**					**Min**	**Persepsi**
		1	**2**	**3**	**4**	**5**		
1	Ketersediaan lapisan keselamatan seperti tembok api di Hospital Pakar KPJ Ipoh membantu melindungi peranti daripada serangan luaran yang tidak diingini.	-	-	-	38 (95%)	2 (5%)	4.05	Positif
2	Kewujudan perisian antivirus dalam setiap peranti penting untuk melindungi daripada ancaman jangkitan perisian hasad dan virus.	-	-	3 (7.5%)	37 (92.5%)	-	3.93	Positif
3	Pelaksanaan protokol pengesahan yang kukuh, seperti dua faktor pengesahan (*two-factor authentication*) membantu meningkatkan keselamatan akses ke sistem dan data sensitif.	-	-	-	15 (37.5%)	25 (62.5%)	4.63	Positif
4	Kawalan akses yang ketat dapat membantu memastikan hanya pengguna yang dibenarkan sahaja yang mempunyai akses ke sistem, fail dan data hospital.	-	-	-	27 (67.5%)	13 (32.5%)	4.33	Positif
5	Akses akan dinyahaktifkan apabila peranti hilang atau dicuri penting untuk melindungi data sensitif.	-	-	-	38 (95%)	2 (5%)	4.05	Positif
6	Hospital Pakar KPJ Ipoh mematuhi undang-undang privasi dan peraturan keselamatan data yang berkenaan seperti *Personal Data Protection Act* (PDPA).	-	-	-	36 (90%)	4 (10%)	4.10	Positif

Berdasarkan jadual 4.3, dapat disimpulkan bahawa persepsi responden terhadap faktor keselamatan di Hospital Pakar KPJ Ipoh adalah positif. Sebanyak 95% responden iaitu 38 responden bersetuju bahawa ketersediaan lapisan keselamatan seperti tembok api membantu melindungi peranti daripada serangan luar yang tidak diingini. Manakala, selebihnya sangat bersetuju.

Tambahan pula, majoriti 37 responden iaitu 92.5% bersetuju bahawa kewujudan perisian antivirus dalam setiap peranti adalah mencukupi untuk melindungi daripada ancaman perisian hasad dan jangkitan virus. Tiga orang responden kurang setuju terhadap penyataan tersebut. Responden mungkin tidak pernah mengalami insiden serius yang melibatkan jangkitan perisian hasad atau virus pada peranti mereka. Pengalaman tanpa kerumitan ini boleh membuatkan mereka merasakan bahawa perisian antivirus tidak penting.

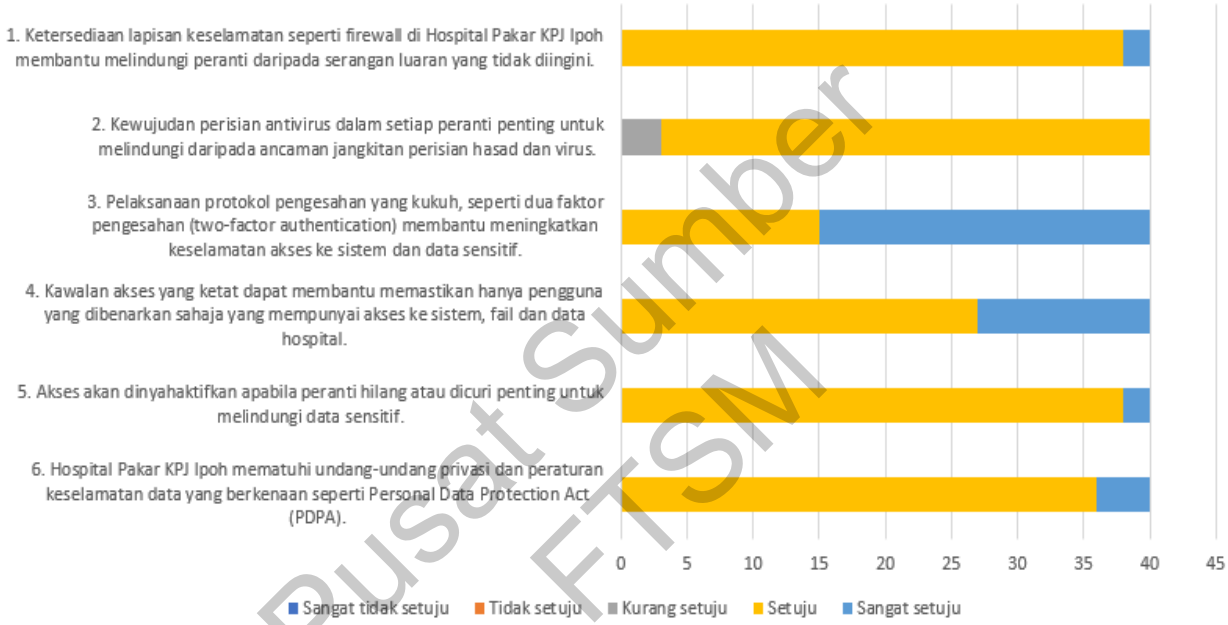
Selain itu, majoriti 25 responden, iaitu 62.5%, sangat bersetuju bahawa pelaksanaan protokol pengesahan yang kukuh, seperti pengesahan dua faktor, membantu meningkatkan keselamatan akses kepada sistem dan data sensitif. 15 responden menjawab bersetuju. Seterusnya, 27 responden (67.5%) pula bersetuju bahawa kawalan capaian yang ketat boleh memastikan hanya pengguna yang dibenarkan sahaja yang mempunyai akses kepada sistem, fail dan data hospital. 13 responden lagi menjawab sangat bersetuju.

Di samping itu, sebanyak 95% iaitu 38 responden bersetuju bahawa akses akan dilumpuhkan apabila peranti hilang atau dicuri, ini penting untuk melindungi data sensitif. Manakala, baki dua responden menjawab sangat bersetuju. Akhir sekali, 36 responden (90%) menyatakan bahawa Hospital Pakar KPJ Ipoh mematuhi undang-undang privasi dan peraturan keselamatan data yang terpakai, seperti Akta Perlindungan Data Peribadi (PDPA). Manakala, empat responden lagi menjawab sangat bersetuju.

Secara keseluruhannya, hasil analisis jadual menunjukkan responden mempunyai persepsi yang positif terhadap faktor keselamatan dalam pelaksanaan BYOD di Hospital Pakar KPJ Ipoh. Ini menunjukkan bahawa usaha yang dilakukan oleh hospital dalam menggunakan langkah keselamatan yang betul, seperti penggunaan tembok api, perisian antivirus, protokol pengesahan yang kuat, kawalan akses yang ketat, dan pematuhan undang-undang privasi dan peraturan data, telah berjaya

mendapatkan kepercayaan responden. berkaitan dengan keselamatan menggunakan peranti BYOD.

Dengan pemahaman ini, hospital boleh terus mengukuhkan usaha mereka dalam mengekalkan keselamatan BYOD dan memastikan perlindungan data sensitif dan privasi pesakit. Hasil analisis ini juga menyediakan asas yang kukuh untuk hospital meningkatkan strategi keselamatan dan melaksanakan garis panduan yang sesuai untuk pelaksanaan BYOD yang selamat. Rajah 4.9 menunjukkan taburan skala Faktor Keselamatan.



Rajah 4.9 Taburan skala Faktor Keselamatan

4.2.4 Seksyen C: Kajian Faktor Organisasi

Seksyen ini direka untuk mengkaji faktor organisasi yang berkaitan dengan pelaksanaan selamat BYOD di Hospital Pakar KPJ Ipoh. Fokus diberikan kepada pengurusan peranti dan kepatuhan terhadap dasar yang berkaitan. Terdapat enam soalan yang dirumuskan untuk menilai pengurusan peranti dan perundangan yang berkaitan. Analisis jawapan kepada soalan ini membantu dalam menilai sejauh mana organisasi hospital memenuhi keperluan dan langkah amalan yang berkaitan dengan penggunaan peranti mudah alih BYOD. Dengan memahami situasi semasa dan menyesuaikan strategi dan dasar pengurusan yang sesuai, Hospital Pakar KPJ Ipoh boleh memastikan pelaksanaan

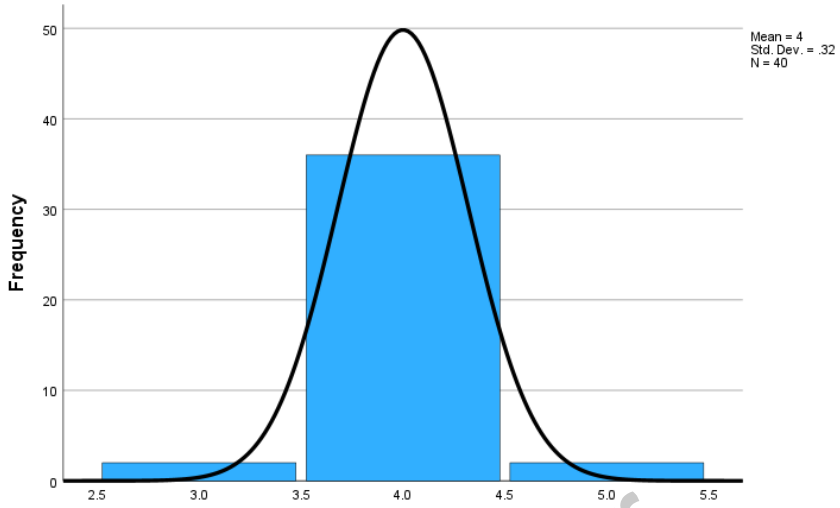
BYOD yang selamat. Jadual 4.5 memaparkan hasil analisis berdasarkan jawapan responden mengikut soalan-soalan yang dikemukakan.

Jadual 4.5 Analisis data bagi Faktor Organisasi

Bil.	Soalan	Skala					Min	Persepsi
		1	2	3	4	5		
1	Hospital Pakar KPJ Ipoh memiliki dasar yang jelas mengenai penggunaan peranti mudah alih.	-	-	22 (55%)	18 (45%)	-	3.45	Negatif
2	Ketersediaan dasar dan prosedur yang jelas berkaitan penggunaan peranti BYOD di Hospital Pakar KPJ Ipoh adalah penting untuk melindungi data sensitif.	-	-	-	24 (60%)	16 (40%)	4.40	Positif
3	Hospital Pakar KPJ Ipoh mengenalpasti dengan baik tanggungjawab dan peranan yang berkaitan dengan penggunaan peranti mudah alih bagi setiap jabatan di dalam organisasi.	-	-	2 (5%)	36 (90%)	2 (5%)	4.00	Positif
4	Hospital Pakar KPJ Ipoh melibatkan semua jabatan yang berkaitan dalam pembangunan dan pelaksanaan dasar BYOD.	-	-	1 (2.5%)	37 (92.5%)	2 (5%)	4.03	Positif
5	Hospital Pakar KPJ Ipoh melibatkan pihak atasan dalam pengurusan dan pemantauan penggunaan peranti mudah alih untuk menjaga kepatuhan dan keselamatan.	-	-	8 (20%)	30 (75%)	2 (5%)	3.85	Positif
6	Pematuhan terhadap dasar dan prosedur penggunaan peranti adalah tanggungjawab setiap individu di Hospital Pakar KPJ Ipoh.	-	-	-	30 (75%)	10 (25%)	4.25	Positif

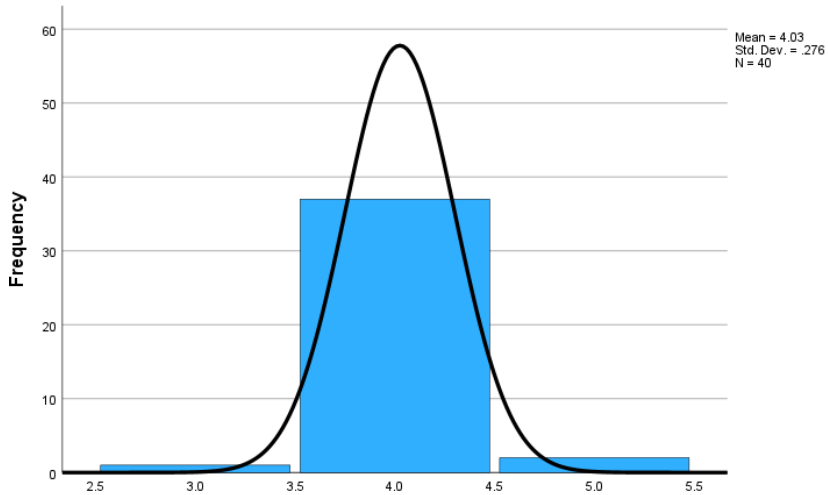
Hasil analisis menunjukkan beberapa penemuan penting. Pertama, Hospital Pakar KPJ Ipoh mempunyai polisi yang jelas mengenai penggunaan peranti mudah alih. Seramai 18 responden iaitu 45% daripada responden bersetuju dengan kejelasan dasar tersebut, manakala majoriti selebihnya 22 responden (55%) memberikan persepsi kurang setuju mengenai dasar tersebut. Responden mungkin tidak mengetahui atau tidak mendapat maklumat yang mencukupi tentang dasar sedia ada mengenai penggunaan peranti mudah alih di hospital. Maklumat tentang dasar ini mungkin tidak disebarkan atau disampaikan dengan cukup baik kepada pengguna di hospital. Kedua, ketersediaan polisi dan prosedur yang jelas berkaitan penggunaan peranti BYOD di Hospital Pakar KPJ Ipoh dianggap penting untuk melindungi data sensitif. 24 responden (60%) menyatakan persetujuan terhadap kepentingan kewujudan dasar ini, dan 16 responden (40%) memberikan persepsi yang lebih positif.

Seterusnya, responden juga mengakui bahawa Hospital Pakar KPJ Ipoh dapat mengenal pasti dengan betul tanggungjawab dan peranan berkaitan penggunaan peranti mudah alih bagi setiap jabatan dalam organisasi. Persetujuan kepada penyataan ini telah diberikan oleh 36 responden iaitu sebanyak 90% menunjukkan pemahaman yang baik tentang tanggungjawab dan peranan setiap jabatan dalam penggunaan peranti BYOD (Rajah 4.10). Manakala, terdapat dua responden yang kurang setuju. Responden mungkin merasakan bahawa tanggungjawab dan peranan mereka yang berkaitan dengan penggunaan peranti mudah alih tidak cukup jelas atau tidak ditakrifkan dengan baik oleh pihak pengurusan. Kekaburan ini boleh menyebabkan kekeliruan dalam menjalankan tugas yang berkaitan dengan penggunaan peranti.



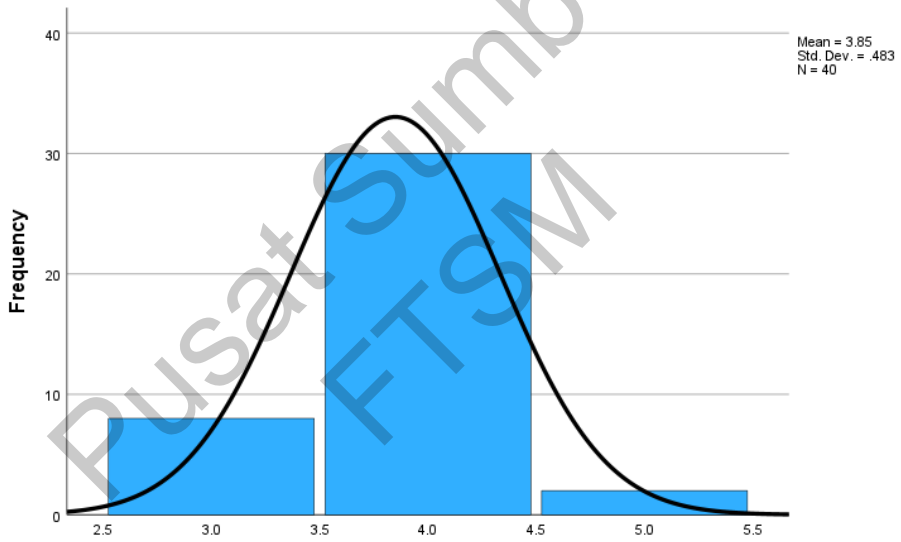
Rajah 4.10 Tanggungjawab dan peranan yang berkaitan dengan penggunaan peranti mudah alih

Selain itu, hasil analisis (Rajah 4.11) juga menunjukkan Hospital Pakar KPJ Ipoh melibatkan semua jabatan berkaitan dalam pembangunan dan pelaksanaan dasar BYOD. Hanya seorang responden (2.5%) kurang bersetuju dengan penyataan ini. Responden tersebut mungkin merasa bahawa jabatannya tidak dilibatkan secara aktif dalam proses pembangunan dan pelaksanaan dasar BYOD. Mungkin ada kekurangan dalam komunikasi atau konsultasi dengan jabatan terkait sehingga mereka merasa tidak terlibat. Manakala majoriti 39 responden (97.5%) memberikan persepsi yang tinggi.



Rajah 4.11 Penglibatan semua jabatan yang berkaitan dalam pembangunan dan pelaksanaan dasar BYOD

Kepentingan penglibatan pihak atasan dalam pengurusan dan pemantauan penggunaan peranti mudah alih turut ditekankan dalam hasil analisis (Rajah 4.12). Terdapat sebilangan kecil responden (20%) iaitu lapan responden yang kurang bersetuju. Responden mungkin merasakan pihak atasan tidak terlibat dengan secukupnya dalam penggunaan peranti mudah alih, menyebabkan kurangnya pemahaman tentang keperluan dan cabaran yang dihadapi oleh pengguna peranti. Ini boleh menyebabkan dasar atau keputusan yang tidak tepat dalam pengurusan dan pemantauan. Bagaimanapun, 32 responden (80%) memberikan persepsi yang positif tentang kepentingan penglibatan pihak atasan dalam menjaga pematuhan dan keselamatan dalam penggunaan peranti BYOD.

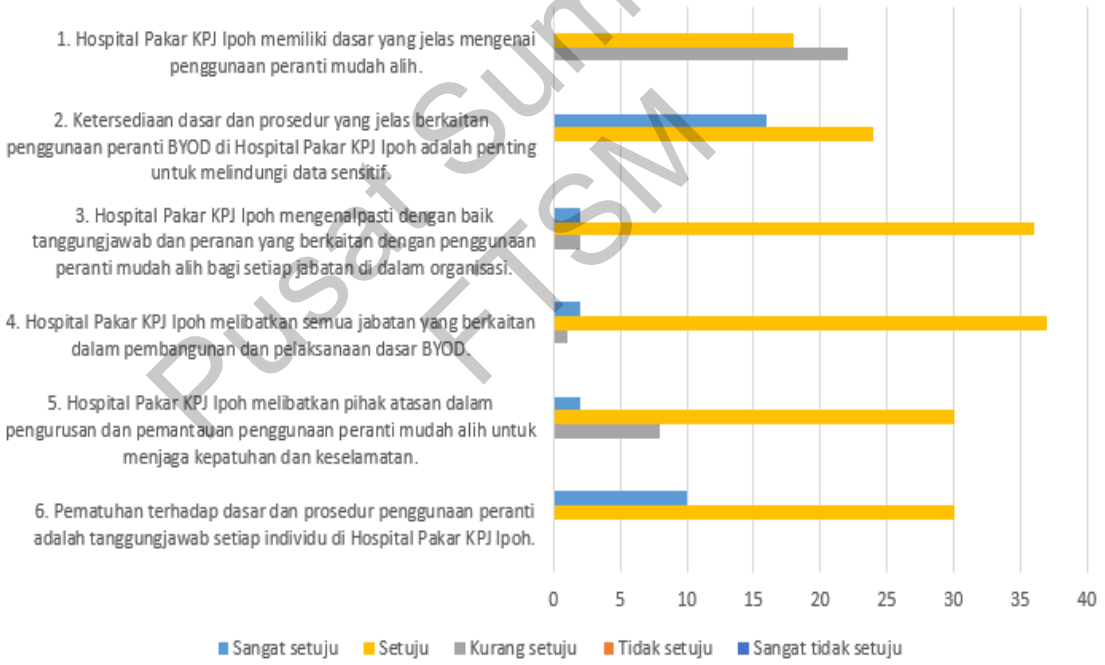


Rajah 4.12 Penglibatan pihak atasan dalam pengurusan dan pemantauan penggunaan peranti mudah alih

Akhir sekali, pematuhan kepada dasar dan prosedur penggunaan peranti juga dianggap sebagai tanggungjawab setiap individu di Hospital Pakar KPJ Ipoh. Majoriti 30 responden (75%) menyatakan persetujuan dengan penyataan ini, manakala 10 responden (25%) memberikan persepsi yang lebih positif.

Secara keseluruhannya, hasil analisis menunjukkan Hospital Pakar KPJ Ipoh telah melakukan usaha yang baik dalam menguruskan faktor Organisasi dalam pelaksanaan BYOD.

Maklum balas positif responden terhadap kejelasan dasar, penglibatan jabatan dan tanggungjawab individu dalam pematuhan menegaskan kesedaran yang kukuh tentang kepentingan faktor organisasi dalam mengekalkan keselamatan dan kejayaan menggunakan peranti mudah alih BYOD di hospital ini. Dengan pemahaman yang mendalam tentang faktor Organisasi, Hospital Pakar KPJ Ipoh boleh meneruskan usaha mereka untuk menambah baik dan mengukuhkan langkah organisasi yang menyokong pelaksanaan BYOD yang selamat. Langkah-langkah ini termasuk kejelasan dasar, penglibatan semua jabatan yang berkaitan, dan pemantauan pematuhan dengan dasar dan prosedur yang ditetapkan. Dengan melakukan ini, hospital boleh terus mengoptimumkan penggunaan peranti mudah alih BYOD dengan mengutamakan keselamatan data sensitif dan mengekalkan pematuhan kepada peraturan dan undang-undang yang berkenaan. Rajah 4.13 adalah hasil analisis Faktor Organisasi.



Rajah 4.13 Taburan skala Faktor Organisasi

4.2.5 Seksyen D: Kajian Faktor Manusia

Seksyen ini bertujuan untuk menganalisis faktor Manusia dalam pelaksanaan selamat BYOD di Hospital Pakar KPJ Ipoh.

Analisis jawapan kepada soalan-soalan ini memberikan gambaran tentang sejauh mana pengguna peranti di Hospital Pakar KPJ Ipoh memahami dan mematuhi dasar dan prosedur yang berkaitan. Di samping itu, analisis ini membantu dalam mengenal pasti tahap kesedaran dan pemahaman pengguna tentang keselamatan peranti dan data sensitif, serta tanggungjawab dan peranan masing-masing. Jadual 4.6 menjelaskan hasil analisis berdasarkan jawapan yang diberikan oleh responden berkenaan faktor Manusia dalam pelaksanaan selamat BYOD di Hospital Pakar KPJ Ipoh.

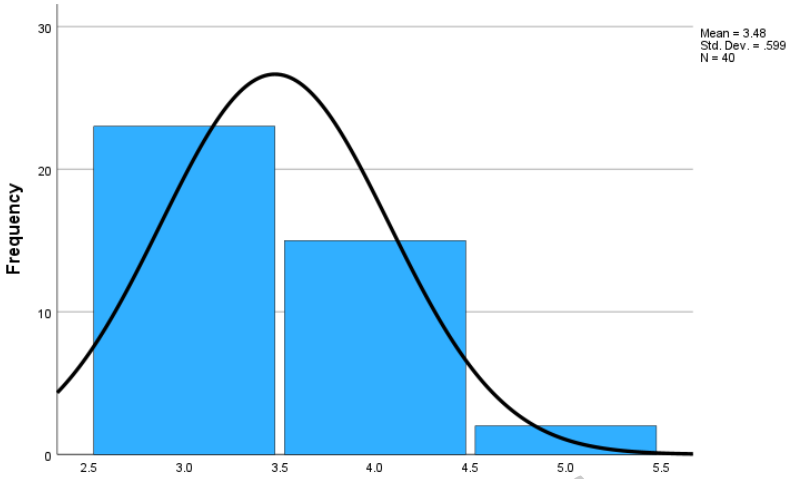
Jadual 4.6 Analisis data bagi Faktor Manusia

Bil.	Soalan	Skala					Min	Persepsi
		1	2	3	4	5		
1	Kakitangan dan pengguna Hospital Pakar KPJ Ipoh sedar tentang tanggungjawab mereka dalam menjaga keselamatan peranti mudah alih dan data sensitif yang diakses melalui peranti tersebut.	-	-	-	36 (90%)	4 (10%)	4.10	Positif
2	Pengguna peranti mudah alih mematuhi dasar dan prosedur keselamatan sedia ada yang ditetapkan.	-	-	-	37 (92.5%)	3 (7.5%)	4.08	Positif
3	Hospital Pakar KPJ Ipoh memberikan latihan keselamatan yang secukupnya kepada kakitangan dan pengguna peranti mudah alih.	-	-	23 (57.5%)	15 (37.5%)	2 (5%)	3.48	Negatif
4	Jabatan IT menyediakan sokongan teknikal dan nasihat kepada pengguna peranti mudah alih dalam hal keselamatan dan kepatuhan.	-	-	8 (20%)	30 (75%)	2 (5%)	3.85	Positif
5	Jabatan IT memantau dan melaksanakan langkah-langkah keselamatan yang berkaitan dengan penggunaan peranti mudah alih.	-	-	4 (10%)	34 (85%)	2 (5%)	3.95	Positif

bersambung..

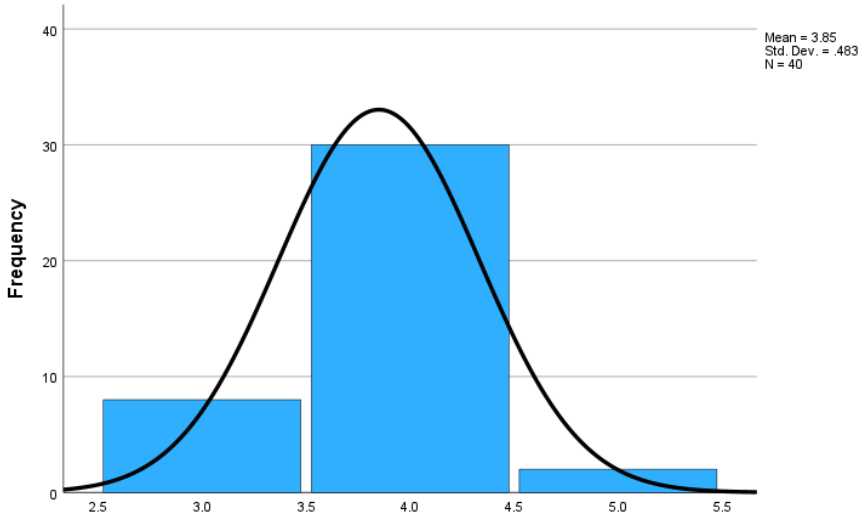
6	Pengguna peranti berhubung rapat dengan pihak atasan atau jabatan IT dalam melaporkan sebarang isu atau pelanggaran keselamatan yang berkaitan dengan penggunaan peranti mudah alih.	-	-	-	36 (90%)	4 (10%)	4.10	Positif

Berdasarkan hasil analisis, dapat disimpulkan bahawa kakitangan dan pengguna sedar akan tanggungjawab mereka dalam menjaga keselamatan peranti mudah alih dan data sensitif yang diakses melalui peranti tersebut. Sebanyak 90% iaitu 36 responden menyatakan persepsi yang positif. Ini menunjukkan kesedaran dan pematuhan yang baik terhadap aspek keselamatan dalam penggunaan peranti mudah alih. Selain itu, pengguna peranti mudah alih juga mematuhi dasar dan prosedur keselamatan yang ditetapkan oleh hospital. Seramai 37 responden (92.5%) menyatakan pematuhan positif terhadap polisi dan prosedur. Ini menunjukkan kesedaran dan pematuhan terhadap langkah keselamatan yang telah ditetapkan. Terdapat hanya 17 responden (42.5%) yang memberikan persepsi positif, terdapat ruang untuk menambah baik latihan keselamatan yang diberikan kepada mereka. Sebanyak 23 responden menjawab kurang setuju. Responden merasakan kekerapan latihan keselamatan yang disediakan oleh Hospital Pakar KPJ Ipoh adalah tidak mencukupi. Latihan yang hanya diberikan secara tidak kerap atau tidak teratur boleh menyebabkan responden berasa kurang bersedia dalam menghadapi situasi kecemasan atau ancaman keselamatan yang mungkin berlaku. Nilai skor purata 3.48 menunjukkan persepsi negatif terhadap latihan keselamatan kepada kakitangan dan pengguna peranti mudah alih seperti yang ditunjukkan dalam rajah 4.14.



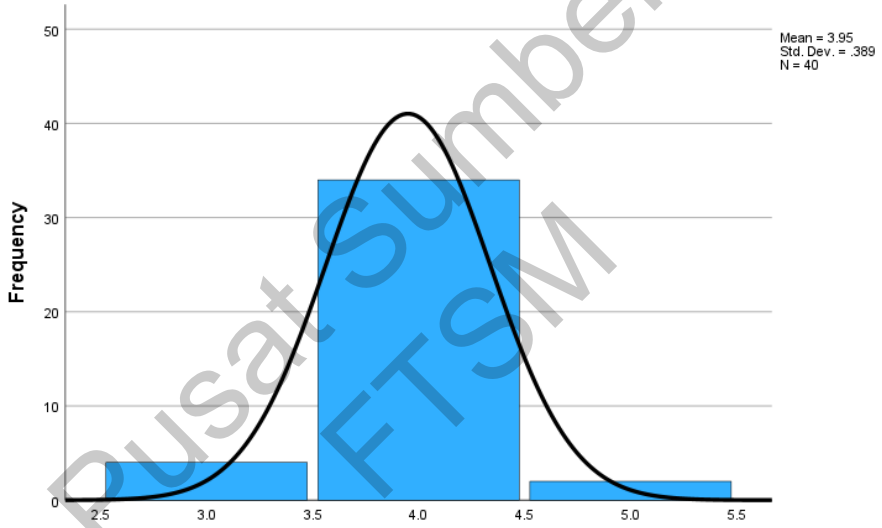
Rajah 4.14 Latihan keselamatan kepada kakitangan dan pengguna peranti mudah alih

Jabatan IT di Hospital Pakar KPJ Ipoh menyediakan sokongan teknikal dan nasihat kepada pengguna peranti mudah alih dalam hal keselamatan dan pematuhan. Sebanyak 75% iaitu 30 responden memberikan persepsi positif terhadap sokongan yang diberikan oleh jabatan IT (Rajah 4.15). Ini menunjukkan kepentingan sokongan teknikal yang berkesan dalam memastikan keselamatan peranti dan pematuhan kepada dasar yang ditetapkan. Malah, terdapat lapan respoden kurang bersetuju terhadap penyataan tersebut. Responden mungkin mengalami kesukaran untuk mendapatkan sokongan teknikal dan nasihat daripada Jabatan IT kerana kekurangan ketersediaan kakitangan atau masa yang terhad untuk memberikan bantuan.



Rajah 4.15 Sokongan Jabatan IT dalam aspek teknikal dan nasihat mengenai peranti mudah alih tentang hal keselamatan dan kepatuhan

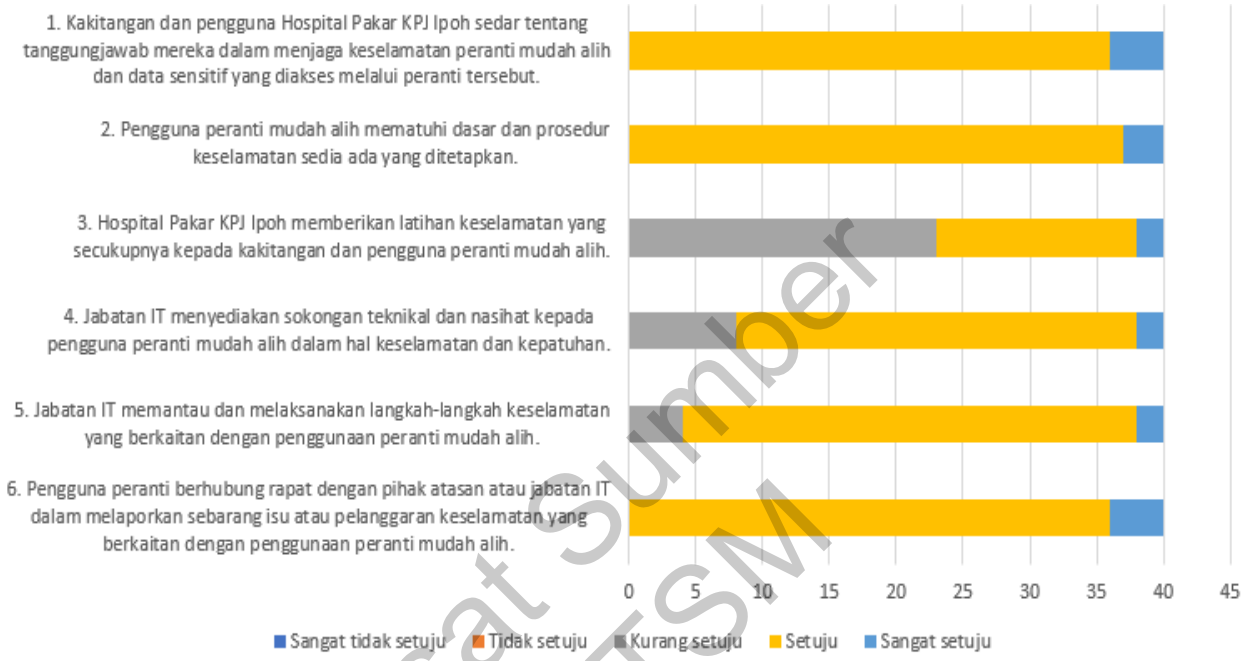
Seterusnya, jabatan IT juga melaksanakan pemantauan dan langkah keselamatan yang berkaitan dengan penggunaan peranti mudah alih. 34 respoden iaitu sebanyak 85% responden memberikan persepsi positif terhadap pemantauan ini, menunjukkan keberkesanan jabatan IT dalam menjaga keselamatan penggunaan peranti (Rajah 4.16). Malah, terdapat juga 4 responden kurang bersetuju. Responden mungkin merasakan walaupun penyataan bahawa pemantauan dan langkah keselamatan dijalankan oleh Jabatan IT, pelaksanaannya tidak konsisten atau kurang berkesan. Jika responden merasakan bahawa langkah keselamatan tidak selalu digunakan dengan baik atau pemantauan tidak mencukupi, mereka mungkin berasa kurang yakin dengan pendekatan tersebut.



Rajah 4.16 Pemantauan langkah-langkah keselamatan yang berkaitan dengan penggunaan peranti mudah alih

Pengguna peranti mudah alih berhubung rapat dengan pihak atasan atau jabatan IT dalam melaporkan sebarang isu atau pelanggaran keselamatan yang berkaitan dengan penggunaan peranti tersebut. Ini ditunjukkan dengan 36 responden (90%) memberikan persepsi yang positif. Manakala, empat responden lagi memberikan persepsi yang sangat positif. Ini menunjukkan kepentingan komunikasi dan kerjasama antara pengguna dan pihak berkepentingan dalam memastikan keselamatan penggunaan peranti mudah alih.

Secara keseluruhan, hasil analisis menunjukkan faktor Manusia dalam pelaksanaan selamat BYOD di Hospital Pakar KPJ Ipoh mendapat persepsi yang positif. Kesedaran, pematuhan, sokongan, latihan, pemantauan dan komunikasi yang baik antara pengguna dan pihak berkepentingan adalah penting untuk memastikan penggunaan peranti mudah alih yang selamat di persekitaran hospital (Rajah 4.17).



Rajah 4.17 Taburan skala Faktor Manusia

4.3 HURAIAN TEMU BUAL PAKAR

Temu bual ini telah dijalankan bersama seorang pakar dalam bidang teknologi maklumat dan keselamatan siber di Jabatan IT Hospital Pakar KPJ Ipoh. Temu bual ini dibuat sebelum tinjauan soal selidik. Tujuannya adalah untuk mendapatkan pandangan dan pendapat pakar dalam pelaksanaan BYOD yang selamat. Pakar membincangkan kepentingan dan cabaran yang berkaitan dengan pelaksanaan BYOD di hospital. Pandangan dan pendapat pakar menggariskan kepentingan faktor teknologi, keselamatan, organisasi dan manusia dalam mengukuhkan keselamatan penggunaan peranti BYOD.

Selain itu, pakar juga membantu menilai risiko untuk mengenal pasti dan mengatasi potensi ancaman keselamatan yang mungkin timbul daripada penggunaan BYOD. Dengan mempertimbangkan nasihat dan cadangan pakar, hospital boleh melaksanakan langkah-langkah yang sesuai untuk memastikan BYOD selamat dan melindungi data sensitif. Hasil temu bual ini juga menjadi asas dan panduan untuk penilaian tinjauan soal selidik yang dijalankan kepada responden dalam skop kajian. Bagi proses temu bual pakar, permohonan untuk menjalankan sesi temu bual dibuat melalui emel, bagi mendapatkan kebenaran serta menetapkan tarikh dan masa. Sebanyak lima soalan berkaitan telah disediakan dan setiap satu akan dihuraikan dan dibincangkan. Pakar memberikan penjelasan terperinci dan analisis untuk setiap soalan yang diajukan.

4.3.1 Soalan 1:

Bagaimana pendapat anda tentang perkembangan dan penggunaan BYOD di tempat kerja pada masa sekarang?

Pakar kurang bersetuju dengan pendapat tentang perkembangan dan penggunaan BYOD di tempat kerja hari ini. Pakar berpendapat bahawa walaupun BYOD telah menjadi trend yang semakin popular, terdapat beberapa kebimbangan dan cabaran yang perlu diambil kira. Pakar merasakan bahawa penggunaan BYOD mungkin membawa risiko keselamatan untuk organisasi. Apabila pekerja menggunakan peranti peribadi mereka untuk mengakses sistem dan maklumat organisasi, ia boleh menimbulkan ancaman keselamatan seperti kebocoran data atau serangan siber. Terdapat kebimbangan bahawa peranti peribadi mungkin tidak mempunyai tahap keselamatan yang sama seperti peranti yang disediakan oleh organisasi.

Selain itu, pakar juga menggariskan bahawa pengurusan dan sokongan teknikal menjadi lebih kompleks dengan BYOD. Dengan pelbagai jenis peranti dan platform yang digunakan oleh pekerja, pentadbir sistem perlu menyediakan sokongan yang meluas dan memastikan keserasian antara peranti dan aplikasi yang digunakan. Ini memerlukan sumber tambahan dan pelarasan dalam aspek pengurusan IT. Walaupun pakar berpendapat kurang setuju, pakar juga menyedari bahawa terdapat faedah yang boleh diperoleh. BYOD boleh meningkatkan produktiviti pekerja dengan menyediakan fleksibiliti dalam akses dan penggunaan peranti.