

**RISIKO PIHAK KETIGA DALAM KESELAMATAN
SIBER : SATU KAJIAN REKA BENTUK DAN
PEMBANGUNAN MODUL LATIHAN**

NURUL AINI BINTI MAT ALI NAPIYAH

UNIVERSITI KEBANGSAAN MALAYSIA

**RISIKO PIHAK KETIGA DALAM KESELAMATAN SIBER: SATU KAJIAN
REKA BENTUK DAN PEMBANGUNAN MODUL LATIHAN**

NURUL AINI BINTI MAT ALI NAPIYAH

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

**FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI**

2025

PENGAKUAN

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

Saya mengakui penggunaan Synthesia AI (synthesia.com) untuk menjana video, audio, animasi dan efek avatar untuk mempersembahkan hasil kajian (modul, papan cerita dan skrip penceritaan) kepada Pakar yang dilantik untuk penilaian. Saya tidak menggunakan sebarang alat atau teknologi AI untuk menyediakan laporan ini.

09 Februari 2025

NURUL AINI BINTI MAT
ALI NAPIYAH
P127014

PENGHARGAAN

Pertama sekali, saya memanjatkan setinggi-tinggi kesyukuran kepada Allah SWT kerana dengan izinNya, saya dapat menyelesaikan disertasi ini sebagai salah satu syarat untuk menamatkan pengajian Sarjana saya.

Saya ingin mengucapkan jutaan terima kasih khas saya tujukan kepada penyelia saya, Dr. Rossilawati binti Sulaiman atas sokongan dan panduan yang tidak berbelah bagi sepanjang perjalanan pengajian saya di UKM. Bimbingan dan sokongan beliau telah memberi inspirasi dan dorongan yang amat bermakna kepada saya dalam menyiapkan kajian ini.

Saya juga ingin merakamkan setinggi-tinggi penghargaan kepada semua pensyarah dan tenaga pengajar dari Fakulti Teknologi dan Sains Maklumat, UKM dan Cybersecurity Malaysia kerana mencurahkan ilmu dan pengalaman serta menyediakan persekitaran yang kondusif bagi kemudahan dan sumber yang diperlukan untuk menyelesaikan pengajian dan disertasi saya ini.

Saya juga amat berterima kasih kepada Kementerian Komunikasi dan Jabatan Digital Negara atas bantuan dan kerjasama yang tidak berbelah bagi sepanjang tempoh penyelidikan ini.

Terima kasih juga kepada Jabatan Perkhidmatan Awam (JPA) atas peluang pembelajaran serta sokongan kewangan yang telah mempermudah urusan pengajian saya.

Ucapan terima kasih tidak terhingga kepada suami tercinta atas kesabaran, dorongan, panduan dan kasih sayang yang tidak pernah putus sepanjang saya menyiapkan disertasi ini. Sokongan dan bantuan tidak berbelah bahagi beliau merupakan tunjang dan kekuatan utama saya dalam menghadapi semua cabaran sepanjang tempoh pengajian ini.

Selain itu, ucapan terima kasih saya kepada ibu dan anak-anak yang sentiasa mendoakan agar saya berjaya menamatkan pengajian dan disertasi ini. Semoga menjadi dorongan kepada anak-anak untuk terus menuntut ilmu tanpa mengenal lelah dan usia.

Akhir sekali, penghargaan ini juga saya tujukan kepada rakan-rakan seperjuangan. Semoga segala usaha yang dicurahkan ini mendapat keberkatan daripada Allah SWT dan memberikan manfaat kepada semua pihak.

ABSTRAK

Kebergantungan organisasi terhadap pihak ketiga tidak dapat dielakkan terutamanya dalam perkembangan teknologi yang pesat. Ini disumbangkan oleh penggunaan aplikasi atau perisian secara meluas, peralihan kepada infrastruktur perkhidmatan awan, penggunaan platform Generatif AI serta penggunaan perkhidmatan sumber luar bagi tujuan penyelenggaraan, audit, pembangunan aplikasi dan sistem serta pengurusan rangkaian. Trend ini mendedahkan organisasi kepada risiko keselamatan yang berpunca dari pihak ketiga akibat dari kelemahan sistem, kecuaiannya manusia, ketidakpatuhan terhadap polisi keselamatan atau perbuatan khianat. Serangan terhadap rantaian bekalan ini telah menjadi trend semasa dan dijangka akan terus meningkat sehingga tahun 2030. Berdasarkan insiden-insiden berprofil tinggi yang dilaporkan, serangan ini mampu memberi impak pada skala global dalam masa yang singkat serta mampu memberi implikasi yang tidak hanya terbatas kepada kerugian wang ringgit dan reputasi tetapi boleh menjejaskan Infrastruktur Maklumat Kritikal Negara (CNII) serta mengancam keselamatan dan nyawa orang awam. Melihat kepada jurang dari sudut kesedaran organisasi dan ketersediaan bahan untuk tajuk ini, terdapat keperluan mendesak untuk membangunkan modul latihan yang berkaitan. Justeru, melalui pendekatan kajian *Design and Development Research* (DDR), kajian ini akan memfokuskan kepada tiga (3) objektif iaitu untuk mengenal pasti kepentingan risiko keselamatan siber yang berpunca daripada pihak ketiga, membangunkan modul latihan dan melaksanakan kesahan modul melalui temu bual pakar. Hasil kajian ini dapat memberikan perspektif yang lebih khusus terhadap risiko keselamatan siber pihak ketiga dan boleh diperluas penggunaannya bagi tujuan Latihan, Kesedaran, Pendidikan atau Pembangunan polisi dan Garis panduan baik di peringkat kerajaan atau organisasi.

THIRD-PARTY RISK IN CYBERSECURITY : A TRAINING MODULE DEVELOPMENT USING DESIGN AND DEVELOPMENT RESEARCH APPROACH

ABSTRACT

With a prevalent use of technology, organisations dependencies towards third parties is inevitable. This is contributed by the widespread use of web and mobile applications, the rise of Generative AI, transitions towards a more digital public service infrastructures and the normalisation of business outsourcing practices that include public cloud adoption, managed infrastructure services, audit and system development. This trend has exposed organisations to multiple risks caused by a third-party that can be attributed to the weaknesses in the third-party's systems, human errors, non-compliance or violation againsts information security policy, sabotage and criminal activities. Attacks targeting the supply chains has been rising for the past few years and is expected to continuously increase until 2030. Based on the high-profile incidents that have been reported, the attacks are capable of bringing negative impacts on a global scale within a short amount of time. The implications are not only limited to financial losses and reputational damage but can affect the country's National Critical Information Infrastructure (CNII) which indirectly can threaten public safety and privacy. From our gap analysis study, the organisation's awareness and learning material readiness on this topic are lacking, prompting for urgent development of related modules. Hence, by employing Design and Development Research (DDR) approach this research will focus on three (3) main objectives which include the studies on the importance of third-party cybersecurity risks, the design and development of related module and content validation by experts. The outcome of this research is intended to give new perspective on cybersecurity awareness that focused on third-party risk. This module can be further utilized as a supporting material for various internal or external cybersecurity program or alternatively can be used to develop policies, procedures and guidelines for the governance of security at national or organisational level.

KANDUNGAN

		Halaman
PENGAKUAN		ii
PENGHARGAAN		iii
ABSTRAK		iv
ABSTRACT		v
KANDUNGAN		vi
SENARAI JADUAL		ix
SENARAI ILUSTRASI		xi
SENARAI SINGKATAN		xii
BAB I	Pengenalan	
1.1	Pendahuluan	1
1.2	Latar Belakang Kajian	3
1.3	Permasalahan Kajian	5
1.4	Persoalan Kajian	7
1.5	Objektif Kajian	8
1.6	Skop Kajian	8
1.7	Kepentingan Kajian	9
1.8	Definisi Operasional	10
1.9	Organisasi Kajian	11
BAB II	KAJIAN KESUSASTERAAN	
2.1	Pengenalan	13
2.2	Konsep dan Definisi	14
2.3	Peranan Pihak Ketiga Dan Kebergantungan Organisasi Kepada Pihak Ketiga Dalam Transformasi Digital	16
2.4	Risiko Keselamatan Pihak Ketiga	19
	2.4.1 Kerentanan dan Kelemahan Pihak Ketiga	22
	2.4.2 Ancaman Keselamatan Dari Pihak Ketiga	25
	2.4.3 Impak dan Kesan Ancaman daripada Pihak Ketiga	29
2.5	Pengurusan Risiko Pihak Ketiga	32
	2.5.1 Kerangka Pengurusan Risiko Pihak Ketiga	32

2.5.2	<i>Due Care dan Due Diligence</i>	33
2.5.3	Strategi Mitigasi	35
2.5.4	Praktis Terbaik	36
2.6	Keperluan Latihan dan Kesedaran Keselamatan Siber	37
2.7	Rujukan Berkaitan Risiko Keselamatan Pihak Ketiga	42
2.8	Pembangunan Modul Kesedaran Keselamatan Siber	43
2.8.1	Kajian-kajian Berkaitan	44
2.9	Metodologi Kajian	46
2.10	<i>Design and Development Research (DDR)</i>	49
2.10.1	Kajian Berkaitan DDR	51
2.11	Model Reka Bentuk Pengarahan (<i>Instructional Design Model (ID)</i>)	52
2.12	Pengaplikasian Teori Berkaitan	55
2.12.1	Teori Kesahan Kandungan	55
2.12.2	Teori Pembelajaran	58
2.13	Kesimpulan	60
BAB III	KAEDAH KAJIAN	
3.1	Pengenalan	61
3.2	Kaedah Kajian <i>Design and Development Research (DDR)</i>	61
3.2.1	Fasa Analisis Keperluan	63
3.2.2	Fasa Reka Bentuk dan Pembangunan	65
3.2.3	Fasa Penilaian DDR	67
3.3	Instrumen Kajian	71
3.3.1	Pembangunan Soalan Temu Bual Semi Struktur	71
3.3.2	Bahagian 1: Soalan Umum	72
3.3.3	Bahagian 2: Penilaian Kandungan Modul	73
3.3.4	Bahagian 3 : Soalan Terbuka	75
3.4	Populasi dan Sampel Kajian	75
3.5	Pertimbangan Etika	77
3.6	Kesimpulan	78
BAB IV	REKA BENTUK DAN PEMBANGUNAN	
4.1	Pengenalan	80
4.2	Analisis	81
4.2.1	Penetapan sasaran	81
4.2.2	Objektif Modul	81
4.3	Reka Bentuk	82

4.3.1	Penetapan Isi Kandungan	82
4.3.2	Reka Bentuk Papan Cerita	87
4.3.3	Pemilihan Peralatan dan Platform untuk Pembangunan	92
4.4	Pembangunan	94
4.4.1	Persediaan Ruang Kerja Synthesia	94
4.4.2	Video Modul yang Dihasilkan	98
4.5	Pelaksanaan	105
4.6	Penilaian Modul	106
4.7	Kesimpulan	106
BAB V DAPATAN KAJIAN		
5.1	Pengenalan	107
5.2	Analisis Dapatan / Hasil Kajian	108
5.2.1	Fasa 1 : Analisis Keperluan Kajian	108
5.2.2	Fasa 2 : Reka Bentuk dan Pembangunan	114
5.2.3	Fasa 3 : Penilaian	120
5.3	Kesimpulan	135
BAB VI PERBINCANGAN DAN RUMUSAN		
6.1	Sumbangan dan Kepentingan Kajian	136
6.2	Cadangan Kajian Hadapan dan Rekomendasi	137
6.3	Pencapaian Objektif Kajian	139
6.4	Kesimpulan	139
RUJUKAN		141
LAMPIRAN		
Lampiran A	Surat Lantikan Pakar	152

SENARAI JADUAL

No. Jadual		Halaman
Jadual 2.1	Perbezaan antara VRM,TPRM dan SCRM	21
Jadual 2.2	Teknik dan taktik yang digunakan berserta aset pihak ketiga yang disasarkan	27
Jadual 2.3	Kerangka Pengurusan Risiko Pihak Ketiga	33
Jadual 2.4	Perbezaan metodologi kajian	48
Jadual 2.5	Perbezaan jenis reka bentuk dan pembangunan (DDR)	49
Jadual 2.6	Kaedah yang biasa digunakan dalam DDR	50
Jadual 2.7	Perbezaan Model Reka Bentuk Pengarahan	54
Jadual 2.8	Nilai Kritikal Lawshe	57
Jadual 3.1	Reka bentuk kajian menggunakan pendekatan DDR	62
Jadual 3.2	Soal analisis kajian keperluan	64
Jadual 3.3	Nilai Kritikal mengikut bilangan pakar	70
Jadual 3.4	Objektif soalan umum dan contoh coalan temu bual	72
Jadual 3.5	Objektif soalan penilaian kandungan modul dan contoh soalan	74
Jadual 3.6	Objektif soalan terbuka dan contoh soalan	75
Jadual 3.7	Senarai Profil Pakar	75
Jadual 4.1	Fasa reka bentuk dan pembangunan melalui pendekatan ADDIE	80
Jadual 4.2	Cadangan Modul Risiko Pihak Ketiga dalam Keselamatan Siber	82
Jadual 4.3	Papan cerita (<i>Storyboard</i>) dan reka bentuk	88
Jadual 4.4	Antara contoh keratan video yang dihasilkan	98
Jadual 5.1	Pemetaan objektif kajian kepada dapatan kajian mengikut fasa DDR	107
Jadual 5.2	Paparan yang diekstrak dari video modul yang dihasilkan	115
Jadual 5.3	Pendapat pakar mengenai kepentingan tajuk	125

Jadual 5.4	Penilaian kesahan kandungan untuk Topik A, B, C, D, E, F berdasarkan <i>Content Validity Ratio</i> (CVR) oleh 12 Pakar	129
Jadual 5.5	Nilai Kritikal <i>Content Validity Ratio</i> (CVR) berdasarkan bilangan panel penilai mengikut Kaedah Lawshe (1975)	130
Jadual 5.6	Jawapan Pakar berkenaan ketepatan, kejelasan, struktur dan penyampaian modul	131
Jadual 5.7	Cadangan tambahan Pakar untuk penambahbaikan	132
Jadual 5.8	Jawapan Pakar untuk cadangan penggunaan modul	133
Jadual 5.9	Jawapan Pakar berkenaan impak modul kepada organisasi	134

LIBRARY FETSM

SENARAI ILUSTRASI

No. Rajah		Halaman
Rajah 1.1	Insiden keselamatan siber yang disebabkan vendor dan sukar untuk diuruskan	6
Rajah 2.1	Dasar Pengurusan Risiko Pihak Ketiga	36
Rajah 2.2	Pengurusan keselamatan dan hubungan dengan pembekal	42
Rajah 2.3	Model ADDIE	53
Rajah 2.4	Taksonomi Bloom	59
Rajah 2.5	Dua tahap dalam Taksonomi Bloom	59
Rajah 3.1	Fasa Penilaian dalam DDR	71
Rajah 3.2	Reka Bentuk Kajian (<i>Research Design</i>)	79
Rajah 4.1	Antara muka platform Synthesia	94
Rajah 4.2	Antara muka untuk pemilihan avatar dan suara	95
Rajah 4.3	Antara muka untuk pemilihan <i>full body</i> atau <i>half body</i>	96
Rajah 4.4	Antara muka untuk menambah animasi atau efek ke atas objek	97
Rajah 4.5	Antara muka untuk menerbitkan (<i>publish</i>) video	97
Rajah 4.6	Contoh konsol dari sudut pandangan pentadbir sistem.	105
Rajah 4.7	Contoh konsol dari sudut pandangan pengguna (Penilai Pakar)	106
Rajah 5.1	Responden yang menerima latihan keselamatan risiko pihak ketiga	112
Rajah 5.2	Senarai ancaman dalam senarai daftar risiko aset	113
Rajah 5.3	Senarai bilangan aset dan kerentanan oleh pemilik aset	113

SENARAI SINGKATAN

API	Application Programmable Interface
C-SCRM	Cybersecurity Supply Chain Risk Management
C-TPRM	Cyber Third-Party Risk Management
CNII	Critical National Information Infrastructure
CVI	Critical Value Indeks
CVR	Critical Value Ratio
DDR	Design and Development Research
DDoS	Distributed Denial of Service
ENISA	European Union Agency for Cyber Security
FDM	Fuzzy Delphy Method
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
NACSA	National Cyber Security Agency, Malaysia
NC4	National Cyber Coordination and Command Centre
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
SaaS	Software as a Service
SBoM	Software Bill of Materials
SDLC	Software Development Life Cycle
TPRM	Third-Party Risk Management
VRM	Vendor Risk Management
UKM	Universiti Kebangsaan Malaysia

BAB I

PENGENALAN

1.1 PENDAHULUAN

Perkembangan teknologi dan digital seperti teknologi 5G, IoT, Kecerdasan Buatan (AI), Realiti Terimbuh (AR) dan teknologi awan pada hari ini telah menjadi pemangkin kepada ekosistem digital yang lebih kompleks dan saling berhubung kait antara satu sama lain. Teknologi 5G merancakkan lagi pembangunan platform seperti perbandaran pintar, kereta *autonomous*, *smart utility*, *smart grid* dan sebagainya. Ini memberi peluang yang luas kepada penyedia perkhidmatan ICT untuk menjadi sebahagian ekosistem dalam pelbagai industri seperti logistik, pengangkutan, perbandaran, perkilangan, pertanian, kesihatan dan sebagainya. Penyedia perkhidmatan ICT di mana sebelum ini hanya terhad kepada pembangunan sistem aplikasi, penyedia internet dan sebagainya.

Sebagai contoh dengan perkembangan teknologi awan, penyedia perkhidmatan awan dapat menawarkan pelbagai perkhidmatan yang terdiri daripada infrastruktur (IaaS), platform (PaaS), software (SaaS) dan sebagainya yang dapat membantu menjalankan operasi pelbagai sektor termasuk sektor kerajaan dan swasta. Pada hari ini, kebanyakan organisasi tidak lagi perlu membangunkan infrastruktur ICT sendiri, sebaliknya boleh terus melanggan aplikasi yang telah siap dibina untuk urusan produktiviti kerja seperti *Microsoft 365*, *Google Workspace*, *HR in the Box*, sistem perakaunan dan sebagainya (Xu & Mahenthiran 2021). Malahan, saling integrasi antara sistem boleh juga berlaku di peringkat pengekodan dengan menggunakan API (*Application Programming Interface*), yang membenarkan dua sistem atau lebih yang dibangunkan secara berasingan dapat melakukan pertukaran data bagi melaksanakan pemrosesan secara masa sebenar. Ini adalah kerana pembangunan aplikasi moden

pada hari ini tidak lagi dibangunkan secara monolit di mana semua modul perisian perlu dikompil sebagai satu program yang besar dan kompleks. Sebaliknya dalam pembangunan aplikasi moden, pendekatan pembangunan perkhidmatan mikro (*microservice*) lebih banyak digunakan di mana setiap modul atau program dibangunkan secara berdiri sendiri (*stand-alone*) dan dilengkapi dengan API yang membolehkan sesebuah modul perisian itu berinteraksi dengan modul perisian lain. Sebagai contoh sebuah aplikasi logistik boleh mendapatkan maklumat berkenaan ramalan cuaca daripada sistem data terbuka dan jadual kargo dari syarikat penyedia perkhidmatan logistik seperti KTMB (Kereta Api Tanah Melayu Berhad). Baru-baru ini Malaysia telah melancarkan sistem PADU (Pangkalan Data Utama) yang membolehkan pelbagai agensi Kerajaan Malaysia berkongsi data bagi tujuan menguruskan ekonomi rakyat Malaysia. Ini membuktikan bahawa landskap teknologi telah berubah dan telah meningkatkan saling kebergantungan ekosistem terhadap perkhidmatan yang disediakan oleh pihak ketiga. Walau bagaimanapun, dengan kelebihan teknologi yang saling berhubung ini, turut meluaskan permukaan serangan (*attack surface*) atau risiko keselamatan khususnya terhadap rantai bekalan yang berpunca daripada kelemahan pihak ketiga.

Sesungguhnya, kekuatan sebuah rantai (ekosistem) adalah bergantung kepada titik hubungan yang paling lemah dalam rantai tersebut. Justeru, sebuah organisasi perlu berusaha memperkukuhkan setiap penjuru rantai pembekalan perkhidmatan sebaliknya penggodam hanya perlu mengenal pasti dan mengeksploitasi satu sahaja titik kelemahan dalam rantai tersebut. Risiko ini bukan sahaja bersifat teknikal malah ia boleh disebabkan oleh kelemahan atau ketidakpatuhan terhadap polisi keselamatan oleh individu atau organisasi penyedia perkhidmatan seperti vendor, pembangun perkhidmatan, pembangun aplikasi dan sebagainya.

1.2 LATAR BELAKANG KAJIAN

Kajian ini adalah berkaitan pihak ketiga yang lebih dikenali dalam konteks industri atau perniagaan khususnya berkenaan dengan *supply chain* (rantai bekalan), namun aspek pengurusan risiko keselamatan daripada pihak ketiga ini hanya mula mendapat perhatian pada beberapa tahun kebelakangan ini. Ini berikutan peningkatan insiden-insiden keselamatan berprofil tinggi yang berpunca dari kelemahan pihak ketiga atau pada rantai bekalan. Insiden SolarWinds Hack (Bronson 2022; Takefuji 2023) adalah salah satu contoh penting di mana perisian pemantauan infrastruktur rangkaian dan sistem yang terkenal iaitu SolarWinds Orion telah berjaya di kompromi oleh sekumpulan penggadam semasa peringkat pembangunan lagi. Ini mengakibatkan perisian yang telah dikompromi disebarluaskan secara sistematik dan meluas ke semua rantai pelanggan dari seluruh dunia semasa mengemaskini perisian. Impak dan skala serangan *supply chain* ini sangat luas kerana perisian ini telah diguna pakai diseluruh dunia oleh pelbagai organisasi serta agensi kerajaan termasuklah FBI, Microsoft dan sebagainya. Perisian yang dikompromi ini tanpa disedari telah membuka pintu belakang (*backdoor*) bagi membolehkan penggadam mengakses rangkaian ICT pelanggan dan mendedahkan setiap organisasi ini kepada pelbagai ancaman lain seperti kecurian data sensitif, pelanggaran privasi, pencerobohan sistem organisasi dan sebagainya.

Hal ini selari dengan laporan landskap keselamatan siber terkini yang menunjukkan peningkatan yang ketara pada jumlah insiden yang berpunca daripada pihak ketiga. Bronson (2022) membincangkan lapan (8) insiden bersumber daripada pihak ketiga di mana industri kewangan dan kesihatan sebagai sasaran utama. Berdasarkan kajian tersebut, pelanggaran data dalam sektor kewangan global adalah yang kedua tertinggi dari segi kos selepas sektor penjagaan kesihatan, dengan purata USD5.72 juta bagi setiap insiden.

Menurut Bronson (2022) lagi, kelemahan perisian yang berasal dari pihak ketiga menyumbang kepada 14% daripada keseluruhan pelanggaran data di semua industri, manakala 44% daripada kes pelanggaran yang dianalisis melibatkan kehilangan maklumat peribadi pelanggan (PII). Kajian tersebut juga mendapati bahawa organisasi yang gagal menilai serta meningkatkan langkah-langkah keselamatan mereka yang

mengakibatkan pelanggaran data secara umumnya akan menghadapi kos tambahan sebanyak USD750,000.

Garcia-Granados dan Bahsi (2020) telah menjalankan kajian literatur secara berstruktur berkaitan keselamatan siber dan memberi skor markah pada setiap insiden keselamatan siber dalam jurnal yang dikaji. Antara dapatan kajian tersebut, sebanyak 35% daripada senarai literatur yang dikaji melibatkan insiden berkaitan rantaian bekalan yang berpunca daripada pihak ketiga.

Selain daripada kajian terhadap insiden, terdapat juga kajian yang membincangkan kaedah pengurusan risiko keselamatan pihak ketiga yang dijalankan oleh Keskin et al. (2021). Menurut beliau, konsep *Cyber Third-Party Risk Management* (C-TPRM) yang merupakan topik baharu dalam domain keselamatan siber perlu diberi perhatian dan telah mula digunakan secara meluas dalam sektor perniagaan dan insurans siber. Kajian beliau turut mencadangkan satu kaedah penilaian berdasarkan data bagi mengisi jurang keperluan C-TPRM.

Kumar dan Mallipeddi (2022) turut menyokong bahawa risiko daripada pihak ketiga ini perlu diberi perhatian bagi kajian masa hadapan berikutan pergantungan yang tinggi khususnya terhadap teknologi pintar dalam operasi dan produksi. Beliau menganalisa beberapa contoh insiden yang memberi impak tinggi antaranya ialah serangan perisian tebusan (*ransomware*) terhadap syarikat pembekal komponen bagi produk Apple yang beroperasi di Taiwan. Insiden ini menyebabkan kebocoran akses dan maklumat sensitif syarikat Apple yang melibatkan tuntutan wang tebusan bernilai USD50juta. Kajian ini turut mencadangkan isu keselamatan dalam rantaian bekalan ini sebagai salah satu daripada domain penting yang perlu dikaji dalam bidang Pengurusan dan Operasi (*Production and Operation Management*).

Antara rujukan utama yang akan digunakan dalam kajian ini adalah buku bertajuk *Cybersecurity and Third Party Risk* (Gregory 2021) yang diterbitkan oleh (ISC)² pada tahun 2021. Buku ini membincangkan dengan terperinci berkenaan pengurusan risiko Pihak Ketiga yang merangkumi aspek penilaian dan pengoperasian secara praktikal. Buku ini turut menyenaraikan dan membincangkan sebahagian daripada 60 contoh insiden dari tahun 2013 hingga 2021 yang menunjukkan peningkatan ketara sejak tahun 2018 hingga 2021. Antara insiden berprofil tinggi adalah

insiden SolarWinds Hack yang melibatkan sebuah perisian pemantauan rangkaian yang melibatkan puluhan ribu organisasi besar termasuk Malaysia yang turut terkesan dengan penularan insiden ini.

Menurut MCMC (2023), dalam tempoh beberapa tahun terakhir ini, Malaysia juga tidak ketinggalan menyaksikan perkembangan yang signifikan dalam ekonomi digitalnya, di mana peningkatan kebergantungan teknologi oleh organisasi dan individu menjadi lebih ketara. Menerusi agenda Malaysia Digital contohnya, kerajaan telah mensasarkan 80% data kerajaan untuk dipindahkan ke perkhidmatan perkomputeran awan yang dilantik (MOF 2022). Perkongsian data yang meluas berpotensi untuk meningkatkan risiko yang disebabkan oleh pihak ketiga (Takefuji 2023). Sebagai contoh sebanyak 61% organisasi di United States pernah mengalami kebocoran maklumat yang melibatkan rantaian bekalan (Bronson 2022). Selain itu, budaya kerja secara jarak jauh oleh para pekerja dan pembekal juga menyumbang kepada peningkatan kebocoran maklumat sensitif dan Harta Intelek (Olubunmi et al. 2024). Dengan pengenalan Akta Keselamatan Siber 2024, senarai asas keselamatan atau *baseline* telah diwartakan turut menekankan kepentingan menguruskan keselamatan rantaian bekalan dari sudut perhubungan dengan pembekal pada klausa 3.3 (Government of Malaysia 2024).

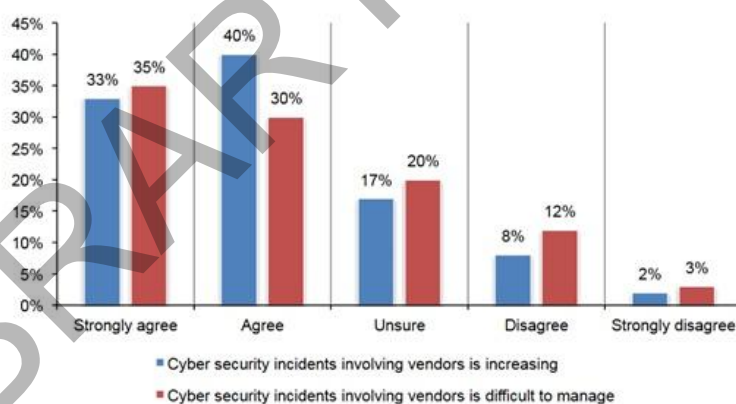
Secara kesimpulannya, ancaman terhadap rantaian bekalan perkhidmatan adalah sesuatu yang nyata dan mampu memberi impak pada skala yang sangat dahsyat baik dari sudut kewangan, keselamatan, privasi, kecurian harta intelek, kebocoran data sensitif dan boleh menyebabkan kehilangan nyawa. Ini turut disokong daripada beberapa laporan dan kajian yang menekankan peningkatan kes-kes berprofil tinggi yang berpunca daripada pihak ketiga. Dalam konteks Malaysia pula, dengan pelbagai agenda kerajaan dalam transformasi digital menyebabkan kebergantungan yang tinggi terhadap perkhidmatan pihak ketiga, secara tidak langsung ini mendedahkan infrastruktur kerajaan kepada risiko ini.

1.3 PERMASALAHAN KAJIAN

Transformasi digital yang pesat dan saling hubungan antara organisasi menyebabkan peningkatan pergantungan pada vendor, rakan kongsi, dan penyedia perkhidmatan pihak ketiga dalam ekosistem rantaian bekalan (Moller 2023). Walaupun ini memberi

manfaat daripada segi produktiviti dan inovasi, ia turut membawa risiko keselamatan siber yang signifikan. Data menunjukkan hanya 35% profesional keselamatan siber sedar dan mengetahui secara jelas berkenaan jumlah vendor yang mengakses sistem dalaman mereka (VanHoy 2021). Ini bermakna sebahagian besar sistem terdedah kepada ancaman yang berpunca daripada kelemahan dan ketidakpatuhan pihak ketiga. VanHoy (2021) juga turut menyatakan bahawa banyak organisasi gagal untuk menangani risiko ini secara menyeluruh menyebabkan mereka terdedah kepada serangan siber melalui hubungan pihak ketiga.

Melalui satu kajian oleh *Phenomenan Institute* seperti Rajah 1.1, sehingga 73% responden bersetuju bahawa terdapat peningkatan insiden keselamatan yang berpunca daripada pihak ketiga dan sehingga 65% bersetuju bahawa menguruskan insiden keselamatan siber melibatkan pihak ketiga adalah sukar. Ini juga turut disokong oleh (Crider et al. 2023) yang melaporkan bahawa pelanggaran data disebabkan oleh pihak ketiga semakin tinggi dan sukar untuk diuruskan.



Rajah 1.1 Insiden keselamatan siber yang disebabkan vendor dan sukar untuk diuruskan

Sumber: Tempy 2019

VanHoy (2021) pula menegaskan bahawa banyak organisasi tidak memberikan fokus terhadap ancaman dan pengurusan risiko oleh pihak ketiga. Secara tidak langsung, perbincangan mengenai peranan latihan dan kesedaran pekerja dalam mengurangkan risiko ini adalah sangat kurang. Oleh yang demikian, Fallatah et al. (2024) dan VanHoy (2021) menegaskan bahawa terdapat keperluan mendesak untuk membangunkan modul latihan khusus yang dapat meningkatkan pemahaman risiko ini dan menyediakan strategi mitigasi yang efektif untuk organisasi.

Meskipun risiko pihak ketiga semakin mengancam keselamatan siber, modul latihan yang fokus secara khusus pada pengurusan risiko pihak ketiga masih terhad. Latihan keselamatan siber yang sedia ada banyak memberi penekanan kepada keselamatan am tetapi kekurangan fokus dalam pengurusan risiko pihak ketiga, menyebabkan organisasi lebih mudah terdedah kepada ancaman yang berpunca dari pihak ketiga (Award 2022; StandardFusion 2024).

Berdasarkan dapatan di atas, jelas bahawa terdapat keperluan untuk mengkaji kepentingan berkenaan risiko pihak ketiga dan memberi pendedahan kepada organisasi terhadap risiko tersebut. Justeru, kajian ini dilakukan untuk mengenal pasti kepentingan risiko keselamatan siber yang berpunca daripada pihak ketiga dalam konteks organisasi dan seterusnya membangunkan modul latihan keselamatan siber yang disahkan oleh pakar.

1.4 PERSOALAN KAJIAN

Bagi memberi pendedahan kepada umum berkenaan risiko ini, asas pengetahuan dan bahan yang sesuai dan mudah difahami perlu dibangunkan. Untuk tujuan tersebut, kajian ini akan menjawab persoalan kajian seperti berikut:

1. P1 - Apakah risiko keselamatan yang berpunca daripada pihak ketiga, mengapakah ia perlu diberi perhatian dan apakah tahap kesedaran dalam organisasi?
2. P2 – Apakah kandungan, struktur dan penceritaan (naratif) yang sesuai bagi menghasilkan sebuah modul latihan untuk tajuk Risiko Pihak Ketiga dalam Keselamatan Siber?
3. P3 - Apakah maklum balas pakar berkenaan tajuk ini khususnya bagi mengesahkan kandungan modul yang dihasilkan?

1.5 OBJEKTIF KAJIAN

Untuk menjawab personal kajian seperti para 1.4 di atas, kajian ini akan menyasarkan TIGA objektif utama:

1. Mengenal pasti kepentingan risiko keselamatan siber berpunca daripada pihak ketiga;
2. Menghasilkan modul latihan yang menjelaskan berkenaan risiko keselamatan siber berpunca daripada pihak ketiga; dan
3. Mengesahkan kandungan modul secara menemu bual pakar.

1.6 SKOP KAJIAN

Definisi pihak ketiga pada dasarnya merangkumi satu ekosistem yang luas dan kompleks kerana melibatkan pelbagai pemegang taruh termasuk pengilang, pengedar, pembangun perisian, logistik, pembekalan makanan, perkhidmatan bangunan, perkhidmatan ikhtisas, hospitaliti, perkhidmatan ICT dan sebagainya. Menurut Angle (2019) dalam penerbitan laporan yang dikeluarkan oleh *Cloud Security Alliance (CSA)* sebuah badan piawai keselamatan awan telah mengkategorikan risiko keselamatan rantaian bekalan ini kepada dua iaitu 1) *Cyber Supply Chain Risk Management* dan 2) *Supply Chain Cyber Risk Management*. *Cyber Supply Chain Risk Management* melibatkan pembekalan produk dan perkhidmatan ICT manakala *Supply Chain Cyber Risk Management* pula merujuk kepada risiko penggunaan ICT dalam pengurusan bekalan rantaian produk atau perkhidmatan yang lebih luas. Skop kajian ini akan menumpukan pada konteks *Cyber Supply Chain Risk Management*.

Setiap pemegang taruh dalam rantaian bekalan juga mempunyai ekosistem sendiri. Sebagai contoh, penyedia perkhidmatan awan (CSP) juga turut mempunyai rangkaian vendor yang membekal, membangun dan menguruskan infrastruktur awan (yang dikenali sebagai pihak keempat, *subprocessor*, *subcontractor* dan sebagainya). Oleh yang demikian skop bagi kajian ini hanya akan memfokuskan kepada aspek-aspek berikut:

1. Kajian ini adalah terhad kepada organisasi di Malaysia (sebagai contoh, kumpulan pakar yang akan dikenal pasti untuk ditemu bual akan memberi pandangan dan penilaian berkenaan risiko pihak ketiga dalam konteks organisasi di Malaysia);
2. Jenis perkhidmatan yang menjadi fokus kajian ini adalah perkhidmatan Teknologi Maklumat (ICT) yang juga merujuk kepada *Cyber Supply Chain Risk Management* (ini tidak termasuk rantaian bekalan seperti logistik, pembekalan makanan, perkhidmatan bangunan, perkhidmatan ikhtisas, hospitaliti dan sebagainya);
3. Penilaian pakar adalah bersifat *internal validation* yang memfokuskan ke atas modul yang dibangunkan bagi memastikan modul yang relevan dan penggunaan fakta yang sahih di samping elemen tambahan seperti kejelasan dan struktur kandungan.
4. Oleh yang demikian, penilaian terhadap keberkesanan kandungan dan kualiti penyampaian (video/audio) tidak termasuk dalam kajian ini (*external validation*).

1.7 KEPENTINGAN KAJIAN

Kepentingan hasil kajian ini secara umumnya adalah seperti berikut:

1. Dapat membantu organisasi kerajaan dan swasta untuk memastikan infrastruktur yang selamat dan dipercayai untuk menjayakan agenda transformasi digital;
2. Dalam konteks perkhidmatan kerajaan, rakyat akan lebih yakin menggunakan infrastruktur kerajaan khususnya dalam perkongsian data peribadi dan maklumat sulit;

3. Dalam konteks organisasi pula, kajian ini dapat membantu organisasi mengenal pasti risiko berkaitan pihak ketiga dan menangani risiko dan kelemahan yang berpunca daripadanya;
4. Modul latihan yang dihasilkan juga sesuai digunakan oleh organisasi dan boleh diolah bagi tujuan kempen kesedaran, sosial media, latihan keselamatan siber atau sebagai latihan induksi (*staff onboarding*) sama ada organisasi kerajaan atau swasta.
5. Dengan kefahaman terhadap risiko tersebut organisasi dapat mengurangkan risiko keselamatan siber yang secara tidak langsung mengelakkan implikasi seperti reputasi yang buruk, kerugian kewangan, kehilangan nyawa, kebocoran maklumat sensitif, pelanggaran data privasi, kecurian harta intelek dan ketidakpatuhan undang-undang, perbuatan khianat, penyalahgunaan maklumat dan sebagainya yang berpunca daripada pihak ketiga.
6. Hasil kajian ini boleh digunakan bagi melaksanakan polisi keselamatan berkaitan pihak ketiga sama ada di peringkat nasional atau peringkat organisasi. Sebagai contoh modul latihan ini juga boleh menjadi garis panduan kepada organisasi supaya dapat melaksanakan tindakan sewajarnya.

1.8 DEFINISI OPERASIONAL

Definisi operasional yang digunakan dalam kajian ini:

1. Pihak ketiga merujuk kepada pembekal, penyedia perkhidmatan, pembangun perisian, alatan (*tools*), penyedia rangkaian, penyedia infrastruktur awan, pengintegrasian sistem, penilai (*auditor / pentester*), pembangun perisian sumber terbuka yang menyediakan atau memberikan perkhidmatan secara langsung atau tidak langsung kepada pengguna akhir, sumber terbuka (*open source*), pustaka perisian (*software library*) atau apa-apa perkhidmatan.
2. Risiko pihak ketiga dalam keselamatan siber - ancaman dan kelemahan yang berpunca daripada pihak ketiga khususnya dalam keselamatan siber.

3. Modul latihan adalah susunan kandungan dan bahan yang mengandungi topik-topik penting dan penerangan secara terperinci berkenaan risiko keselamatan pihak ketiga yang dibangunkan sebagai hasil kajian yang disahkan oleh pakar.
4. Pakar ialah pakar yang mempunyai kelayakan atau menjalankan fungsi rasmi sebagai pengurus keselamatan atau profesional yang menguruskan teknologi maklumat dengan sekurang-kurangnya 8 tahun pengalaman.
5. Organisasi merujuk kepada entiti kerajaan atau swasta atau pekerja-pekerja yang menjalankan operasi perniagaan.

1.9 ORGANISASI KAJIAN

Kajian ini disusun kepada beberapa Bab seperti berikut:

1. Bab I akan memberikan gambaran menyeluruh tentang pengenalan dan latar belakang kajian, permasalahan kajian, persoalan kajian, objektif kajian, skop kajian dan kepentingan kajian serta ringkasan bagaimana tesis ini persembahkan.
2. Bab II menghimpunkan kajian kesusasteraan daripada pelbagai sumber akademik dan industri, buku, dokumen rasmi merangkumi garis panduan, rangka keselamatan dan polisi serta dokumen piawaian keselamatan.
3. Bab III mengandungi penerangan metodologi kajian yang digunakan iaitu Kajian Reka Bentuk dan Pembangunan (*Design and Development Research (DDR)*) dan beberapa metode, model dan kerangka teori yang digunakan. Ini termasuklah model reka bentuk instruksional, teori pembelajaran dan metode kesahan kandungan (*content validation*). Selain itu, pembangunan soalan temu bual pakar dan prosedur temu bual juga dibincangkan dalam bab ini. Fasa pertama DDR iaitu analisis keperluan juga diterangkan dalam bab ini bagi menyediakan input kepada fasa reka bentuk dan pembangunan.
4. Bab IV membincangkan implementasi kajian iaitu fasa kedua DDR yang merangkumi fasa reka bentuk (berasaskan model ADDIE) dan pembangunan

modul. Ini termasuklah aktiviti penyusunan kandungan, penstrukturan modul dan membangunkan papan penceritaan.

5. Bab V akan melaporkan modul yang telah dibangunkan yang dipersembahkan dalam format video untuk penilaian pakar. Dapatan dari temu bual dilaporkan dan dianalisis untuk menjawab persoalan kajian iaitu menentusahkan kepentingan tajuk modul serta mengesahkan modul yang dihasilkan daripada segi relevansi, ketepatan fakta dan kejelasan. Selain itu, maklum balas juga dianalisis untuk mendapatkan cadangan penambahbaikan dan cadangan pelaksanaan modul ini dalam persekitaran sebenar.
6. BAB VI akan membincangkan sumbangan dan kepentingan kajian, cadangan kajian pada masa hadapan serta rekomendasi yang boleh dilaksanakan. Akhir sekali, bab ini juga akan merumuskan bagaimana kajian ini memenuhi persoalan kajian dan objektif kajian yang telah ditetapkan.

BAB II

KAJIAN KESUSASTERAAN

2.1 PENGENALAN

Bab ini membicarakan sorotan kesusasteraan yang akan menyokong dan membantu untuk mencapai objektif kajian ini. Selain itu, bab ini memperincikan semua perbincangan seperti disebutkan dalam pengenalan dan latar belakang kajian dalam Bab I.

Perkembangan teknologi yang pesat telah menyebabkan pergantungan yang tinggi terhadap perkhidmatan pihak ketiga yang turut mendedahkan organisasi terhadap risiko-risiko keselamatan yang berpunca daripada pihak ketiga. Oleh yang demikian, beberapa aspek penting berkaitan pihak ketiga dalam keselamatan siber akan dibincangkan.

Sumber kajian kesusasteraan diambil daripada jurnal dan prosiding akademik, tesis, penerbitan-penerbitan oleh badan keselamatan, dokumen rasmi seperti akta, garis panduan, kod amalan, polisi dan juga kerangka keselamatan yang disediakan oleh badan-badan piawaian dan sebagainya. Selain itu, laporan landskap keselamatan terkini yang disediakan oleh pemain-pemain industri juga diteliti. Sorotan kesusasteraan ini juga merangkumi aspek-aspek kajian lain seperti metodologi dan kerangka teori bagi membentuk hala tuju kajian ini.

2.2 KONSEP DAN DEFINISI

Dalam sorotan kesusasteraan yang dijalankan terdapat pelbagai konsep yang merujuk kepada pihak ketiga seperti rantaian bekalan (*supply chain*), vendor dan sumber luar (*outsourcing*). Segmen ini akan membincangkan pelbagai definisi yang dipetik daripada pelbagai sumber dan mencadangkan terminologi yang akan digunakan sepanjang kajian ini.

Menurut kamus Dewan Bahasa dan Pustaka pihak ketiga merujuk kepada orang lain yang tidak berpihak dalam urusan. Sebagai contoh, dalam konteks kerajaan Malaysia yang menyediakan infrastruktur digital kepada rakyat, pihak pertama merujuk kepada kerajaan manakala rakyat ialah pihak kedua yang menerima perkhidmatan secara langsung daripada kerajaan. Pihak ketiga pula merujuk kepada mana-mana individu atau organisasi yang membantu kerajaan memberikan perkhidmatan kepada rakyat. Dalam hal ini pihak ketiga tidak mempunyai kepentingan atau dengan kata lain tidak mendapat kesan dan implikasi secara langsung sekiranya terdapat kegagalan dalam penyampaian perkhidmatan tersebut.

Istilah pihak ketiga bukanlah sesuatu yang baru sebaliknya ia telah digunakan dalam pelbagai sektor khususnya logistik, kewangan, perkilangan dan sebagainya. Pihak kerajaan Amerika Syarikat contohnya telah mula mewajibkan bank-bank di Amerika untuk membuat kawalan terhadap risiko pihak ketiga sejak tahun 2013. Dokumen yang bertajuk “OCC 2013-2019” telah mendefinisikan pihak ketiga sebagai organisasi atau entiti yang berurusan dengan sesebuah organisasi termasuk vendor, pembekal, rakan niaga, *affiliate*, broker, pengilang dan agen. Ini termasuklah entiti yang mempunyai hubungan kontraktual atau tidak (Gregory 2021).

Beberapa dokumen rasmi kerajaan Malaysia juga telah mengguna pakai istilah pihak ketiga yang ditakrifkan sebagai sumber luar atau pembekal yang memenuhi syarat-syarat yang telah ditetapkan oleh kerajaan. Ini dinyatakan di dalam Surat Pekeliling Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam dan Dasar Keselamatan Siber yang mensyaratkan pihak ketiga yang dilantik supaya dapat menyediakan perkhidmatan atau produk yang mematuhi piawaian

keselamatan, kualiti dan kecekapan yang diperlukan oleh sektor (JPM 2024; PLANMalaysia 2023).

Selain itu, terdapat juga perbincangan berkenaan perbezaan antara pihak ketiga dan pihak keempat, walau bagaimanapun kajian ini menggunakan istilah pihak ketiga kerana ia mempunyai kesan yang sama. Tambahan pula sesebuah organisasi hanya boleh mengawal atau mengambil tindakan terhadap pihak ketiga yang mempunyai kontrak secara langsung (Lauren 2024).

Agensi piawaian NIST pula mendefinisikan hubungan pihak ketiga sebagai entiti luar yang merangkumi penyedia perkhidmatan, vendor, rakan kongsi di pihak pembekalan, rakan kongsi di pihak permintaan, pakatan, konsortium dan pelabur yang boleh terdiri daripada pihak yang terikat dengan kontrak mahupun tanpa kontrak (Stouffer et al. 2019).

Dalam istilah lain, pihak ketiga juga dirujuk sebagai rantaian bekalan (*supply chain*) yang didefinisikan sebagai rangkaian sumber dan proses yang saling berkait di pelbagai peringkat dalam sesebuah organisasi. Setiap peringkat bertindak sebagai penerima yang memulakan proses dengan perolehan produk dan perkhidmatan serta merangkumi keseluruhan kitaran hayat produk dan perkhidmatan tersebut (Boyens et al. 2020). Menurut Hammi et al. (2023) rantaian bekalan ialah rangkaian global yang menyediakan bahan mentah, produk, dan perkhidmatan kepada pelanggan akhir melalui aliran maklumat, pengedaran fizikal dan wang yang direka bentuk. Walau bagaimanapun kajian ini akan memfokus hanya kepada bekalan ICT atau rantaian bekalan siber (*cyber supply chain*).

Dalam konteks perniagaan, pihak ketiga juga dikenali sebagai entiti yang menjalankan kerja-kerja bagi sesebuah organisasi dan dikenali sebagai penyedia perkhidmatan atau sumber luar (*outsourcing*). Ia merupakan perjanjian perniagaan yang melibatkan pemindahan fungsi atau kecekapan teras syarikat kepada pembekal yang kompeten, sama ada di dalam atau luar negara sama ada secara lisan atau bertulis. Ini adalah sebagai sebahagian inisiatif pengurusan strategik untuk meningkatkan kecekapan, keberkesanan dan kelebihan daya saing. Sumber luar tidak hanya terhad

kepada produk atau perkhidmatan, tetapi juga boleh merangkumi proses perniagaan, asalkan ia membantu syarikat meningkatkan kualiti dan produktiviti (Yingying et al. 2021).

Dengan pelbagai terminologi yang telah dibincangkan, dapat disimpulkan bahawa pihak ketiga ialah pihak yang memberi perkhidmatan dan tidak mempunyai kepentingan secara langsung terhadap data atau infrastruktur yang dimiliki oleh sesebuah organisasi. Pihak ketiga juga tidak terkesan secara langsung sekiranya berlaku apa-apa insiden keselamatan dalam organisasi. Oleh yang demikian, kajian ini akan menggunakan definisi pihak ketiga sebagai individu atau syarikat yang berurusan dengan organisasi yang berperanan sebagai vendor, pembekal, pembangun perisian, pengeluar, juru audit, pengintegrasian sistem atau penyedia infrastruktur (pengkomputeran awan, infrastruktur SaaS). Definisi ini juga terpakai kepada semua syarikat yang mempunyai kontrak atau tidak, dan pihak keempat yang memberi perkhidmatan kepada pihak ketiga seperti penyedia perisian pustaka (*software library*), subkontraktor, dan semua peralatan atau perkhidmatan yang digunakan oleh pihak ketiga dalam rantai bekalan siber. Walau bagaimanapun, kesemua istilah di atas diguna pakai bagi tujuan carian kesusasteraan.

2.3 PERANAN PIHAK KETIGA DAN KEBERGANTUNGAN ORGANISASI KEPADA PIHAK KETIGA DALAM TRANSFORMASI DIGITAL

Menurut laporan Gartner oleh Bryan (2019), pada tahun 2019 sebanyak 71% organisasi yang disoal selidik telah melaporkan peningkatan mendadak keterlibatan pihak ketiga dan dijangka akan terus meningkat pada kadar yang sama sehingga tahun 2022. Kajian tersebut juga melaporkan bahawa 60% organisasi bekerja dengan lebih daripada 1000 organisasi pihak ketiga.

Peranan pihak ketiga adalah sangat penting untuk kelangsungan organisasi global masa kini. Dengan tahap kebergantungan yang tinggi antara organisasi, tiada misi perniagaan yang akan berjaya tanpa menerima produk atau perkhidmatan daripada pihak ketiga (Keskin et al. 2021). Yingying et al. (2021) telah mengkaji literatur secara sistematik berkenaan pihak ketiga dan penggunaan perkhidmatan sumber luar oleh

organisasi. Menurut beliau, sebanyak 390,000 artikel berkaitan tajuk ini telah diterbitkan sejak tahun 2010.

Di Malaysia, di bawah Rangka Tindakan Ekonomi Digital Malaysia (MyDigital) kerajaan menyasarkan 80% data sektor awam disimpan di pengkomputeran awan melalui inisiatif MyGovCloud@PDSA iaitu Pemindahan Pusat Data Sektor Awam (PDSA) kepada perkhidmatan awan. Kerajaan turut melantik empat (4) penyedia perkhidmatan awan (*Cloud Service Provider*) sebagai sebahagian dari ekosistem yang akan menjayakan agenda ini. Ini secara tidak langsung telah menggalakkan penggunaan perkhidmatan pihak ketiga. Dengan penyertaan ini, transformasi digital dapat dipacu secara holistik, sekali gus meningkatkan kecekapan operasi dan merangsang pertumbuhan ekonomi digital negara (Bahagian Perolehan Kerajaan 2022; MOF 2022).

Seiring dengan transformasi digital, penggunaan perisian telah mengambil alih fungsi-fungsi penting dan aktiviti kehidupan seharian dan perniagaan serta khidmat kerajaan. Ini turut dibantu oleh penggunaan aplikasi mobil dan teknologi-teknologi seperti 5G dan jalur lebar. Pada hari ini perisian-perisian yang dibangunkan telah menunjukkan trend peralihan seni bina secara monolit kepada mikro servis (Auer et al. 2021; Kaloudis 2024). Seni bina monolit merupakan kaedah pembangunan legasi di mana semua modul di kumpul dalam satu program yang besar. Manakala melalui mikro servis program-program ini dibangunkan secara modular dan mempunyai kebolehan berinteraksi secara bebas untuk mengambil input dan mengeluarkan output dari sistem yang dibangunkan oleh pihak ketiga ke sistem lain dengan menggunakan antara muka aplikasi program atau *Application Programming Interface* (API) .

Trend seni bina ini digunakan oleh syarikat-syarikat gergasi seperti Amazon, Netflix dan sebagainya untuk membangunkan aplikasi syarikat mereka. Banyak aplikasi pada hari ini telah melalui pemodenan aplikasi (*application modernization*) untuk beralih kepada seni bina mikro servis (Kaloudis 2024; Moller 2023). Kerajaan juga turut menyasarkan sehingga 50% data kerajaan untuk di kongsi secara terbuka melalui API dalam dokumen Sasaran Strategik 2021-2025 (Bahagian Perundingan ICT MAMPU 2021). Selain daripada seni bina moden yang bersifat mikro servis hakikatnya pembangunan perisian pada hari ini melibatkan 70% kod program yang diguna semula

dalam bentuk pustaka perisian yang dibangun oleh pihak ketiga sama ada secara komersial atau sumber terbuka (W3Computing 2023). El Moustako (2020) pula melaporkan sehingga 60% laman web pada hari ini menggunakan sumber terbuka iaitu Apache dan NGIX sebagai pelayan web. Manakala 90% pengurus ICT dilaporkan menggunakan perisian sumber terbuka untuk pengurusan ICT organisasi mereka. Ini membuktikan bahawa perisian atau aplikasi yang dibangun oleh pihak ketiga telah mendominasi pembangunan perisian pada hari ini.

Adaptasi Penggunaan *Software as a Service* (SaaS) juga telah menunjukkan peningkatan sejak tahun 2000. Pada hari ini kita menggunakan SaaS dalam urusan pekerjaan seharian seperti Microsoft 365, Google Works Space, Zoom dan ChatGPT dengan berleluasa. Semua perisian SaaS ini disediakan oleh pihak ketiga yang bertanggungjawab terhadap infrastruktur seperti rangkaian dan platform yang digunakan dan pengguna diberikan akses tanpa perlu menyelenggara aset ICT. Dengan pendekatan ini peranan pihak bertiga semakin signifikan. Saiz pasaran SaaS dijangka terus meningkat sehingga USD720 billion menjelang 2028 (Rowell 2023). Pada tahun 2022, Vailshery (2024) menyatakan setiap organisasi secara purata menggunakan 130 aplikasi SaaS. Penggunaan SaaS juga telah lama dimulakan oleh Kerajaan Malaysia melalui perkhidmatan MyGovUC yang menawarkan perkhidmatan e-mel, penyimpanan data, perbualan maya dan telesidang yang pada umumnya diuruskan oleh pihak ketiga. Selain dari itu, banyak perkhidmatan ICT kerajaan diperolehi daripada penyedia perkhidmatan terurus seperti infrastruktur rangkaian dan keselamatan ICT (Bahagian Perundingan ICT MAMPU 2021; MOF 2022).

Kesimpulannya, peranan pihak ketiga tidak dinafikan adalah sangat penting malah tanpa disedari telah digunakan secara meluas oleh organisasi dalam pelbagai urusan yang merangkumi penyediaan infrastruktur fizikal (bangunan), rangkaian, sistem-sistem kritikal organisasi, platform perkhidmatan awan (SaaS, PaaS, IaaS) sehinggalah kepada aplikasi pengguna seperti aplikasi mobil, portal dan sebagainya. Peranan pihak ketiga ini turut disentuh dalam kerangka undang-undang, piawaian dan dokumen rasmi kerajaan. Perbincangan mengenai perkara ini akan diperincikan pada segmen 2.7.

2.4 RISIKO KESELAMATAN PIHAK KETIGA

Dengan agenda transformasi digital secara global dan nasional, kita dapat melihat perkembangan teknologi digital dan ICT yang dimungkinkan dengan perkembangan teknologi baharu seperti AI, IoT, data analitik, pengkomputeran awan, 5G dan penggunaan aplikasi mobil yang berleluasa (Hammi et al. 2023). Walau bagaimanapun, semua perkhidmatan ini tidak dapat ditawarkan tanpa pergantungan yang tinggi terhadap ekosistem rantai bekalan siber yang diuruskan oleh pihak ketiga. Ekosistem yang saling terhubung ini (*hyperconnected*) telah mendedahkan organisasi terhadap risiko keselamatan khususnya yang disebabkan oleh pihak ketiga. Ini kerana organisasi tidak mempunyai akses atau kawalan sepenuhnya ke atas infrastruktur pihak ketiga. Lebih membimbangkan ialah sebarang kegagalan atau insiden yang berlaku terhadap pihak ketiga ini akan memberi kesan langsung kepada organisasi yang menerima perkhidmatan sekiranya risiko ini tidak diuruskan dengan baik.

Risiko ditakrifkan sebagai kesan dari ketidakjelasan terhadap sesuatu objektif (ISO 2018). Risiko diukur berdasarkan kebarangkalian (*likelihood*) berlakunya sesuatu insiden yang disumbangkan oleh beberapa faktor termasuklah kerentanan atau kelemahan, ancaman dari dalam atau luar serta impak sesuatu insiden (ISO/IEC 2022). Dalam konteks keselamatan siber, impak diukur terhadap sejauh mana sesuatu insiden memberi kesan terhadap kriteria keselamatan seperti *Confidentiality*, *Integrity* dan *Availability* (CIA) sesebuah aset atau organisasi.

Pengurusan risiko atau *risk management* ialah domain yang telah matang dan mempunyai pelbagai piawaian yang telah dibangunkan sebagai rujukan. Secara umumnya, hampir semua piawaian dalam domain keselamatan siber menetapkan keperluan pengurusan risiko sebagai kawalan keselamatan yang perlu dipatuhi. Sebagai contoh ISO/IEC 27001 adalah kerangka pengurusan keselamatan siber yang berteraskan risiko (Keskin et al. 2021; Olubunmi et al. 2024), manakala piawaian ISO 31000 pula menyediakan prinsip dan garis panduan pengurusan risiko secara umum. Dalam domain keselamatan maklumat, ISO 27005 menjadi rujukan atau garis panduan bagi pengurusan risiko keselamatan maklumat (Gregory 2021; Sánchez-García et al. 2023). Selain dari itu, AICPA TSP 100 yang merupakan syarat bagi pensijilan SOCII turut mempunyai komponen berkenaan pengurusan risiko (Gregory 2021). Manakala,

agensi NIST (*National Institute of Standard and Technology*) turut menerbitkan garis panduan sendiri berkenaan pengurusan risiko melalui kerangka NIST RMF (*Risk Management Framework*) (Force 2017). Selain dari kerangka pengurusan risiko keselamatan maklumat, terdapat kerangka yang memfokuskan pengurusan risiko pihak ketiga atau rantaian bekalan (*supply chain*) secara khusus. Antaranya adalah TPRM (*Third-Party Risk Management*), C-TPRM (*Cyber Third-Party Risk Management*), SCRM (*Supply Chain Risk Management*), C-SCRM (*Cyber Supply Chain Risk Management*) dan VRM (*Vendor Risk Management*).

Third-Party Risk Management atau TPRM ditakrifkan sebagai proses mengenal pasti, menilai dan mengurus risiko yang berkaitan dengan penglibatan pihak luar seperti vendor, pembekal, penyedia perkhidmatan dan kontraktor (Galvanize 2021; Temitayo et al. 2024). Risiko ini termasuklah risiko terhadap data, operasi dan kewangan. Kajian terdahulu oleh Keskin et al. (2021), TPRM telah digunakan selama bertahun-tahun oleh organisasi, tetapi ia masih agak baru dalam domain siber. Beliau turut menggunakan istilah Pengurusan Risiko Pihak Ketiga Siber (C-TPRM) secara bergantian dengan Risiko Siber Vendor (*Vendor Cyber Risk*) dan rantaian bekalan siber (*Cyber Supply Chain*). Dengan C-TPRM yang berkesan, sesebuah organisasi boleh mengurangkan risiko disebabkan kebergantungan kepada pihak ketiga.

NIST telah menerbitkan kerangka pengurusan risiko rantaian bekalan siber yang dinamakan *Cybersecurity Supply Chain Risk Management* (C-SCRM) merangkumi aktiviti yang meliputi keseluruhan Kitaran Hayat Pembangunan Sistem (SDLC), termasuk penyelidikan dan pembangunan, reka bentuk, pembuatan, pemerolehan, penghantaran, integrasi, operasi dan penyelenggaraan, pelupusan, serta pengurusan menyeluruh produk dan perkhidmatan sesebuah organisasi (Boyens et al. 2020). NIST turut mencadangkan agar organisasi mengintegrasikan pengurusan risiko dalam kitaran SDLC.

Hubungan dengan pembekal dan vendor tidak hanya menyumbang kepada keberkesanan operasi dalam organisasi, tetapi juga meningkatkan potensi ancaman siber kepada organisasi tersebut. Seperti yang dinyatakan oleh Gregory (2021), risiko ini memerlukan pendekatan yang sistematik untuk memastikan keselamatan rantaian

bekalan secara keseluruhan. Singh (2021) pula menyatakan bahawa organisasi berusaha untuk menguruskan vendor dengan menggunakan proses VRM (*Vendor Risk Management*) yang umum yang merangkumi enam (6) langkah iaitu *1.INITITATE*, *2.COLLECT*, *3.QUALIFY*, *4.ACCEPT*, *5.SELECT* dan *6.MONITOR*. Walau bagaimanapun *Vendor Risk Management* (VRM) adalah berbeza dan perlu disesuaikan pada setiap organisasi. Singh (2021) juga menyatakan peranan VRM dalam landskap ancaman siber telah menjadi semakin penting dan menggusarkan pakar keselamatan siber. Walau bagaimanapun, kerangka VRM tidak banyak dibincangkan di kalangan penyelidik akademik. Beliau juga membandingkan beberapa kaedah atau pemarkahan (*scoring*) untuk tujuan penilaian vendor dalam konteks ancaman siber.

Berdasarkan sorotan kesusasteraan, boleh disimpulkan terdapat tiga konsep utama yang digunakan dalam pengurusan risiko berkaitan pihak ketiga dan rantaian bekalan iaitu *Vendor Risk Management* (VRM), *Third Party Risk Management* (TPRM) dan *Supply Chain Risk Management* (SCRM) (Paulsen 2022). VRM menilai pihak yang berurusan secara langsung dengan pembekal tanpa mengambil kira rantaian bekalan yang digunakan oleh vendor. Manakala, TPRM dan SCRM pula membincangkan skop yang lebih luas merangkumi rantaian bekalan yang melibatkan pihak keempat dan sebagainya. Walau bagaimanapun, TPRM dan SCRM memperkenalkan domain siber dalam kerangka masing-masing iaitu C-TPRM dan C-SCRM yang lebih relevan dengan skop kajian ini. Perbezaan ketiga-tiga konsep ini boleh diringkaskan Jadual 2.1.

Jadual 2.1 Perbezaan antara VRM,TPRM dan SCRM

	Vendor Risk Management (VRM) (Singh 2021)	Third-Party Risk Management (TPRM) (Dua et al. 2024)	Supply Chain Risk Management (SCRM) (Paulsen 2022)
Skop	Melibatkan pihak vendor atau pembekal secara langsung.	Semua vendor ialah pihak ketiga dan tidak semua pihak ketiga ialah vendor. Ini melibatkan hubungan yang merangkumi rantaian pembekal sama ada yang membayar atau tidak.	Vendor atau rantaian pihak ketiga yang terlibat dalam rantaian bekalan terhadap produk atau perkhidmatan yang dibangunkan dan biasanya melibatkan rantaian yang mempunyai hubungan secara komersial.

bersambung...

...sambungan

Matlamat	Menilai potensi impak vendor terhadap organisasi, keselamatan organisasi dan pelan kesinambungan perniagaan (BCP)	Mengenal pasti dan menangani risiko dengan entiti atau pihak luar yang berurusan dengan organisasi sama ada berbayar atau tidak dan matlamatnya adalah untuk mengurangkan risiko yang dibawa pihak ketiga terhadap organisasi.	Menilai dan menangani risiko yang boleh menjejaskan produk atau perkhidmatan organisasi dari sudut kualiti, integriti dan kebolehcapaian perkhidmatan
Contoh	ISP, Kontraktor, Pengeluar dan sebagainya	Kontraktor dan subkontraktor, rakan kongsi, penyedia perkhidmatan, anak syarikat, affiliate, juruaudit, pihak berkuasa (<i>regulator</i>), perisian sumber terbuka, data terbuka kerajaan, penyelidik dan sebagainya	Pembekal bahan mentah, logistik, pengilang, perkhidmatan, servis penyelenggaraan dan sebagainya.

Berdasarkan Jadual 2.1, kajian ini memilih untuk menggunakan istilah pihak ketiga iaitu C-TPRM yang lebih merangkumi hubungan organisasi sama ada komersial atau tidak. Ini kerana terdapat hubungan rantaian yang diambil dari sumber terbuka dan hubungan rakan kongsi yang bukan merupakan vendor secara langsung dan tidak mengkhususkan kepada produk (SCRM). Walau bagaimanapun dari sudut kerangka pengurusan risiko, ketiga-tiga ini tidak mempunyai perbezaan yang signifikan dari segi pengurusan risiko kerana hanya berbeza pada skop dan matlamat.

2.4.1 Kerentanan dan Kelemahan Pihak Ketiga

Seperti yang dibincangkan pada awal segmen 2.4, faktor utama yang menyumbang kepada risiko adalah kerentanan atau kelemahan sesuatu sistem serta ancaman atau potensi berlakunya insiden terhadap sasaran. Kerentanan boleh ditafsirkan sebagai kelemahan yang disebabkan oleh individu atau organisasi, proses atau teknologi termasuklah kelemahan perisian, ketiadaan kawalan keselamatan dan sebagainya (Sindhuja & Kunnathur 2015). Ancaman pula ialah potensi serangan oleh pihak luar atau pihak dalam yang mempunyai kepentingan sebagai contoh ialah serangan penafian perkhidmatan secara teragih (*Distributed Denial of Service* (DDoS)), serangan perisian tebusan, *cyberwarfare*, *hacktivism*, kecurian maklumat, perbuatan khianat dan sebagainya (Sindhuja & Kunnathur 2015). Kerentanan dan ancaman diukur

berdasarkan kebarangkalian ianya boleh dieksploitasi dan dari segi impak yang di bawa sebagaimana diterangkan sebelum ini. Sebagai contoh, sesebuah sistem yang tidak kritikal pada lazimnya mempunyai kurang ancaman yang perlu dibimbangkan berbanding sistem yang menguruskan aset maklumat yang kritikal. Sebuah sistem kritikal yang tidak dilengkapi dengan kawalan keselamatan boleh dianggap mempunyai risiko yang lebih tinggi berbanding sistem yang lengkap dengan kawalan keselamatan.

Rantainya bekalan IT yang kompleks membawa cabaran besar kepada keselamatan siber, terutamanya apabila pembangunan dan pengedaran perisian yang melibatkan pelbagai lapisan teknologi. Kelemahan perisian boleh wujud dalam pustaka perisian pihak ketiga atau komponen sumber terbuka yang tidak di selenggara. Tambahan pula, walaupun kelemahan ini melibatkan komponen yang kecil tetapi mampu memberi implikasi yang besar terhadap keseluruhan rantai bekalan perisian. Penceroboh yang berniat jahat kebiasaannya akan menyuntik perisian hasad melalui komponen yang lemah dan mudah di eksploitasi untuk mewujudkan pintu belakang dan mengakses infrastruktur secara konsisten (Olubunmi et al. 2024).

Kajian Li et al. (2023) pula mendapati bahawa sebanyak 81% daripada perisian yang diaudit mengandungi sekurang-kurangnya satu kerentanan keselamatan. Hal ini menunjukkan bahawa kerentanan pada perisian sumber terbuka atau perisian yang diguna semula bukan satu masalah yang terasing tetapi memberi impak yang serius kepada sesuatu sistem akibat saling kebergantungan dalam ekosistem perisian. Oleh itu, wujud keperluan mendesak untuk melaksanakan pemantauan dan pengurusan risiko yang komprehensif bagi menangani isu kerentanan dalam rantai bekalan perisian.

Wilusz dan Tasiemski (2023) juga mempunyai dapatan yang sama dan melaporkan bahawa kerentanan yang disebabkan oleh vendor ataupun pembangun perisian sumber terbuka telah wujud sejak proses pembangunan lagi sama ada disengajakan atau akibat kelalaian pembangun perisian. Ini termasuklah pepijat (*bug*) dalam kod sumber atau di dalam pustaka perisian atau kesilapan semasa konfigurasi dan semasa pengujian. Pengguna pula akan terdedah dengan kerentanan ini apabila mereka memuat turun untuk membangunkan perisian atau mengemas kini sistem mereka.

Terdapat pelbagai contoh insiden terkini yang berpunca daripada perisian pihak ketiga seperti insiden CrowdStrike yang telah mengakibatkan gangguan kepada infrastruktur kritikal di seluruh dunia (Navetta & Egan 2024). Insiden ini dilaporkan berpunca dari kelalaian di pihak pengeluar yang membekalkan perisian kemas kini yang tidak diuji dengan sempurna. Dalam insiden berkaitan SolarWinds pula penceroboh menyasarkan kelemahan proses pembangunan perisian dan berjaya menyuntik perisian hasad dan akhirnya menjadi sebahagian daripada pakej kemas kini rasmi yang disebarkan kepada seluruh pengguna (Kruti et al. 2023; Kshetri & Voas 2019). Dalam satu lagi insiden melibatkan pihak ketiga yang menyediakan platform ChatGPT, penggunaan pangkalan data dari sumber terbuka (Redis) yang mempunyai pepijat telah mengakibatkan pengguna ChatGPT dapat mengakses sejarah aktiviti atau *prompt* pengguna lain (Ravie 2023). Ini menyumbang kepada pelanggaran data privasi pelanggan dan menyebabkan implikasi yang serius kepada organisasi.

Kelemahan utama pihak ketiga juga wujud akibat daripada kelemahan proses dalaman seperti kurangnya pengamalan dan pematuhan terhadap piawaian atau pelaksanaan dasar keselamatan yang konsisten. Prosedur yang tidak jelas dan kegagalan untuk memantau pelaksanaan dasar keselamatan membuka ruang kepada ancaman keselamatan yang signifikan (Ghadge et al. 2020). Kekurangan pemantauan ini menyebabkan organisasi sukar mengenal pasti dan menangani risiko secara proaktif. Tambahan pula, ketiadaan polisi atau garis panduan dalam menguruskan risiko memburukkan keadaan kerana ia menyukarkan kerjasama antara pihak berkepentingan dalam memastikan keselamatan yang menyeluruh (Malatji et al. 2022). Wong et al. (2022) dalam kajiannya berpendapat bahawa penguatkuasaan terhadap pekerja untuk mengikuti prosedur dan mematuhi polisi melangkaui masalah teknikal dan teknologi sebaliknya bergantung pada motivasi pekerja atau faktor manusia.

Secara umumnya, kelemahan dari sudut kecuaihan manusia wujud dalam mana-mana organisasi termasuk pihak ketiga. Menurut kajian Sindhuja dan Kunnathur (2015), pekerja merupakan titik kelemahan terbesar kerana sikap cuai mereka terhadap keselamatan data. Sebagai contoh, pekerja sering mendedahkan maklumat sensitif secara tidak sengaja atau menulis kata laluan di tempat yang mudah dilihat, menjadikan maklumat tersebut terdedah kepada eksploitasi. Menurut ENISA manusia boleh

membuat kesilapan yang tidak disengajakan ketika melaksanakan kawalan asas dalam pengurusan sistem dan tabiat penggunaan e-mel mereka (Bronson 2022).

Selain itu, kelemahan pekerja di organisasi sama ada disengajakan atau tidak, turut menjadi cabaran besar kepada organisasi tersebut. Kelemahan ini sering berpunca daripada kurangnya kesedaran dan latihan dalam kalangan pekerja untuk memahami peranan mereka dalam menjaga keselamatan data organisasi (Ghadge et al. 2020). Selain daripada kecuaiian, kajian menunjukkan bahawa tindakan khianat seperti eksploitasi data sulit secara sengaja atau tindakan balas dendam terhadap organisasi boleh membawa kepada pelanggaran keselamatan yang serius (Sharma & Routroy 2016).

Di Malaysia, maklumat melibatkan amaran keselamatan berkenaan kerentanan dan ancaman yang berkaitan dengan organisasi di Malaysia boleh dirujuk kepada *National Cyber Coordination and Command Centre* (NC4) yang dikelolakan oleh NACSA. Antara amaran kerentanan yang dikeluarkan pada tahun 2024 ialah isu keselamatan yang melibatkan pembekalan peralatan atau perisian ICT seperti Fortinet, CrowdStrike, Cisco Firewall, SolarWinds, Search Engine, Microsoft, Apache, Log4j, Whatsapp dan sebagainya. Selain itu, NC4 juga mengeluarkan amaran semasa berkaitan risikan ancaman (*threat intelligence*), aktiviti atau kempen serangan yang menyasarkan kepentingan kerajaan atau organisasi.

Kesimpulannya, kerentanan atau kelemahan yang berpunca daripada pihak ketiga disebabkan oleh tiga aspek iaitu 1) kelemahan dari sudut pengurusan sumber manusia akibat ketidakpatuhan dan kecuaiian, 2) kelemahan proses penguatkuasaan dan tadbir urus keselamatan yang baik dan 3) kelemahan teknologi yang disebabkan kelemahan perisian atau ketiadaan infrastruktur keselamatan yang sesuai.

2.4.2 Ancaman Keselamatan dari Pihak Ketiga

Selain daripada kerentanan atau kelemahan, faktor kebarangkalian berlakunya ancaman terhadap organisasi turut diambil kira untuk mengenal pasti risiko (ISO/IEC 2022). Dengan perkembangan teknologi yang baru ancaman dan serangan juga semakin maju dan berubah mengikut masa. Dengan penggunaan perisian secara meluas dalam urusan

harian, penggunaan SaaS dan aplikasi mobil serta kemajuan internet jalur lebar yang lebih murah banyak urusan penting dan kritikal dapat dijalankan secara atas talian. Ini bermakna lebih banyak transaksi boleh dilakukan dan data boleh diakses dengan lebih mudah pada setiap masa dan tempat dengan menggunakan pelbagai peranti. Semua infrastruktur ini tidak mungkin dapat disediakan secara sendiri, sebaliknya memerlukan ekosistem yang disediakan oleh pihak ketiga. Kebergantungan organisasi terhadap pihak ketiga telah menambahkan lagi risiko terhadap organisasi tersebut kerana perlu memberi kepercayaan penuh kepada pihak ketiga untuk menguruskan keselamatan data dan infrastruktur yang diamanahkan.

Terdapat banyak laporan industri yang menerbitkan landskap ancaman keselamatan siber yang menunjukkan peningkatan ancaman yang melibatkan rantaian bekalan siber dari tahun ke tahun. Ini berdasarkan laporan ENISA (*European Union Agency For Cybersecurity*) bertajuk *Landscape for Supply Chain Attacks* (ENISA 2021) yang mengkaji insiden berkaitan pihak ketiga dari tahun 2020 hingga 2021. Dalam satu laporan lain yang diterbitkan bertajuk “*Foresight Cybersecurity Threats for 2030*”, ENISA telah menyenaraikan serangan kepada rantaian bekalan atau pihak ketiga sebagai ancaman yang paling tinggi berdasarkan kebarangkalian insiden dan skala impak yang mengatasi faktor-faktor ancaman lain seperti masalah kemahiran, masalah kesilapan manusia, eksploitasi sistem legasi, serta penyalahgunaan AI, ancaman fizikal ke atas infrastruktur dan lain-lain. Kaji selidik ini dilakukan ke atas 24 pakar keselamatan (ENISA 2024). Menurut ENISA walaupun isu keselamatan rantaian bekalan ini telah lama dipantau tetapi berlaku peningkatan yang mendadak dengan peningkatan kes yang melibatkan serangan secara tersusun sejak tahun 2020 dan mengakibatkan implikasi yang sangat serius dari sudut kebolehcapaian perkhidmatan, kerugian kewangan dan menjatuhkan reputasi organisasi. Oleh yang demikian, ancaman serangan berkaitan pihak ketiga ini penting untuk dikaji kerana serangan terhadap satu komponen rantaian boleh merebak ke seluruh ekosistem rantaian bekalan. Antara rumusan daripada laporan ini adalah :

1. Sebanyak 50% adalah serangan terancang dari kumpulan yang dikenali, manakala 42% masih tidak dapat dikenal pasti.

2. Sehingga 62% serangan menyasarkan organisasi pelanggan dengan mengambil peluang daripada kepercayaan kepada pihak ketiga.
3. Sehingga 62% insiden dilakukan melalui serangan perisian hasad (*malware*).
4. Sebanyak 58% serangan menyasarkan data manakala 16% menyasarkan sumber manusia.

Laporan ini telah menyertakan secara terperinci taksonomi serangan terhadap rantaian bekalan yang mengandungi teknik, taktik, sasaran serta membincangkan sebanyak 24 senarai insiden berkaitan pihak ketiga termasuk lima (5) serangan berprofil tinggi seperti 1. SolarWinds Orion: Perisian Pengurusan IT dan Pemantauan Jarak Jauh, 2. *Mimecast*: Perkhidmatan Keselamatan Awan, 3. Hardware Wallet, 4. Kaseya: Perkhidmatan Pengurusan IT di kompromi oleh perisian tebusan dan 5. SITA: Sistem Perkhidmatan Penerbangan. Dalam taksonomi yang diterbitkan, senarai teknik dan taktik serta aset milik pihak ketiga yang menjadi sasaran seperti dalam Jadual 2.2.

Jadual 2.2 Teknik dan taktik yang digunakan berserta aset pihak ketiga yang disasarkan

Teknik yang digunakan	Aset pihak ketiga yang disasarkan
<ul style="list-style-type: none"> • Jangkitan perisian hasad • <i>Social Engineering</i> • Serangan <i>Brute Force</i> • Mengeksploitasi kelemahan perisian • Mengeksploitasi kelemahan konfigurasi • <i>Open-Source Intelligence</i> (OSINT) 	<ul style="list-style-type: none"> • Perisian sedia ada • Kod <i>library</i> • Konfigurasi • Data • Proses • Perkakasan • Sumber Manusia Pihak Ketiga

Sumber: *Foresight Cybersecurity Threats For 2030- Update*

Kajian akademik mengenai pihak ketiga juga dilakukan oleh Benaroch (2021) yang membuat kajian terhadap 1397 insiden siber di firma awam dari tahun 2000 hingga 2020, di mana sebanyak 246 adalah melibatkan pihak ketiga. Beberapa dapatan menarik daripada kajian ini termasuklah:

1. Dari segi bilangan insiden, peningkatan kes berkaitan pihak ketiga tidak mendadak seperti insiden lain, walau bagaimanapun, impak dan skala serangan meningkat dengan mendadak dari satu insiden ke insiden lain. Ini termasuklah peningkatan bilangan data rahsia yang terlibat dalam insiden.
2. Pihak yang paling terkesan ialah pihak pengguna dan pihak ketiga yang bersaiz kecil, manakala organisasi pihak ketiga yang besar tidak begitu terkesan dengan insiden berkaitan rantai bekalan.

Dalam kajian lain, Khokhar et al. (2024) telah mengkategorikan ancaman pihak ketiga kepada ancaman fizikal dan ancaman siber. Ancaman secara fizikal boleh berlaku contohnya dengan pemalsuan kad akses secara fizikal, kecurian perkakasan dan penyebaran aset secara haram serta pengubahsuaian peralatan. Manakala ancaman siber menyasarkan data, perisian, perkakasan dan rangkaian.

Menurut Keskin et al. (2021), terdapat 98% kebarangkalian organisasi pengeluar akan mengalami gangguan terhadap rantai bekalan dalam masa 24 bulan. Dalam laporan yang lain oleh Colicchia et al. (2019), penyedia perkhidmatan menyumbang kepada 23% daripada jumlah insiden berkaitan kebocoran data siber. Manakala rakan kongsi bertanggungjawab menyebabkan 45% daripada jumlah insiden keseluruhannya. Menurut kajian institut The Phenomen pula, 56% organisasi berpengalaman mengalami kebocoran data dengan 75% daripada insiden tersebut adalah disebabkan oleh pihak ketiga (Garcia-Granados & Bahsi 2020).

Serangan terhadap pihak ketiga atau aset pihak ketiga adalah sasaran yang strategik bagi perisian tebusan kerana peranan kritikalnya dan potensinya untuk menyebarkan perisian hasad ke rangkaian pengguna yang lebih luas. Lazimnya, serangan strategik ini dikendalikan oleh pelaku yang ditaja oleh sesebuah negara (*state sponsored*) yang bertujuan melakukan aktiviti risikan untuk mencuri harta intelek, mengganggu operasi dan menceroboh rantai pembekalan bagi kegunaan strategik (Melnyk et al. 2022). Pelaku jenis ini mempunyai keupayaan yang canggih yang boleh bertahan dalam masa yang lama untuk mencapai objektif serangan (Olubunmi et al. 2024).

Perisian tebusan juga merupakan salah satu ancaman keselamatan siber yang semakin meningkat di Malaysia yang kebanyakannya dilakukan dengan cara mengeksploitasi kelemahan sistem pihak ketiga. Menurut pemerhatian oleh Pusat Penyelarasan dan Kawalan Siber Negara (NC4), kumpulan perisian tebusan sering mengeksploitasi beberapa kelemahan tertentu dan menunjukkan pengkhususan dalam pemilihan sasaran. Contohnya, kumpulan Magniber secara khusus menyasarkan kelemahan dalam produk Microsoft, manakala kumpulan CLOP cenderung menyerang kelemahan dalam platform pemindahan fail seperti Accellion dan SolarWinds (NACSA 2024a). Kecenderungan kumpulan ini untuk mengeksploitasi kelemahan pihak ketiga ini menimbulkan risiko yang sangat serius kepada organisasi yang bergantung kepada perkhidmatan atau teknologi luar. Ini menunjukkan betapa pentingnya pengurusan keselamatan siber yang ketat bukan sahaja di peringkat dalaman tetapi juga dalam memilih dan memantau keselamatan pihak ketiga yang mempunyai akses kepada infrastruktur kritikal organisasi.

Sejumlah 45 insiden serangan perisian tebusan yang menyerang pelbagai sektor dan industri telah menjejaskan beberapa organisasi dilaporkan pada tahun 2018 (Nur Sarida & Ahmad Rizal 2022). Ini berpunca daripada pengamalan dasar keselamatan yang lemah malah ada yang tidak mempunyai dasar dan polisi keselamatan siber di agensi mereka. Kakitangan dan individu pengguna juga kebanyakannya tidak mengamalkan etika penggunaan siber yang selamat menyebabkan terdedah menjadi mangsa ancaman keselamatan siber (Wong et al. 2022).

2.4.3 Impak dan Kesan Ancaman daripada Pihak Ketiga

Serangan terhadap rantai bekalan atau pihak ketiga mampu memberi impak kepada skala yang besar dan dahsyat (Cletus et al. 2022; Fadi & Hatem 2021). Ini terbukti dengan beberapa insiden seperti SolarWinds Hack dan CrowdStrike. Dalam insiden SolarWinds Hack sebanyak 18,000 organisasi di seluruh dunia telah terkesan dan kebanyakannya adalah organisasi yang strategik seperti FBI, Pentagon, Microsoft, FireEye, Cisco dan agensi kerajaan seperti jabatan perbendaharaan negara dan beberapa kementerian strategik (Kruti et al. 2023). SolarWinds Orion merupakan perisian pemantauan pengurusan rangkaian yang terkenal dan menjadikan ia sasaran yang strategik kerana rangkaian penggunaannya yang sangat besar di seluruh dunia. Perisian

ini telah di kompromi di peringkat pembangunan di mana perisian hasad disuntik ke dalam pakej kemas kini perisian yang rasmi yang akan disebarikan kepada pengguna. Impak daripada insiden ini, sangatlah besar dan tidak terbatas kerana penceroboh berjaya meletakkan perisian hasad atau pintu belakang (*backdoor*) yang boleh diakses untuk menjalankan pelbagai serangan lanjutan sama ada bertujuan untuk mencuri data sensitif atau melakukan sabotaj atau serangan lain yang sebahagian besarnya tidak dilaporkan. Dalam kajian Benaroch (2021), sehingga 60% insiden yang melibatkan pihak ketiga tidak dilaporkan oleh organisasi.

Pada tahun 2024, berlaku satu insiden besar dan berskala global yang disebabkan oleh pihak ketiga iaitu CrowdStrike, sebuah syarikat penyedia perisian keselamatan telah menyebarkan perisian kemas kini yang tidak diuji dengan sempurna yang mengakibatkan sistem *crash* (*blue screen*) pada pelayan atau perisian agen CrowdStrike di seluruh dunia. Sekurang-kurangnya 1/3 daripada infrastruktur kritikal di seluruh dunia yang menggunakan perisian ini telah mengalami gangguan sistem dan menyebabkan kegagalan perkhidmatan di lapangan terbang, hospital, pasaran saham dan infrastruktur kerajaan yang boleh mengancam keselamatan atau melibatkan kerugian berbilion ringgit (Basheer et al. 2024). Insiden ini turut memberi kesan kepada organisasi kritikal di Malaysia (NACSA 2024b).

Selain daripada implikasi kewangan dan keselamatan awam serta reputasi organisasi, insiden keselamatan yang melibatkan pihak ketiga juga boleh menyebabkan pelanggaran terhadap hak privasi. Ini berlaku pada insiden ChatGPT, satu platform *Generative AI* yang pada awalnya dibangunkan menggunakan perisian pangkalan data sumber terbuka iaitu Redis yang mempunyai kelemahan (*bug*) dan mengakibatkan pendedahan rekod dan aktiviti pengguna ChatGPT lain. Mengikut laporan awal, data-data yang telah di muat naik ke platform ChatGPT termasuklah data sensitif, data peribadi, data perubatan, kod sumber, harta intelek, data pengguna dan lain-lain (Ravie 2023). Ketiga-tiga insiden berskala global ini membuktikan bahawa serangan melibatkan pihak ketiga atau rantaian bekalan ini boleh berlaku dengan sangat pantas dan memberi implikasi yang sangat besar.

Benaroch (2021) telah membuat satu kajian empirikal untuk mengkaji kesan atau impak serangan rantaian bekalan ini dan melaporkan bahawa kelemahan pihak ketiga merupakan punca kedua terbesar yang menyebabkan kerugian purata sebanyak USD4.5juta untuk setiap insiden. Sebagai contoh syarikat penyedia platform jualan (Salesforce) telah menghadapi gangguan yang sangat lama disebabkan kesilapan pekerjaanya yang memberikan pengguna akses kepada semua data secara tidak sengaja (Mei 2019). Insiden kebocoran data di CapitalOne pula didapati berpunca daripada bekas pekerja pengkomputeran awan Amazon yang menggodam lebih 100 juta akaun pelanggan (Julai 2019). Selain daripada itu, gangguan perkhidmatan Google Cloud (Jun 2019) telah menyebabkan gangguan terhadap YouTube, Gmail dan Snapchat di seluruh dunia. Antara insiden berprofil tinggi yang dilaporkan turut melibatkan pemberian akses secara tidak sengaja yang melibatkan organisasi seperti Target Cooperation (melibatkan kebocoran 45 juta maklumat kad kredit dan kad debit), Home Depot (melibatkan 56 juta akaun pembayaran), Equifax (kebocoran data peribadi 140 juta pelanggan), beberapa rangkaian hotel yang ternama, Barclays, AT&T dan Goodwill. turut membuat perbandingan untuk mengaitkan reaksi pasaran saham terhadap organisasi pihak ketiga dan mendapati organisasi pengguna dan pihak ketiga yang berskala kecil mendapat impak yang lebih besar berbanding firma pihak ketiga yang mempunyai modal yang besar (Benaroch 2021). Antara kesan buruk yang dihadapi organisasi adalah kerugian kewangan yang disebabkan peningkatan kos operasi, kegagalan perkhidmatan, kerosakan dari sudut reputasi dan kehilangan kepercayaan pelanggan (Basheer et al. 2024). Kos yang ditanggung juga adalah melibatkan kos pemulihan dan kos khidmat pelanggan serta potensi kerugian akibat tuntutan perundangan.

Pelbagai penyelidik telah meneliti impak risiko keselamatan siber yang berpunca daripada pihak ketiga ke atas organisasi. Kajian menunjukkan bahawa insiden keselamatan yang melibatkan pihak ketiga boleh menyebabkan kerugian kewangan yang ketara, terutama apabila organisasi terpaksa menanggung kos pemulihan serta denda daripada pihak pengguna. Kehilangan data sensitif akibat kebocoran daripada pihak ketiga bukan sahaja menjejaskan operasi organisasi tetapi juga mengancam reputasi dan mengurangkan kepercayaan pelanggan dan rakan kongsi. Selain itu, serangan melalui pihak ketiga berpotensi mengganggu operasi perniagaan yang

menyebabkan kehilangan produktiviti dan memerlukan tempoh pemulihan yang panjang (Alharbi et al. 2021).

Kesimpulannya, walaupun insiden pihak ketiga secara statistiknya tidak menunjukkan peningkatan yang signifikan berbanding serangan yang lain, tetapi ia melibatkan peningkatan yang sangat signifikan dari sudut impak dan boleh tersebar dengan cepat dan sistematik pada skala yang besar. Lebih malang lagi, penggadam hanya perlu mengenal pasti dan mengeksploitasi satu titik lemah sahaja dalam rantaian bekalan atau pihak ketiga yang mempunyai hubungan dengan organisasi. Manakala sesebuah organisasi pula perlu mengenal pasti semua titik lemah dalam organisasi yang berpunca daripada pihak ketiga.

2.5 PENGURUSAN RISIKO PIHAK KETIGA

Pengurusan risiko pihak ketiga adalah aspek kritikal dalam melindungi keselamatan organisasi, terutama dalam era digital yang semakin kompleks. Kebergantungan yang tinggi kepada pihak ketiga seperti vendor, pembekal, dan kontraktor mendedahkan organisasi kepada pelbagai ancaman keselamatan yang berpunca daripada kelemahan pada pihak tersebut. Justeru, pengurusan risiko pihak ketiga menjadi keutamaan untuk memastikan keselamatan data, reputasi, dan keberkesanan operasi organisasi. Segmen ini akan membincangkan komponen pengurusan risiko pihak ketiga yang merangkumi kerangka pengurusan risiko, cara-cara mengenal pasti risiko dengan membuat penilaian wajar, praktis terbaik dan strategi mitigasi untuk dijadikan panduan oleh organisasi untuk menguruskan risiko ini.

2.5.1 Kerangka Pengurusan Risiko Pihak Ketiga

Kerangka pengurusan risiko adalah proses atau kitaran aktiviti untuk menguruskan risiko pihak ketiga (Olubunmi et al. 2024). Terdapat beberapa pendekatan yang boleh diambil atau diadaptasi oleh organisasi seperti yang disenaraikan Jadual 2.3.

Jadual 2.3 Kerangka Pengurusan Risiko Pihak Ketiga

ISO 31000 Pengurusan Risiko	TPRM	C-SCRM NIST
1. Penetapan Skop, Konteks dan Kriteria	1. Penetapan hubungan dengan pihak ketiga	1. Frame – menetapkan kerangka berkenaan hubungan dengan pihak ketiga
2. Penilaian Risiko (Kenal pasti, analisis dan menilai)	2. Penilaian risiko berkaitan pihak ketiga	2. Penilaian risiko
3. Perawatan Risiko	3. Pelaksanaan strategi mitigasi	3. Memberi Tindak balas
4. Pemantauan dan semakan semula		4. Pemantauan
5. Komunikasi dan konsultasi		
6. Rekod dan pelaporan		

Berdasarkan Jadual 2.3, secara umumnya setiap kerangka mempunyai proses yang hampir sama yang bermula dengan meletakkan konteks yang betul dan sesuai dengan keperluan organisasi. Sebagai contoh, organisasi boleh melakukan kajian impak perniagaan (*Business Impact Analysis (BIA)*) untuk menyesuaikan keperluan organisasi dan mengenal pasti *business dependency* serta meletakkan matlamat atau objektif-objektif penting yang hendak dicapai dalam program pengurusan risiko. Seterusnya proses penilaian risiko dilakukan dengan mengambil kira kebarangkalian dan impak setiap risiko terhadap aspek kerahsiaan, integriti dan kebolehcapaian serta privasi. Dalam proses ini setiap risiko yang dikenal pasti dan dikategorikan mengikut keutamaan dan cadangan dibuat sama ada untuk menerima risiko (tanpa mitigasi), memindahkan risiko, mengelakkan risiko atau merawat risiko. Risiko yang perlu dirawat memerlukan dengan pelan rawatan risiko (*risk treatment plan*) yang bersesuaian (ISO 2018).

Seterusnya pelan rawatan risiko yang telah dikenal pasti akan dilaksanakan mengikut perancangan contohnya dengan memperkenalkan kawalan keselamatan yang baru melalui pemasangan teknologi, penambahbaikan proses kerja atau latihan kemahiran. Akhir sekali, proses pemantauan yang berterusan perlu dilaksanakan dan sentiasa dikemas kini sekiranya berlaku perubahan proses dan mengemas kini strategi sekiranya perlu.

2.5.2 *Due Care dan Due Diligence*

Antara konsep yang penting dan sering digunakan dalam keselamatan siber dan risiko pihak ketiga adalah *due care* dan *due diligence*. *Due care* merujuk kepada usaha wajar

atau tindakan yang diambil untuk melindungi kepentingan organisasi. Sebagai contoh organisasi perlu merangka polisi, piawai dan garis panduan atau prosedur yang bersesuaian untuk memastikan keselamatan organisasi. *Due diligence* atau penilaian wajar pula adalah penyiasatan yang perlu dilakukan sebelum mengambil apa-apa tindakan. Penilaian wajar ini perlu dilakukan sebagai satu bentuk penilaian risiko dalam setiap fasa pelaksanaan projek (Gregory 2021; Temitayo et al. 2024).

Penilaian risiko boleh dimulakan dengan melakukan penilaian wajar pada peringkat sebelum projek bermula atau *onboarding*. Di peringkat ini, organisasi perlu melakukan pemeriksaan latar belakang pihak ketiga, termasuk sejarah keselamatan dan kompetensi syarikat terbabit. Organisasi perlu memastikan semua spesifikasi keselamatan dimasukkan semasa pemerolehan dan sekiranya perlu ujian pembuktian konsep boleh dilaksanakan. Dalam konteks pembangunan aplikasi, organisasi boleh memastikan pihak ketiga menyediakan *Software Bill of Material* (SBOM) yang menyenaraikan semua komponen pustaka perisian dan dikemas kini agar ia berada pada postur yang paling baik. Organisasi juga boleh memastikan pihak ketiga mengadaptasi amalan pembangunan yang selamat (SDLC) dengan menjalankan semakan kod perisian serta melakukan ujian kerentanan dan ujian penembusan sistem (Olubunmi et al. 2024).

Seterusnya penilaian wajar perlu terus dijalankan semasa projek (*ongoing due diligence*) berjalan dengan memastikan pihak ketiga menyediakan rekod untuk diaudit (Temitayo et al. 2024) dan menyediakan laporan secara berkala serta memastikan pihak ketiga mengemas kini pensijilan keselamatan mereka. Penilaian wajar di lapangan atau *onsite due diligence* boleh dilakukan dengan membuat lawatan ke premis pihak ketiga seperti pusat data, pejabat atau kilang bagi melihat sendiri keupayaan dan persekitaran yang sebenar untuk membuat kesahan terhadap maklumat yang diperolehi dari pihak ketiga. Organisasi juga boleh memastikan pihak ketiga mampu menyediakan maklumat yang diperlukan seperti rakaman CCTV sekiranya diperlukan bagi tujuan forensik. Penilaian wajar juga perlu dilakukan selepas projek tamat (*offboarding due diligence*) di mana organisasi perlu membatalkan semua akses kepada pihak ketiga dan memastikan data disanitasi atau dipindahkan dengan sempurna serta didokumentasikan dengan baik. Kesemua keperluan penilaian wajar ini mestilah difahami oleh pihak

ketiga dan dimasukkan dalam spesifikasi projek serta dokumen perjanjian (Gregory 2021).

2.5.3 Strategi Mitigasi

Penilaian risiko yang wajar merupakan langkah asas dalam mengenal pasti risiko-risiko yang wujud serta jurang yang ada dalam sistem keselamatan siber organisasi. Berdasarkan penilaian ini, beberapa strategi mitigasi boleh dilaksanakan untuk menguruskan risiko pihak ketiga dengan lebih berkesan. Dalam buku yang ditulis oleh Gregory (2021) salah satu strategi utama adalah dengan mewujudkan strategi mitigasi yang komprehensif merangkumi fasa sebelum, semasa, dan selepas berlakunya insiden. Pendekatan ini memastikan organisasi mengambil langkah proaktif dalam membuat persediaan untuk menangani pelbagai kemungkinan ancaman.

Sebelum berlaku insiden, organisasi perlu mewujudkan daftar risiko yang mengandungi pelan pengurusan risiko dan pelan pengurusan insiden yang sesuai untuk setiap jenis ancaman. Daftar ini menjadi panduan penting untuk organisasi dalam mengenal pasti risiko-risiko yang spesifik serta langkah-langkah mitigasi yang perlu dilaksanakan. Antara strategi mitigasi yang boleh dilaksanakan sebelum berlaku insiden adalah dengan meningkatkan kapasiti dan keupayaan pasukan keselamatan siber, memperbaiki infrastruktur teknologi keselamatan atau mendapatkan perlindungan insurans sekiranya perlu untuk mengurangkan kesan risiko kepada operasi perniagaan.

Semasa insiden, organisasi perlu mengaktifkan pelan pengurusan insiden yang telah disediakan. Pelan ini mesti merangkumi prosedur yang jelas dan langkah-langkah tindak balas yang boleh dilaksanakan dengan segera dan mengikut jangka masa yang telah ditetapkan. Pendekatan ini memastikan tindakan yang diambil adalah teratur, pantas dan berkesan untuk mengurangkan impak insiden terhadap organisasi. Selain itu, koordinasi yang baik antara pasukan dalaman dan pihak ketiga yang terlibat amat penting untuk memastikan tindak balas yang cekap.

Strategi mitigasi yang diambil selepas berlaku insiden pula menumpukan kepada pelaporan insiden secara terperinci dan proses penambahbaikan sekiranya perlu.

Pelaporan ini bukan sahaja membantu mengenal pasti kelemahan dalam pelan pengurusan risiko pihak ketiga tetapi juga menyediakan asas untuk memperbaiki pelan sedia ada berdasarkan pengajaran yang diperoleh daripada insiden. Dengan ini, pelan pengurusan risiko organisasi kekal relevan dan bersedia untuk menangani cabaran baharu yang mungkin timbul sama ada pada organisasi atau pihak ketiga. Proses ini turut melibatkan penilaian semula keperluan teknologi dan koordinasi organisasi dengan pihak ketiga serta peningkatan keupayaan pasukan untuk mengukuhkan daya tahan keselamatan siber kedua-dua pihak.

Strategi mitigasi ini perlu dilaksanakan bersama proses pemantauan yang berterusan dan audit secara berkala bagi meningkatkan keberkesanan strategi yang diambil dan memastikan pihak ketiga mematuhi strategi dan polisi yang ditetapkan. Dengan pendekatan yang sistematik ini, organisasi dapat memastikan keselamatan dan kestabilan operasi mereka terjamin dengan kerjasama daripada pihak ketiga. Rajah 2.1 merupakan ringkasan daripada strategi mitigasi yang dibincangkan.



Rajah 2.1 Dasar Pengurusan Risiko Pihak Ketiga

2.5.4 Praktis Terbaik

ENISA (2024), Gregory (2021) dan Lauren (2024) mencadangkan beberapa amalan terbaik bagi menguruskan risiko pihak ketiga. Pertama, organisasi perlu mengemas kini proses serta dokumen dengan pihak ketiga untuk memastikan dokumen relevan dengan perkembangan teknologi dan ancaman siber terkini. Kedua, organisasi

dinasihatkan untuk mewujudkan hubungan dan komunikasi yang berterusan dengan pihak ketiga untuk menyalurkan maklumat secara berkesan (Temitayo et al. 2024). Ketiga, organisasi perlu peka perkembangan teknologi, ancaman siber, undang-undang dan piawaian terkini. Keempat, Organisasi disarankan untuk melaksanakan proses penilaian wajar atau *due diligence* di setiap fasa projek, iaitu sebelum, semasa dan selepas penamatan kontrak. Kelima, organisasi perlu memastikan pihak ketiga dan kakitangan organisasi mendapatkan latihan dan kesedaran berkenaan risiko keselamatan siber. Keenam organisasi hendaklah memantau prestasi pihak ketiga dan membuat penilaian berterusan untuk memastikan pematuhan pihak ketiga terhadap polisi keselamatan. Sebagai contoh memastikan pihak ketiga mempunyai pensijilan seperti ISO 27001 atau SOC II serta melaksanakan audit dan mesyuarat secara berkala.

Kesimpulannya, pihak organisasi perlu mewujudkan program pengurusan risiko pihak ketiga dengan strategi yang merangkumi proses pengurusan risiko serta mewujudkan amalan terbaik seperti yang dibincangkan.

2.6 KEPERLUAN LATIHAN DAN KESEDARAN KESELAMATAN SIBER

Walaupun kemajuan teknologi seperti kecerdasan buatan (AI) dan pembelajaran mesin (ML) telah meningkatkan keupayaan organisasi untuk menangani ancaman siber, faktor manusia kekal sebagai kelemahan utama (Saif et al. 2024). Secara umumnya, latihan keselamatan siber dapat meningkatkan kesedaran pekerja, memperbaiki pematuhan polisi keselamatan dan membentuk budaya keselamatan yang kukuh. Ia diperlukan kerana gabungan elemen *People, Process, dan Technology* (PPT) dalam organisasi sering menunjukkan ketidakseimbangan dan perlu dibangunkan seiring dengan perkembangan teknologi dan proses. Menurut Sabillon et al. (2019) terdapat keperluan mendesak untuk memberi tumpuan kepada elemen-elemen lain seperti latihan kakitangan, penetapan proses dan kawalan yang efektif, serta pematuhan kepada peraturan yang berkaitan untuk mengukuhkan perlindungan siber organisasi.

Saif et al. (2024) mencadangkan bahawa faktor manusia harus diberi penekanan dalam mengekalkan keselamatan organisasi. Kajian empirikal beliau mencadangkan bahawa peningkatan kesedaran keselamatan siber dalam kalangan pekerja ialah kunci untuk memperbaiki sikap dan amalan pengurusan keselamatan serta pematuhan kepada

polisi organisasi. Pendapat ini disokong oleh Olubunmi et al. (2024) yang melaporkan kesilapan manusia sebagai kelemahan yang paling signifikan dalam keselamatan siber dan mencadangkan latihan kesedaran untuk mengurangkan risiko ini. Organisasi perlu memperkasakan pekerja supaya mampu mengenal pasti dan menangani ancaman keselamatan siber kerana mereka dianggap barisan pertahanan yang paling kritikal dalam mana-mana organisasi (Marble et al., 2015; Nobles, 2018). Kajian Moen et al. (2024) pula menunjukkan bahawa kegagalan organisasi menjalankan latihan keselamatan secara berkala menyumbang kepada tahap kesedaran keselamatan yang rendah. Kajian ini mendapati bahawa pekerja yang tidak menerima latihan keselamatan siber cenderung menghadapi kesukaran mengenal pasti dan menangani ancaman siber. Garcia-Granados dan Bahsi (2020) mengatakan kegagalan organisasi untuk mewujudkan pekerja yang berpengetahuan dalam bidang keselamatan adalah disebabkan oleh kurangnya latihan kepada pekerja dan kurang pemindahan latihan teknologi daripada vendor.

Kshetri (2022) menekankan keperluan diadakan latihan kesedaran keselamatan siber disebabkan beberapa faktor termasuklah peningkatan aktiviti atas talian, peningkatan ancaman sosial media, penggunaan data internet dan *instant message*, kekurangan peralatan perlindungan keselamatan dan kekurangan program latihan keselamatan. Selain dari itu, terdapat peningkatan ancaman pancingan (*phishing*) dan pemalsuan iklan yang mendedahkan organisasi kepada serangan siber. Beliau juga berpendapat latihan ini juga penting untuk melindungi data organisasi dan menanamkan sikap serta kesedaran terhadap keselamatan persekitaran organisasi.

Walaupun latihan keselamatan ini penting, terdapat beberapa cabaran yang perlu diatasi oleh organisasi. Dalam sebuah kajian soal selidik, Wong et al. (2022) mendapati lebih daripada 60% responden menyatakan bahawa mereka tidak menganggap keselamatan siber sebagai keutamaan dalam kerja harian mereka. Hal ini menunjukkan bahawa walaupun polisi dan panduan keselamatan siber wujud, tetapi tahap pematuhan dan kesedaran pekerja masih rendah. Kajian ini juga menekankan bahawa polisi sahaja tidak mencukupi tetapi latihan perlulah dilaksanakan secara berterusan dan disesuaikan dengan suasana kerja yang sebenar. Sabillon et al. (2019) juga memberi pendapat yang sama di mana walaupun latihan secara konsisten mampu

memperkuat pemahaman keselamatan di kalangan pekerja, namun pengaruhnya terhadap perubahan tingkah laku pekerja adalah minimum sekiranya latihan tersebut tidak disesuaikan dan diperbaharui mengikut konteks kerja sebenar. Oleh itu, adalah kritikal bagi organisasi untuk tidak hanya menyediakan latihan awal tetapi juga mengamalkan pendekatan latihan yang berterusan dan kontekstual bagi memastikan pekerja dapat mengaplikasikan prinsip keselamatan dalam operasi harian. Moen et al. (2024) mencadangkan pengenalan program latihan keselamatan siber yang lebih tersusun dan kerap dalam organisasi supaya dapat meningkatkan tahap kesedaran dan mengurangkan risiko ancaman siber.

Bada dan Nurse (2019) pula berpendapat kesedaran memerlukan sikap proaktif oleh pekerja. Realitinya kebanyakan pekerja akan lebih mengutamakan prestasi kerja mereka berbanding keselamatan. Fallatah et al. (2024) pula menyentuh berkenaan kurangnya bahan latihan yang komprehensif berkenaan keselamatan siber. Menurut Saif et al. (2024), kebergantungan terhadap sumber berbahasa Inggeris dalam latihan keselamatan siber telah mengehadkan keberkesanan latihan keselamatan siber di peringkat global, terutamanya bagi pengguna dari latar belakang budaya dan bahasa yang berbeza. Beliau juga mencadangkan agar pendekatan latihan keselamatan siber secara inklusif dan merangkumi aspek kepelbagaian bahasa dan konteks budaya untuk meningkatkan keberkesanan modul latihan.

Menurut Wong et al. (2022), dengan menyediakan modul latihan keselamatan siber yang kontekstual dan berterusan, organisasi dapat meningkatkan sikap pekerja terhadap keselamatan dan menjadikan mereka sebagai "*human firewall*" yang mampu melindungi organisasi daripada ancaman siber. Program latihan ini perlu melibatkan pekerja di seluruh peringkat lapisan dalam organisasi agar ia lebih berkesan (Sabillon et al. 2019). Axelos (2015) menekankan bahawa latihan kesedaran keselamatan siber perlu komprehensif supaya kekal relevan dengan perubahan landskap keselamatan siber. Latihan ini harus mendedahkan pekerja kepada polisi keselamatan, proses dan pawaian serta amalan terbaik untuk membantu meningkatkan organisasi secara keseluruhan (Cletus et al. 2022; Fadi & Hatem 2021). Menurut Fallatah et al. (2024) pula program latihan keselamatan siber melibatkan aspek perundangan dapat meningkatkan kadar pematuhan dan mewujudkan budaya yang lebih cakna terhadap

keselamatan siber. Dalam masa yang sama, organisasi yang mengabaikan aspek ini akan menghadapi kesukaran dalam menguatkuasakan keselamatan di organisasi dan kurang efektif dalam program latihan keselamatan yang dijalankan. Faktor lain yang lebih menyumbang kepada kejayaan latihan keselamatan adalah dengan menerapkan elemen kebimbangan dan ketakutan yang boleh menjadi motivasi untuk pekerja memberi komitmen yang tinggi pada latihan yang dijalankan.

Tahap kesedaran terhadap keselamatan siber bergantung pada peringkat hierarki di mana program ini dilaksanakan (Melnyk et al. 2022). Inisiatif atau program latihan keselamatan tidak boleh dilaksanakan dari peringkat bawahan tetapi perlu dimulakan di peringkat pengurusan dan kepimpinan supaya ia dapat dilanjutkan di semua peringkat organisasi (Bada et al. 2019; Melnyk et al. 2022).

Menurut Amankwa et al. (2016), sesebuah model latihan keselamatan dan kesedaran terhadap pekerja harus memfokuskan kepada aspek meningkatkan kemahiran dan pengetahuan pekerja serta mempromosikan budaya keselamatan siber dalam organisasi. Latihan ini haruslah memastikan pekerja memberikan perhatian yang serius terhadap isu-isu keselamatan terkini dan mewajibkan pematuhan terhadap penguatkuasaan polisi keselamatan organisasi.

Pelaburan dalam teknologi keselamatan siber yang canggih perlu diimbangi dengan latihan kesedaran yang komprehensif untuk pekerja dan semua pihak yang berurusan dengan organisasi. Keseimbangan ini penting dalam memastikan semua aspek keselamatan dilindungi termasuklah risiko yang melibatkan pihak ketiga (Saif et al. 2024).

ENISA menekankan bahawa semua pekerja pihak ketiga juga harus terlibat dengan latihan keselamatan, memandangkan mereka juga mendapat akses kepada sistem pengguna. Dengan memberi latihan kepada setiap pekerja dalam rantai bekalan, organisasi dapat mengurangkan pendedahan terhadap risiko keselamatan siber (Bronson 2022). Walau bagaimanapun, menurut Taherdoost (2024a) latihan keselamatan siber banyak tertumpu pada konteks umum dan kurang membincangkan berkenaan risiko yang berpunca dari pihak ketiga. Boyens et al. (2020) mencadangkan

bahawa pembentukan budaya dan kesedaran haruslah berasaskan perkongsian nilai, amalan, matlamat dan sikap sesebuah organisasi yang menjadi kunci kejayaan sesebuah program pengurusan risiko pihak ketiga. Ia melibatkan proses pembelajaran yang mempengaruhi sikap individu atau organisasi serta kefahaman terhadap kepentingan pengurusan risiko pihak ketiga dan implikasi buruk sekiranya gagal. Kajian Bada dan Nurse (2019) sependapat dalam hal ini dan menekankan perkara yang sama dalam kerangka penambahbaikan infrastruktur kritikal. NIST turut menggalakkan organisasi untuk menyediakan latihan kesedaran kepada pekerja dan rakan kongsi supaya mereka dapat melaksanakan tanggungjawab dengan konsisten dalam mematuhi polisi, prosedur dan perjanjian. Ini bermakna setiap dari pekerja termasuk pihak ketiga, pemegang taruh, pegawai atasan, pekerja keselamatan fizikal dan siber perlu menjalani latihan dan kesedaran keselamatan. Dalam menangani keselamatan siber dalam rantaian bekalan, bekas Presiden Amerika Syarikat iaitu Joe Biden telah menggesa supaya kajian terhadap isu ini dipertingkatkan kerana terdapat desakan dan keperluan yang tinggi untuk menguruskan risiko serangan terhadap rantaian bekalan (Melnyk et al. 2022).

Kesimpulannya, keperluan terhadap latihan dan kesedaran keselamatan siber adalah tinggi walaupun terdapat jurang dan cabaran dalam pelaksanaan oleh organisasi. Modul latihan yang baik perlulah komprehensif dan merangkumi semua peringkat bermula daripada pihak atasan sehinggalah peringkat bawahan. Modul tersebut juga perlulah sesuai dengan konteks persekitaran kerja, bahasa dan budaya serta sentiasa relevan dan mendedahkan pekerja kepada landskap ancaman terkini. Modul yang efektif juga perlu dibangunkan dengan menekankan pembinaan nilai dan budaya yang sentiasa cakna dengan isu keselamatan siber di samping menekankan tentang kepentingan dan kebimbangan terhadap akibat serta impak buruk terhadap organisasi. Sebagai tambahan, modul tersebut boleh menerapkan aspek perundangan, polisi dan prosedur supaya ia mudah dipatuhi dan mudah dilaksanakan. Latihan kesedaran ini juga perlu melibatkan semua pekerja di setiap lapisan termasuklah pekerja pihak ketiga bagi mengelakkan risiko atau ancaman yang berpunca daripada kelemahan organisasi atau daripada pihak ketiga. Terdapat juga keperluan yang mendesak terhadap pembangunan modul latihan berkenaan risiko ini kerana ancaman terhadap pihak ketiga ini memberi impak yang sangat besar dan pada masa yang sama, rujukan dan perhatian terhadap modul latihan berkaitan pihak ketiga ini masih kurang.