Asia-Pacific Journal of Information Technology and Multimedia 15(1) 2026: 99 – 122
https://doi.org/10.17576/apjitm-2026-1501-06

Critical Success Factors for Strategic Information Security Policy Implementation in Malaysia's Public Sector

Faktor Kejayaan Kritikal Pelaksanaan Polisi Keselamatan Maklumat Strategik Dalam Sektor Awam Malaysia

Surayahani Hasnul Bhaharin, Umi Asma' Mokhtar, Maryati Mohd Yusof, Rossilawati Sulaiman*

Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia

**Corresponding author: Umi Asma' Mokhtar (umi.mokhtar@ukm.edu.my)*

Received 19 February 2026
Accepted 27 April 2026, Available online 30 June 2026

ABSTRACT

The implementation of strategic information security policy in Malaysia's public sector faces various challenges that require an understanding of critical success factors. This study addresses challenges arising from governance gaps in effective information security management in Malaysia's public sector. This study aims to examine the critical success factors that influence the implementation of strategic information security policy and provide a comprehensive understanding of the key elements that contribute to effective implementation. This study employs a qualitative case study approach, with data collected through semi-structured interviews with key stakeholders involved in information security governance in government agencies. Thematic analysis was used to identify and analyze critical success factors across four main factors: (i) leadership and management support, (ii) human and organizational factors, (iii) environmental factors, and (iv) process factors. The findings indicate that effective policy implementation requires holistic integration among these factors, specifically focusing on organizational culture, stakeholder perceptions, regulatory compliance, and continuous risk management. This study contributes practical insights for developing security frameworks that are contextually appropriate and tailored to the unique administrative and legislative complexities of Malaysia's public sector, as well as contributing to the literature on information security governance by providing empirical evidence and strategic recommendations to enhance information security policy implementation practices.

Keywords: Information security, information governance, strategic information, public sector, information security policy, information security management.

ABSTRAK

Pelaksanaan polisi keselamatan maklumat strategik dalam sektor awam Malaysia menghadapi pelbagai cabaran yang memerlukan pemahaman terhadap faktor kejayaan kritikal. Kajian ini

menangani cabaran disebabkan jurang tadbir urus dalam pengurusan keselamatan maklumat yang berkesan di sektor awam Malaysia. Kajian ini bertujuan mengkaji faktor kejayaan kritikal yang mempengaruhi pelaksanaan polisi keselamatan maklumat strategik serta memberi pemahaman yang komprehensif tentang elemen utama yang menyumbang kepada pelaksanaan yang berkesan. Kajian ini menggunakan pendekatan kajian kes kualitatif, data dikumpul melalui temu bual separa berstruktur dengan pihak berkepentingan utama yang terlibat dalam tadbir urus keselamatan maklumat dalam agensi kerajaan. Analisis tematik digunakan untuk mengenal pasti dan menganalisis faktor kejayaan kritikal merentas empat faktor utama iaitu (i) kepimpinan dan sokongan pengurusan, (ii) faktor manusia dan organisasi, (iii) faktor persekitaran, dan (iv) faktor proses. Dapatan kajian menunjukkan bahawa pelaksanaan polisi yang berkesan memerlukan integrasi holistik di antara faktor-faktor ini mengkhusus kepada budaya organisasi, persepsi pihak berkepentingan, pematuhan peraturan, dan pengurusan risiko berterusan. Kajian ini menyumbang pandangan praktikal untuk membangun kerangka keselamatan yang sesuai dengan konteks dan disesuaikan dengan kerumitan pentadbiran dan perundangan yang unik dalam sektor awam Malaysia, serta menyumbang dalam literatur mengenai tadbir urus keselamatan maklumat dengan menyediakan bukti empirikal dan cadangan strategik untuk meningkatkan amalan pelaksanaan polisi keselamatan.

Kata kunci: Keselamatan maklumat, tadbir urus maklumat, maklumat strategik, sektor awam, polisi keselamatan maklumat, pengurusan keselamatan maklumat.

PENGENALAN

Meskipun banyak organisasi terkesan dengan pandemik Covid-19, perbelanjaan organisasi untuk penyelesaian keselamatan TMK di seluruh dunia meningkat sebanyak 8.1% setahun (2020-2024) yang dianggar mencapai 174.7 bilion dolar AS menjelang 2024 (Columbus 2020). Usaha organisasi untuk membangun strategi bagi mengatasi ketirisan maklumat menjadi genting kerana maklumat semakin mudah dicipta namun sukar untuk dikesan apabila melibat media sosial dan peranti mudah alih.

Kajian yang dilakukan oleh Maynard et al. (2018) mendapati isu keselamatan maklumat yang sering dihadapi organisasi ialah: (i) kekurangan panduan serta kesukaran melaksana misi dan visi organisasi; (ii) kepelbagaian yang terhad dalam membuat keputusan; (iii) mengguna pendekatan ‘bawah-atas’ dalam membangun strategi keselamatan organisasi. Isu ini boleh ditangani dengan memberi fokus mendalam terhadap konteks strategik keselamatan. Objektif dan strategi yang dibangun perlu meluas dan bukan hanya tertumpu kepada aspek risiko dan kawalan sahaja. Maka, terdapat keperluan untuk memperkukuh strategi keselamatan maklumat yang berupaya menjadi alat untuk mentransformasi pengurusan dengan memastikan amalan tadbir urus yang dikenal pasti ditangani dengan berkesan.

Antara cabaran utama yang dihadapi oleh organisasi ialah memasti pematuhan terhadap polisi yang dikuatkuasa (Ali et al. 2021; Palanisamy et al. 2020). Ini kerana, organisasi pada kebiasaannya mempunyai pelbagai jenis polisi keselamatan berdasar isu yang berbeza seperti pengenalan dan keizinan, capaian Internet, pelan kontingensi serta penggunaan media sosial. Akibatnya, banyak kajian lepas memfokus kepada faktor pencegahan dan kawalan dalam pematuhan polisi keselamatan oleh kakitangan.

Faktor yang dikaji termasuk sekatan (Bulgurcu et al. 2010), persepsi terhadap pelaksanaan polisi secara mandatori (Aurigemma 2013), kebimbangan (Salminen & Hossain 2018; van Bavel et al. 2019), kepercayaan moral (Vance & Siponen 2012) dan tekanan berkaitan polisi

keselamatan (D'Arcy et al. 2014). Bagaimanapun, terdapat aliran kajian yang berpandangan bahawa pendekatan mengguna kuasa majikan terhadap pekerja mungkin tidak berkesan. Kefahaman dan penilaian kakitangan perlu diutama sebelum penguatkuasaan peraturan atau polisi dilaksana. Berbanding kerangka pematuhan tradisional yang berasas kepada kawalan, nilai dan peranan kakitangan dalam pembangunan serta pelaksanaan polisi (Cram et al. 2017; Kolkowska et al. 2017).

Kertas ini membincang faktor kejayaan kritikal pelaksanaan polisi keselamatan maklumat strategik sektor awam, dengan menganalisis kajian lampau untuk mengkaji faktor kejayaan dan mengesahkan melalui pakar tempatan sama ada faktor tersebut bersesuaian dengan konteks negara.

CABARAN DAN MASALAH

Proses pembangunan polisi keselamatan maklumat yang berkesan adalah kompleks yang melangkaui sekadar perumusan. Lazimnya, ia memerlukan pertimbangan yang teliti terhadap sokongan pengguna dan objektif strategik yang lebih luas untuk mengelakkan dasar yang kurang dirancang atau tidak relevan (Flowerday danTuyikeze 2016). Kajian semasa menunjukkan masalah biasa yang mana spesifikasi teknikal diutamakan berbanding keperluan organisasi, yang memfokus kepada tekno-sentrik dan mengabaikan elemen manusia (Dhillon, Torkzadeh, dan Chang 2018).

Tambahan pula, penjajaran teknologi maklumat (TM) dengan strategi perniagaan sering menghadapi cabaran pelaksanaan disebabkan tanggungjawab yang tidak jelas dan kekurangan penyelesaian jangka panjang (Shaw dan Ramteke 2023). Menurut AlGhamdi, Win, dan Vlahu-Gjorgievska (2020), keberkesanan polisi keselamatan maklumat banyak dipengaruhi oleh faktor manusia, kepimpinan, dan pihak berkepentingan. Terdapat jurang di antara pemahaman kepimpinan terhadap pergantungan teknologi dan implikasi yang lebih luas terhadap pengurusan polisi keselamatan. Laporan industri mendapati pemimpin atasan mengabaikan keselamatan dalam pengurusan teknologi, yang menunjukkan jurang dalam peranan kepimpinan dalam menjajar teknologi dengan polisi keselamatan secara strategik (Pollini et al. 2021).

Pematuhan merupakan antara faktor kejayaan pelaksanaan keselamatan maklumat, namun ia tidak mencerminkan kelakuan sebenar kakitangan (Wiafe et al. 2020). Meskipun terdapat banyak kajian secara kualitatif dijalankan bagi memahami kelakuan manusia dan budaya keselamatan, masih wujud jurang kajian dalam menyepadu pengetahuan kepada kerangka polisi keselamatan yang praktikal dan boleh diperluaskan untuk konteks sektor awam (Silverman 2013). Jadual 1 merumuskan ringkasan isu dan cabaran dalam pelaksanaan polisi keselamatan maklumat yang dikumpul dari kajian lampau.

JADUAL 1. Rumusan Isu dan Cabaran dalam Pelaksanaan Polisi Keselamatan Maklumat

Ringkasan isu dan cabaran	Isu	Sumber
Ancaman keselamatan yang dihadapi oleh organisasi adalah disebabkan eksploitasi ke atas kelemahan manusia dan teknikal	Eksploitasi kelemahan manusia dan teknikal	Klahr et al. (2017)
Aspek manusia perlu diambil kira secara holistik dalam memastikan pengurusan keselamatan maklumat yang berkesan.	Kecuaian, sikap tidak peduli, tahap kesedaran yang rendah menyebabkan berlakunya	Safa & Maple (2016)

	ketirisan maklumat	
Kakitangan dalaman memberi ancaman kepada usaha melindungi keselamatan maklumat strategik organisasi.	Ancaman dalaman dari kakitangan	Amjad Mahfuth et al. (2017)
Penggubal polisi tidak menyediakan instrumen bagi mengukur tahap pematuhan polisi yang dibangun	Ketiadaan instrumen pengukuran	Angraini et al. (2019b) -
Ancaman keselamatan yang meningkat memberi impak kepada keyakinan pengguna, perlindungan maklumat sensitif dan perkembangan ekonomi.	Keyakinan pengguna terhadap pengurusan keselamatan maklumat organisasi	Mubarak (2016); Srinivas et al. (2018)
Halangan dalam pekerjaan, kebimbangan sistem keselamatan, dan tingkah laku rakan sekerja mempengaruhi ketidak patuhan kakitangan.	Pengaruh nilai organisasi, persekitaran kerja	S. S. Kim & Kim (2017); Mubarak 2016)
Kaedah analisis keselamatan semasa tidak berupaya mengesan rasional sikap patuh dan ketidakpatuhan kakitangan	Kelemahan kaedah analisis yang tidak lengkap	Kolkowska et al. (2017)
Persepsi kakitangan dan pengurus keselamatan maklumat terhadap polisi keselamatan maklumat adalah berbeza.	Persepsi mempengaruhi kejayaan atau kegagalan pelaksanaan polisi keselamatan maklumat	Samonas et al. (2020)
Etika, pengurusan keselamatan maklumat, keselamatan sistem maklumat, perlanggaran polisi keselamatan.	Interaksi antara tingkah laku Kelemahan etika pengurusan pematuhan	Gwebu et al. (2019)
Kewujudan konflik dan alternatif dalam melaksana polisi keselamatan maklumat, menyebabkan kakitangan mempunyai pilihan untuk sama ada untuk patuh atau tidak mematuhi polisi.	Konflik di antara pematuhan dan tidak patuh kepada polisi keselamatan maklumat	K. C. Chang & Seow (2019); Hedström et al. (2011); Kolkowska & de Decker (2012); Mayer et al. (2017)
Pengaruh kepercayaan (kompetensi, integriti dan kebajikan) dan kepimpinan organisasi terhadap tahap kepatuhan kakitangan	Kepercayaan dan kepimpinan tidak diberi perhatian dalam mengkaji tingkah laku pematuhan kakitangan	Paliszkiewicz (2019)
Norma sosial, tekanan sosial, pengaruh sosial dan norma subjektif mempengaruhi tingkah laku pematuhan kakitangan.	Sukar menentukan makna sebenar apabila melibatkan norma sosial kerana pelbagai terma diguna dalam kajian lepas serta bagaimana pengaruhnya terhadap tingkah laku kakitangan	Yazdanmehr & Wang (2016)
Pembangunan, reka bentuk dan pematuhan polisi keselamatan maklumat melibatkan pelbagai formula dan pelaksanaan.	Polisi keselamatan maklumat mempunyai kitar hayat yang perlu diambil kira dalam pembangunan. Kebanyakan organisasi tidak mengenal pasti langkah yang diperlukan dalam pembangunan polisi.	Flowerday & Tuyikeze (2016); Karlsson, Hedström, et al. (2017); Paananen et al. (2020); Yayla & Sarkar (2018)

Faktor manusia dalam keselamatan siber memerlukan pendekatan antara disiplin merangkumi psikologi, budaya organisasi, dan sains komputer bagi menangani isu pematuhan dan tingkah laku keselamatan.	Kelemahan faktor manusia dalam keselamatan siber	Khadka & Ullah (2025)
Cabaran dalam mengurus aspek organisasi, individu dan teknologi dalam pelaksanaan keselamatan maklumat termasuk persekitaran bekerja secara jauh.	Cabaran holistik dalam pengurusan keselamatan maklumat	Topa & Karyda (2025)
Cabaran kritikal pelaksanaan Zero Trust dalam organisasi termasuk isu kepercayaan, identiti dan pengurusan akses yang kompleks.	Cabaran pelaksanaan model keselamatan baharu	Pigola & Meirelles (2025)
Halangan dan daya inersia yang menghalang pembangunan keupayaan pembelajaran keselamatan siber secara dinamik dalam organisasi penjagaan kesihatan.	Halangan pembelajaran keselamatan siber dinamik	Nyakasoka & Naidoo (2024)

KAEDAH KAJIAN

Kajian ini menggunakan pendekatan kualitatif dengan reka bentuk kajian kes untuk mengkaji faktor pelaksanaan polisi keselamatan maklumat dalam sektor awam Malaysia. Kajian ini juga merujuk kepada dokumen polisi dan garis panduan keselamatan maklumat yang sedia ada sebagai data sekunder disahkan oleh dapatan dari temu bual.

Kaedah pengumpulan data yang digunakan adalah melalui temu bual separa berstruktur dengan pegawai-pegawai yang terlibat secara langsung dalam tadbir urus dan pelaksanaan keselamatan maklumat di agensi-agensi kerajaan. Informan kajian dipilih menggunakan teknik persampelan bertujuan berdasarkan pengalaman dan peranan dalam pengurusan keselamatan maklumat strategik.

Data dari dokumen dan temu bual dianalisis menggunakan analisis tematik untuk mengenal pasti tema dan pola yang berkaitan dengan faktor kejayaan kritikal dalam pelaksanaan polisi keselamatan maklumat. Proses analisis melibatkan transkripsi data, pengekodan awal, pengelompokan kod kepada tema, dan penyemakan semula tema untuk memastikan kesahan dan kebolehpercayaan dapatan kajian.

Seramai 16 orang informan telah ditemu bual dalam kajian ini, terdiri daripada pegawai di peringkat strategik (S1–S5), teknikal (T1–T5) dan pelaksana (P1–P6) daripada pelbagai agensi sektor awam Malaysia. Informan dipilih menggunakan teknik persampelan bertujuan berdasarkan pengalaman antara 10 hingga 28 tahun dalam pengurusan maklumat strategik. Setiap sesi temu bual berlangsung antara 30 hingga 45 minit dan dirakam menggunakan aplikasi Voice Memos dengan kebenaran informan. Transkripsi verbatim dibuat sebelum proses analisis dijalankan menggunakan perisian Atlas.ti, berpandukan enam fasa analisis tematik Braun dan Clarke (2006): (i) pembiasaan data, (ii) penjanaan kod awal, (iii) pencarian tema, (iv) semakan tema, (v) penamaan tema, dan (vi) penulisan laporan.

ANALISIS DATA

FAKTOR YANG MEMPENGARUHI PELAKSANAAN POLISI KESELAMATAN MAKLUMAT

Faktor yang mempengaruhi pelaksanaan polisi keselamatan maklumat strategik dikelaskan kepada faktor dan elemen. Kaedah ini membantu proses pembangunan kerangka pelaksanaan polisi keselamatan maklumat strategik. Kajian lepas lazimnya mengkaji isu pematuhan, pembudayaan, kesedaran dan tingkah laku terhadap polisi keselamatan maklumat. Namun, isu tersebut hanyalah sebahagian daripada proses pelaksanaan polisi keselamatan maklumat. Penyelidik lepas mempunyai pandangan yang berbeza tentang faktor yang mempengaruhi pelaksanaan polisi keselamatan maklumat.

Walaupun terdapat faktor yang sama diguna tetapi mempunyai skop dan intensiti yang berbeza. Antara contoh faktor yang diguna oleh penyelidik lepas adalah: tanggungjawab dan akauntabiliti, kesedaran, pematuhan, penilaian (pengauditan), pengukuran, pelaporan dan pemantauan (AlGhamdi et al. 2020); polisi, norma yang subjektif, jangkaan menyukarkan, kecekapan diri dan jangkaan hasil (Ahmad et al. 2019); komitmen organisasi, budaya organisasi, ganjaran, jangkaan kos, kecekapan diri, sikap dan kepercayaan moral (Angraini et al. 2020); kecekapan bertindak, ancaman, habit, peranan nilai, kebimbangan, naturalisasi, perhatian dan tindak balas (Moody et al. 2018).

Kepelbagaian faktor yang disaran oleh penyelidik lepas memberi gambaran bahawa tidak ada ketetapan dalam menentu isu pelaksanaan polisi keselamatan maklumat. Ini kerana ia menjurus kepada persepsi dan tafsiran penyelidik lepas serta teori yang digunakan. Kajian ini mengambil pendekatan merujuk serta berpandu kepada kajian lepas dalam menentukan faktor dan elemen. Penentuan faktor dan elemen bagi kajian ini adalah berdasar kajian oleh Alhogail (2015) dari disiplin keselamatan maklumat, Bennett (2017) dari disiplin tadbir urus maklumat dan Teori Aktiviti oleh Engeström (2000) sebagai kerangka bagi menganalisis dan memahami proses sesuatu aktiviti yang saling berinteraksi dalam mencapai objektif yang ditetapkan. Dalam kajian ini aktiviti merujuk kepada pelaksanaan polisi keselamatan maklumat yang holistik supaya maklumat strategik kerajaan terjamin keselamatannya. Penerangan terperinci Teori Aktiviti adalah seperti di bahagian 0.1. Penggunaan faktor daripada pelbagai disiplin adalah diperlu bagi menangani isu keselamatan maklumat strategik dan tambahan pula ia saling berkait antara satu sama lain (Goodman 2018; Haufe et al. 2016; Lomas 2010, 2020; Shepherd, Bunn, et al. 2019).

Alhogail (2015), berpandangan mempunyai persekitaran yang selamat memerlukan gabungan kawalan teknikal dan kawalan manusia sebagai tambahan kepada faktor lain. Kebanyakan kerangka sedia telah memberi tumpuan kepada satu isu sahaja, seperti hubungan antara budaya keselamatan maklumat dan persekitaran, organisasi, polisi, dan strategi. Faktor strategi, teknologi, organisasi, manusia dan persekitaran adalah faktor yang diberi tumpuan. Faktor tersebut bersifat dinamik, dipengaruhi oleh teori dan mempengaruhi pelaksanaan polisi keselamatan maklumat. Setiap elemen pula saling berkaitan, menyokong dan memberi kesan antara satu dengan yang lain.

Bennett (2017), pula melihat faktor polisi, prosedur, manusia dan teknologi sebagai komponen utama kerangka tadbir urus maklumat. Elemen yang menyokong adalah keselamatan siber; perlindungan data dan privasi; PRM; tadbir urus data; eDiscovery; data analitik; serta risiko

dan pematuhan. Tadbir urus maklumat merupakan sebuah sistem (termasuk polisi, proses, dan teknologi) yang mengurus di mana maklumat digunakan, diproses, dikawal dan perlindungan keselamatan yang diberikan. Bagi memperoleh nilai daripada maklumat, organisasi perlu membuat perolehan teknologi dan sistem aplikasi yang kompetitif supaya penyampaian perkhidmatan kepada pihak berkepentingan dapat dimaksimumkan. Ini termasuk pelaksanaan data analitik bagi memperbaiki atau membangun perkhidmatan atau produk baharu dan meningkatkan sistem perkongsian. Contohnya, peruntukan sumber untuk meningkatkan perlindungan keselamatan maklumat strategik di sektor awam.

Faktor dan elemen yang mempengaruhi pelaksanaan polisi keselamatan maklumat yang diguna pakai dalam kajian ini adalah berdasarkan kepada isu pelaksanaan yang dikenal pasti melalui sorotan susastera. Setiap isu seperti yang dirumus kelas berpandu kepada faktor dan elemen dari disiplin keselamatan maklumat dan tadbir urus maklumat. Sebagai contoh isu berkaitan 'pembangunan dan reka bentuk polisi keselamatan maklumat' dikelas kepada faktor pembangunan polisi dan dikategori dalam faktor proses. Jika terdapat isu yang tidak dapat dikelas semasa proses pengelasan, faktor dan elemen baharu diwujud seperti di JADUAL .

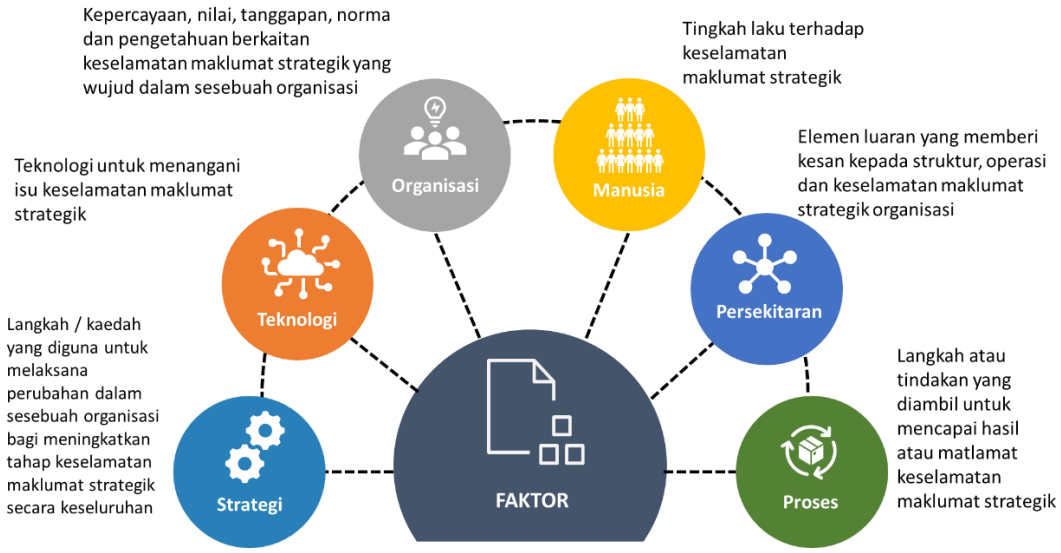
JADUAL 2. Faktor dan elemen yang mempengaruhi pelaksanaan polisi keselamatan maklumat

Faktor	**Elemen**	**Isu yang mempengaruhi pelaksanaan polisi keselamatan maklumat**
Strategi	Tadbir urus maklumat	Menyediakan kerangka yang holistik dengan merangkumi keperluan maklumat pelbagai peringkat dan membolehkan proses penciptaan , perkongsian, pengurusan, pemilikan dan hak termasuk hak pengekalan dan penghapusan, ekonomi, akauntabiliti dan keterbukaan dengan mempertimbangkan keperluan kerahsiaan, privasi dan keselamatan (Ali et al. 2020; Borgman et al. 2016; Datta et al. 2019; Kooper et al. 2011; Lomas et al. 2019; Tallon et al. 2013).
	Keselamatan maklumat	Mengekalkan pertahanan keselamatan TMK yang berkesan kerana teknologi berkembang lebih cepat daripada keselamatan (Antoniou 2018; Furnell et al. 2021; P. Mayer et al. 2017; Mubarak 2016)
Teknologi	Keupayaan	membantu organisasi untuk memenuhi keperluan polisi keselamatan maklumat, seperti keupayaan dan kebolehgunaan teknologi keselamatan tertentu, dan kebolehpercayaan untuk mengesan dan mencegah ancaman dan kelemahan keselamatan maklumat (Alkalbani et al. 2014; D. K. Allen et al. 2013; Keita Nojiri 2015; Snyman & Kruger 2021; Zaydi & Nasserddine 2016; Zhao et al. 2021)
	Infrastruktur	Perkembangan teknologi yang pesat memberi pelbagai faedah tetapi mewujudkan ancaman baharu (Furnell et al. 2021; Ibrahim Ghafir et al. 2018; Yadav et al. 2018)
Organisasi	Nilai organisasi	Nilai yang dipegang bersama dalam organisasi dalam mencapai objektif yang telah ditetapkan (Amankwa et al. 2017; Koohang et al. 2020; Tu et al. 2018; Yayla & Lei 2018)
	Budaya keselamatan	Pengurusan atasan dapat memupuk budaya keselamatan yang baik, dan budaya keselamatan membantu membentuk tingkah laku pekerja (Da Veiga et al. 2020; Schlienger & Teufel 2002; Soon et

		al. 2009; Tang et al. 2016)
	Komitmen pengurusan	Komitmen dan pemahaman pengurusan tentang kepentingan keselamatan maklumat. Pihak pengurusan perlu memberi sokongan yang kuat dengan melaksana polisi dan memberi latihan yang mencukupi kepada kakitangan (Aurigemma & Panko 2012; Barton e tal. 2016; Chulkov 2017; Guan & Hsu 2020; Kajtazi e tal. 2018; C. Liu et al. 2020)
Persekitaran	Perundangan, Peraturan dan prosedur	Tekanan dari agensi penguatkuasaan yang memaksa organisasi untuk melaksana polisi dan piawaian keselamatan maklumat. Tekanan ini memaksa organisasi untuk memasukkan keperluan undang-undang dalam amalan keselamatan maklumat untuk memenuhi tuntutan perundangan (AlKalbani et al. 2017; Parsons et al. 2010; Rubino et al. 2017; Zhao et al. 2021)
	Tekanan sosial	Jangkaan pihak berkepentingan terhadap keselamatan maklumat memberi tekanan dalam organisasi untuk mengukuhkan pelaksanaan keselamatan maklumat mereka. Tuntutan pihak berkepentingan memainkan peranan penting dalam meningkatkan tingkah laku pematuhan kakitangan dalam organisasi awam (AlKalbani et al. 2017; Alkalbani et al. 2019; Hou et al. 2018; Tang et al. 2016)
Manusia	Peranan dan tanggungjawab	Peranan dan tanggungjawab yang bersesuaian dan boleh diterima oleh kakitangan apabila dikaitkan dengan sifat kerja yang dilaksanakan (Alter 2019; Koohang et al. 2020; Moody et al. 2018)
	Tingkah laku	Tingkah laku keselamatan maklumat memberi tumpuan kepada tingkah laku individu, yang berkaitan dengan melindungi aset maklumat, termasuk infrastruktur rangkaian, perkakasan komputer dan maklumat organisasi (Ali et al. 2021; Alzahrani et al. 2018; Kolkowska et al. 2017; Paliszkiewicz 2019; Yazdanmehr & Wang 2016)
Proses	Kesedaran dan kefahaman	Program membantu organisasi dengan strategi pengurangan risiko, mengoptimumkan pelaksanaan keselamatan dan keupayaan untuk melindungi aset maklumat organisasi. Menangani sikap pengguna yang ingkar terhadap polisi keselamatan maklumat dengan memupuk budaya keselamatan. (Bauer & Bernroider 2017; X. Chen et al. 2016; Furnell et al. 2021; Hwang et al. 2019; Koohang et al. 2019; McCormac et al. 2017)
	Kitar hayat maklumat	Maklumat dikendali dengan cara yang bersesuaian dari dicipta sehingga dilupus (Al-Fedaghi 2008; ARMA International 2019b; Hagmann 2013; Nguyen et al. 2014; Oppitz & Tomsu 2017)
	Kitar hayat Pembangunan polisi	Pembangunan polisi yang teliti dan komprehensif dengan cara yang memastikan aset maklumat dilindungi daripada pelbagai ancaman. Polisi yang dibangun perlu selari dengan matlamat dan amalan kecekapan organisasi supaya keselamatan maklumat tidak menjadi halangan, kerana pada kebiasaan secara praktikalnya yang paling selamat bukanlah yang paling cekap dan sebaliknya. (Alqahtani 2017; Brechbühl et al. 2010; Flowerday & Tuyikeze 2016; Ismail et al. 2017; Niemimaa & Niemimaa 2019; Paananen et al. 2020; Williams 2013)

Penilaian dan pengukuran	Menilai keadaan organisasi dan untuk meningkatkan keupayaan organisasi dengan menentukan kaedah penambahbaikan, mengenal pasti prosedur terbaik untuk meningkatkan keberkesanan dan kecekapan proses pelaksanaan polisi (Al-Matari et al. 2021; W. Chen et al. 2017; Proença & Borbinha 2018; Yulianto et al. 2016)
Pemantauan	Organisasi akan mendapat manfaat daripada pemantauan keselamatan maklumat dengan menggalakkan tingkah laku keselamatan yang melangkaui polisi keselamatan (Ahmad et al. 2019; Alkalbani et al. 2019; Horcas et al. 2016; Kam et al. 2021; Yeng et al. 2021)
Penilaian risiko	Merupakan topik yang penting dalam keselamatan maklumat yang menjadi perkara utama bagi perlindungan maklumat. Ia adalah proses mengenal pasti risiko, menilai magnitud risiko yang relatif dan mengambil tindakan untuk mengawal risiko ke tahap yang boleh diterima (Institute of Internal Auditors 2013; Joshi & Singh 2017; Maynard et al. 2018; Shepherd, Sexton, et al. 2019; Silva & Soares 2018; B. Von Solms & Von Solms 2004; Whitman & Mattord 2018; Yaokumah et al. 2016)

RAJAH merumus faktor yang mempengaruhi kejayaan kritikal pelaksanaan polisi yang telah dikenal pasti daripada kajian susastera dan menjadi pemacu utama mewajar keperluan kerangka pelaksanaan polisi keselamatan maklumat.



RAJAH 1. Faktor yang mempengaruhi pelaksanaan polisi keselamatan maklumat

Terdapat enam faktor yang dikenal pasti, dan berikut adalah keterangan setiap faktor tersebut:

1. *Strategi*
   Kaedah pelaksanaan strategi keselamatan maklumat yang teratur seperti pelan tindakan, polisi, objektif, amalan terbaik, piawaian dan garis panduan yang dibangun bagi

memberi panduan kepada organisasi dalam mencapai matlamat melindungi keselamatan maklumat strategik organisasi.

2. *Teknologi*
   Teknologi keselamatan seperti perkakasan, perisian, perkhidmatan, peralatan dan aplikasi yang digunakan organisasi bagi melindungi keselamatan maklumat strategik organisasi. Teknologi yang digunakan mempunyai peranan membentuk budaya keselamatan maklumat dan budaya keselamatan maklumat pula perlu menyokong keberkesanan teknologi keselamatan yang digunakan.

3. *Organisasi*
   Struktur organisasi mempunyai pengaruh yang signifikan kepada budaya keselamatan maklumat sesebuah organisasi. Dalam konteks kajian ini, organisasi adalah berkaitan dengan kepercayaan, nilai, tanggapan, norma dan pengetahuan yang menjadi amalan di dalam organisasi.

4. *Manusia*
   Manusia merupakan teras utama kepada budaya keselamatan maklumat yang memainkan peranan utama di dalam proses keselamatan maklumat. Dimensi ini berkaitan dengan tingkah laku seseorang dalam mengurus keselamatan maklumat strategik organisasi.

5. *Persekitaran*
   Faktor ini bermaksud persekitaran sekeliling dan budaya setempat dan budaya tempatan organisasi tersebut berada yang memberi impak besar kepada budaya keselamatan maklumat sesebuah organisasi. Dalam konteks kajian ini, sebarang elemen yang dikenal pasti memberi kesan kepada struktur dan pengoperasian organisasi terhadap pembudayaan keselamatan maklumat strategik. Ia merupakan faktor luaran yang memberi kesan kepada tingkah laku keselamatan seperti budaya tempatan, etika, inisiatif kerajaan, undang-undang dan peraturan; dan sistem

6. *Proses*
   Faktor proses merujuk kepada langkah atau tindakan yang diambil untuk mencapai hasil atau matlamat keselamatan maklumat strategik. Proses ini penting bagi memastikan polisi dan prosedur keselamatan maklumat strategik dilaksanakan dengan berkesan, cekap dan konsisten di dalam organisasi. Proses menyediakan pendekatan berstruktur untuk pengurusan risiko keselamatan, membantu memastikan polisi dilaksana secara konsisten, menyediakan mekanisme untuk memantau dan mengukur pematuhan; dan memastikan peningkatan berterusan terhadap tahap keselamatan maklumat strategik organisasi.

Rajah 2 menggambarkan kerangka konseptual yang menunjukkan hubungan antara keenam-enam faktor kejayaan kritikal yang dikenal pasti. Faktor Strategi dan Persekitaran bertindak sebagai pemacu luaran yang membentuk persekitaran pelaksanaan secara keseluruhan. Faktor Organisasi dan Teknologi pula berfungsi sebagai pemboleh daya yang menyokong proses pelaksanaan. Manakala Faktor Manusia dan Proses merupakan elemen dalaman yang menjadi pengantara utama kepada kejayaan pelaksanaan polisi keselamatan maklumat strategik. Kesemua faktor ini saling berinteraksi secara holistik bagi memastikan keberkesanan pelaksanaan polisi keselamatan maklumat strategik di sektor awam Malaysia.

RAJAH 2. Kerangka Konseptual Pelaksanaan Polisi Keselamatan Maklumat Strategik

FAKTOR KEJAYAAN PELAKSANAAN POLISI KESELAMATAN MAKLUMAT STRATEGIK SEKTOR AWAM

Analisis dalam bahagian ini memfokus kepada persoalan pertama yang dikemuka oleh kajian iaitu '*Apakah faktor kejayaan kritikal pelaksanaan polisi keselamatan maklumat strategik sektor awam*?'. Analisis ini bagi memahami strategi pelaksanaan dan amalan pengurusan keselamatan maklumat strategik yang dilakukan dalam sektor awam.

Setiap faktor dihurai bersama elemen yang diperoleh melalui pandangan berkaitan pelaksanaan polisi keselamatan maklumat strategik sektor Awam di Malaysia. Penyelidik menulis dan mentafsirkan perspektif informan mengenai topik ini berdasar kepada keadaan, persekitaran, gerak isyarat (*gesture*), bahasa badan, dan faktor lain. Ekspresi wajah dan bahasa badan dapat memberikan petunjuk tentang perasaan sebenar informan (Zairul 2021). Misalnya, senyuman atau kerutan dahi dapat menunjukkan sama ada informan berasa selesa atau tertekan. Dengan memahami emosi ini, penyelidik dapat menyesuaikan pendekatan mereka untuk mendapatkan maklumat yang lebih mendalam dan tepat. Dengan memahami dan menggunakan tanda non-verbal dengan efektif, penyelidik dapat meningkatkan keupayaan untuk mendapatkan maklumat yang tepat dan mendalam daripada informan. Ini bukan sahaja memperkaya data yang dikumpulkan tetapi juga meningkatkan kualiti interaksi antara penyelidik dan informan

Pelbagai faktor penting mengenai amalan serta pelaksanaan polisi pelaksanaan polisi keselamatan maklumat strategik telah dikenal pasti melalui sesi temu bual dan pemerhatian di lapangan. Protokol temu bual yang telah dibangun dijadikan panduan semasa sesi temu bual. Bagi mengkaji faktor kejayaan pelaksanaan polisi keselamatan maklumat strategik sektor awam, kajian ini memperoleh data daripada pelbagai perspektif iaitu kumpulan strategik, teknikal dan pelaksana. Secara umumnya, persoalan tertumpu kepada faktor pelaksanaan polisi keselamatan maklumat strategik dan amalan pengurusan keselamatan maklumat strategik.

FAKTOR STRATEGI

Strategi dalam faktor ini berkaitan dengan pelaksanaan strategi keselamatan maklumat yang berbeza seperti pelan tindakan, dasar, objektif, amalan terbaik, piawaian, garis panduan, dan

keutamaan yang dirancang untuk memberi panduan kepada warga organisasi bagi melindungi aset maklumat. Polisi, amalan terbaik, garis panduan dan kawalan membantu kakitangan menerima mesej yang konsisten dan jelas tentang apa yang dilarang dan akibat jika berlaku ketidakpatuhan. Strategi yang baik diperlukan kerana dapat menyokong pelaksanaan polisi keselamatan maklumat dan seterusnya mencapai tahap pematuhan yang tinggi.

Analisis data mendapati faktor yang didasari oleh faktor strategi terdiri daripada elemen tadbir urus, pengoperasian dan kawal selia.

Elemen 1: Tadbir Urus

Elemen tadbir urus merangkumi pelan pelaksanaan pengurusan maklumat strategik dan tatacara pengendalian maklumat strategik. Elemen ini penting dan perlu ditekan dalam memastikan kejayaan inisiatif pengurusan keselamatan maklumat strategik sektor awam. Peranan dan tanggungjawab juga perlu ditentukan supaya pelaksanaan polisi keselamatan maklumat strategik menjadi amalan dan dipantau pelaksanaannya. Analisis data daripada temu bual menunjukkan tiada strategi yang jelas tentang pelaksanaan tadbir urus maklumat strategik.

Ini terbukti apabila setiap peringkat pengurusan mempunyai pandangan yang berbeza. Pada peringkat strategik, polisi keselamatan maklumat strategik merupakan satu keperluan perkhidmatan dalam pengurusan maklumat strategik serta menjana tadbir urus yang baik. Manakala pada peringkat teknikal pula adalah satu keperluan dasar dan peraturan, tanggungjawab yang perlu dilaksana bagi melindungi keselamatan maklumat strategik. Peringkat pelaksana pula melihat dari aspek keberkesanan dan kecekapan pelaksanaan proses pengurusan maklumat strategik.

Berdasarkan temu bual, boleh disimpulkan bahawa polisi dan prosedur yang lengkap tidak memberi jaminan pematuhan dalam kalangan kakitangan organisasi. Tadbir urus yang jelas juga mempunyai peranan yang penting di mana setiap peringkat di dalam organisasi mempunyai peranan serta tanggungjawab yang perlu dilaksana dalam menjayakan inisiatif keselamatan maklumat strategik. Tanpa peranan dan tanggungjawab yang dinyatakan dengan jelas (didokumen, hala tuju yang direncana sukar dicapai. Elemen kawal selia juga penting yang bertindak sebagai pemboleh daya meningkatkan pematuhan polisi.

Elemen 2: Pengoperasian

Pengoperasian adalah elemen kedua yang diperoleh melalui analisis data berkaitan dengan faktor strategi. Kumpulan pengoperasian bertanggungjawab untuk pelaksanaan operasi program keselamatan maklumat yang berterusan bagi memastikan operasi bisnes tiada gangguan.

Elemen 3: Kawal selia

Elemen hala tuju keselamatan maklumat merujuk kepada penyediaan panduan dan hala tuju keseluruhan dalam tadbir urus. Hasil daripada analisis data yang dikumpul, didapati bahawa tadbir urus keselamatan maklumat ialah peraturan dan dipacu oleh bisnes organisasi. Kawal selia yang mendorong pelaksanaan polisi keselamatan maklumat muncul dengan jelas dalam semua temu bual bersama informan. Keperluan mengawal selia mempunyai pengaruh yang

signifikan terhadap keselamatan maklumat kerana keperluan ini ditentukan oleh agensi peneraju.

Keperluan kawal selia muncul sebagai elemen penting yang memacu tadbir urus keselamatan maklumat. Kajian ini dapat menyimpulkan bahawa agensi peneraju yang menjadi pihak berkepentingan dalam keselamatan maklumat, bertanggungjawab untuk menentukan semua keperluan. Organisasi tidak mempunyai pilihan selain mematuhi keperluan yang ditentukan oleh agensi peneraju, yang secara amnya merupakan agensi yang bertanggungjawab dalam mengawal keselamatan maklumat strategik kerajaan.

Pengurusan atasan yang mempunyai tanggungjawab terhadap agensi peneraju bertanggungjawab untuk memastikan organisasi mematuhi keperluan kawal selia. Ini disahkan secara konsisten oleh informan. Keperluan kawal selia ini adalah input utama dalam pelan strategik dan pengurusan risiko organisasi yang akan digunakan untuk mengesah strategi dan objektif keselamatan maklumat.

FAKTOR TEKNOLOGI

Teknologi dalam faktor ini berkaitan dengan teknologi keselamatan seperti perkakasan, perisian, perkhidmatan, peralatan dan aplikasi yang digunakan dalam organisasi untuk melindungi aset maklumat. Teknologi yang diguna oleh organisasi mempunyai peranan dalam membentuk budaya keselamatan maklumat organisasi, dan budaya keselamatan maklumat akan menyokong keberkesanan langkah keselamatan yang diguna pakai. Teknologi menjadi faktor penting dalam kejayaan pelaksanaan polisi keselamatan maklumat kerana organisasi secara agresif mengguna teknologi dalam melaksana operasi bisnes. Teknologi juga menyediakan alat dan sumber untuk menyempurnakan aktiviti (tugasan) melalui proses yang sistematik.

Elemen yang didasari oleh faktor teknologi ialah keupayaan, kos dan automasi.

Elemen 1: Keupayaan

Faktor teknologi juga termasuk langkah proaktif dan reaktif yang terdiri daripada alat, teknik dan sumber (perkakasan dan perisian, ketara dan tidak ketara) yang diguna untuk memastikan keselamatan maklumat strategik. Pelbagai penyelesaian teknikal telah dibangun untuk melindungi keselamatan maklumat strategik, dengan mengambil kira prinsip CIA namun insiden keselamatan masih berlaku. Walaupun infrastruktur TMK membolehkan integrasi proses bisnes dan mengurangkan risiko keselamatan maklumat. Namun isu kesukaran seperti memastikan ketersediaan, penggunaan yang sesuai, dan keupayaan pelaksanaan teknologi boleh membawa kepada kegagalan yang ketara dan ketidakupayaan untuk mencapai objektif penggunaan teknologi tersebut.

Keupayaan teknologi merujuk kepada keupayaan untuk memenuhi keperluan keselamatan dari sudut teknikal. Ia mempunyai kesan dalam meningkatkan kepercayaan dan keyakinan pengguna, yang membawa kepada pematuhan keselamatan maklumat yang lebih besar. Keupayaan teknologi juga membantu organisasi memenuhi keperluan polisi keselamatan maklumat, seperti keupayaan dan kebolehgunaan teknologi keselamatan tertentu, dan kebolehpercayaan untuk mengesan dan mencegah ancaman dan kelemahan keselamatan maklumat. Ancaman dalaman sangat membimbangkan kerana kakitangan mempunyai capaian kepada sistem dan maklumat organisasi, menjadikannya lebih mudah untuk mereka

menyebabkan kerosakan atau mencuri maklumat. Manakala ancaman luaran lebih mencabar kerana ia berasal dari luar rangkaian organisasi. Pada kebiasaannya penyelesaian teknologi seperti tembok api, sistem pengesanan pencerobohan, dan kemas kini perisian secara berkala, dapat membantu melindungi terhadap ancaman luaran.

Keupayaan teknologi juga merujuk kepada keupayaan untuk menangani ancaman dalaman dan ancaman luaran. Teknologi memainkan peranan yang penting dalam mitigasi ancaman dalaman dan luaran. Antara teknologi yang biasa digunakan di sektor awam dalam mengekang ancaman dalaman ialah Sistem Perlindungan Ketirisan Data (*Data Leakage Protection*), Sistem Pengurusan Identiti dan Kawalan Akses (*Identity Acsess Management* (IAM)) dan *Security Information and Event Management* (SIEM). Manakala bagi ancaman luaran pula ialah *Firewall* dan Sistem Pengesanan Pencerobohan (IDS), Penyulitan (*Encryption*) dan Pengesahan Pelbagai Faktor (*Multi Factor Authentication*).

Ancaman dalaman adalah daripada individu dalam organisasi yang mempunyai kebenaran akses kepada aset organisasi. Individu ini terdiri daripada kakitangan, bekas kakitangan dan kontraktor, atau pihak ketiga yang mempunyai kepentingan. Ancaman dalaman boleh berlaku dalam pelbagai bentuk, seperti kecurian data, sabotaj, atau pendedahan maklumat yang tidak dibenarkan. Mereka merupakan risiko yang signifikan, terutamanya dalam sektor-sektor seperti kesihatan, kewangan, dan kerajaan, di mana data sensitif mempunyai nilai yang tinggi.

Ancaman luaran pula sebaliknya, ia datang daripada individu atau kumpulan di luar organisasi. Ancaman ini biasanya melibatkan individu atau organisasi yang mempunyai niat jahat seperti penggodam, penjenayah siber, atau *hacktivists* yang tidak mempunyai akses yang dibenarkan kepada sumber organisasi. Bentuk-bentuk ancaman luaran termasuk phishing, malware dan virus, kejuruteraan sosial dan advanced persistent threats (APTs). Kedua-dua ancaman dalaman dan luaran mengeksploitasi kelemahan dalam organisasi.

Informan berpandangan bahawa keupayaan teknologi meningkatkan keyakinan dan prestasi kakitangan, yang boleh membawa kepada peningkatan penggunaan kawalan keselamatan yang lebih tinggi. Informan juga mengesahkan bahawa keupayaan teknologi keselamatan yang pelbagai dapat meningkatkan fleksibiliti dalam melaksana kawalan keselamatan maklumat dalam sektor awam. Semua informan bersetuju bahawa kebolehpercayaan teknologi dalam mengesan dan mencegah ancaman keselamatan maklumat, sejauh mana ia mudah diguna dan dikonfigurasi, dan ketersediaan sokongan teknikal perlu dipenuhi untuk meningkatkan penerimaan teknologi kawalan keselamatan dalam organisasi.

Data temu bual juga mendapati tahap kesesuaian antara teknologi yang diguna pakai dan budaya serta norma organisasi mempengaruhi pelaksanaan polisi dalam organisasi. Teknologi yang diguna pakai perlu sesuai dan menyokong objektif keselamatan maklumat organisasi. Kesesuaian teknologi yang diguna pakai memboleh teknologi keselamatan mematuhi keperluan keselamatan yang telah ditetapkan. Informan berpandangan bahawa setiap teknologi adalah sangat berbeza serta pelbagai jenis, dan kadang kala sangat lama / uzur, maka ia meningkatkan kerumitan kawalan keselamatan maklumat dalam jabatan. Informan juga menegaskan bahawa isu pematuhan keselamatan maklumat yang berbeza perlu ditangani secara berbeza daripada perspektif kesesuaian teknologi. Ini termasuk keperluan keselamatan maklumat jabatan, keserasian antara teknologi keselamatan dan teknologi pengoperasian, dan kesan yang dijangka seperti kos teknikal.

Elemen 2: Kos

Data temu bual mendapati pembangunan teknologi memerlu komitmen kewangan yang tinggi dan berterusan. Kos merupakan salah satu halangan dan halangan sedia ada kepada organisasi untuk mengguna pakai teknologi keselamatan maklumat.

Kos teknologi memainkan peranan penting dalam membentuk pelaksanaan dasar keselamatan maklumat. Organisasi mesti menyeimbangkan keperluan keselamatan mereka dengan sekatan kewangan, membuat keputusan strategik mengenai pelaburan teknologi yang selaras dengan keperluan toleransi risiko dan pematuhan mereka. Keselamatan maklumat yang berkesan memerlukan bukan sahaja teknologi yang betul tetapi juga latihan dan sumber yang mencukupi untuk memastikan bahawa dasar dipahami dan diikuti oleh semua pekerja. Kos perolehan teknologi memainkan peranan penting dalam membentuk pelaksanaan dasar keselamatan maklumat. Organisasi mesti menyeimbangkan keperluan keselamatan dengan peruntukan kewangan yang terhad, membuat keputusan strategik mengenai pelaburan teknologi yang selaras dengan keperluan risiko dan pematuhan. Keselamatan maklumat yang berkesan memerlukan bukan sahaja teknologi yang betul tetapi juga latihan dan sumber yang mencukupi untuk memastikan bahawa polisi difahami dan dipatuhi oleh semua warga organisasi.

Elemen 3: Automasi

Organisasi boleh memudahkan pengurusan keselamatan maklumat dengan mengguna teknologi bagi mengautomasi proses keselamatan maklumat dan mengurang kerumitan pengurusan keselamatan maklumat. Memanfaatkan perisian dan strategi yang disokong perisian berasas kecerdasan buatan (AI) berupaya meningkat keselamatan organisasi dengan ketara terutama menangani isu yang memerlukan penilaian manusia yang terdedah kepada kesilapan.

Walaupun didapati AI dapat meningkat keselamatan maklumat dengan ketara, namun ia masih memerlu kepakaran dan pertimbangan manusia. Malah, penglibatan manusia masih penting untuk membuat keputusan kritikal bagi menangani isu keselamatan yang kompleks yang mana memerlu pemahaman kontekstual serta pertimbangan etika.

FAKTOR ORGANISASI

Faktor organisasi mempunyai pengaruh yang kuat terhadap pelaksanaan polisi keselamatan maklumat organisasi. Dalam faktor organisasi, elemen berkaitan adalah komitmen pengurusan, budaya keselamatan, dan; fasiliti dan peruntukan sumber.

Elemen 1: Komitmen Pengurusan

Komitmen pengurusan ialah inisiatif pengurusan dalam melaksana polisi keselamatan maklumat strategik. Antara inisiatif yang dilaksana ialah menubuhkan pasukan khusus untuk pengurusan polisi keselamatan maklumat sebagai salah satu penanda aras komitmen pengurusan. Penubuhan pasukan khusus oleh pihak pengurusan menunjukkan kepada kakitangan komitmen pengurusan. Pengurusan tertinggi mengenal pasti pihak berkepentingan utama dan menjelaskan peranan dan tanggungjawab mereka. Penglibatan pihak berkepentingan di dalam proses pelaksanaan polisi adalah petunjuk kejayaan inisiatif pengurusan keselamatan maklumat.

Inisiatif pengurusan keselamatan maklumat strategik perlu digerak oleh kumpulan khas yang terdiri daripada kakitangan pelbagai bahagian yang berkongsi pengalaman mereka berkaitan manfaat keseluruhan inisiatif. Matlamat utama pasukan ini ialah untuk membangun budaya amalan cemerlang di kalangan jabatan. Jabatan juga dinilai secara keseluruhan amalan pengurusan keselamatan maklumat strategik melalui inspektorat keselamatan dan diberi anugerah berdasar pematuhan yang dicapai. Penilaian ini secara tidak langsung menuntut komitmen pengurusan tertinggi terhadap pelaksanaan polisi keselamatan maklumat strategik.

Elemen 2: Budaya Organisasi

Budaya organisasi merujuk kepada satu set andaian, kepercayaan dan nilai berkekalan yang menggambarkan organisasi dan ahli organisasi. Budaya organisasi juga merupakan keupayaan organisasi untuk mengamalkan perubahan dalam melaksana tadbir urus. Jika organisasi terlepas pandang faktor ini boleh menyebabkan pelaksanaan tadbir urus yang tidak berjaya. Selain itu, ia juga sebahagian daripada pengurusan perubahan dalam organisasi. Penerapan budaya pengurusan keselamatan maklumat strategik mampu memacu pematuhan polisi keselamatan maklumat strategik.

Elemen 3: Fasiliti dan peruntukan sumber

Pengurus keselamatan maklumat sentiasa mendapati sukar untuk mendapat peruntukan yang mencukupi daripada pengurusan atasan. Pengurusan atasan mungkin berterusan enggan memperuntukkan sumber yang munasabah kepada fungsi keselamatan. Maka terdapat keperluan bagi pengurus keselamatan untuk memberi kesedaran dan meyakinkan pengurusan atasan bahawa tanpa peruntukan yang mencukupi, hampir mustahil untuk mempunyai amalan keselamatan maklumat yang berkesan.

Perkara ini menunjukkan bahawa organisasi menghadapi cabaran untuk mendapat dana yang mencukupi bagi melaksana pengurusan keselamatan maklumat. Kekurangan peruntukkan menyebab kelewatan pelaksanaan amalan keselamatan dalam organisasi. Akibatnya, organisasi akan mengalami kerugian besar daripada insiden keselamatan semasa hendak memulakan semula fungsi pentadbiran selepas insiden. Selain itu, pengurusan atasan perlu diyakinkan bahawa peruntukan yang mencukupi adalah penting untuk melaksana pengurusan keselamatan maklumat yang berkesan.

Faktor Manusia

Faktor manusia adalah teras pelaksanaan polisi keselamatan maklumat, kerana manusia memainkan peranan utama dalam proses keselamatan maklumat. Selain itu manusia juga memainkan peranan penting dalam rantaian keselamatan yang menyumbang kepada kejayaan pelaksanaan polisi keselamatan maklumat. Usaha mengenal pasti kelemahan dan melaksana tindakan pembetulan bukan sahaja tertumpu kepada kakitangan tetapi wajar diperluas kepada pembekal luar dan pihak ketiga yang berurusan dengan organisasi. Perkara ini penting dalam memastikan mereka mempunyai perlindungan keselamatan maklumat yang sesuai bagi mencegah serangan kepada sistem maklumat organisasi.

Dalam faktor manusia, elemen yang dikenal pasti adalah kompetensi teknikal, dan latihan dan kesedaran.

Elemen 1: Kompetensi Teknikal

Keseimbangan antara faktor teknikal dan sosial juga mempengaruhi kejayaan pelaksanaan polisi keselamatan maklumat. Tahap kompetensi teknikal kumpulan pengurusan berupaya meningkatkan kejayaan pelaksanaan polisi. Kemahiran dan kecekapan dalam TMK boleh memacu kawalan dan amalan pelaksanaan polisi keselamatan Kakitangan teknikal yang kompeten berupaya mengendalikan sumber TMK dengan efisien. Maka ia meningkatkan keupayaan teknologi dalam proses pembangunan dan pelaksanaan kawalan keselamatan maklumat organisasi. Sehubungan itu kawalan keselamatan seperti polisi dan kawalan operasi (sandaran data dan kawalan capaian) dalam menyumbang kejayaan pelaksanaan polisi keselamatan.

Pembangunan kapasiti kakitangan juga merupakan isu yang perlu ditangani. Hasil pemerhatian di dapati organisasi tidak mempunyai kakitangan mahir yang mencukupi untuk mengendali projek berasas teknologi. Selain itu informan juga menegaskan bahawa kekurangan latihan secara praktikal terhadap teknologi yang diguna pakai juga masih kurang dan terhad. Terdapat juga informan yang mengutara masalah pertukaran kakitangan teknikal yang kerap juga menjadi isu yang serius dan perlu ditangani dengan baik.

Kompetensi teknikal juga sebagai pemboleh daya kepada organisasi untuk merangka cara pemikiran baharu dalam merancang, mengatur, melaksana, dan perolehan (pelaburan) dalam keselamatan maklumat dengan cekap. Integrasi antara strategik dan operasi berlaku apabila sumber dan kompetensi teknikal berupaya menyokong proses pelaksanaan polisi serta pencapaian objektif keselamatan maklumat organisasi. Sehubungan itu, terdapat keperluan berterusan untuk memberi latihan kepada kakitangan bagi meningkatkan kemahiran keselamatan maklumat mereka dan memastikan semua kakitangan terlibat dalam agenda melindungi serta mempertahankan keselamatan maklumat.

Elemen 2: Latihan dan Kesedaran

Pelaksanaan latihan dan kesedaran untuk kakitangan juga membantu memelihara keselamatan maklumat strategik di samping mengurangkan kesilapan dan kecuaian manusia. Walaupun kakitangan bersedia untuk menerima sebarang perubahan, namun latihan berterusan diperlukan dan bukannya sekali sahaja sesi latihan. Jabatan terpaksa berbelanja besar bagi melaksana program latihan bagi memastikan pematuhan yang berterusan dan perbelanjaan yang dikeluarkan adalah berbaloi.

Walaupun semua informan bersetuju teknologi adalah penting bagi menyokong pelaksanaan polisi keselamatan maklumat strategik, namun sektor awam memberi penekanan kepada penggunaan teknologi yang bukan untuk tujuan pelaksanaan pengurusan keselamatan maklumat strategik. Perkara ini disebab oleh kapasiti dan keupayaan pegawai yang terhad (khususnya dari aspek kompetensi dan tenaga terlatih) selain daripada peruntukan kewangan.

FAKTOR PERSEKITARAN

Persekitaran dan budaya yang mana organisasi beroperasi mempunyai kesan yang besar terhadap budaya keselamatan maklumat yang menjadi amalan di dalam organisasi tersebut. Dalam konteks kajian ini, faktor persekitaran adalah berkaitan unsur luaran organisasi yang dikenal pasti boleh mempengaruhi struktur, operasi dan keselamatan maklumat serta budaya keselamatan maklumat. Faktor luaran yang mempengaruhi pelaksanaan polisi keselamatan

maklumat termasuk budaya setempat, inisiatif kerajaan dan; sistem perundangan dan peraturan. Dua elemen yang mempengaruhi faktor persekitaran iaitu persekitaran organisasi serta perundangan dan peraturan.

Elemen 1: Persekitaran Organisasi

Persekitaran organisasi merangkumi nilai bersama, kepercayaan, sikap, dan tingkah laku dalam sesebuah organisasi. Budaya berorientasi keselamatan yang wujud di dalam persekitaran organisasi berupaya memupuk kefahaman kakitangan terhadap kepentingan keselamatan maklumat.

Elemen 2: Perundangan dan peraturan

Keperluan pematuhan kepada perundangan dan peraturan mempunyai kesan yang signifikan terhadap bagaimana organisasi membangun, melaksana, dan mengekalkan polisi keselamatan maklumat. Pematuhan kepada perundangan dan peraturan ini bukan sahaja merupakan kewajipan undang-undang tetapi juga salah satu cara untuk melindungi maklumat strategik, mengekal kepercayaan pelanggan, dan mengelakkan penalti kewangan.

Ringkasnya, pelaksanaan polisi keselamatan maklumat dipengaruhi oleh faktor persekitaran yang merangkumi keperluan persekitaran organisasi dan; perundangan dan peraturan. Pendekatan secara holistik perlu juga mengambil kira keadaan ekonomi, trend teknologi, konteks geopolitik, piawaian, kepelbagaian budaya, dan kesinambungan bisnes. Elemen-elemen ini perlu ditangani secara kolektif bagi membantu memasti strategi keselamatan maklumat yang komprehensif dan berkesan. Penting bagi organisasi untuk mempertimbangkan faktor persekitaran ini apabila membangun dan melaksanakan polisi keselamatan maklumat untuk memastikan keberkesanan dan kejayaan inisiatif pengurusan keselamatan maklumat strategik.

FAKTOR PROSES

Faktor proses adalah langkah atau tindakan yang diambil untuk mencapai hasil atau matlamat keselamatan maklumat strategik. Faktor proses mempunyai elemen seperti kitar hayat maklumat, pembangunan polisi, pengurusan risiko, penilaian dan pengukuran, serta pemantauan.

Elemen 1: Kitar Hayat Maklumat

Kitar hayat maklumat dalam konteks keselamatan maklumat merujuk kepada peringkat maklumat yang dilalui dari penciptaannya hingga pelupusannya. Peringkat ini termasuk maklumat diwujud atau dikumpul, pemprosesan, penyebaran, penggunaan, penyimpanan dan pelupusan. Maklumat perlu diberi perlindungan berdasar risiko keselamatan pada setiap peringkat tersebut. Pemahaman terhadap kitar hayat maklumat dan risiko keselamatan yang berkaitan membantu organisasi membangun serta melaksana kawalan keselamatan untuk melindungi maklumat strategik. Kawalan ini merangkumi kawalan akses, penyulitan, pencegahan kehilangan data dan prosedur tindak balas insiden.

Organisasi menghadapi pelbagai cabaran dalam mengurus maklumat strategik di setiap peringkat kitar hayat. Antara cabaran yang dinyatakan oleh informan ialah jumlah maklumat yang dikumpul dan disimpan oleh organisasi sentiasa bertambah. Maka timbul kesukaran untuk menjejaki semua maklumat dan memastikan ia dilindungi dengan betul. Selain itu, Kerumitan

sistem maklumat yang digunakan oleh organisasi untuk menyimpan dan memproses maklumat menjadi semakin kompleks. Ini menjadikannya sukar untuk melaksana dan mengekalkan kawalan keselamatan yang berkesan. Informan juga menyatakan landskap ancaman yang berkembang dan organisasi perlu sentiasa mengemas kini kawalan keselamatan mereka untuk terus dilindungi daripada ancaman. Walaupun menghadapi pelbagai cabaran, adalah penting bagi organisasi untuk mengurus keselamatan maklumat di semua peringkat kitar hayat maklumat. Usaha yang dilaksana secara tidak langsung dapat membantu melindungi maklumat strategik dan mengurangkan risiko pelanggaran keselamatan.

Elemen 2: Pembangunan Polisi

Polisi keselamatan maklumat yang dibangun perlu menggabungkan keperluan bisnes organisasi, pengurusan risiko dan analisis faedah-kos. Ancaman keselamatan yang sentiasa berubah menuntut organisasi sentiasa menyemak dan mengemaskini polisi keselamatan maklumat. Maka, adalah penting supaya amalan, prosedur dan polisi keselamatan diselaras dengan operasi bisnes.

Elemen 3: Pengurusan Risiko

Pengurusan risiko secara keseluruhan ialah kemungkinan ancaman, kemungkinan kejadian ancaman berlaku dan impak yang mungkin terhadap organisasi. Hasil temu bual mendapati kumpulan strategik juga menggunakan definisi yang sama dan memahami risiko seperti yang dinyatakan di dalam kajian lepas. Risiko adalah keterukan dan berkemungkinan bergabung dengan isu keselamatan. Keselamatan maklumat ialah pelaksanaan pengurusan risiko kerana memberi keutamaan dan mengenal pasti tindakan balas yang baik.

Menurut kumpulan strategik, sektor awam mempunyai pengurusan risiko berdasarkan piawaian tertentu seperti MS ISO / IEC 27000 atau NIST. Proses pengurusan risiko yang lengkap ialah yang mana semua pihak berkepentingan bekerjasama menangani risiko keselamatan maklumat.

Informan juga menekankan bahawa tadbir urus keselamatan maklumat yang baik ialah dengan memastikan jabatan mengenal pasti risiko berkaitan, melaksana langkah keselamatan yang berkesan, dan melindungi maklumat strategik. Selain itu, adalah penting untuk memahami keselamatan maklumat secara meluas dalam konteks pengurusan risiko dan tadbir urus maklumat dalam memastikan perlindungan secara komprehensif diberi kepada maklumat strategik.

Elemen 4: Penilaian dan pengukuran

Penilaian dan pengukuran adalah penting bagi organisasi untuk memasti bahawa langkah keselamatan maklumat dan pengurusan risiko keselamatan maklumat dilaksana secara berkesan serta berobjektif.

Apabila penilaian risiko yang tepat dilaksana, organisasi berupaya mengenal pasti jurang keselamatan dan menentukan langkah seterusnya yang diperlu untuk meningkatkan tahap kematangan keselamatan maklumat. Selain itu, ia membantu organisasi mengenal pasti, menilai dan melaksana kawalan keselamatan serta memberi tumpuan kepada pencegahan kerentanan keselamatan yang dikenal pasti. Pelaksanaan langkah ini, berupaya meningkatkan

postur keselamatan organisasi dan tahap perlindungan daripada ancaman keselamatan menjadi lebih baik.

Elemen 5: Pemantauan

Pemantauan adalah untuk memasti polisi, prosedur dan kawalan dilaksana mengikut piawaian yang ditetap dan dipatuhi dalam pengurusan maklumat strategik. Pemantauan merangkumi proses pematuhan dan pemantauan tingkah laku pengguna maklumat strategik. Analisis data temu bual menunjukkan elemen ini membantu organisasi mengenal pasti kedudukan pelaksanaan polisi di dalam organisasi.

Secara keseluruhan, memantau aktiviti pengguna adalah elemen penting dalam pengurusan keselamatan maklumat yang dapat membantu organisasi mengenal pasti aktiviti yang mencuriga, menilai pelaksanaan keselamatan, meningkatkan pematuhan, menganalisis tindakan berisiko, dan membolehkan peningkatan berterusan.

KESIMPULAN

Kajian ini telah mengenal pasti faktor kejayaan kritikal dalam pelaksanaan polisi keselamatan maklumat strategik di sektor awam Malaysia. Dapatan kajian menunjukkan bahawa faktor kepimpinan dan sokongan pengurusan, faktor manusia dan organisasi, faktor persekitaran, serta faktor proses memainkan peranan penting dalam memastikan keberkesanan pelaksanaan polisi keselamatan maklumat. Faktor ini perlu ditangani secara holistik dan bersepadu untuk membangunkan kerangka yang praktikal dan berskala untuk konteks sektor awam.

Walaupun kajian ini memberikan sumbangan yang bermakna, terdapat beberapa limitasi yang perlu diambil kira. Pertama, kajian ini melibatkan 16 orang informan daripada agensi-agensi kerajaan tertentu sahaja, yang mungkin tidak mewakili keseluruhan sektor awam Malaysia secara menyeluruh. Kedua, dapatan kajian mungkin tidak dapat digeneralisasi kepada sektor swasta atau konteks negara lain memandangkan kajian ini khusus kepada konteks pentadbiran awam Malaysia. Ketiga, pendekatan kualitatif yang digunakan bergantung kepada tafsiran penyelidik, walaupun langkah-langkah seperti semakan peserta (member checking) dan triangulasi data telah dilaksanakan bagi memastikan kesahan dan kebolehpercayaan dapatan kajian.

PENGHARGAAN

Kajian ini menggunakan geran penyelidikan univesiti (GUP-2024-045).

RUJUKAN

Abidin, Norhafizah Zainal, Charli Sitinjak, Hasani Mohd Ali, Muhamad Helmi Md Said, Jady Zaidi Hassim & Rasyikah Md Khalid. 2024. Exploring the role of knowledge in social acceptance of ELV policy in Malaysia. *International Journal of Sustainable Development and Planning* 19(3): 1203.

Abohatem, Abdulkarem Yahya, Abdualmajed A.G. Al-Khulaidi & Fadl Mutaher Ba-Alwi. 2023. Suggestion cybersecurity framework (CSF) for reducing cyber-attacks on information systems.

Aflakhah, Elok & Benfano Soewito. 2023. Assessing information security using COBIT 2019 and ISO 27001:2013 for developing a mitigation plan. *International Journal of Engineering Trends and Technology* 71(10): 223.

Ahmad, Zuraini, Rabiah Ahmad & Noor Azah Samsudin. 2019. Information security policy compliance among government employees: The role of non-monetary incentives. *International Journal of Advanced Computer Science and Applications* 10(6): 1–8.

Al-Fedaghi, Sabah. 2008. A conceptual foundation for the Shannon-Weaver model of communication. *International Journal of Soft Computing* 3(1): 1–14.

Aladiyan, Anbarasu. 2025. Digital safeguards: Unravelling the complex interplay between emerging threats and proactive cyber defence strategies. *Journal of Internet Services and Information Security* 15(1): 348.

Albalas, T., Modjtahedi, A. & Abdi, R. 2022. Cybersecurity governance: A scoping review. *International Journal of Professional Business Review* 7(4): e0629.

Alfiani, Husna, Silfa Kurnia Aditya, Sofian Lusa, Dana Indra Sensuse, Prasetyo Adi Wibowo Putro & Sofiyanti Indriasari. 2024. E-government issues in developing countries using TOE and UTAUT frameworks: A systematic review. *Policy & Governance Review*. Indonesian Association for Public Administration.

AlGhamdi, Sultan, Khin Than Win & Elena Vlahu-Gjorgievska. 2020. Information security governance challenges and critical success factors: Systematic review. *Computers & Security* 99: 102030.

Alguliyev, Rasim, Yadigar İmamverdiyev, Rasim Mahmudov & Ramiz M. Aliguliyev. 2020. Information security as a national security component. *Information Security Journal: A Global Perspective* 30(1): 1.

Alhogail, Areej. 2015. Design and validation of information security culture framework. *Computers in Human Behavior* 49: 567–575.

Alhosani, Khalid Eisa Haidar Abdalla, Shamsul Kamal Ahmad Khalid, Noor Azah Samsudin, Sapiee Jamel & Kamaruddin Malik Mohamad. 2019. A policy driven, human oriented information security model: A case study in UAE banking sector. hlm. 12.

Ali, Auwal Shehu, Zarul Fitri Zaaba, Manmeet Mahinderjit Singh, Nor Badrul Anuar & Mohd Noor Mohd Shariff. 2025. Advancing cybersecurity in ASEAN: Current trends, emerging challenges, and opportunities for enhanced resilience. *International Journal of Information Security* 24(5).

Alter, Steven. 2019. Opportunities to ground, enrich, and advance IS research using work system theory. *Pacific Asia Journal of the Association for Information Systems* 11(2): 1–24.

Alzahrani, Ahmad, James Johnson & Thad Crews. 2018. Examining the relationship between information security compliance and employees perceived workload. *Journal of International Technology and Information Management* 27(2): 1–22.

Amankwa, Eric, Marianne Loock & Elmarie Kritzinger. 2017. Establishing information security policy compliance culture in organisations. *Information & Computer Security* 25(4): 452–472.

Angraini, Adhi Susilo & Okfalisa. 2020. Information security policy compliance: Systematic literature review. *International Journal of Advanced Computer Science and Applications* 11(4): 536–543.

Aurigemma, Salvatore. 2013. A composite framework for behavioral compliance with information security policies. *Journal of Organizational and End User Computing* 25(3): 32–51.

Azni, A.H., Farida Ridzuan, Sakinah Ali Pitchay, Najwa Hayaati Mohd Alwi, Maziahtusima Ishak & R. Radzali. 2024. Certificate authority capacity and digital signature market demand in promoting interoperability in Malaysia. *ITM Web of Conferences* 63: 1005.

Bauer, Stefan & Edward W.N. Bernroider. 2017. From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems* 48(3): 44–68.

Bennett, Edna. 2017. Information governance and records management. Dlm. *Encyclopedia of Library and Information Sciences*, edisi ke-4. CRC Press.

Bhuiyan, Mohammad Rakibul Islam, Md Wali Ullah, Shainjida Ahmed, Md Khokan Bhuyan, Tanzina Sultana & Al Amin. 2024. Information security for an information society for accessing secured information: A PRISMA based systematic review. *International Journal of Religion* 5(11): 932.

Bulgurcu, Burcu, Hasan Cavusoglu & Izak Benbasat. 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34(3): 523–548.

Chisty, Nur Mohammad Ali, Parikshith Reddy Baddam & Ruhul Amin. 2022. Strategic approaches to safeguarding the digital future: Insights into next-generation cybersecurity. *Engineering International* 10(2): 69.

Columbus, Louis. 2020. 2020 roundup of cybersecurity forecasts and market estimates. *Forbes*, 5 April.

Cram, W. Alec, John D'Arcy & Jeffrey G. Proudfoot. 2017. Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly* 41(2): 525–554.

D'Arcy, John, Tejaswini Herath & Mindy K. Shoss. 2014. Understanding employee responses to stressful information security requirements. *Journal of Management Information Systems* 31(2): 285–318.

Dhillon, Gurpreet, Gholamreza Torkzadeh & Jerry Chang. 2018. Strategic planning for IS security: Designing objectives. Dlm. *Lecture Notes in Computer Science*, hlm. 285. Springer Science+Business Media.

Dornheim, Peter & Rüdiger Zarnekow. 2023. Determining cybersecurity culture maturity and deriving verifiable improvement measures. *Information and Computer Security* 32(2): 179.

Engeström, Yrjö. 2000. Activity theory as a framework for analyzing and redesigning work. *Ergonomics* 43(7): 960–974.

Ervural, Beyzanur Çayır & Bilal Ervural. 2017. Overview of cyber security in the industry 4.0 era. Dlm. *Springer Series in Advanced Manufacturing*, hlm. 267. Springer International Publishing.

Figueroa, V., Luis Sánchez, Antonio Santos-Olmo, David G. Rosado & Eduardo Fernández-Medina. 2025. Building a holistic cybersecurity framework for e-government based on a systematic analysis of proposals. *International Journal of Information Security* 24(3).

Flowerday, Stephen & Tite Tuyikeze. 2016. Information security policy development and implementation: The what, how and who. *Computers & Security* 61: 169.

Ghaban, Wad. 2023. Integrated information security policy model for Saudi Arabia organizations. *Journal of Computer Science* 19(4): 454.

Halim, Haslidah & Maryati Mohd Yusof. 2019. Framework for digital data access control from internal threat in the public sector. *International Journal of Advanced Computer Science and Applications* 10(8).

Hamid, Nor Aziati Abdul, Chin Wei Liew, Nor Hazana Abdullah & Siti Sarah Omar. 2019. The role of information technology human capability in the implementation of information technology governance (ITG): A systematic literature review on Malaysian organizations. *Advances in Science Technology and Engineering Systems Journal* 4(4): 314.

Jha, Amaresh & Ananya Jha. 2024. Securing tomorrow's urban frontiers: A holistic approach to cybersecurity in smart cities. *Information System and Smart City* 3(1).

Kamil, Yasmin, Sofia Lund & M. Sirajul Islam. 2023. Information security objectives and the output legitimacy of ISO/IEC 27001: Stakeholders' perspective on expectations in private organizations in Sweden. *Information Systems and E-Business Management* 21(3): 699.

Khadka, Kalam & Abu Barkat Ullah. 2025. Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security* 24(3).

Kolkowska, Ella, Fredrik Karlsson & Karin Hedström. 2017. Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method. *Journal of Strategic Information Systems* 26(1): 39–76.

Koohang, Alex, Alojzy Z. Nowak, Joanna Paliszkiewicz & Jeretta Horn Nord. 2019. Information security policy compliance: Leadership, trust, role values, and awareness. *Journal of Computer Information Systems* 60(1): 1.

Kooper, M., Rik Maes & E.E.O. Roos Lindgreen. 2010. On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management* 31(3): 195.

Kovács, László, András Nemeslaki, Ákos Orbók & A. Szabo. 2017. Structuration theory and strategic alignment in information security management: Introduction of a comprehensive research approach and program. *Academic and Applied Research in Military and Public Management Science* 16(1): 5.

Masrek, Mohamad Noorman, Tri Soesantari, Asad Khan & Aang Kisnu Dermawan. 2021. Examining the relationship between information security effectiveness and information security threats. *International Journal of Business and Society* 21(3): 1203.

Maynard, Sean B., Ahmad Mohmood & Atif Ahmad. 2018. Reconceptualising information security strategy to reduce the impact of cyber attacks: A practical approach. *Journal of the Australian Institute of Professional Intelligence Officers* 26(1): 3–22.

Mishra, Alok, Yehia Ibrahim Alzoubi, Memoona J. Anwar & Asif Qumer Gill. 2022. Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers & Security* 120: 102820.

Mojir, Kayvan Yousefi. 2018. Information systems development for emerging public sector cross-sector collaborations: The case of Swedish emergency response.

Moody, Gregory D., Mikko Siponen & Seppo Pahnila. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly* 42(1): 285–311.

Munusamy, Thavaselvi & Touraj Khodadi. 2023. Building cyber resilience: Key factors for enhancing organizational cyber security. *Journal of Informatics and Web Engineering* 2(2): 59.

National Institute of Standards and Technology. 2018. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*.

Noguerra, Crispin P. 2023. Ethical and legal challenges in information system development and implementation. *International Journal of Advanced Research in Science Communication and Technology*, Julai, hlm. 852.

Nyakasoka, Lawrence & Rennie Naidoo. 2024. Understanding the inertial forces impeding dynamic cybersecurity learning capabilities. *South African Computer Journal* 36(1).

Obiokafor, Ifeyinwa Nkemdilim & Ogochukwu Mbonu. 2025. The intersection of digital policy and cybersecurity: Implications for sustainable development. *World Journal of Advanced Engineering Technology and Sciences* 14(3): 77.

Ording, Lovisa Göransson, Shang Gao & Weifeng Chen. 2022. The influence of inputs in the information security policy development: An institutional perspective. *Transforming Government: People, Process and Policy* 16(4): 418.

Palanisamy, Ravi, Alaa Nour Mohammad & Muneeb Ahmad. 2020. Challenges in information security implementation in government organisations. *Journal of Global Information Management* 28(1): 1–24.

Perumal, Sundresan, Sakinah Ali Pitchay, Ganthan Narayana Samy, Bharanidharan Shanmugam, Pritheega Magalingam & Sameer Hasan Albakri. 2018. Transformative cyber security model for Malaysian government agencies. *International Journal of Engineering & Technology* 7: 87.

Pigola, Angélica & Fernando de Souza Meirelles. 2025. Zero trust in cybersecurity: Managing critical challenges for effective implementation. *Journal of Systems and Information Technology* 27(4): 517.

Pollini, Alessandro, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi & Davide Guerri. 2021. Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition Technology & Work* 24(2): 371.

Ramli, Nor Syafiqah Ahmad & Nor Aishah Mohd Ali. 2024. Integrating technology in government internal audit: Catalysts and challenges. *Information Management and Business Review* 16: 124.

Razak, Rosida Ab & Mohamad Shanudin Zakaria. 2017. The information and communication technology governance maturity level for Malaysian public sector. hlm. 1.

Rostami, Elham, Fredrik Karlsson & Shang Gao. 2023. Policy components – a conceptual model for modularizing and tailoring of information security policies. *Information and Computer Security* 31(3): 331.

Sabtu, Saiful Bahari Mohd & Kamaruddin Malik Mohamad. 2020. Critical information infrastructure protection requirement for the Malaysian public sector. Dlm. *Advances in Intelligent Systems and Computing*, hlm. 371. Springer Nature.

Salminen, Minna & Syed Masum Hossain. 2018. A systematic review of cognitive biases in cybersecurity and online privacy decisions. *Computers & Security* 78: 402–421.

Samonas, Spyridon, Gurpreet Dhillon & Ahlam Almusharraf. 2019. Stakeholder perceptions of information security policy: Analyzing personal constructs. *International Journal of Information Management* 50: 144.

Saydazimova, Umida, Kim Yun Hoe, Durdona Ergasheva, Won Soon Jae, Jung Jae Yeon, Kim Lina & S.A. Nazarova. 2025. Cybersecurity threat models and linguistic-pedagogical approaches in Korean critical infrastructure education. *Journal of Internet Services and Information Security* 15(2): 285.

Schinagl, Stef & A. Shahim. 2020. What do we know about information security governance? *Information and Computer Security* 28(2): 261.

Schneider, G. 2025. The importance of cybersecurity in digital government implementations. *COGNITIONIS Scientific Journal* 8(1).

Serna, Carlos Andres Agudelo. 2023. Mitigating the risk of knowledge leakage in knowledge intensive organizations: A mobile device perspective. *arXiv (Cornell University)*, Ogos.

Shaw, Karan & Vidyavati Ramteke. 2023. Importance of information technology governance in modern business environment. *AIP Conference Proceedings* 2613: 20102.

Silverman, David J. 2013. *Doing Qualitative Research: A Practical Handbook*. Edisi ke-4. London: SAGE Publishing.

Smallwood, Robert F. 2018. Information governance principles. Dlm. *Productivity Press eBooks*, hlm. 19.

Sparrius, Martin, Moufida Sadok & Peter Bednár. 2021. What can we learn from the analysis of information security policies? The case of UK's schools. Dlm. *IFIP Advances in Information and Communication Technology*, hlm. 81. Springer Science+Business Media.

Toit, Tiny du, Hennie Kruger, Lynette Drevin & Nicolaas Maree. 2022. Deep learning affective computing to elicit sentiment towards information security policies. *Advances in Science Technology and Engineering Systems Journal* 7(3): 152.

Tolah, Alaa, Steven Furnell & Maria Papadaki. 2019. A comprehensive framework for understanding security culture in organizations. Dlm. *IFIP Advances in Information and Communication Technology*, hlm. 143. Springer Science+Business Media.

Topa, Ioanna-Aikaterini & Maria Karyda. 2025. Addressing organisational, individual and technological aspects and challenges in information security management: Applying a framework in workplace and teleworking. *Organizational Cybersecurity Journal: Practice, Process and People*, Jun.

Van Bavel, Rene, Nuria Rodriguez-Priego, Jose Vila & Pere Escobar. 2019. Using protection motivation theory in the design of nudges to improve online security behaviour. *Computers & Security* 82: 168–185.

Vance, Anthony & Mikko Siponen. 2012. IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing* 24(1): 21–41.

Wiafe, Isaac, Felix Nti Koranteng, Abigail Wiafe, Emmanuel Nyarko Obeng & Winfred Yaokumah. 2020. The role of norms in information security policy compliance. *Information and Computer Security* 28(5): 743.

Wong, Chee Kong. 2023. A process model to improve information security governance in organisations. *arXiv (Cornell University)*.

Yuliana, Rika & Zainal Arifin Hasibuan. 2022. Best practice framework for information technology security governance in Indonesian government. *International Journal of Electrical and Computer Engineering* 12(6): 6522.

Yulianto, Semi, Benfano Soewito, Ford Lumban Gaol & Aditya Kurniawan. 2024. The crucial role of red teaming: Strengthening Indonesia's cyber defenses through cybersecurity drill tests. *International Journal of Safety and Security Engineering* 14(4): 1231.

Zairul, Mohd Nizam. 2021. A thematic review on student-centred learning in the studio education. *Journal of Cleaner Production* 309: 127718.