bidang
TEKNIK

ANCAMAN KESELAMATAN INTERNET SEBAGAI ISU UTAMA NEGARA: ISU-ISU KONTEMPORARI, PENDEKATAN, DAN PENYELESAIAN

OEMAR HAMDAN, ABD.MANAF ISMAIL
Kolej Undang-Undang, Kerajaan & Pengajian Antarabangsa
Universiti Utara Malaysia

Isu keselamatan siber merupakan isu utama masa kini yang mendapat perhatian dari pelbagai pihak termasuklah pengguna individu, masyarakat, pihak Kerajaan, organisasi perniagaan, dan sebagainya. Isu ini seakan tidak ada penyelesaian lantaran ancaman berterusan seperti serangan pengodam terhadap komputer masih berlaku, malah di sesetengah negara is agak membimbangkan. Untuk itu, kertas kerja ini membincangkan sorotan kajian berkaitan isu-isu keselamatan siber termasuklah di Malaysia. Secara khususnya, kod profesional ICT akan dibincangkan untuk melihat sejauhmanakah ianya berkesan dalam membendung permasalahan ini. Kertas kerja ini juga mengupas pendekatan berasaskan ICT yakni sejauhmanakah pendekatan ini berupaya menangani permasalahan berkenaan. Akhir sekali, cadangan untuk mempertingkatkan kesedaran terhadap bahaya ancaman ini adalah penting agar para pengguna peka terhadap sebarang amaran mengenai ancaman siber.

PENDAHULUAN

Secara umumnya, strategi pembangunan dan perkembangan organisasi korporat masa kini amat bergantung kepada Teknologi Maklumat dan Komunikasi (ICT) untuk meningkatkan produktiviti, keupayaan perniagaan, mempertingkatkan daya saing, serta menggalakkan perkembangan aktiviti perniagaan baru secara dalam talian. Dalam pada itu, didapati bahawa hamper di seluruh dunia tumpuan diberikan kepada meningkatkan keyakinan dalam urusniaga berasaskan platform elektronik, membangun sumber manusia, merapatkan jurang digital serta mewujudkan peluang dan aktiviti perniagaan baru. Dalam usaha memastikan kejayaan perniagaan berteraskan penggtmaan ICT, keyakinan pengguna juga hams dititikberatkan khususnya sebagai pihak utama dalam pasaran barangan secara dalam talian. Namun demikian, kemajuan ICT turut diiringi oleh isu serangan siber sekaligus mencetus satu polimik terhadap keselamatan siber. Nurharyani (2006) menjelaskan bahawa dominasi dan pertumbuhan pesat ICT telah menjadikan serangan siber sebagai satu bentuk senjata yang `menarik dan berkesan' untuk digunakan ke atas sesebuah negara. Ini adalah kerana kosnya yang murah berbanding dengan kos yang diperlukan untuk pembangunan, penyelengaraan serta penggunaan keupayaan ketenteraan yang canggih. Apa yang diperlukan hanyalah, usaha yang minima iaitu merekrut agen atau pengintip yang berkebolehan mencipta maklumat palsu, memanipulasi maklumat atau melancarkan kod merbahaya *(malicious code)* ke atas sesebuah sistem maklumat yang dihubungkan melalui prasarana telekomunikasi yang dikongsi secara global.

Madon (2000) menganggarkan bilangan pengguna laman web seluruh dunia dianggarkan sekitar 200 milion pada tahun 2005 dan dijangka terns meningkat kepada 250 milion (2006), 290 milion (2007) dan 350 milion (2008). Namun demikian, perangkaan yang diberikan oleh Madon tersebut adalah berdasarkan teknologi Internet berwayar semata-mata dan tidak mengambilkira perkembangan kontemposari dalam Internet global. Ini kerana, pengenalan alatan teknologi tanpa wayar seperti Internet tanpa wayar, protokol aplikasi tanpa wayar (WAP), Internet Protokol V6 (IPv6), telefon berasaskan web, anjakan teknologi 2G kepada 3G, dan sebagainya sebenarnya menyebabkan bilangan pengguna yang akses laman web akan menjadi lebih besar. Rasionalnya, teknologi tanpa wayar akan memudahkan para pengguna untuk mengakses dan melayari laman web. Pada masa kini pula wujudnya peranti elektronik mudahalih seperti telefon bimbit, jam tangan, personel digital assistant (PDA), dan sebagainya yang menyediakan browser kepada penguna untuk akses kepada Internet dan situasi ini pastinya mempertingkatkan jumlah pengunjung laman web pada masa hadapan. Lantaran itu, serangan siber juga telah memasuki episod baru di mana serangan boleh dilancarkan melalui mana-mana peranti atau rangkaian sedia ada.

Malaysia telah menyedari tentang peri pentingnya keselamatan ICT negara terutama jika Malaysia berhasrat untuk bersaing dengan negara-negara maju yang lain. Pada April 2001, Malaysia telah membentuk sebuah agensi pemantauan keselamatan berkaitan teknologi maklumat dan komunikasi (ICT) bagi menangani masalah insiden-insiden keselamatan ICT negara. Penubuhan Pusat Respons Kecemasan dan Keselamatan ICT Kebangsaan (NISER) telah dipersetujui oleh Majlis Teknologi Maklumat Negara (NITC) sejak Januari 1998. Penyediaan perkhidmatan keselamatan oleh NISER dijalankan dengan usaha sama lain-lain agensi kerajaan, sektor swasta, masyarakat dan orang perseorangan. Isu keselamatan ICT bukan sahaja mendapat perhatian serius Malaysia malah negara-negara ASEAN turut memberilcan perhatian terhadap isu ini. Negara-negara ASEAN telah mengumumkan rancangan untuk berkongsi maklumat dalam keselamatan komputer serta membentuk unit jenayah siber menjelang tahun 2005. Sebagai langkah permulaan setiap negara ASEAN akan membentuk Pasukan Respon Kecemasan Komputer (CERT) mereka sendiri. Dengan adanya pasukan ini perkongsian maldumat dijangka dapat dijalankan dengan lebih mudah dan efektif Rancangan kerjasama tersebut diharap akan diperluaslcan ke seluruh rantau Asia dan juga turut disertai diperingkat Asia Pasifik dan global. Di Malaysia misalnya, Menteri Tenaga, Telekomunikasi dan Multimedia, Datuk Amar Leo Moggie telah mengajak rakyat Malaysia ke arah kesedaran bagi menggunakan Internet untuk tujuan baik. Beliau juga telah mencadangkan supaya sistem penapisan Internet digunakan secara meluas termasuk dalam bidang pendidikan dan juga korporat (Utusan Malaysia, 1999). Penggunaan sistem ini bertujuan untuk mewujudkan satu persekitaran penggunaan sumber Internet yang bersih dan segala unsur negatif.

SOROTAN TERHADAP ISU KESELAMATAN SIBER

Ancatnan siber sering berlaku apabila media dan ICT disalahgunakan sebagai platform sama ada secara langsung atau tidak langsung untuk melaksanakan aktiviti subedit' yang boleh menyebabkan gangguan atau kerosakan sama ada secara sengaja atau tidak kepada mangsa atau para pengguna. Haryani (2006) menjelaskan bahawa ancaman siber juga merupakan ancaman yang mana kesan sebenar ancaman banyak bergantung kepada nilai maklumat dan prasarana maklumat yang dijadikan sasaran oleh penjenayah siber untuk mengeksploitasikan kelemahan *(loopholes)* yang wujud. Apa yang pasti ialah keganasan siber masa kini mampu merebak dengan sangat pantas tanpa mengira sempadan lc.awasan. Kesan yang wujud akibat ancaman siber ini sebenarnya lebih buruk padahnya daripada apa yang jangkakan dan tahap keseriusan ancaman berbeza-beza dan amat bergantung kepada tahap

penggunaan infrastruktur dan kesedaran tentang peri pentingnya perlindungan terhadap ICT negara. Internal Auditor (1996) mendedahkan satu kajian yang dijalankan oleh CSI, 41% responden menyatakan ia pemah menceroboh atau menggunakan sistem komputer tanpa keizinan dalam tempoh 12 bulan, lebih 50 % sektor korporat Amerika Syarikat adalah mangsa serangan pencerobohan. Tambahan pula lebih 50% tiada polisi bertulis yang menerangkan bagaimana menghadapi pencerobohan rangkaian komputer, lebih 20% yang tidak tahu sistem komputernya telah dicerobohi, dan hanya 17% sahaja yang menggunakan khidmat pertmdangan jika menyedari menjadi mangsa. Selain itu, 70% rospendon menyatakan pencerobohan tidak dilaporkan kepada pihak berkuasa kerana khuatir ia akan menjejaskan reputasi organisasi.

Menurut satu kajian yang dijalankan oleh CSI, 41% responden menyatakan ia pemah menceroboh atau menggunakan sistem komputer tanpa keizinan dalam tempoh 12 bulan, lebih 50 % sektor korporat Amerika Syarikat adalah mangsa serangan pencerobohan. Tambahan pula lebih 50% tiada polisi bertulis yang menerangkan bagaimana menghadapi pencerobohan rangkaian komputer, lebih 20% yang tidak tahu sistem komputernya telah dicerobohi, dan hanya 17% sahaja yang menggunakan khidmat perundangan jika menyedari menjadi mangsa. Selain itu, 70% rospendon menyatakan pencerobohan tidak dilaporkan kepada pihak berkuasa kerana khuatir ia akan menjejaskan reputasi organisasi (Internal Auditor, 1996). Hingga kini, kesna daripada ancaman siber ini telah berlaku secara berterusan walaupun pelbagai irtisiatif telah dilaksanakan bagi menanganinya.

Menurut Dr. Seah Boon Keong, Ketua Pembangunan dan Penyejidikan MSC Trustgate.com, ancaman siber masih berleluasa kerana kebanyakan syarikat masih mengamalkan dasar keselamatan yang lemah atau tidak mempunyai langsung dasar atau polisi keselamatan ICT di syarikat mereka. Untuk itu, polisi keselamatan ICT syarikat juga merupakan elemen penting dalam memastikan ancaman siber ini dapat dibanteras. Ini kerana Polisi keselamatan ICT menyenaraikan prosedur dan pelan tindakan keselamatan yang harus dilakukan dan pihak yang bertanggungjawab yang boleh dihubungi sekiranya sesuatu ancaman berlaku di samping turut menggariskan pelbagai panduan yang boleh dijadikan rujukan oleh pekerja di sesebuah organisasi. Pendek kata, polisi ini perlu didedahkan kepada semua pekerja syarikat agar mereka faham dan melaksanakan apa yang terkandung dalam polisi tersebut (Haryani, 2006).

Punca kepada tercetusnya masalah ini juga menimbulkan persoalan kepada para akademik. Misalnya, pada tahun 1994, kebimbangan terhadap bahan-bahan tidak sesuai untuk pelajar dan remaja yang mudah didapati di Internet telah mendapat perhatian umum terutama di Amerika sepertiamna pandangan Turow (1999). Dalam satu bancian oleh USA Today/CNN pada bulan Mei 1999, didapati 65% remaja mengatakan internet merupakan antara penyumbang kepada terjadinya keganasan seperti yang berlaku di Littleton, Colorado. Dalam kejadian itu, dua pelajar remaja berusia 18 dan 17 tahun telah menembak mati 13 orang pelajar dan seorang guru di sekolah mereka. Bureau of Alcohol, Tobacco and Firearms, agen pusat Amerika Syarikat telah mengenalpasti sekurang-kurangnya 30 kejadian bom dan 4 cubaan mengebom antara 1985 dan Jun 1996 berlaku kerana golongan yang disyaki telah mendapatkan literasi membuat born dari Internet. Dalam bulan Februari 1996, tiga pelajar sekolah tinggi di Syracuse, New York telah dituduh atas kesalahan membuat bom buatan sendiri berdasarkan plan yang mereka perolehi dari Internet.

Dalam pada itu, keselamatan merupakan satu isu penting bagi sesuatu sistem perdagangan dalam talian dan menurut Pfleeger (1997), keselamatan sesuatu sistem komputer meli-

batkan penyelenggaraan tiga ciri utama iaitu Kerahsiaan, Keutuhan, dan Ketersediaan. Manakala, Nurharyani (2006) menjelaskan bahawa kebanyakan komputer hari ini mempunyai sambungan ke Internet, maka tidak hairanlah jika kadar jenayah siber semakin meningkat setiap tahun. Ini adalah kerana Internet merupakan satu tempat yang bersifat terbuka dan di atas faktor tersebut, maka para penjenayah siber dikatakan agak `bebas' untuk melakukan aktiviti-aktiviti seperti menyebarkan virus, melakukan penggodaman *(hacking)* dan juga mencuri data untuk tujuan risikan pemiagaan atau kerajaan. Jenayah-jenayah ini ternyata tidak boleh dipandang ringan dan perlu dibanteras dengan secepat mungkin. Ini dapat dibuktikan pada tahun 2003 dimana Malaysia telah dianggarkan mengalami kerugian sejumlah RM 31 juta disebabkan oleh serangan virus. Virus yang telah menyerang itu dikenal pasti sebagai Blaster, Nachi dan Sobig-F.

Dalam pada itu, bilangan pengguna laman web seluruh dunia dijangka taus meningkat dari tahun ketahun dan berdasarkan pengangkaan daripada beberapa pembekal perkhidmatan Internet (ISP) penting dunia, didapati bahawa terdapat empat aplikasi berasaskan web iaitu *web/digital media properties,* laman web (biasa), laman web pendidikan, dan laman web kerajaan yang penting. Secara keseluruhannya, pengguna web/digital media properties merupakan segmen terbesar iaitu keseluruhan berjumlah 194.63 juta dan diikuti oleh segmen pengguna laman web (145.63 juta), laman web kerajaan (8.79 juta) dan segmen pengguna laman web pendidikan (6.68 juta). (http://exportit.ita.doc.gov). Sebagai natijahnya, sekiranya serangan ini tidka ditangani dengan baik sudah tentu kerugian yang besra bakal dialami oleh pelbagai pihak termasuklah pengguna persendiriaan, sektor perniagaan dan perbankan, kerajaan dan sebagainya.

Malaysia telah menyedari tentang pen pentingnya keselamatan ICT negara terutama jika Malaysia berhasrat untuk bersaing dengan negara-negara maju yang lain. Pada April 2001, Malaysia telah membentuk sebuah agensi pemantauan keselamatan berkaitan teknologi maklumat dan komunikasi (ICT) bagi menangani masalah insiden-insiden keselamatan ICT negara. Penubuhan Pusat Respons Kecemasan dan Keselamatan ICT Kebangsaan (NISER) telah dipersetujui oleh Majlis Teknologi Maklumat Negara (NITC) sejak Januari 1998. Penyediaan perkhidmatan keselamatan oleh NISER dijalankan dengan usaha sama lain-lain agensi kerajaan, sektor swasta, masyarakat dan orang perseorangan (Nurharyani, 2006). Secara asasnya, NISER bertanggungjawab ke atas lima bidang kerja yang utama dalam kerangka keslamatan ICT di Malaysia, iaitu mengekalkan kemahiran teknikal dalam bidang keselamatan; bergerak dan bertindak secara pro-aktif; menjalinkan usaha-usaha sama; menjadi badan yang bebas dan berkecuali; dan serta tidak mengambil keuntungan. NISER turut memberikan perkhidmatan-perkhidmatan seperti reaksi terhadap insiden yang membabitkan keselamatan ICT, penilaian teknologi dan penyelidikan, akulturasi, insurans keselamatan, pembangunan polisi keselamatan dan seketeriat serta perkhidmatan pakar. Selain itu, MyCERT di bawah naungan MIMOS merupakan pasukan yang bertanggungjawab ke atas insiden keselamatan ICT negara. Namun demikian, MyCERT kini telah diserapkan di bawah NISER yang nyata mempunyai organisasi dan wawasan kerja yang lebih komprehensif Jadi, persediaan flan keseriusan Malaysia dalam isu keselamatan merupakan inisiatif bersungguh bagi menjamin pemiagaan dan aktiviti dalam talian sentiasa dilindungi dari sebarang ancaman siber.

Terdapat kes-kes yang melibatkan jenayah siber berlaku di Malaysia seperti penyalahgtmaan kemudahan perbankan Internet, pencerobohan *(hacking),* menjual maklumat dan sebagainya. Antara bentuk-bentuk ancaman siber yang popular adalah seperti

aktiviti pencerobohan *(intrusion activity),* capaian yang tidak sah *(unauthorized access),* serangan DoS *(Denial of Service Attack),* serangan virus, trojan dan cecacing *(worm)* dan tidak kurang juga serangan yang disebabkan oleh penggodam *(hackers)* komputer itu sendiri sama ada untuk tujuan peribadi atau lain-lain tujuan. Ancaman-ancaman siber ini mungkin dilakukan secara berasingan atau mungkin juga boleh dilancarkan secara gabungan dan serentak. Contohnya, aktiviti pencerobohan *(intrusion activity)* yang dilakukan ke atas sistem maklumat sesebuah organisasi boleh menyebabkan capaian yang tidak sah dilakukan oleh pihak luar yang tidak bertanggungjawab. Apabila ini berlaku, kerahsiaan maklumat syarikat atau organisasi sudah tidak dapat dilindungi. Ini sangat merbahaya kepada sesebuah syarikat sekiranya maklumat rahsia syarikat berada di tangan pihak pesaing yang mana sudah tentu syarikat bakal mengalami kerugian yang besar dan turut kehilangan peluang perniagaan. Dalam pada itu, serangan virus dan cecacing (*worm*) turut menduduki tangga teratas dalam senarai bentuk ancaman siber yang agak popular. Walaupun serangan tersebut kedengaran biasa bagi kita, namun kesan yang terpaksa ditanggung adalah luar daripada jangkaan kita. Sebagai contoh cecacing (*worm*) *Code Red* telah melancarkan serangannya pada tanggal 18 Jun 2001. Serangan ini memfokus kepada komputer pelayan (*server computer)* berjenis Microsoft yang tidak mempunyai kod aturcara keselamatan (*security coding patches*) yang terkini. Walaupun pihak Microsoft telah mengeluarkan kod aturcara keselamatan (*security coding patches*), namun ramai dikalangan pentadbir sistem (system administrator) yang tidak mengemaskini kod tersebut. Akibatnya, ia telah memberi peluang kepada penjenayah siber untuk melancarkan serangan cecacing (worm) yang seterusnya iaitu *Code Red II*, diikuti dengan *Code Red III* dan *Nimba*. (Nurharyani, 2006).

Antara bentuk-bentuk ancaman siber yang popular adalah seperti aktiviti pencerobohan (*intrusion activity*), capaian yang tidak sah (*unauthorized access*), serangan DoS (*Denial of Service Attack*), serangan virus, trojan dan cecacing (*worm*) dan tidak kurang juga serangan yang disebabkan oleh penggodam (*hackers*) komputer itu sendiri sama ada untuk tujuan peribadi atau lain-lain tujuan. Ancaman-ancaman siber ini mungkin dilakukan secara berasingan atau mungkin juga boleh dilancarkan secara gabungan dan serentak. Contohnya, aktiviti pencerobohan (intrusion activity) yang dilakukan ke atas sistem maklumat sesebuah organisasi boleh menyebabkan capaian yang tidak sah dilakukan oleh pihak luar yang tidak bertanggungjawab. Apabila ini berlaku, kerahsiaan maklumat syarikat atau organisasi sudah tidak dapat dilindungi. Ini sangat merbahaya kepada sesebuah syarikat sekiranya maklumat rahsia syarikat berada di tangan pihak pesaing yang mana sudah tentu syarikat bakal mengalami kerugian yang besar dan turut kehilangan peluang perniagaan.

Selain daripada bentuk ancaman siber yang dinyatakan di atas, serangan virus dan cecacing (*worm*) turut menduduki tangga teratas dalam senarai bentuk ancaman siber yang agak popular. Walaupun serangan tersebut kedengaran biasa bagi kita, namun kesan yang terpaksa ditanggung adalah luar daripada jangkaan kita. Sebagai contoh cecacing (*worm*) *Code Red* telah melancarkan serangannya pada tanggal 18 Jun 2001. Serangan ini memfokus kepada komputer pelayan (*server computer*) berjenis Microsoft yang tidak mempunyai kod aturcara keselamatan (security coding patches) yang terkini. Walaupun pihak Microsoft telah mengeluarkan kod aturcara keselamatan (*security coding patches*), namun ramai dikalangan pentadbir sistem (*system administrator*) yang tidak mengemaskini kod tersebut. Akibatnya, ia telah memberi peluang kepada penjenayah siber untuk melancarkan serangan cecacing (worm) yang seterusnya iaitu *Code Red II*, diikuti dengan *Code Red III* dan *Nimba.*

kepesatan teknologi terutama lebuhraya maklumat, perlindungan maklumat sulit dan sangat penting semakin menjadi kritikal. Ia memerlukan suatu jaminan terhadap sesuatu produk atau sistem yang digunakan, yang menyediakan keselamatan yang kukuh untuk memenuhi objektif keselamatan yang dimulai oleh "Orange Book"-TCSEC pada tahun 1985 di Amerika Syarikat. Dan sini maka lahirlah pelbagai inisitiatif negara-negara tertentu untuk pembangunan penilaian kriteria polisi keselamatan maklumat mereka sendiri untuk menandingi TCSEC seperti di Eropah-ITSEC (1991), Canada-CTCPEC(1993), US-Federal Criteria (Draft 1993) dan 'The Common Criteria-ISO/IEC 15408 — Evaluation Criteria for Information Technology Security' yang digunakan di dalam pembangunan kriteria penilaian keselamatan teknologi maldumat yang digunakan di dalam komuniti antarabangsa (Mazrifirdaus, 2006).

Penubuhan piawaian *(standard)* keselamatan ICT juga merupakan satu perkara yang penting dan harus diperkukuhkan pada masa akan datang. Perkembangan ICT yang mendorong pelbagai maklumat perlu disimpan dengan kaedah terbaik tentunya memerlukan piawaian (standard) yang boleh diikuti oleh syarikat-syarikat dalam menjamin keselamatan maklumat tersebut. Misalnya, di Malaysia, bagi memberi peluang kepada syarikat tempatan melaksanakan kaedah perlindungan data terbaik, SIRIM Berhad telah memperkenalkan sijil bagi mencapai paiwaian *(standard)* tersebut. Paiwaian *(standard)* yang dikenali sebagai Pengurusan Keselamatan Maklumat berasaskan paiwaian BS7799 *(British Standard)* tersebut dikendalikan oleh anak syarikat SIRIM iaitu SIRIM QAS secara percubaan dengan kerjasama NISER. Untuk itu, Mazrifirdaus (2006) menjelaskan bahawa terdapat beberapa piawaian polisi keselamatan maklumat yang diterima pakai di peringkat antarabangsa seperti British Standard 17799 dan ISO 7799, Orange Book Standards, White Book Standard, Green Book, dan Australian Standard dan standard ini seringkali dipertingkatkan berikutan meningkatnya ancaman serangan siber. Namun demikian, kajian mengenai keberkesanan piawai ini masih perlu dilakukan kerana pars pengodam mempunyai latar belakang yanag berbeza.

KOD PROFESIONAL ICT

Secara umumnya, profesional ICT adalah merujuk kepada sumber manusia yang mempunyai imej profesional sepertimana tenaga pakar dalam jurusan lain seperti kedoktoran, kehakiman, keguaman, kejuruteraan, dan sebagainya. Namun demikian, latihan dan perlesenan profesional terhadap tenaga pakar mempunyai kesan tertentu kepada masyarakat (Gleason, 2004). Tavani (2004) mendefinisikan profesional sebagai seseorang yang memerlukan latihan lanjutan dan memiliki pengalaman berkaitan dengan sesuatu bidang. Profesional juga merupakan individu yang mempraktikkan *discretion and judgment* semasa atau sepanjang masa bekerja. Biasanya, kandungan kerja golongan ini tidak boleh dipiawaikan. Dengan ini, profesional dirumuskan sebagai seorang yang berpengetahuan tinggi dan berpengalaman dalam pengendalian sesuatu kerja di samping mempraktikkan amalan sebagai seorang profesional dalam konteks sebenar persekitaran kerja harian. Hakikatnya, majoriti individu yang terlibat dengan serangan siber adalah terdiri daripada kumpulan profesional ICT sama ada berdaftar dengan pertubuhan ICT ataupun tidak.

Standard pengendalian perkhidmatan ICT oleh profesional ICT adalah melibatkan beberapa perkara utama. Menurut Hogg (2002), perkara-perkara berkaitan dengan standard pengendalian ialah kepentingan awam, integriti, kesulitan *(confidentiality),* keobjektifan dan kebebasan, *competence, keeping up-to-date, subordinates,* bertanggungjawab terhadap pelanggan (pihak berkepentingan), mempromosikan IT dan imej profesion, dan kepentingan masyarakat. Dengan memahami keperluan atau pertimbangan ini, maka seseorang profesional ICT dapat meningkatkan status

Manakala, Ariffudin Aizuddin (2001) pula berpendapat bahawa dengan peningkatan pencerobohan sistem keselamatan dan profesion IT. Pematuhan terhadap standard pengendalian tersebut juga berperanan melindungi merit profesional *(professional merits)* seseorang profesional ICT secara berterusan dalam konteks persekitaran sebenar masyarakat. Sungguhpun demikian, wujud persoalan sejauhmanakah konsep profesional ICT dapat membendung permasalahan berkaitan serangan siber.

Apabila perbincangan mengenai standard pengendalian profesional ICT dilakukan, maka kod pengendalian profesional IT adalah dirujuk. Secara umumnya, kod etika profesional IT menurut Hamelink (2000) menjelaskan bahawa seseorang profesional perlu bekerja dengan *competence and integrity* serta tidak melalculcan perkara-perkara yang boleh menjejaskan reputasi sebagai seorang profesional. Pada masa yang sama, profesional ICT perlu mengambilkira pertimbangan -pertimbangan tertentu dan kesan-kesan sosial yang bakal berlaku yang berkaitrapat dengan perkhidmatan ICT. Di samping itu, profesional ICT perlu membekalkan masyarakat dengan maklumat yang mencukupi mengenai teknologi komputer. Namun demikian, hingga kini masih belum ada kajian yang membuktikan bahawa kod profesional ICT dapat membendung masalah berkaitan serangan siber.

Kod Profesional IT mempunyai berperanan penting dalam pengendalian perkhidmatan ICT. Peranan utama ialah sebagai *formal expression* mengenai jangkaan dan keperluan terhadap pengendalian ICT di kalangan ahli-ahli profesional dan ianya diiktiraf dan digunapakai oleh organisasi profesional. Selain itu, kod profesional juga berperanan menghubungkan secara langsung seseorang profesional dengan peraturan pengendalian dan amalan IT sekaligus berperanan menggariskan ciri-ciri seseorang profesional ICT. Kod ini bukan sahaja bertindak sebagai panduan berguna kepada profesional ICT malahan juga penting kepada masyarakat. Ini kerana, masyarakat akan mengetahui standard pengendalian ICT dan hak-hak mereka sebagai pengguna atau pelanggan ICT. Namun demikian, persoalannya adakah masyarakat sedar akan bahaya ancaman siber?

Terdapat beberapa kod pengendalian profesional IT yang terkemuka dan diasaskan oleh badan profesional antarabangsa. Antara badan atau institusi yang telah mengasaskan kod pengendalian 1CT ialah *Association for Computing Machinery* (ACM), *Association of Information Technology Professionals* (AITP), dan *Computer Society of the Institute of Electrical and Electronics Engineers* (IEEE-CS). IEEE dan ACM misalnya telah mengasaskan *IEEEüAC Code of Professional Conduct* dan *BCS Code of Professional Conduct.* Walau bagaimanapun, kod pengendalian IT di antara negara adalah unik dan is diasaskan dengan mengambilkira pertimbangan terhadap faktor-faktor ekonomi, sosial, pentadbiran dan teknologi di sesebuah negara. Jadi, setiap negara dikatakan memiliki (akan memiliki bagi negara yang belum ada) dan menggunakan kod pengendalian profesional ICT masing-masing bersama dengan kod profesional ICT antarabangsa yang diasaskan oleh badan atau institusi antarabangsa. Namun demikian, masih terdapat *hacker* (pengodam) yang tidak mendaftar di mana-mana pertubuhan professional ICT sekaligus menyebabkan kod ini tidka efektif ke atas mereka.

Di negara Australia misalnya, *Australian Computer Society* telah mengasaskan tiga kod penting berkaitan profesional ICT iaitu kod etika, kod pengendalian profesional, dan kod amalan profesional. Ketiga-tiga kod ini adalah penting apabila membincangkan mengenai pengendalian ICT secara profesional. Ketiga-tiga kod ini bukan sahaja berperanan melindungi syarikat, pengguna, dan masyarakat Australia, malahan juga berupaya mewujudkan perkembangan positif dalam persekitaran industri ICT (Hogg, 2002). Kod etika secara umumnya bertujuan untuk

melindungi pengguna daripada aktiviti yang kurang beretika. Antara aktiviti yang kurang beretika menurut Hogg (2002) ialah cetak rompak perisian, *invasion of privacy,* dan *hacking* dan perbuatan yang memberikan kesan negatif kepada pelbagai pihak kepentingan. Jadi, tanggungjawab sosial dan integriti merupakan perkara pokok yang perlu diberikan perhatian sewajarnya dalam konteks perlaksanaan dan pematuhan terhadap kod etika ini.

Kod pengendalian profesional pula menyediakan panduan *authoritative* terhadap standard pengendalian profesional IT yang diterima dan dipraktiskan di dalam industri IT. Ia adalah sesuai dan diterimapakai oleh profesional ICT kerana is berkaitrapat dengan peranan atau bidang kepakaran khusus seseorang profesional IT. Menurut Hogg (2002), salah satu daripada *hallmark*s bagi profesion IT adalah komitmen di kalangan ahli mengenai standard tinggi dalam pengendalian IT secara profesional. Ahli-ahli berdaftar dengan *Australian Computer Society* adalah dijangka sentiasa menguna dan mengekalkan standard pengendalian IT. Manakala, kod amalan profesional merupakan panduan terhadap kaedah-kaedah yang diterimapakai mengenai praktis di dalam industri IT. Antara perkara yang perlu diberikan perhatian ialah keutamaan *(priorities), competence, honesty,* implikasi sosial, pembangunan profesional dan profesion ICT. Dalam pada itu, pensijilan dan perlesenan merupakan pengiktirafan penting mengenai amalan profesional. Pensijilan merupakan proses yang ditadbir oleh profesion atau badan yang berperanan untuk mengiktiraf kecekapan dalam set-set kemahiran profesional ICT. Perlesenan pula merupakan proses secara umumnya ditadbir oleh badan profesional yang mengambilberat terhadap keupayaan dan bukti seseorang itu boleh mempraktiskan profesional dalam kerjaya mereka secara beretika dan tidak menjejaskan kepentingan masyarakat (Hogg, 2002). Oleh demikian, pengasasan kod profesional ICT adalah tidak memadai kerana masyarakat juga perlu sedar akan bahawa ancaman ini.

PENDEKATAN ICT

1. Perisian Penapisan Internet

Penggunaan perisian penapis Internet merupakan antara kaedah teknologi yang diguna bagi melindungi para pengguna Internet. Center for Media Education (1999) menjejaskan bahawa terdapat 4 mekanisme yang paling banyak digunakan oleh perisian penapisan iaitu senarai hitam *(blacklist),* senarai putih *(whitelist),* kata kunci *(keyword)* dan sistem pengkelasan *(rating system).* Mekanisme tersebut adalah seperti berilcut:

a. Senarai hitam tidak membenarkan capaian bagi halaman yang terdapat dalam senarainya.
b. Senarai putih hanya membenarkan capaian bagi halaman yang ada di dalam senarainya sahaja.
c. Mekanisme kata kunci adalah dengan cara memeriksa teks dalam tajuk atau kandungan laman web yang mengandungi kata kunci yang ditetapkan akan disekat jika terdapat kata kunci yang sepertimana yang dikehendaki.
d. Kaedah sistem pengkelasan membenarkan pemilik halaman web untuk menetapkan sendiri tahap kandungan halaman tersebut berdasarkan beberapa kategori seperti bahasa, seks dan keganasan dengan setiap kategori dilabelkan mengikut tahap (0,1,2,3,4). Di sini perisian penapisan akan menapis halaman mengikut tahap yang dibenarkan.

Internet tanpa tapisan juga merupakan ancaman kepada perniagaan kerana dalam kebanyakan kes internet tanpa tapisan juga menjadi saluran kepada penjenayah siber untuk menyerang atau mengodam pada pengguna. Selain itu, internet tanpa tapisan juga mempengaruhi pengguna dan secara tidak langsung mewujudkan kesan kepada masyarakat. Turow (1999) berpandangan bahawa kebimbangan terhadap bahan-bahan tidak sesuai untuk pelajar dan remaja yang mudah didapati di Internet telah mendapat perhatian umum terutama di Amerika.

personel mereka sebagai profesional ICT sekaligus mengekalkan kreadibiliti dan prestasi

Dalam satu bancian oleh USA Today/CNN pada bulan Mei 1999, didapati 65% remaja mengatakan internet merupakan antara penyumbang kepada terjadinya keganasan seperti yang berlaku di Littleton, Colorado. Dalam kejadian itu, dua pelajar remaja berusia 18 dan 17 tahun telah menembak mati 13 orang pelajar dan seorang guru di sekolah mereka. Bureau of Alcohol, Tobacco and Firearms, agen pusat Amerika Syarikat telah mengenalpasti sekurang-kurangnya 30 kejadian born dan 4 cubaan mengebom antara 1985 dan Jun 1996 berlaku kerana golongan yang disyaki telah mendapatkan literasi membuat born dan Internet. Dalam bulan Februari 1996, tiga pelajar sekolah tinggi di Syracuse, New York telah dituduh atas kesalahan membuat born buatan sendiri berdasarkan plan yang mereka perolehi dan Internet. Selain itu, Laporan oleh Ayre (2001) turut menyatakan bahawa pasaran perisian penapisan ini telah berkembang dalam beberapa tahun kebelakangan berdasarkan maldum balas dan persepsi masyarakat terhadap tiga situasi. Pertama, kebimbangan meningkatnya kejadian gangguan seksual di tempat kerja dan dipercayai bahawa penggunaan Internet akan menyebabkan suasana tidak selamat di tempat kerja. Kedua, kebimbangan terhadap penurunan produktiviti di tempat kerja berikutan pekerja terlalu leka menggunakan Internet untuk tujuan yang tidak berkaitan dengan kerjanya. Ketiga, peningkatan kebimbangan terhadap kesan pomografi ke atas kanak-kanak dan dipercayai bahawa Internet telah menjadi sumber yang mudah untuk mendapatkan gambar-gambar pomografi.

Sungguhpun demikian, keupayaan teknologi penapis internet masih dipertikaikan. Berdasarkan kajian yang dikendalikan dalam Projek Penilaian Penapisan Internet (TIFAP) dari April hingga September 1997, ia mendapati setiap mekanisme yang digunakan untuk menapis kandungan Internet mempunyai beberapa kekurangan, iaitu:

a. Mekanisme senarai hitam dan putih hanya bergantung kepada penilaian kandungan intemet yang dilakukan secara manual oleh pengeluar perisian tersebut. Bagi kaedah ini, sekumpulan pekerja akan membuat pencarian ke atas laman-laman web yang dilarang atau dibenarkan. Kaedah ini boleh mengakibatkan penilaian yang tidak adil dan memerlukan sumber tenaga yang akan mengemaskini senarai tersebut dari semasa ke semasa.
b. Bagi mekanisme pengkelasan, hanya 4% daripada jumlah keseluruhan halaman web yang menggunakan mekanisme tersebut. Isu kebolehpercayaan akan wujud apabila pembangun halaman sendiri dibenarkan untuk melabel halaman mereka.
c. Mekanisme kata kunci didapati tidak dapat menapis dengan baik kerana ia akan menghalang halaman yang mengandungi walaupun satu daripada kata kunci tersebut. la merupakan kaedah yang digunakan di permulaan carian dan kebanyakan sistem yang menggunakan kaedah ini menghasilkan reputasi yang buruk. Halaman yang disekat menggunakan mekanisme katakunci tidak boleh dilaksanakan tanpa mengecualikan sebahagian daripada perkataan *non-pornographic* ataupun yang seakan-akan perkataan *pornographic.* Contohnya perkataan seperti *breast* akan menghalang capaian ke laman *breast cancer* dan *sex* akan menghalang capaian ke laman *Ann Sexton.* Maka ini akan menyekat penyebaran maklumat kepada pengguna yang ingin mencari bahan yang berkaitan dengan perkataan yang ditapis.

2. Pendekatan Kata Laluan

Pendekatan Kata laluan adalah kaedah teknologi yang dianggap sebagai konvensional dalam menangani ancaman siber dan secara umumnya kata laluan adalah satu set *characters* yang hanya diketahui oleh

seseorang bagi memenuhi syarat dalam mendapatkan capaian ke sesuatu. Pfleeger (1997) menjelaslcan bahawa satu kata laluan boleh diumpamakan seperti kunci, tanpanya pintu tidak dapat dibuka. Kebiasaannya satu kata laluan membuktikan anda adalah pengguna yang sah pada sate capaian dibenarkan. Kata laluan juga merupakan perkataan rahsia untuk membezakan kawan dengan musuh. Walau bagaimanapun jika seseorang mengetahui kata laluan bagi sesuatu akaun pengguna (rahsia), maka orang itu adalah pengguna yang berdaftar bagi akaun dan sistem komputer tersebut. Sesiapa sahaja boleh mencuba untuk log masuk ke dalam sistem komputer Setiap sesuatu dari semua kad bank sehingga akaun e-mail memerlukan suatu kata laluan. Seperti juga kunci, kata laluan adalah diperlukan apabila kits memerlukan keselamatan. Pilihan selain daripada menggunakan kata laluan adalah seperti cap jari dan pengesanan retina tetapi ia hanya digunakan dalam sesetengah situasi sahaja.

Satu kata laluan boleh diumpamakan seperti kunci, tanpanya pintu tidak dapat dibuka. Kebiasaannya satu kata laluan membuktikan anda adalah pengguna yang sah pada satu capaian dibenarkan. Kata laluan juga merupakan perkataan rahsia untuk membezakan kawan dengan musuh. Walau bagaimanapun jika seseorang mengetahui kata laluan bagi sesuatu akaun pengguna (rahsia), maka orang itu adalah pengguna yang berdaftar bagi akaun dan sistem komputer tersebut. Pada masa dahulu, untuk memecah sesuatu kata laluan, penggodam *(hackers)* akan mencuba secara manual dengan meneka papan kekunci *(keyboard).* Proses itu amat meletihkan serta membosankan. Jadi, diciptakan program automatik yang dapat memecahkan sebarang kata laluan sistem. Kesemua teknik pemecahan kata laluan mempunyai kelebihan dan keburukan. Setiap teknik yang digunakan bergantung kepada keadaan kata laluan yang digunakan. Sesetengah teknik kuat pada sesuatu keadaan, manakala teknik yang lain pula lemah pada keadaan tertentu. Teknik-teknik ini juga bergantung kepada kekuatan dan kelajuan pemprosesan dan komputer yang digunakan. Jika setiap individu mempunyai tahap kerajinan dan kesungguhan untuk mendapatkan pengetahuan ini. Mereka pasti boleh menggunakan pengetahuan tersebut untuk memastikan keselamatan kata laluan sistem komputer mereka terjamin. Namun demikian, terdapat perisian khusus yang direka bagi mencari kaka lalu ini dan sudah tentu penggunaan kata laluan tidak memberilcan jaminan kepada para pengguna siber.

3. *Password Cracker*

Kaedah yang selalu digunakan oleh sekumpulan atau seseorang individu untuk memasuki sesuatu sistem untuk tujuan kebaikan (atau pencerobohan) ialah melalui *password cracking.* Ia merupakan kaedah biasa dan sering digunakan di atas semua *platform* komputer. *Password cracker* adalah sejenis program automatik yang digunakan untuk memecahkan kata laluan sesuatu sistem. Sistem kata laluan tidak boleh dipecahkan kerana ia disulitkan *(encrypted).* Program *password cracker* hanyalah boleh memecahkan pengenkripan jika ada kata laluan yang sama terdapat di dalam fail kamusnya *(dictionary file).* Selalunya program *password cracker* seperti *jack the ripper* atau *crackerjack* yang mempunyai satu fail yang dipanggil *dictionary file.* Kandungan fail ini terdapat beribu kata laluan yang selalu digunakan oleh pengguna untuk log masuk ke sesuatu sistem. Nama bagi setiap kata laluan yang difikirkan dapat memecahkan sistem itu diletakkan di dalam *dictionary file.* Jadi *cracker* atau *hacker* cuma perlu memulakan program itu dan program *password cracker* akan melakukan tugas yang seterusnya. Perlu diingat sekali lagi bahawa kata laluan sesuatu sistem hanya dapat dipecahkan jika ada kata laluan yang sama di dalam *dictionary file.* Kebanyakkan program *password cracker* diciptakan untuk sistem UNIX, AIX, VMS atau sistem yang berlatarbelakangkan bahasa pengaturcaraan C. Tetapi sekarang, program ini telah diintegrasikan ke dalam sistem Microsoft Window dan DOS. Lebih menarik lagi, penggunaannya lebih mudah kerana penggunaan antaramuka pengguna berasaskan grafik atau GUI.

Oleh demikian, kebijaksanaan individu yang melakukan aktiviti ini boleh menyebabkan kesan kepada para pengguna dalam talian.

4. Tandatangan *Digital*

Untuk mengesahkan suatu tandatangan digital, sijil kunci awam *(public key certificate)* mesti diperoleh terlebih dahulu. Perolehan kunci awam tersebut perlu memastikan bahawa kunci tersebut bersesuaian dengan penanda kunci sulit dan merupakan milik kepada penanada itu. Walau bagaimanapun, pasangan kunci awam dan sulit ini adalah sangat penting. Untuk itu, strategi kawalan yang terjamin hams digunakan, Dalam menyekutukan segugus kunci berpasangan dengan bakal penanda, suatu sijil akan dikeluarkan. Dengan ini, suatu rekod elektron yang menyediakan segugus kunci awam dan rupa bakal penanda akan dicamkan dalam sijil yang memuat kunci kesulitan penyesuaian. Bakal penanda itu diistilahkan sebagai pelan,gan. Dengan demikian, fungsi utama sijil ialah mengecam gugusan kunci pasangan seorang pelanggan sup* tandatangan digital tersenarai di dalam sijil dan disahkan. Dengan cara ini, ia mewujudkan jaminan bahawa kunci sulit yang sepadan itu adalah dibawah penguasaan pelanggan seperti tersenarai dalam sijil tersebut. Untuk menyakinkan ketulenan dan keesahan sijil, maka kekuasaan kepingan dari bentuk digital akan menandatanganinya. Tandatan&an digital kepingan di atas sijil kekuasaan itu dapat mengesahkan bahawa tandatangan digital mempunyai keaslian yang secukupnya. Oleh yang demikian, mencipta segugus kunci awam dan pengecaman secara khnsns dengan mudah, maka sijil Web diterbilkan sebagai penggantian. Penggantian adalah digunakan untuk mendapatkan semula pangkalan data sijil dan ianya boleh didapati secara *online.* Namun demikian, teknologi tandatangan digital juga gagal memberikan penyeiesaian kepada ancaman keselamatan siber secara keseluruhannya.

CADANGAN DAN KESIMPULAN

Isu keselamatan siber ICT adalah isu strategik di peringkat nasional dan global dan seharusnya isu ini tidak boleh dikorapronil kerana implikasinya amat besar kepada negara dan organisasi perniagaan antarabangsa termasuklah masyarakat umum di seluruh dunia. Persekitaran ICT yang selamat dapat disediakan dengan wujudnya undang-undang dan polisi serta usaha meningkatkan keselamatan ranokaian di peringkat organisasi. Nanum demikian, pada masa yang sama, penjenayah siber akan terus mencipta serangan dalam bentuk baru, mungkin di laur tafrifan undang-undang. Tambahan pula, fenomena sirangan siber yang tidak pemah putus menjadikan undang-undang siber sentiasa diuji. Pendek kata, isu dan cabaran ICT menuntut komitmen dan semua pihak untuk meningkatkan penggunaan dan penerimaan ICT secara positif di semua peringkat masyarakat.

Dalam konteks Malaysia, NISER telah merumuskan empat langkah penting bagi menangani ancaman keselamatan siber, iaitu (a) Menyatakan; tahap keseriusan berkenaan bagi menghasilkan III dalc balo susulan dengan seberapa segera; (b) Merangka dasar berkaitan isu keselamatan sistem rangkaian computer, (c) Menyelaras tindakan antara penyedia perkhidmatan Internet; dan (d) Membuat hebahan kepada orang ramai supaya mengambil langkah bet·lag-a-jags· Langkah vans dibuat oleh NISER adalah tepat kerana menurut Harvani (2006) isu keselamatan giber ini bukanlah isu yang boleh ditangani secara berseorangan. Walaupun mungkin serangan yang dilakukan datangnya daripada seorang individu, namun semua pihak hams sedar akan peranan yang dimainkan oleh semua individu bagi memastikan ancaman ini dapat dibanteras segera. Kerjasama pihak media massa amat penting bagi memastikan maklumat penting mengenai sesuatu ancaman siber dapat disebarkan kepada orang ramai kerana bukan semua golongan di dalam masyarakat arif dan tahu tentang isu ini.

DAFTAR PUSTAKA

Abdul Manaf Bohari, Salina Ismail & Ezanee Mohamed Alias (2003). *Aplikasi komputer dalam pengurusan.* Model Pendidikan Jarak Jauh. Sintok: PACE UUM.

Abdul Manaf Bohari (2006). *isu-lsu Proksional 1CT di Malaysia.* Kuala Lumpur : 11:IS Book Publication.

Abraham, R., Jas, F., & Russell, W. (1995). *The web empowerment book,* California: Telos Library.

Ause, W., & Arpajian,. S. (1996). *How to use the WWW.* California: Macmillan Computer Publishing

Asniza Musa (2005). *Faisafah, akta dan polisi teknologi* makiumat di *malt:vsia pada masa kini serta* implikasinya *terhadapsistempendidikan negara.* Retrieved May 25, 2005 fromhttp://www.asnizamusa.tripod.comige6543tugl.html

Ayre, Ft_ (2001). *Internet filtering option anolyNk• An interim report Infappaplp Project_*

Ayres Robert (1999). *The essence of professional issues in computing.* New Jersey: Prentice Hall.

Alexander, M. (1996). *The Underground Guide To Computer Security: Slightly Askew Advice From A Winword Wizard.* United States Of America: Addison-Wesley Publication Company.

Beuselinck, C. (1998). *A look at interne/ filtering technologies.* Odyssey '98 Conference. Canada.

Cashman, T. J., Shelly, G. B., $r. Vermaat, M. E (2000). *Discovering computers 2001: Concepts for a connected world, web and cnn enhanced* New York: Course Technology.

Duoper.J. Chrit„ Larry Hu ,,,,,,,,, Karait Siyan, William & Peter (1995). *Implementing* inlet·ma securi;y. New York: New Riders Publishing.

Fazli Azzali, Ali Yusni Daud, & Ezanee Mohamed Alias (2006). Pengukuhan teknologi kata laluan sebagai kaedah menghadapi serangan siber. Dalam _Abdul Manaf Bohari (2006), *Isu-isu. Prolerional ICT di Malaysia.* Kuala Lumpur : IBS Book Publication.

G., Iteyvaud, R., & Rounds, L. (2004). *Professional development in ICT: A range of possibilities.* (Online: http://www.aset.org.au/confs/2002).

Gleason (2004). *Professional context of ICT.* (Online: http://www.cse.dmu.ac.uk).

Hamelink (2000). *ICT for Information Age.* New Jersey: Prentice Hall.

Hazaruddin Harun & Hamirul'Aini Hambali (2006). Internet dan ancaman terhadap peradaban manusiawi. Dalam Abdul Maitar-Bohari (2006). Isu-lsu Prfilifsiunal *ICT di MlaysiKuala* Lumpur : IBS Book Publication: Hogg, D. L. *(2002). Introduction to ICT.* New Jersey: Prentice Hali.

Howard, G.S (1995). *Introdution to internet security: From basic to beyond.* New York: Prima Publishing.

Hunter, *C.* D. (2000). *Negotiating the global internet rating and filteringsystem: Opposing views of the rertelsmarin foundation's self-regulation of internet content proposal.* Computers, Freedom, and Privacy 2000 Conference (Toronto). April 2000.

Hunter, C. D. (2000). Internet Filter Effectiveness: Testing Over and Underinclusive Blocking Decisions of Four Popular Filters. *Social Science Computer Review,* Vol. 18, No. 2, Summer 2000.

Jongwoo Han (2004). *Contemporary issues in the information age.* (Online: http://classes.maxwell.syr.edu/PSC300_103/)

Johnston, D., Hand·. S., 2, Morgan, C (1998). *Cyber law.* Kuala Lumpur: Pei-and:LA Publications.

Malaysia *(2003). Knilan sepriruh penozal rrincanzan malaysia kPloban 1:100-7005.* Koala Lumpur Unit Perancangan Ekonomi,

Jabatan Perdana Menteri (JPM).

Malaysia (2000). *Rancangan malaysia kelapan 2000-2005.* Kuala Lumpur: Unit Perancangan Ekonomi, Jabatan Perdana Menteri (JPM).

Mazrifirdaus (2006). *Standard dan pengukuran polisi dalam pemhangunan keselamatan maklumat organisasi.* Dalam Abdul Manaf Bohari (2006). *Isu-Isu Profesional ICT di Malaysia.* Kuala Lumpur : IBS Book Publication.

Iviohd Safar (2002). *Mengenali undang-undang media dan siber.* Kuala Lumpur: Utusan Publications.

Multimedia Development Corporation (2005). *Multimedia super corridor.* Retrieved May 25, 2005 from http://www.mdc.com.my

Na` :a Abdul ';S nap 1,[1]2001). ..*Peogenalan keiwida undang-una'ang komersial* di Malaysia. Suntingan Sakina Shall-Ahmad Yusoff. 1LBS: Kuala Lumpur.

Nurharyani (2006). Isu-isu keselamatan Siber di Malaysia Dalam Abdul Manaf Bohari (2006). *Isu-Isu Profesional*

ICT di Malaysia. Kuala Lumpur : IRS Rook Publication.

Turow, J., (1999). *The Internet and the Family: The View from parents the view from the press.* Annenberg Public

Policy Center of the University of Pennsylvania. Report No. 27.

Pfleeger, C. P. (1997). *Security In Computing:* New Jersey: Prentice Hall.

Rogerson, S. (1998). The ethics of information and communication technologies (OCT) in business. *Journal Of International Management Information Systems,* Volume 8 (2).

Siponen, M.T. (2001). Five Dimensions of Information Security Awareness. *Computers and Society Magazine:* Pg [1]4 —[1]9.

Siponen, M.T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management and Computer Security.* 8(1). Pg 31—41

Spading, P. (1995). Promoting Security Awareness and Commitment. *Information: Management and Computer Security.* 3(2) Pg 20 - 26

Taber, M. (1997). *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network.* United States of America: San-net.

Tavani, H. T. (2004). *Ethics and technology: Ethical issues in an age of information and communication technology.* New York: Wiley & Son.

Turban, E., McLean, E., & Wetherbe, J. (2001). *Information technology for management: Making connection for strrgegic ';fivcsntogas; cr[d] ed.).* l'gew Vnrk: Jr.hn WilPy z cnns.

Thomson, M.F. & Von, S.R. (1997). An Effective Security Awareness Program for *Industry. Proceeding of WG 11.2 and WG 11.1 of TCII (IFIP).*

Thomson. M.F. & Von. S.R. (1998). Information Security Awareness: Education Our Users *Effectively. Information Management and Computer Security.* 6 (4). Pg 167 — 173.

Wooding, S., Anhal A. & Valeri L. 2003. *Rising Citizen Awareness of Information Security: A Practical Guide.* Berlin : E-aware Publisher.