Bab 4

Penyeliaan Teknologi Maklumat : Kajian di dalam aspek tatacara dan teknikal (penapisan dan keselamatan).

4.1 Pengenalan

Di dalam perkembangan sistem jaringan komputer yang boleh dilihat di mana-mana, samada mini siberkafe yang terdapat di rumah ataupun suatu jaringan komputer antarabangsa seperti internet, mewujudkan suatu perasaan yang tidak senang di kalangan ibu-bapa, guru-guru dan sehinggalah kepada pengurus suatu sistem jaringan komputer. Ancaman daripada program berbentuk vandalisma seperti virus komputer, cacing, *Trojan horse*, *time bomb* dan capaian(*access*) yang tidak sepatutnya seperti capaian kepada laman-laman web pornografi, laman web jenayah seperti kaedah terbaru untuk membuat bom serta ancaman gerakan *subversif* yang menentang kerajaan, jenayah kolar putih dan perkauman seakan-akan tidak dapat dikawal lagi (Deborah G. Johnson 1995 : 89). Sejak zaman revolusi Amerika dan revolusi Perancis, masyarakat mula memberi perhatian terhadap nilai-nilai etika yang menekankan aspek kebebasan dan keselamatan untuk individu serta harta benda peribadi. Prinsip-prinsip etika tersebut dianggap oleh Mason sebagai belum sempurna dan kehadiran Teknologi Maklumat memerlukan kawalan secara alternatif iaitu aspek tatacara dan aspek teknikal di dalam menangani jenayah siber masa kini. (Richard O. Mason et al. 1995 : 227).

4.2 Aspek tatacara di dalam penggunaan sistem komputer.

4.2.1 Asas pembentukan suatu sistem kod etika.

Tatacara bermaksud disiplin aturan bagi sesuatu sistem atau bagi menyelia tingkah laku. Tatacara juga dikenali sebagai suatu sistem kod tingkahlaku (W.T.McLeod 1976 : 343).

Kod tingkahlaku bukanlah satu mekanisma untuk menyelesaikan masalah dilema etika tetapi anya berfungsi sebagai salah satu faktor ke arah itu (Pritchard J. 1993 : 1-10).Bagi sesuatu Kod tingkah laku yang hendak dirangka, ia mestilah berdasarkan peringkat golongan mana ang hendak dijadikan sasaran. Samada di peringkat organisasi, keluarga/sekolah ataupun ndividu (Paul F. Burton 1996 : 4 – 6). Kod tingkah laku haruslah berdasarkan prinsip-prinsip laripada etika normatif yang berkaitan dengan Hak dan Tanggungjawab. Kedua-dua prinsip tika ini berbentuk *Deontological*. Prinsip-prinsip ini memberikan suatu jawapan kepada esuatu dilema etika tingkahlaku. Prinsip-prinsip yang diberi juga dapat digunakan di dalam es-kes lain yang serupa (Ernest A. Kallman et al. 1996 : 13 – 15).

.2.1.1 Prinsip Hak.

Hak untuk mengambil tahu.

Satu had sempadan yang jelas mestilah dibuat supaya pengguna dapat memahami sehingga mana mereka berhak untuk mengetahui maklumat yang boleh dicapai.

Hak Keperibadian individu (*The right of privacy*).

Penjelasan sehingga tahap mana seseorang itu dapat mengawal maklumat yang dimiliki.

Hak kepemilikan (*The right of property*).

Penjelasan sehingga tahap mana seseorang itu dapat melindungi maklumat yang dimilikinya daripada dimanipulasi atau dirosakkan..

.2.1.2 Tanggungjawab.

Tanggungjawab memelihara amanah. Tanggungjawab untuk menepati dan memenuhi sebarang kontrak atau urusniaga.

Tanggungjawab untuk bersikap jujur kepada orang lain samada mereka adalah pekerja ataupun pelanggan.

Tanggungjawab menjadi seorang yang bersikap dengan benar dan tulus ikhlas kepada orang lain.

Tanggungjawab menjadi seorang yang adil. Ini adalah kerana keadilan menuntut supaya sebarang urusan mestilah saksama (kedua-dua pihak mendapat manfaat). Iaitu mereka yang telah memberikan khidmatnya, harus dibayar dan mereka yang didapati menipu mesti dihukum.

Tanggungjawab untuk melaksanakan *beneficence*(tanggungjawab untuk menolong orang lain supaya dapat hidup dengan lebih baik) dan tanggungjawab melaksanakan *non-malifecence*(tidak menyakiti orang lain).

Tanggungjawab untuk menyatakan penghargaan kepada mereka yang telah berbuat kebaikan dan sentiasa memperbaiki kesilapan yang telah dilakukan ke atas orang lain.

Tanggungjawab untuk berusaha ke arah memperbaiki diri sendiri.Apabila kita berusaha untuk tidak mengulangi kesalahan yang pernah kita lakukan, kita sebenarnya bertindak berdasarkan tanggungjawab memperbaiki diri sendiri (Ernest A. Kallman et al. 1996 : 13 – 15).

Tugas di dalam sesebuah organisasi adalah suatu bentuk tanggungjawab. Apa yang isyorkan oleh Kallman merupakan garis panduan bagi tugas yang lebih spesifik kepada seseorang individu yang bekerja di bawah sebuah organisasi. Garis panduan yang disyorkan leh Kallman dapat membezakan tanggungjawab di antara individu biasa dengan seorang akar bagi sesebuah organisasi.

4.2.2. Tatacara peribadi (*self-regulation*).

Tatacara peribadi bersifat penyeliaan dalaman (*internal monitoring*). Ia mungkin merupakan suatu sistem bagi tingkah laku ke atas seseorang ataupun bagi sesebuah organisasi itu secara khusus. Samada individu ataupun seorang professional , ia bersifat autonomi[1]. Kod etika bagi tatacara jenis ini biasanya dikembangkan secara berasingan dan khusus untuk diterapkan di tempat persendirian. Tetapi adakalanya ia tidak terhad tertakluk ke atas ahli sahaja, sesiapa yang hendak masuk ke sesuatu lama web atau pengkalan data tertentu kepunyaan individu atau organisasi tertentu, ia juga tertakluk kepada aturan tersebut (Paul F Burton 1996 : 7).

Contohnya Jawatankuasa Persatuan Komputer Sekolah-sekolah British telah pun mengeluarkan garis panduan untuk mencegah penyalahgunaan komputer. Ini merupakan usaha di peringkat sekolah yang bersifat khusus bagi pelajar-pelajar (Jawatankuasa Persatuan Komputer Sekolah-sekolah British 1995)[2]. Ini menunjukkan pihak barat sendiri secara tidak langsung telah mengakui terdapatnya bahan-bahan yang bersifat mengancam dan membahayakan generasi muda sekiranya dibiarkan terus disebarkan di dalam laman web walaupun British secara umumnya sangat mementingkan kebebasan bersuara sebagai asas sistem di dalam masyarakat mereka.

4.2.3. Tatacara Professionalisma.

Tatacara professional diterbitkan daripada etika gunaan dan ianya di terapkan secara praktikal di dalam sesuatu organisasi dan di dalam kerangka profesional. Etika profesional merupakan satu set aturan atau kod bagi tingkah laku yang spesifik, dirumus dan diwajibkan ke atas setiap profesional. Tatacara professional melibatkan aplikasi teori etika dan terikat

kepada nilai yang menjadi prinsip etika yang utama contohnya seperti prinsip menghormati orang lain (Christine Henry 1995: 8-9).

Di dalam perkataan lain, tatacara profesional bukan sekadar suatu pembentukan kod bagi suatu amalan profesional yang dikembangkan oleh para professional, tetapi ia mencakupi lebih luas dan mendalam daripada itu, yang melibatkan persoalan normatif dan menggunakan aplikasi bersifat teoritikal (*theoritical application*) tertentu untuk menyelesaikan dilema moral (Christine Henry 1995 : 8-9)[3].

Bagi sesuatu organisasi yang mewakili profesionalisma tertentu, kod etika merupakan tatarcara secara formal yang harus dipenuhi oleh setiap ahli yang bernaung di bawahnya. Walaupun kod etika bagi sesuatu organisasi bersifat mengikat ahli-ahli yang bernaung, ia lebih bersifat individu yang mana sesiapa jua mesti mempunyai perasaan bertanggungjawab untuk terikat kepada tatacara yang telah digariskan. Ini termasuklah kepada mereka yang menawarkan perkhidmatan kepada orang lain walaupun ia sendiri tidak mempunyai formaliti di dalam sesuatu profesionalisma (Duncan Langford 1995: 7).

Sebagai contohnya kod etika yang digariskan oleh ACM (*Association for Computing Machinery*) yang menggariskan 4 prinsip kewajipan yang telah diterima pakai oleh ahli-ahlinya pada 16 Oktober 1992 (Sila rujuk lampiran A). Empat prinsip kewajipan itu ialah:

a) Kewajipan moral secara umum.

b) Kewajipan tanggungjawab professional yang lebih khusus.

c) Kewajipan untuk memimpin organisasi.

d) Tanggungjawab untuk terikat kepada kod etika yang digariskan.

Contoh kod etika yang lain ialah Kod dan Amalan BCS(*British Computer Society*). Ia berasaskan kepada 4 prinsip tanggungjawab. Empat prinsip tersebut ialah:

a) Mementingkan kepentingan masyarakat,

b) Tanggungjawab kepada majikan dan pelanggan,

c) Tanggungjawab kepada profesion.

d) Tanggungjawab kepada kemahiran dan kewibawaan.

(Sila rujuk lampiran A).

4.2.4. Tatacara Keluarga/Sekolah.

Kawalan secara menyelia oleh guru dan ibubapa dihadkan oleh masa dan tempat. Walaupun kawalan secara menyelia oleh guru dan ibu-bapa berjaya tetapi kanak-kanak atau remaja masih dapat memasuki internet di masa lain yang tidak dapat diselia oleh ibu-bapa sepanjang masa. Terdapat dua kaedah penyeliaan di peringkat ini iaitu samada dengan kaedah memberikan pendidikan formal atau informal dan secara penyeliaan berbentuk teknikal.

Menurut Paul F. Burton (1996), Ibu-bapa atau guru harus mendedahkan kepada semua anak didik mereka tentang ancaman yang terkandung di dalam internet supaya mereka faham terhadap bahaya yang selalu diperkatakan. Ia dapat diumpamakan seperti mengajar anak didik mereka tentang bahaya sekiranya tidak berhati-hati semasa melintas jalan raya. Walaupun ia tidak semudah yang digambarkan, langkah pertama mesti diambil sejak kanak-kanak itu masih kecil.

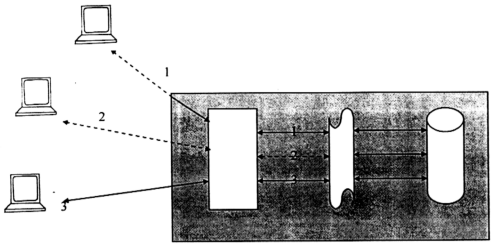
Penyeliaan secara teknikal dapat dilakukan dengan bantuan perisian-perisian berbentuk keluarga seperti Enuff, ChiBrow atau FamilyCam.(Paul F. Burton 1996 : 10). Ini dibincangkan dengan lebih lanjut di bawah tajuk teknik penapisan komputer.

4.3. Teknik penapisan komputer.

4.3.1. Pengenalan.

Penggunaan sistem tapisan(*filteration systems*) ataupun kaedah pengesahan(*rating systems*) dianggap sebagai satu alternatif sekiranya kod etika tidak dapat dijadikan sebagai satu tanggungjawab yang mesti dipatuhi . Teknik yang terdapat di dalam perisian tapisan secara amnya sama. Perisian penapisan berperanan menjadi perantara pengguna dan pengkalan data. Perisian akan melakukan format terhadap permintaan pengguna melalui penyaringan(*screening*) terhadap semua data yang sensitif berdasarkan data yang telah dimasukkan terlebih dahulu oleh penyelia ke dalam pengkalan data perisian. Peranan sistem ini dapat digambarkan di dalam rajah 4.1.

Daripada gambarajah tersebut, ia dapat menerangkan kepada kita bagaimana berlakunya interaksi di antara pengguna komputer, sistem etika dan suatu sistem operasi pengkalan data. Setiap pengguna komputer akan melalui suatu sistem etika penggunaan komputer, tetapi keputusan muktamad terletak pada pengguna tersebut. Daripada gambarajah di atas, terdapat tiga keadaan yang biasa ditemukan. Pertama, pengguna yang berniat jahat tetapi setelah memahami kod etika yang telah digariskan dan menjadikannya sebagai asas perbuatannya, dia kembali menggunakan komputer dengan betul. Bagi keadaan yang kedua, pengguna mempunyai niat yang jahat dan setelah melalui kod etika yang telah digariskan, dia masih berdegil dan tetap meneruskan niat jahatnya di dalam penggunaan komputer tetapi apabila tiba di bahagian sistem kawalan keselamatan yang ketat, dia terpaksa akur dan terpaksa mengikut peraturan yang telah digariskan. Keadaan yang ketiga adalah pengguna biasa. Di dalam model ini, ditunjukkan bagaimana aspek teknikal berfungsi untuk menghalang sebarang bentuk salah-laku komputer setelah sistem etika telah dilanggar.



Petunjuk :

Pengguna

Sistem pengurusan data

Sistem Kawalan

Pengkalan Data

Berniat jahat

Berniat baik

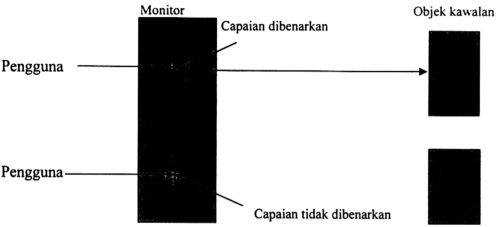
Sistem etika

Rajah 4.1. Model asas Interaksi Di antara Sistem Etika, Pengguna dan Sistem Operasi Pengkalan Data.

a) Model *Monitor*.

Salah satu kaedah penyeliaan capaian maklumat ialah kaedah *monitor* yang diringkaskan di dalam rajah 4.2. Ia adalah pintu perantara di antara pengguna dan juga objek capaian yakni maklumat yang hendak dicapai. Seperti yang ditunjukkan di dalam rajah tersebut, pengguna akan mencari capaian tertentu kepada sesuatu objek menerusi *monitor*. *Monitor* akan mempertimbangkan permintaan sesuatu capaian yang hendak dilakukan dengan

merujuk kepada maklumat kawalan dan samada diberikan kebenaran untuk melakukan capaian atau tidak membenarkan sebarang capaian.(Hoare C. 1974: 548 – 577).



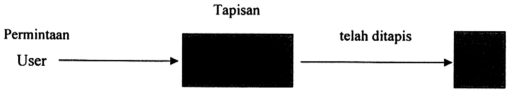
Rajah 4.2. Bentuk kawalan capaian kaedah monitor. (Sumber : Charles P. Pfleeger 1989 : 244).

b) Model pengaliran maklumat.

Model ini bertindak sebagai penapis bijak di mana ia mengawal pengaliran maklumat bagi sesuatu capaian yang dibenarkan ke atas objek tertentu seperti yang ditunjukkan di dalam rajah 4.3. Model maklumat ini dapat menghuraikan potensi capaian bagi program yang telah disusun. Kaedah ini melibatkan analisis aliran maklumat untuk setiap penyataan bagi program. Denning (1977) menunjukkan bahawa model pengaliran maklumat boleh digunakan untuk menerangkan potensi-potensi capaian sebelum sesuatu program itu dihidupkan. Kaedah ini biasanya dilaksanakan oleh *compiler*[4] yang mana melibatkan analisis pengaliran maklumat untuk setiap penyataan di dalam program. Analisis ini dapat

membuktikan bahawa pengaliran maklumat yang sensitif dan tidak sensitif saling tidak bergantungan. Jadi, seseorang pengguna yang tidak berkelayakan tidak akan dapat mencapai maklumat yang sensitif dan pada masa yang sama dapat mencapai maklumat yang dia kehendaki. Iaitu pengguna yang tidak berdaftar masih dapat melakukan capaian tetapi bagi maklumat yang sensitif hanya pengguna yang berdaftar sahaja yang akan dapat melakukan capaian kepada maklumat yang sensitif. Model ini memberi fleksibiliti kepada capaian tetapi mengawal pengaliran maklumat. (Denning D. 1977 : 243).

Model pengaliran maklumat ini sesuai bagi data tunggal ataupun terkumpul seperti sesuatu fail. Ia memberi jaminan tidak akan ada sebarang kebocoran maklumat bagai sesuatu sistem operasi. Ini sangat sesuai untuk membina sebuah sistem operasi yang terpercaya (*trustworthy operating system*). Terdapat tiga kategori di dalam perlaksanaan perisian penapisan (*filteration software*) iaitu sistem penapisan untuk keluarga, sistem penapisan untuk sekolah dan sistem penapisan untuk organisasi.



Rajah 4.3. Model pengaliran maklumat (Sumber :Charles P. Pfleeger 1989 : 245).

4.3.2. Penapisan Keluarga.

Kawalan secara menyelia dihadkan oleh masa. Walaupun kawalan secara menyelia oleh ibu-bapa berjaya tetapi kanak-kanak/remaja masih dapat memasuki internet di masa lain yang tidak dapat diselia oleh ibu-bapa sepanjang masa. Melalui teknik penapisan komputer,

ibu-bapa dapat menyelia penggunaan komputer oleh anak-anak mereka tanpa kehadiran mereka di sisi anak-anak. Terdapat beberapa jenama perisian penapisan komputer yang menyediakan kemudahan bagi ibu-bapa untuk menyelia penggunaan komputer oleh anak-anak mereka. Di antaranya ialah Enuff. ChiBrow.

a. Enuff.

Salah satu perisian penapisan yang bersifat menyeluruh ialah Enuff. Perisian ini berfungsi melalui 2 fungsi serentak iaitu berfungsi sebagai penapis dan berfungsi untuk mempertahankan dirinya sendiri daripada diubahsuai atau dipadamkan oleh pangguna khususnya kanak-kanak.

Di antara fungsi-fungsinya sebagai penapis ialah :

- Menghalang kanak-kanak daripada menggunakan sebahagian atau seluruh sistem.
- Menentukan dan menghapuskan katalaluan kanak-kanak.
- Mencapai log pengguna untuk menentukan pengguna waktu dan tempoh penggunaan sistem.
- Menetapkan laman web yang mana boleh digunakan oleh kanak-kanak.
- Membenarkan kanak-kanak menggunakan komputer untuk jangka masa yang panjang tetapi tidak bermain permainan komputer.

Di dalam program ini terdapat juga tatacara yang dilaksanakan dengan membenarkan penggunaan komputer untuk tempoh masa yang ditentukan (misalnya 2 jam) tetapi penggunaan internet hanya untuk selama 30 minit bagi laman-laman yang telah pun ditentukan oleh ibu-bapa.

Peringkat penapisan kedua pula menghalang kanak-kanak daripada :

- Merubah data yang direkod oleh carta log komputer seperti tarikh atau masa dan laman yang telah dilawati.
- Memadamkan program Enuff.
- Menukar sebarang konfigurasi yang telah ditetapkan oleh ibu-bapa
- Memasuki internet tanpa kebenaran.
- Menangkis pengoperasian Enuff (http://www.akrontech.com/enuff-need.html>28Jan2000).

b. ChiBrow.

Perisian ini membolehkan kanak-kanak untuk meneroka/menjelajah Laman web di internet. Ianya dilaksanakan dengan membolehkan ibu-bapa menentukan laman web yang mana boleh dilawati oleh seseorang kanak-kanak itu. Kebanyakan keluarga mempunyai masaalah di dalam memilih perisian tapisan internet kerana kebanyakan perisian cenderung untuk menyekat laman web pendidikan yang lain hanya kerana mempunyai beberapa perkataan yang mirip menggambarkan kelucahan.

ChiBrow membantu ibu-bapa mengemaskini pengkalan data yang mengandungi laman web yang mana seseorang kanak-kanak itu dihadkan kepada "*Drop-Down List*" yang terdapat di susunan ikon, dan apabila laman-laman web tersebut telah dipaparkan, kanak-kanak dapat lawati dengan menggunakan *hyperlinks*[5] yang mengandungi laman-laman tertentu. Setiap *link*[6] sebelum itu akan disahkan selamat untuk dilawati oleh kanak-kanak. Biasanya *links* yang dibenarkan adalah yang terdapat pada domain atau yang juga terdapat di pengkalan data URL[7](<http://www.chibrow.com/informat.htm> 20 Jan 2000).

4.3.3. Penapisan Sekolah.

Teknologi komunikasi maklumat telah mewujudkan cabaran pendidikan yang baru kepada guru-guru di sekolah di dalam menyelia penggunaan komputer di makmal-makmal komputer sekolah mereka. Mereka mempunyai kesulitan di dalam mengenalpasti penggunaan komputer sekolah yang tidak produktif oleh para pelajar. Antara perisian yang sesuai digunakan untuk menyelia penggunaan sistem komputer di kalangan pelajar ialah FamilyCam (juga boleh digunakan oleh ibu-bapa) ,Webkeys Prowler dan SurfPass.

a. FamilyCam.

FamilyCam merupakan satu sistem yang memberi kelebihan kepada pihak guru untuk menguatkuasakan sebarang polisi penggunaan komputer di sekolah. Ia adalah sebagai alat bagi guru untuk menyelia penggunaan komputer di kalangan murid-murid di sekolah secara pasti. Perisian FamilyCam biasanya disertakan dengan satu contoh polisi yang boleh dijadikan panduan untuk guru menyediakan satu tatacara bagi penggunaan komputer di sekolah bagi murid-murid.

Ciri khas yang terdapat pada aplikasi ini ialah guru boleh menyelia murid-murid dengan memerhatikan apa yang sedang mereka lakukan melalui skrin komputer utama di meja penyelia. Apa yang sedang dilihat di skrin murid pada masa yang sama akan dapat dilihat di skrin guru. Apabila di dapati murid-murid telah melanggar polisi penggunaan yang telah ditetapkan, guru akan serta merta mengambilalih penggunaan komputer melalui kawalan komputer berpusat dan mengembalikan murid kepada aktiviti asal yang telah ditugaskan. Dengan ini guru tidak perlu sentiasa berjalan untuk memeriksa setiap terminal komputer pada setiap masa tetapi hanya mengawal melalui terminal utama(<http://www.silverstone.net/html/familycam.html > 28 Januari 2000).

b. Webkeys Prowler.

Sistem ini beroperasi dengan cara menghalang sebarang capaian(*access*) kepada laman dewasa yang dikenalpasti tidak sesuai untuk pelajar. Perisian ini beroperasi di dalam latarbelakang yang telus kepada pelajar. Ianya hanya bertindak apabila sesuatu laman web dewasa dilawati oleh pelajar. Apabila sesuatu laman web dewasa telah dikesan, ia akan menghalang laman web itu dibuka dan memberi pilihan kepada pelajar untuk kembali ke laman sebelumnya.

Ciri-ciri khas:

- Membolehkan guru untuk mengawal apakah yang sedang dilihat oleh pelajar.
- Melindungi pelajar daripada mencapai bahan-bahan bersifat dewasa yang dianggap mengancam pemikiran pelajar yang belum matang.
- Pelbagai *settings*[8] pengguna.
- Percuma dan boleh diperolehi daripada internet(<www.webkeys.com/teachers.htm>28 Januari 2000)..

c. SurfPass.

Perisian ini membolehkan guru-guru untuk menghadkan tempoh penggunaan internet oleh para pelajar memandangkan tempoh pengajian di sekolah adalah terhad. Bahkan SurfPass membolehkan juga guru untuk merekodkan semua aktiviti *log* setiap komputer yang digunakan pelajar dengan terperinci. Ini dapat dilakukan dengan menyenaraikan semula laman-laman yang telah dilawati oleh pelajar. Pelajar yang menggunakan sesuatu terminal boleh dikenalpasti melalui nama dan katalaluan yang direkodkan di dalam senarai *log*.

Ciri-ciri khas:

- Setiap pelajar yang menggunakan komputer akan dikenalpasti samada melalui nama, katalaluan ataupun melalui kad pintar yang digunakan. Ini membolehkan penyelia untuk mengenalpasti nama pelajar yang telah melawati laman-laman yang tidak dibenarkan.
- Setiap akaun pelajar akan ditetapkan semasa penggunaan dan boleh diubah berdasarkan keperluan tugasan.
- Penyelia dapat menetapkan masa penggunaan komputer. Ini dapat menghalang sebarang penggunaan komputer pada masa yang tidak dibenarkan.
- Memutuskan talian terminal secara otomatik apabila sesuatu selang masa penggunaan yang tidak aktif dikenalpasti (<http://www.surfpass.com/html/b_tech.html>2 Januari 2000.

4.3.4. Penapisan Organisasi.

Persaingan di alaf baru menyebabkan syarikat komersial (perkhidmatan, industri, perdagangan) terpaksa mengikuti perkembangan internet dan terlibat di dalam komunikasi jaringan teknologi maklumat. Ini memberikan ancaman yang harus dihadapi oleh syarikat. ancaman yang bersifat kemanusiaan dan teknikal lebih hebat disebabkan oleh sifat teknologi yang memudahkan manusi melakukan sesuatu keburukan yang sebelumnya tidak dapat dilakukan olehnya (Robert E McGinn 1991 : 17). Di antara ancaman yang dihadapi oleh syarikat-syarikat yang terlibat di dalam Teknologi Komunikasi Maklumat ialah penyalahgunaan talian internet oleh kakitangan yang melawati laman web yang tidak memberi keuntungan kepada syarikat seperti laman web pornografi, hiburan, sukan, iklan-iklan untuk membeli-belah yang mana laman-laman ini mudah untuk dicapai di dalam internet. Ancaman-ancaman ini menyebabkan Teknologi Komunikasi Maklumat yang pada asalnya menjadi alat canggih yang pernah dicipta bertukar kepada ancaman yang lebih

berbahaya daripada ancaman persaingan di dalam perniagaan itu sendiri. Terdapat beberapa perisian yang dapat membantu syarikat di dalam menangani masaalah ini. Diantaranya ialah *X-Stop, Disk Tracy, CyberSentinel.*

a. X-Stop.

X-Stop menghalang sebarang unsur pornografi dan juga laman-laman berbahaya seperti laman membuat bom, kumpulan penghasut dan dadah pada masa yang sama membenarkan capaian kepada laman-laman yang berfaedah. X-Stop akan menyediakan laporan tentang pengguna individu, penggunaan internet, keganasan dan juga laman-laman yang telah dilawati.

Ciri-ciri khas :

- Meminimumkan masa yang diluangkan para pekerja untuk melawati laman-laman yang tidak memberikan faedah kepada syarikat.
- Memaksimumkan produktiviti pekerja.
- Mengelakkan kos pendakwaan kerana disebabkan gangguan seksual oleh pekerja lelaki terhadap pekerja wanita yang mana ini dipercayai berpunca daripada pengaruh laman-laman web yang memaparkan unsur-unsur pornografi(<http://www.xstop.com> 28 Jan 2000).

b. Disk Tracy.

Disk Tracy berfungsi seperti 2 program di dalam satu. Iaitu ia merangkumi (i) Fail penganalisa *patem* yang akan mencari dan menunjukkan sebarang bahan yang mungkin tidak sesuai untuk dicapai oleh pengguna atau yang disimpan di dalam pengkalan data stesenkerja sistem komputer (ii) Ia mengandungi kemudahan-kemudahan untuk menyelia penggunaan

pengguna di dalam membuat capaian ke dalam internet. Kemudahan yang disediakan oleh sistem Disk Tracy sangat anjal sehingga syarikat boleh mengubahsuai sistem penyeliaan di dalam Disk Tracy berdasarkan kehendak syarikat

Ciri-ciri khas :

- *Log* aktiviti (yang merekodkan semua aktiviti-aktiviti yang berkaitan dengan *browsing*[9] termasuklah sebarang percubaan untuk mencapai laman *chatting*),
- Penyekatan Dinamik (samada penyekatan secara teks mahupun kandungannya.),
- Penyekatan Laman (Menyekat alamat URL yang telah ditentukan),
- Penyekatan penggunaan(menyekat pengguna daripada *chatting* atau *newsgroup*[10]),

c. CyberSentinel.

CyberSentinel merupakan salah satu perisian penapisan yang canggih pada masakini. Sebagai pihak majikan, mustahil untuk berada di sisi setiap pekerja setiap kali mereka menggunakan komputer samada untuk melakukan kerja seharian mahupun melakukan capaian ke dalam internet. Perisian ini direkacipta di dalam rangka usaha untuk mengatasi masaalah majikan di dalam menyelia penggunaan komputer di kalangan pekerjanya. Penyeliaan yang dijalankan termasuklah melakukan analisa, penapisan, penyekatan, eksploitasi dan juga pengaliran maklumat yang jelas mempunyai bahaya daripada pengaruh unsur-unsur sex.

Salah satu ciri cybersentinel ini ialah satu set pengumpulan data tentang bahan-bahan larangan yang telah dicapai oleh pengguna melalui internet pada sesuatu komputer atau di dalam suatu sistem komputer. Ia juga boleh berfungsi secara senyap dengan merekod semua aktiviti pengguna dan kemudian disemak oleh penyelia sistem.

Cybersentinel telah memberikan majikan suatu kelebihan di dalam menentukan laman web yang manakah yang boleh dilawati oleh pekerja dan laman web manakah yang dilarang untuk mereka lawati.

Ciri-ciri khas:

- Mempunyai rekabentuk keselamatan internet yang berkonsepkan masa depan.
- Penyeliaan di dalam laman *chat*, kandungan *e-mail, search engine, browsers.*
- Boleh berfungsi di dalam mod senyap dan juga mod aktif (boleh dilihat)
- Memberikan notis kepada majikan secara e-mail sekiranya terdapat laman-laman atau bahan-bahan larangan yang dicapai oleh pekerja mereka atau juga yang ada disimpan di dalam pengkalan data sistem komputer mereka.
- Memberi kelebihan kepada majikan memilih laman, domain, dan perkhidmatan yang boleh dilawati oleh pekerja mereka.
- Pengurusan capaian kepada internet berdasarkan penentuan masa yang sesuai.
- Dibenarkan dari segi penguatkuasaan undang-undang.
- *Interface*[11] komputer yang mudah.

Kelebihan utama yang terdapat pada Cybersentinel ialah mekanisme carian yang canggih dimajukan oleh jurutera daripada *Security Software Systems*. Kelebihan mekanisme carian ini ialah ia sangat pantas, jimat dan sangat cekap. Ujian juga menunjukkan Cybersentinel berjaya menapis maklumat yang gagal ditapis oleh perisian lain. Sistem yang terdapat pada Cybersentinel sangat ringkas sehinggakan pengguna yang kurang mempunyai maklumat tentang komputer juga mampu untuk melakukan format perisian ini ke dalam sistem mereka.

Antara ciri lain yang khas Cybersentinel di dalam menapis data yang terdapat di dalam sistem ialah apabila sesuatu data yang diragukan keselamatannya. sedang dicapai oleh pengguna, data tersebut akan dirakam di dalam pengkalan data Cybersentinel dan kemudian secara automatik ia akan mengirimkan e-mail kepada penyelia sistem tentang rekod capaian data tersebut dari segi masa, tarikh dan siapa yang telah mencapai data tersebut. Melalui peringatan kepada penyelia melalui e-mail ini, akan memberi kelebihan kepada penyelia untuk menyelia penggunaan komputer di kalangan pekerja syarikat walaupun penyelia itu berada di rumah(<http:www.securitysoft.com/home.html> 20hb Jan 2000).

4.4. Keselamatan Komputer.

4.4.1. Pengenalan.

Terdapat 2 klasifikasi di dalam pendekatan sistem keselamatan komputer ; iaitu kawalan berbentuk fizikal dan kawalan berbentuk teknikal. Kedua-dua pendekatan ini digunakan baik di dalam perkara yang bersangkutan dengan keselamatan perkakasan komputer dan juga keselamatan perisiannya. Walaubagaimanapun, hanya keselamatan perisian sahaja yang akan dibincangkan di dalam bab ini.

4.4.2. Keselamatan Perisian.

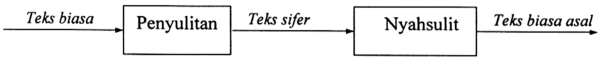
4.4.2.1. Penyulitan

i. Penyulitan (*Encryption*).

Penyulitan bermaksud kaedah atau proses untuk menukarkan data dalam persekitaran yang tidak selamat melalui penggunaan kaedah algoritma (Richard H. Baker 1995: 140-147).

Penyulitan bertujuan mencegah sebarang gangguan ke atas maklumat seperti sampukan(*interuption*), pintasan(*intercept*) ubahsuai dan direka.

ii. Algoritma penyulitan



Rajah 4.4 . Algoritma mudah kaedah penyulitan (Sumber : Charles P. Pfleeger 1989 : 85-90).

Di dalam proses penyulitan seperti yang ditunjukkan di dalam rajah 4.4, teks biasa yang hendak disulitkan akan dienkod untuk menukarnya kepada data-data yang tidak teratur kepada bentuk yang hampir mustahil untuk difahami. Ketika proses penyulitan tersebut suatu algoritma tertentu akan memproses data yang hendak disulitkan. Terdapat dua kaedah penyulitan yang biasa digunakan pada masa ini iaitu:

a) Sistem Kripto Kunci Tunggal (*Single-key-system*).

Sistem ini hanya menggunakan satu ayat tunggal atau frasa sebagai kunci. Kunci yang sama digunakan oleh pengirim untuk menyulitkan dan kunci yang sama untuk menyahsulit data yang disulitkan. Di dalam kaedah ini, pengirim dan penerima hanya mempunyai satu cara untuk iaitu penggunaan kekunci tunggal di dalam proses mengirim utusan daripada pengirim kepada penerima.

Contohnya IDEA (*International Data Encription Algoritma*), DES (*Data Encription Standard*), dan bagi perisian yang beroperasi secara global seperti Netscape, RC2 dan RC4 digunakan. (Charles P. Pfleeger 1989 : 88 - 128).

b) Sistem Kripto Dwi-Kunci (*Public-key-system*).

Kaedah ini menggunakan dua kekunci untuk melindungi maklumat yang disulitkan. Istilah dwi-kunci bermaksud dua kunci yang digunakan oleh pengirim dan penerima yang mana satu kunci disimpan sebagai kunci rahsia manakala yang satu lagi bertindak sebagai kunci umum yang boleh diserahkan kepada sesiapa selain daripada pengirim atau penerima. Oleh itu untuk proses Kripto Dwi-Kekunci ini, 4 kekunci digunakan iaitu 2 digunakan oleh pengirim dan 2 lagi oleh penerima. (Charles P. Pfleeger 1989 : 88 - 128)

Sistem Kripto Dwi-kekunci ini melibatkan 3 langkah:

1. Pengirim dan penerima bertukar-tukar kekunci (kekunci rahsia mereka tidak boleh didedahkan).
2. Pengirim menggunakan kekunci umum penerima untuk menyulitkan maklumat semasa mengirim.
3. Penerima pula akan menggunakan kekunci rahsianya untuk menyahsulit maklumat yang dia terima. Proses yang sama juga berlaku apabila penerima berhasrat untuk membalas yang diterimanya.

Contohnya RSA (*Rivest, Shamir and Alderman*) iaitu pihak yang telah merekacipta kaedah baru ini selepas kaedah Sistem kekunci tunggal.

.4.2.2. Katalaluan.

Katalaluan ialah kaedah keselamatan yang biasa digunakan di dalam membuat capaian epada sesuatu perisian komputer. Katalaluan bermaksud kata atau kod rahsia yang mesti iberi kepada komputer sebelum dibenarkan pengguna melakukan sebarang operasi ke atas erisian. Ia digunakan untuk menjaga keselamatan maklumat di dalam pengkalan data sesuatu omputer atau sistem komputer (Zoraini Wati Abas et al. 1994 : 146). Katalaluan ialah suatu od atau perkataan yang telah ditetapkan di dalam sistem komuter bagi setiap pengguna yang ibenarkan. Penggunaan katalaluan sangat mudah, pertama kerana pengguna akan emasukkan pengenalan dirinya, seperti nama ataupun ID pengguna kemudian barulah iminta untuk memasukkan katalaluan. Biasanya sesuatu sistem itu akan mengaitkan sesuatu atalaluan bagi setiap akaun yang berlainan. Ini bermaksud setiap akaun mempunyai atalaluan yang berlainan. Keselamatan komputer adalah penting untuk mengelakkan engguna yang bukan berdaftar daripada memasuki sistem komputer. Keselamatan komputer ga boleh menyediakan suatu keistemewaan eksklusif kepada pengguna tertentu untuk emasuki sesuatu fail atau rekod.

.4.2.3. Antivirus

Secara umumnya terdapat dua jenis antivirus. Antivirus yang bersifat khusus dan ntivirus yang bersifat umum. Begitu juga kebanyakkan anti-virus di dalam pasaran yang apat dibahagikan kepada dua kategori iaitu perisian antivirus umum dan antivirus khusus. Manakala setiap kategori dapat dibahagikan kepada empat kategori yang lebih khusus. Seperti ang ditunjukkan di dalam jadual 4.5:

Anti Virus Umum	Anti Virus Khusus
Checksumming software	*Scanning software*
Perisian penyeliaan	Perisian penyeliaan
Integrity shells	*Inoculation software*
Virus removal software	*Disinfection software*

Jadual 4.5. Kategori antivirus (Sumber : Jan Hruska 1992 : 120-137).

a) *Scanning software* (virus khusus).

Perisian jenis ini akan mencari virus yang tidak dikenali sebelumnya. Apabila satu virus baru ditemui dan dijumpai, ianya dianalisis, dan ciri-cirinya direkod, program *scanner* akan memeriksa semua arahan-arahan di dalam sesuatu program komputer termasuk sistem operasi dan membanding semua kandungan dengan pengkalan data berkenaan dengan ciri-cirinya. Fungsi ini biasanya digunakan untuk mengimbas disket-disket yang digunakan. Apabila digunakan menerusi sesebuah komputer. Kelemahan perisian ini ia hanya dapat mengesan virus yang ia kenal. Harus dikemaskini selalu untuk mendapatkan ciri-ciri virus baru akan yang muncul.

b) *Checksuming software* (virus umum).

Perisian *checksuming* bergantung kepada pengesanan sebarang bentuk perubahan yang berlaku ke atas arahan-arahan yang terdapat di dalam sesuatu program. *Checksuming* juga dipanggil *fingerprinting*. Jika virus menyerang arahan-arahan di dalam sesuatu program, ia akan merubah arahan tersebut yang mana mengakibatkan *different checksumming*.

- Hanya satu-satu kaedah yang diketahui dapat mengesan semua virus sama ada sekarang, atau akan datang baik untuk jangka panjang bagi sesuatu organisasi.

- Ianya bersifat reaktif daripada proaktif yang bermaksud, serangan virus hanya dikesan setelah ia berlaku. Walaubagaimanapun, penggunaan yang berterusan perisian berkenaan biasanya akan dapat mengesan virus sebelum ia mula bertindak.

c) *Monitoring software* (virus khusus).

Kaedah ini biasanya akan memintas sebarang bentuk aplikasi seperti *LOAD, EXECUTE*, membuka fail dan lain-lain. Biasanya ia dengan sendirinya berada di dalam program TSR (*terminate-stay-resident*)[12] supaya sentiasa bersedia untuk berbuat sesuatu pada ketika aplikasi ini sedang dilaksanakan.

Ciri-ciri khas:

- Pengesanan virus pada waktu sebenar.
- Biasanya menyebabkan sistem operasian komputer menjadi lambat.

d) *Monitoring software* (virus umum).

Perisian ini juga secara automatik akan dimasukan ke dalam sistem TSR. Ia akan memintas dan menyelia sebarang bentuk aplikasi untuk mengesan sebarang bentuk aktiviti virus. Aktiviti virus di sini bermaksud suatu set tindakan yang biasanya dijumpai. Contohnya seperti menulis kepada boot sektor, membuka arahan-arahan tertentu untuk menulis dan sebagainya.

Ciri-ciri khas:

- Virus dikesan pada masa sebenar.
- Tiada suatu peraturan khas tentang apakah yang sepatutnya dan apakah yang tidak sepatutnya dilakukan oleh virus, oleh kerana itu, amaran palsu biasanya berlaku kerana menyangka sesuatu aktiviti itu disebabkan oleh aktiviti virus. Mana-mana virus yang tidak termasuk di dalam konsep virus bagi program *monitoring* akan di abaikan. Di samping itu,

program ini juga menurunkan prestasi sistem dan boleh menyebabkan keseluruhan sistem tidak *compatible* dengan perisian jaringan atau program tertentu yang lain.

e) *Inoculation Software* (virus khusus).

Perisian *inoculation* berfungsi melabel disket atau arahan-arahan di dalam sesuatu program di dalam cara yang mana menyebabkan virus tidak akan menjangkitinya. Masalah yang dihadapi ialah ia tidak dapat melabel bagi semua jenis virus, kerana setiap virus mempunyai ciri-cirinya tersendiri(Jan Hruska 1992 : 87-95).

Kebanyakan syarikat antivirus yang terdapat pada hari ini menghasilkan suatu perisian yang boleh memenuhi semua bentuk antivirus yang telah dihuraikan diatas. Contohnya antivirus McAfee yang merupakan jenis antivirus yang spesifik yang memenuhi semua bentuk antivirus dibawah kategori antivirus spesifik manakala Norton antivirus pula merupakan jenis antivirus yang spesifik yang memenuhi semua ciri-ciri yang terdapat dibawah kategorinya. Perlaksanaannya lebih drastik daripada antivirus McAfee.

[1] Autonomi membawa maksud kemampuan untuk melakukan pilihan. bertanggungjawab dan mampu untuk membuat sebarang penilaian tanpa dipengaruhi oleh pihak lain.(Christine Henry 1995: 4-5).

[2] Lihat Paul F. Burton 1996.

[3] Christine Henry menerangkan bahawa kod tidak boleh menyelesaikan dilema moral tetapi ia mempunyai peranan penting ke arah itu.Lihat Christine Henry Professional Ethics and Organisational change in education and health, 1995. London, Edward Arnold.bab 2 dan bab 5.

[4] *Compiler* bermaksud aturcara khas yang direka untuk menukarkan aturcara yang disediakan dengan bahasa tahap tinggi(bahasa/aturcara punca) ke dalam kod mesin(aturcara objek) sebelum ia boleh dijalankan oleh komputer. Pengkompilasi akan menterjemahkan setiap penyataan kepada kod mesin sambil memasukkan sebarang subrutin dan sambungan antara aturcara di mana perlu dan kemudian menyimpan seluruh aturcara objek itu ke dalam storan sebelum ia dijalankan(Zoraini Wati Abas et. al. 1994 : 42).

[5] *hyperlinks* bermaksud sambungan (*links)* yang bersifat dinamik. Ia akan menghubungkan semua laman web yang mempunyai sebutan yang sama di dalam WWW(World Wide Web). Pengunjung laman-laman ini boleh berpindah dari satu laman ke laman web yang lain hanya dengan mengunakan sebutan perkataan yang diingini (Neil Barret 1996 : 53).

[6] *URL* singkatan kepada (*Uniform resource locator*). Ia membawa maksud kaedah untuk menamakan alamat sumber-sumber di dalam internet. Satu URL akan menentukan jenis sumber dan alamat internet(Cheryl Harris 1996). Ia juga boleh diterangkan sebagai satu bentuk yang menentukan protokol dan alamat bagi capaian maklumat di Internet (Abu Bakar 1998 : 94-117).

[7] *Settings* bermaksud cara yang boleh mengubah ukuran-ukuran bacaan yang dikehendaki(Oxford Advanced Learner's).

[8] *browsing* aktiviti meninjau laman-laman World Wide Web(Abu Bakar 1998 : 94-117).

[9] *newsgroup* adalah nama yang diberikan kepada satu kumpulan perbincangan di dalam *Usenet*. Usenet adalah sistem rangkaian kumpulan perbincangan yang bersambungan ke seluruh dunia melalui talian komputer dan melibatkan penglibatan berjuta-juta orang (Cheryl Harris 1996 : 153).

[10] *Interface* pengantara muka atau penghubung di antara komputer dan mesin atau sistem lain (Abu Bakar 1998 : 94-117).

[11] *TSR* (*Terminate And Stay Resident Program*). Ia adalah satu program yang dimasukkan ke dalam ingatan komputer supaya boleh dilaksanakan untuk membuat sesuatu semasa perisian aplikasi lain sedang digunakan(Zoraini Wati Abas 1994 :183).