**TUGAS MAKALAH**

**Etika Profesi dalam Keamanan Sistem Informasi Dibidang TI yang Bekerja Di CrowdStrike**

****

**DISUSUN OLEH**

 **ULFAH ROJIYYAH (D42114512)**

 **TRI WAHYUNI (D42114507)**

**TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK UNIVERSITAS HASANUDDIN**

**2017**

**KATA PENGANTAR**

Puji dan syukur atas kehadirat Tuhan Yang Maha Esa atas rahmatnya sehingga kami dapat menyelesaikan makalah ini tepat pada waktunya. Makalah ini dibuat untuk memenuhi  tugas mata kuliah Etika Profesi. Dalam makalah ini kami membahas tentang etika, profesi, teknologi informasi, etika profesi di bidang TI, kode etik, CrowdStrike, keamanan dalam sistem informasidanperlunya etika dalam pemanfaatan teknologi informasi. Ucapan terima kasih pun tidak lupakami ucapkan kepada pihak yang telah membantu kami dalam menyelesaikan makalah ini yang tidak dapat disebutkan satu per satu.

 Kami menyadari bahwa makalah ini sangat jauh dari kesempurnaan, oleh karena itu masukan berupa kritikan dan saran sangat kami harapkan demi penyempurnaan makalah ini. Akhir kata,kiranya makalah ini dapat berguna dan bisa menjadi pedoman bagi mahasiswa untuk dapat mempelajari serta memahami tentang etika profesi. Sekian dan terima kasih.

                                                                                     Makassar, 7 Mei 2017

DAFTAR ISI
Kata Pengantar …………………………………………………………………………………...ii
Daftar Isi …………………………………………………………………………………............iii

BAB 1. PENDAHULUAN
1.1 Latar Belakang ……………………………………………………………………………….1

BAB 2 PEMBAHASAN
2.1 Pengertian Etika Profesi ……………………………………………………………………..2
2.2 Pengertian Teknologi InformasI……………………………………………………………...2
2.3 Etika Profesi dalam bidang TI………………………………………………………………..2
2.4 Kode Etik……………………………………………………………………………………..3
2.5 CrowdStrike ………………………………………………………………………………….3
2.6 Keamanan Dalam Sistem Informasi………………………………………………………….4
2.7 Etika Dalam Sistem Informasi………………………………………………………………12

BAB 3 KESIMPULAN
3.1 kesimpulan…………………………………………………………………………………...18
DAFTAR PUSTAKA …………………………………………………………………………...19

BAB I

PENDAHULUAN

I.1 Latar Belakang

Suatu kode etik menggambarkan nilai-nilai profesional suatu profesi yang diterjemahkan ke dalam standart perilaku anggotanya. Nilai professional paling utama adalah keinginan untuk memberikan pengabdian kepada masyarakat. Kode etik dijadikan standart aktivitas anggota profesi, kode etik tersebut sekaligus sebagai pedoman (guidelines).

Kode Etik dapat diartikan pola aturan, tata cara, tanda cara, tanda pedoman etis dalam melakukan suatu kegiatan atau pekerjaan. Kode etik merupakan pola aturan atau tata cara sebagai pedoman berperilaku. Dalam kaitannya dengan profesi, bahwa kode etik merupakan tata cara aturan yang menjadi standart kegiatan anggota suatu profesi.

Kata etika sendiri berasar dari bahasa Yunani yaitu Ethos yang berarti adat istiadat atau kebiasaan.Oteng / Sutisna (1986 : 364) mendefinisikan bahwa kode etik sebagai pedoman yang memaksa perilaku etis anggota profesi. Bahwasannya setiap orang harus menjalankan serta menjiwai akan pola ketentuan aturan, karenapada dasarnya suatau tindakan yang tidak menggunakan kode etik akan berhadapan dengan sanksi.

Salah satu profesi dibidang teknologi informasi adalah Programmer, seorang programmer harus memiliki pengalaman yang cukup dan benar-benar mengusai ilmu dibidangnya, selain itu seorang programmer juga harus mematuhi kode etik yang berlaku. Maka dari itu kode etik programmer perlu dipelajari, dimengerti dan dijalankan.

I.2 Tujuan

Penyusunan makalah ini bertujuan agar pembaca dapat mengetahui dan memahami tentang etika profesi, teknologi informasi, etika profesi di bidang TI, kode etik, keamanan dalam sistem informasi dan etika dalam sistem informasi.

I.3 Rumusan Masalah

Masalah yang akan dibahas dalam makalah ini sebagaimana yang telah dijabarkan dalam latar belakang diatas adalah :

1. Pengertian Etika Profesi dan Teknologi Informasi
2. Etika profesi di bidang TI
3. Kode etik di bidang TI
4. CrowdStrike
5. Keamanan dalam sistem informasi
6. Etika dibidang sistem informasi

BAB II

PEMBAHASAN

**2.1 Pengertian Etika Profesi**
Etik (atau etika) berasal dari kata ethos (bahasa Yunani) yang berarti karakter, watak kesusilaan atau adat. Sebagai suatu subyek, etika akan berkaitan dengan konsep yang dimilki oleh individu ataupun kelompok untuk menilai apakah tindakan-tindakan yang telah dikerjakannya itu salah atau benar, buruk atau baik.Etika merupakan sebuah cabang filsafat yang berbicara mengenai nilai dan norma moral yang menentukan perilaku manusia dalam hidupnya. Profesi adalah pekerjaan yang dilakukan sebagai kegiatan pokok untuk menghasilkan nafkah hidup dan yang mengandalkan suatu keahlian. Berdasarkan pengertian tersebut dapat dijelaskan bahwa etika profesi dalah keterampilan seseorang dalam suatu pekerjaan utama yang diperoleh dari jalur pendidikan atau pengalaman dan dilaksanakan secara kontinu yang merupakan sumber utama untuk mencari nafkah. Etika profesi adalah sikap hidup berupa keadilan untuk memberikan pelayanan profesional terhadap masyarakat dengan ketertiban penuh dan keahlian sebagai pelayanan dalam rangka melaksanakan tugas berupa kewajiban terhadap masyarakat. profesi tidak dapat dipegang oleh sembarang orang, akan tetepi memerlukan suatu persiapan melelui pendidikan dan pelatihan yang dikembangkan khusus untuk itu.

**2.2 Teknologi Informasi (TI)**

Teknologi Informasi atau dalam bahasa Inggris dikenal dengan istilah Information technology (IT) adalah istilah umum untuk teknologi apa pun yang membantu manusia dalam membuat, mengubah, menyimpan, mengomunikasikan dan/atau menyebarkan informasi. TI menyatukan komputasi dan komunikasi berkecepatan tinggi untuk data, suara, dan video. Contoh dari Teknologi Informasi bukan hanya berupa komputer pribadi, tetapi juga telepon, TV, peralatan rumah tangga elektronik, dan peranti genggam modern. TI adalah bidang pengelolaan teknologi dan mencakup berbagai bidang yang termasuk tetapi tidak terbatas pada hal-hal seperti proses, perangkat lunak komputer, sistem informasi, perangkat keras komputer, bahasa program , dan data konstruksi. Singkatnya, apa yang membuat data, informasi atau pengetahuan yang dirasakan dalam format visual apapun, melalui setiap mekanisme distribusi multimedia, dianggap bagian dari TI.

**2.3 Etika Profesi di Bidang IT**

Teknologi, Informasi dan Komunikasi bisa menjadi pilar-pilar pembangunan nasional yang bisa mengadaptasi di setiap permasalahan bangsa sebagai contoh menyerap tenaga kerja baru, mencerdaskan kehidupan bangsa dan sebagai alat pemersatu bangsa. Dalam mengaplikasikan ilmunya atau menjalankan profesi IT bukan mudah dan bukan tidak sukar, yang terpenting adalah kita mampu menempatkan diri pada posisi yang benar. Profesi IT dianggap orang lain adalah profesi khusus karena keahlian yang ia miliki maka dari itu kita bisa menentukan tapi dengan ikatan yang jelas. Profesi IT juga bisa dianggap sebagai 2 mata pisau, bagaimana yang tajam bisa menjadikan IT lebih berguna untuk kemaslahatan umat dan mata lainya bisa menjadikan IT ini menjadi bencana sosial, bencana ekonomi maupun krisis kebudayaan yang saat ini sering terjadi yaitu Pembuatan website porno, seorang hacker melakukan pengacakan rekening sebuah bank dan melakukan kebohongan dengan konten-konten tertentu, dan lain-lain. Kita juga harus bisa menyikapi dengan keadaan teknologi, informasi dan komunikasi saat ini dengan arus besar data yang bisa kita dapat dengan hitungan per detik ataupun dengan kesederhanaan teknologi kita bisa melakukan pekerjaan kita menjadi praktis, tapi kita harus melakukan pembenahan terhadap teknologi sebagai inovasi untuk meringankan maupun memberantas resiko kejamnya teknologi itu sendiri. Dengan membangun semangat kemoralan dan sadar akan etika sebagai orang yang ahli di bidang IT . Tentu saja diharapkan etika profesi semakin dijunjung ketika jenjang pendidikan kita berlatar IT makin tinggi. Sedangkan keahlian dilapangan meningkat seiring banyaknya latihan dan pengalaman.

**2.4 Kode Etik**

Setiap bidang profesi memiliki aturan-aturan / hukum-hukum yang mengatur bagaimana seorang profesional berfikir dan bertindak. Seseorang yang melakukan kesalahan kode etik dinyatakan melakukan malpratek dan bisa mendapatkan sanksi sesuai dengan peraturan yang diberikan. sanksi yang didapat buisa berubah teguran, sebutan tidak profesionalisme, dipecat, bahkan mendapatkan hukum pidana. Kode Etik di bidang IT juga diperlukan untuk mengatur bagaimana para IT profesional ini melakukan kegiatannya. Kode etik yang harus dimiliki oleh seorang IT adalah :

1. Orang IT harus bertanggung jawab terhadap hardware dan software. Yang dimaksud hardware adalah barang-barang IT yang bisa disentuh, seperti monitor,printer,scanner,dll.

2. Peranannya yang sangat besar dan mendasar dalam perusahaan menuntut orang IT untuk mempertanggungjawabkan perbuatannya secara profesi. Orang IT akan berperan penting dalam pengolahan data, penggunaan teknologi, dan peningkatan terus-menerus akan bisnis proses suatu perusahaan agar perusahaan mempunyai daya saing tinggi. Bisnis proses adalah suatu rangkaian proses dalam perusahaan yang melibatkan berbagai input untuk menghasilkan output yang berkualitas secara berkualitas, sehingga perusahaan dapat menghasilkan laba. Karena demikian pentingya suatu bisnis proses dalam suatu perusahaan, maka sudah dipastikan bisnis proses suatu perusahaan tidak boleh bocor ke perusahaan pesaing.

3. Orang IT sebagai orang yang paling tahu akan bisnis proses perusahaan mempunyai kode etik yang mendasar untuk menjaga kerahasiaannya. Perusahaan sendiri mengantisipasi hal ini dengan adanya kontrak kerahasiaan yang wajib ditandatangani oleh orang IT.

4. Sangat diutamakan bahwa seorang IT harus mempunyai etika yang membangun.

**2.5 CrowdStrike**

CrowdStrike merupakan perusahaan cybersecurity yang berfungsi untuk melindungi privasi baik negara, perusahaan, organisasi atau seseorang. CrowdStrike didirikan oleh pengusaha George Kurtz (CEO),[Dmitri Alperovitch](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Dmitri_Alperovitch&usg=ALkJrhi86EKm_HciVBPOlUHudRQ4ywFCYA) (CTO), dan Gregg Marston (CFO, pensiun). Pada tahun 2012, Shawn Henry, mantan eksekutif FBI yang memimpin divisi kejahatan dan cyber FBI, dipekerjakan untuk memimpin perusahaan sejenis CrowdStrike Services, Inc., yang berfokus pada layanan respons proaktif dan insiden.

Perusahaan memperoleh pengakuan karena memberikan intelijen ancaman dan atribusi kepada aktor negara negaramelakukan spionase ekonomi dan pencurian IP. Ini termasuk jalan keluar dari kelompok Cina yang disponsori pemerintah, Putter Panda, terkait dengan mata-mata [China](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/China&usg=ALkJrhhe18YDVuC5i0xlP0WSPiDqZOs8Pw) terhadap [industri](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/China&usg=ALkJrhhe18YDVuC5i0xlP0WSPiDqZOs8Pw) pertahanan dan satelit AS dan satelit.Pada bulan Mei 2014, didukung oleh laporan CrowdStrike, Departemen Kehakiman AS menugaskan lima hacker militer China untuk melakukan spionase cyber ekonomi terhadap perusahaan-perusahaan AS. Demikian pula, perusahaan tersebut dikenal karena mengungkap aktivitas Bear Energetic, sebuah kelompok musuh yang berhubungan dengan Federasi Rusia yang melakukan operasi intelijen melawan berbagai korban global dengan fokus utama pada sektor energi.

Setelah hack Sony Pictures yang sangat umum, CrowdStrike mengajukan atribusi kepada pemerintah Korea Utara dalam waktu 48 jam dan menunjukkan bagaimana serangan tersebut dilakukan selangkah demi selangkah.Pada bulan Mei 2015, perusahaan tersebut merilis temuan Vener, Jason Geffner, sebuah cacat kritis pada hypervisor open source yang disebut Quick Emulator (QEMU), yang digunakan di sejumlah produk virtualisasi umum.

Pada tahun 2014, perusahaan meluncurkan platform Falcon, sebuah teknologi yang menghentikan pelanggaran dengan menggabungkan antivirus, deteksi endpoint dan respons generasi berikutnya, dan perburuan proaktif. Juga pada tahun 2014, CrowdStrike berperan penting dalam mengidentifikasi anggota [PLA Unit 61486](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/PLA_Unit_61486&usg=ALkJrhgCiw4B9lGPdDltZ7FMnLj-fXvOmQ) sebagai pelaku sejumlah serangan cyber pada infrastruktur AS.

Pada bulan Juli 2015, [Google](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Google&usg=ALkJrhhKf5WqPdxE3pIe4f0RguvdL8pK4g) melakukan investasi di bundling pendanaan [Seri C perusahaan](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Series_C_round&usg=ALkJrhhImR1gfZrwptf758qIpRYlscAKww) , yang totalnya mengumpulkan $ 100 juta. Sampai saat ini, CrowdStrike telah mencapai total dana sebesar $ 156 juta, dengan investor lain termasuk [Rackspace](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Rackspace&usg=ALkJrhiQYMx4V8INKL4Q7Nk0z7puOr9RvQ) , [Accel Partners](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Accel_Partners&usg=ALkJrhh7FEn2EfDXOLABKbR5nRZRyePKkw) dan [Warburg Pincus](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/Warburg_Pincus&usg=ALkJrhiCm6xmiUhMHomDyRUTPAEwkNNMoA) . [[15]](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/CrowdStrike&usg=ALkJrhicKEzoVM37AVTYSQYXKB4hDPbRQg#cite_note-15) [[16]](https://translate.googleusercontent.com/translate_c?depth=1&hl=id&prev=search&rurl=translate.google.co.id&sl=en&sp=nmt4&u=https://en.wikipedia.org/wiki/CrowdStrike&usg=ALkJrhicKEzoVM37AVTYSQYXKB4hDPbRQg#cite_note-16) Menurut perusahaan, pelanggannya mencakup tiga dari 10 perusahaan global terbesar berdasarkan pendapatan, lima dari 10 institusi keuangan terbesar, tiga dari 10 penyedia layanan kesehatan teratas, dan tiga dari 10 perusahaan energi teratas.

### **2.6 Keamanan Dalam Sistem Informasi**

Jika kita berbicara tentang keamanan sistem informasi, selalu kata kunci yang dirujuk adalah pencegahan dari kemungkinan adanya virus, hacker, cracker dan lain-lain. Padahal berbicara masalah keamanan sistem informasi maka kita akan berbicara kepada kemungkinan adanya resiko yang muncul atas sistem tersebut (lihat tulisan strategi pendekatan manajemen resiko dalam pengembangan sistem informasi). Sehingga pembicaraan tentang keamanan sistem tersebut maka kita akan berbicara 2 masalah utama yaitu :

1. Threats (Ancaman) atas sistem dan
2. Vulnerability (Kelemahan) atas sistem

Masalah tersebut pada gilirannya berdampak kepada 6 hal yang utama dalam sistem informasi yaitu :

* Efektifitas
* Efisiensi
* Kerahaasiaan
* Integritas
* Keberadaan (availability)
* Kepatuhan (compliance)
* Keandalan (reliability)

Untuk menjamin hal tersebut maka keamanan sistem informasi baru dapat terkriteriakan dengan baik. Adapun kriteria yag perlu di perhatikan dalam masalah keamanan sistem informasi membutuhkan 10 domain keamanan yang perlu di perhatikan yaitu :

1. Akses kontrol sistem yang digunakan
2. Telekomunikasi dan jaringan yang dipakai
3. Manajemen praktis yang di pakai
4. Pengembangan sistem aplikasi yang digunakan
5. Cryptographs yang diterapkan
6. Arsitektur dari sistem informasi yang diterapkan
7. Pengoperasian yang ada
8. Busineess Continuity Plan (BCP) dan Disaster Recovery Plan (DRP)
9. Kebutuhan Hukum, bentuk investigasi dan kode etik yang diterapkan
10. Tata letak fisik dari sistem yang ada

Dari domain tersebutlah isu keamanan sistem informasi dapat kita klasifikasikan berdasarkan ancaman dan kelemahan sistem yang dimiliki.

### ANCAMAN (Threats)

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman yang mungkin timbul dari kegiatan pengolahan informasi berasal dari 3 hal utama, yaitu :

1. Ancaman Alam
2. Ancaman Manusia
3. Ancaman Lingkungan

**Ancaman Alam**

Yang termasuk dalam kategori ancaman alam terdiri atas :

* Ancaman air, seperti : Banjir, Stunami, Intrusi air laut, kelembaban tinggi, badai, pencairan salju
* Ancaman Tanah, seperti : Longsor, Gempa bumi, gunung meletus
* Ancaman Alam lain, seperti : Kebakaran hutan, Petir, tornado, angin ribut

**Ancaman Manusia**

Yang dapat dikategorikan sebagai ancaman manusia, diantaranya adalah :

* Malicious code
* Virus, Logic bombs, Trojan horse, Worm, active contents, Countermeasures
* Social engineering
* Hacking, cracking, akses ke sistem oleh orang yang tidak berhak, DDOS, backdoor
* Kriminal
* Pencurian, penipuan, penyuapan, pengkopian tanpa ijin, perusakan
* Teroris
* Peledakan, Surat kaleng, perang informasi, perusakan

**Ancaman Lingkungan**

Yang dapat dikategorikan sebagai ancaman lingkungan seperti :

* Penurunan tegangan listrik atau kenaikan tegangan listrik secara tiba-tiba dan dalam jangka waktu yang cukup lama
* Polusi
* Efek bahan kimia seperti semprotan obat pembunuh serangga, semprotan anti api, dll
* Kebocoran seperti A/C, atap bocor saat hujan

Besar kecilnya suatu ancaman dari sumber ancaman yang teridentifikasi atau belum teridentifikasi dengan jelas tersebut, perlu di klasifikasikan secara matriks ancaman sehingga kemungkinan yang timbul dari ancaman tersebut dapat di minimalisir dengan pasti. Setiap ancaman tersebut memiliki probabilitas serangan yang beragam baik dapat terprediksi maupun tidak dapat terprediksikan seperti terjadinya gempa bumi yang mengakibatkan sistem informasi mengalami mall function.

### Kelemahan (Vurnerability)

Adalah cacat atau kelemahan dari suatu sistem yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh pelaku yang mencoba menyusup terhadap sistem tersebut. Cacat sistem bisa terjadi pada prosedur, peralatan, maupun perangkat lunak yang dimiliki, contoh yang mungkin terjadi seperti : Seting firewall yang membuka telnet sehingga dapat diakses dari luar, atau Seting VPN yang tidak di ikuti oleh penerapan kerberos atau NAT.

Suatu pendekatan keamanan sistem informasi minimal menggunakan 3 pendekatan, yaitu :

1. Pendekatan preventif yang bersifat mencegah dari kemungkinan terjadikan ancaman dan kelemahan

2. Pendekatan detective yang bersifat mendeteksi dari adanya penyusupan dan proses yang mengubah sistem dari keadaan normal menjadi keadaan abnormal

3. Pendekatan Corrective yang bersifat mengkoreksi keadaan sistem yang sudah tidak seimbang untuk dikembalikan dalam keadaan normal

Tindakan tersebutlah menjadikan bahwa keamanan sistem informasi tidak dilihat hanya dari kaca mata timbulnya serangan dari virus, mallware, spy ware dan masalah lain, akan tetapi dilihat dari berbagai segi sesuai dengan domain keamanan sistem itu sendiri.

**C. Macam-Macam Virus yang Menyerang Komputer**

Karena berbicara tentang keamanan SI maka yang satu inipun tidak boleh dilupakan yaitu virus. Virus Komputer adalah program yang mengganggu sistem kerja komputer, sehingga dapat menyebabkan komputer sering ngehang, lelet, bluescreen, bahkan sampai-sampai untuk mengatasinya kita harus melakukan instal ulang komputer kita. Nah sebelum komputer kita terserang virus ada baiknya sedikit banyak kita mengetahui macam-macam virus komputer. Seperti yang saya kutip dari berbagai sumber, di sini saya akan membagi ilmu saya dengan anda semua. Macam-macam virus:

**1. Virus Compiler**

virus yang sudah di compile sehingga dapat dieksekusi langsung. Ini adalah virus yang pertama kali muncul di dunia komputer, dan mengalami perkembangan pesat sekarang. Virs pertama ini sangatlah sulit dibasmi karena dibuat dengan bahasa rendah, assembler. Memang bahasa ini cocok untuk membuat virus namun sangatlah susah menggunakannya. Keunggulan dari virus ini adalah mampu melakukan hampir seluruh manipulasi yang mana hal ini tidak selalu dapat dilakukan oleh virus jenis lain karena lebih terbatas.

**2. Virus Bagle BC**

virus ini ini termasuk salah satu jenis virus yang berbahaya dan telah masuk peringkat atas jenis virus yang paling cepat mempengaruhi komputer kita. Beberapa jam sejak keluarnya virus ini, sudah terdapat 2 buah varian Bagle ( Bagle BD dan BE )yang menyebar melalui e-mail, jaringan komputer dan aplikasi P2P. Virus ini menyebar melalui e-mail dengan berbagai subyek berbeda. Menurut suatu penelitian dari Panda Software virus Bagle BC ini menyusup ke dalam e-mail dengan subyek antara lain : Re:, Re:Hello, Re:Hi, Re:Thank you, Re:Thanks. Attachment-nya juga bermacam-macam, antara lain : .com, .cpl, .exe, .scr. Virus Bagle BC juga mampu untuk menghentikan kerja program-program antivirus.

**3. Virus File**

adalah virus yang memanfaatkan file yang dapat diijalankan/dieksekusi secara langsung. Biasanya file \*.EXE atau \*.COM. Tapi bisa juga menginfeksi file \*.SYS, \*.DRV, \*.BIN, \*.OVL dan \*.OVY. Jenis Virus ini dapat berpindah dari satu media ke semua jenis media penyimpanan dan menyebar dalam sebuah jaringan.

**4. Virus Sistem**

atau lebih dikenal sebagai virus Boot. Kenapa begitu karena virus ini memanfaatkan file-file yang dipakai untuk membuat suatu sistem komputer. Sering terdapat di disket/tempat penyimpanan tanpa sepengetahuan kita. Saat akan menggunakan komputer(restart), maka virus ini akan menginfeksi Master Boot Sector dan System Boot Sector jika disket yang terinfeksi ada di drive disket/tempat penyimpanan.

**5. Virus Boot Sector**

virus yang memanfaatkan hubungan antar komputer dan tempat penyimpanan untuk penyebaran virus.Apabila pada boot sector terdapat suatu program yang mampu menyebarkan diri dan mampu tinggal di memory selama komputer bekerja, maka program tersebut dapat disebut virus. Virus boot sector terbagi dua yaitu virus yang menyerang disket dan virus yang menyerang disket dan tabel partisi.

**6. Virus Dropper**

suatu program yang dimodifikasi untuk menginstal sebuah virus komputer yang menjadi target serangan. setelah terinstal, maka virus akan menyebar tetapi Dropper tidak ikut menyebar. Dropper bisa berupa nama file seperti Readme.exe atau melalui Command.com yang menjadi aktif ketika program berjalan. Satu program Dropper bisa terdapat beberapa jenis Virus.

**7. Virus Script/Batch**

awalnya virus ini terkenal dengan nama virus batch seperti yang dulu terdapat di file batch yang ada di DOS.Virus script biasanya sering didapat dari Internet karena kelebihannya yang fleksibel dan bisa berjalan pada saat kita bermain internet, virus jenis ini biasanya menumpang pada file HTML (Hype Text Markup Language) dibuat dengan menggunakan fasilitas script seperti Javascript, VBscript,4 maupun gabungan antara script yang mengaktifkan program Active-X dari Microsoft Internet Explorer.

**8. Virus Macro**

virus yang dibuat dengan memanfaatkan fasilitas pemrograman modular pada suatu program aplikasi seperti Ms Word, Ms Excel, Corel WordPerfect dan sebagainya. Walaupun virus ini terdapat didalam aplikasi tertentu tetapi bahaya yang ditimbulkan tidak kalah berbahanya dari virus-virus yang lain.

**9. Virus Polymorphic**

dapat dikatakan virus cerdas karena virus dapat mengubah strukturnya setelah melaksanakan tugas sehingga sulit dideteksi oleh Antivirus.

**10. Virus Stealth**

virus ini menggunakan cara cerdik, yakni dengan memodifikasi struktur file untuk meyembunyikan kode program tambahan di dalamnya. Kode ini memungkinkan virus ini dapat menyembunyika diri. Semua jenis virus lain juga memanfaatkan kode ini. Ukuran-ukuran file tidak berubah setelah virus menginfeksi file.

**11. Virus Companion**

virus jenis ini mencari file \*.EXE untuk membuat sebuah file \*.COM dan menyalin untuk meletakkan virus. Alasannya, file \*.COM berjalan sebelum file \*.EXE.

**12. Worm**

ini adalah sebuah program yang bersifat parasit karena dapat menduplikasi diri. Akan tetapi, worm tidak menyerupai virus karena tidak menginfeksi program komputer lainnya. Oleh karena itu, Worm tidak digolongkan ke dalam virus. Mainframe adalah jenis komputer yang sering diserang Worm. Penyebarannya pada komputer lainnya melalui jaringan. Dalam perkembangannya Worm mengalami “mutasi genetik” sehingga selain membuat suatu file baru, ia pun akan berusaha menempelkan dirinya sendiri ke suatu file, ini biasa disebut virus Hybrid.

**13. Virus Hybrid**

virus ini merupakan virus yang mempunyai dua kemampuan biasanya dapat masuk ke boot sector dan juga dapat masuk ke file. Salah satu contoh virus ini adalah virus Mystic yang dibuat di Indonesia.

**14. Trojan horse**

disebut juga kuda troya. Trojan menginfeksi komputer melalui file yang kelihatannya tidak berbahaya dan biasanya justru tampaknya melakukan sesuatu yang berguna. Namun akhirnya virus menjadi berbahaya, misalnya melakukan format hardisk.

**15. Backdoor Alnica**

virus yang juga berbahaya ini merupakan salah satu tipe virus Trojan Horse. Merupakan salah satu virus backdoor yang jika berhasil menginfeksi komputer akan mampu melakukan akses dari jarak jauh dan mengambil segala informasi yang diinginkan oleh si penyerang. Sistem operasi yang diserang oleh virus tersebut antara lain : Windows 200, Windows 95, Windows 98, Windows Me, Windows NT dan Windows XP. Virus ini berukuran sebesar 57.856 byte

**16. Trojan di Linux.**

Para pengguna linux Red Hat diharapkan untuk berhati-hati terhadap PATCH yang dikirm melalui e-mail dengan alamat "security@redhat.com" karena itu sebenarnya bukannya patch security tetapi virus Trojan yang bisa mengacaukan sistem keamanan. E-mail peringatan dari Red Hat biasanya selalu dikirim dari alamat "secalert@redhat.com" dan ditandatangani secara digital. Virus ini juga pernah menyerang sistem keamanan Windows tahun 2003 dengan subyek menawarkan solusi keamanan.Rupanya di Linux juga bisa kena virus. Inilah salah satu akibat perkembangan teknologi. Mulai sekarang, semakin berhati-hatilah dan jangan sembarangan mengcopy sebuah file dari source lain lalu di-paste ke komputer anda. Dengan mengupdate antivirus dapat meningkatkan security komputer.

**D. MACAM-MACAM HACKER**

Banyak orang mengira hacker itu profesi yang jahat, padahal tidak semua hacker itu jahat. Ada beberapa jenis hacker yang juga bisa berguna. Istilah Hacker biasa dipakai untuk mendeskripsikan seorang individu ahli teknologi yang memiliki kemampuan untuk mengontrol komputer, aplikasi atau situs orang lain melalui tanpa seizin si pelaku.
Akan tetapi, tahukah agan bahwa ada beberapa jenis hacker yang berbeda, dan tidak semuanya adalah jahat?

Berikut ini adalah 6 jenis hacker (Hats Hacker) yang berbeda:

**1. White Hat Hacker**

White hat hacker, mereka juga dikenal sebagai ethical hacker, adalah asal muasal dari information technology, seorang yang secara etik melawan serangan terhadap sistem komputer.
Mereka sadar bahwa internet sekarang adalah perwakilan dari suara umat manusia. Seorang White Hat akan memfokuskan dirinya untuk membangun jaringan keamanan (security system), dimana Black Hat (lawannya) akan mencoba menghancurkannya.White Hat juga seringkali digambarkan sebagai orang yang menerobos jaringan untuk menolong si pemiliki jaringan menemukan cacat pada system keamanannya. Banyak dari mereka yang dipekerjakan oleh perusahaan computer security; mereka disebut sebagai sneakers. Sekumpulan dari orang-orang ini disebut Tiger Teams.Perbedaan mendasar antara White dan Black Hat adalah White Hat Hacker mengklaim mereka mengobservasi dengan Etika Hacker. Seperti Black Hat, White Hat biasanya sangat mengerti internal detail dari security system, dan dapat menciptakan kode untuk memecahkan masalah yang ada.

**2. Red Hat Hacker**
Secara sederhana, Red Hat Hacker berpikir dengan:
\* Hat (Red = Fire) / Perumpamaan Red Hat seperti Api
\* Intuition = Intuisi adalah perasaan yang tak dapat dijelaskan bahwa sesuatu itu benar bahkan ketika Anda tidak punya bukti atau bukti itu
\* Opinion = Pendapat, menilai sesuatu dari sisi yang berbeda.
\* Emotion (subjective) = Emotion is everything.

**3. Yellow Hat Hacker**
Secara sederhana, Yellow Hat Hacker berpikir dengan:
\* Hat (Yellow = Sun) / Perumpamaan Yellow Hat seperti Matahari
\* Praise = Pujian, mereka melakukan itu untuk ketenaran (fame)
\* Positive aspects (objective) = Berbuat untuk mendapatkan aspek yang positif

**4. Black Hat Hacker**
Black hat (juga dikenal sebagai Darkside Hacker) adalah hacker berorientasi criminal dengan sifat perusak.
Biasanya mereka ada diluar security industry dan oleh para modern programmers. Biasanya Black hat adalah seorang yang memiliki pengetahuan tentang kecacatan system dan mengeksploitasinya untuk mendapatkan keuntungan pribadi. Banyak Black Hat mengutamakan kebebasan individu daripada accessibility dari privacy dan security. Black Hats akan mencari cara untuk membuat lubang yang terbuka pada system menjadi semakin lebar; mereka akan melakukan cara-cara untuk membuat seseorang memiliki kontrol atas system. Black hat akan bekerja untuk menghasilkan kerusakan dan/atau untuk mengancam dan memeras seseorang.Black-hat hacking adalah sebuah tindakan yang tidak disetujui untuk membobol system tanpa seijin dari pihak berwenang, biasanya dilakukan pada komputer yang terhubung dengan jaringan.

**5. Green Hat Hacker**
Secara sederhana, seorang Green Hat Hacker berpikir:
\* Hat (Green = Plant) / Perumpamaan Green Hat seperti Tanaman
\* Alternatives = Mempunya beragam cara alternatif
\* New approaches = Pendekatan baru, melakukan sesuatu dengan cara yang baru
\* Everything goes (speculatif) = Sepotong informasi yang bersifat spekulatif, berdasarkan dugaan bukan pengetahuan (Pola pikir Green Hat)

**6. Blue Hat Hacker**
Secara sederhana, Blue Hat Hacker berpkir dengan:
\* Hat (Blue = Sky) / Perumpamaan Blue Hat seperti Langit
\* Big Picture = Mempunyai gambaran yang hebat tentang suatu hal.
\* Conductor hat = Diibaratkan seperti konduktor.
\* Thinking about thinking = Memikirkan apa yang dipikirkan (Genius nih gan) :iloveindonesia
\* Overall process (overview) = Keseluruhan proses.
\* Menunjuk kepada perusahaan konsultasi komputer security yang digunakan untuk menjalankan bug test sebelum system dijalankan.

**7. Grey Hat Hacker**
Grey hat dalam komunitas komputer securityadalah hacker dengan skill yang kadang-kadang bertindak secara legal dengan itikad baik, tapi kadang juga tidak. Ia adalah perpaduan dari white dan black hat hackers. Mereka meng-hack untuk keuntungan pribadi tapi tidak memiliki tujuan yang merusak.Sebagai contoh, sebuah serangan terhadap bisnis perusahaan dengan praktik tidak etis dapat dikatakan sebagai tindakan Black Hat.Tetapi, seorang Gray Hat tidak akan melakukan sesuatu yang jahat, walaupun dia telah melanggar hukum. Jadi bukannya dikatakan sebagai Black Hat, dia dikatakan sebagai Grey Hat Hack. Seorang yang masuk ke system komputer hanya untuk meninggalakan jejak, dan tidak melakukan tindakan perusakan, ini yang dinamakanGrey Hat.

**Contoh Kasus:**
1. **Pencurian dan penggunaan account Internet milik orang lain**. Salah satu kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya account pelanggan mereka yang “dicuri” dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, “pencurian” account cukup menangkap “userid” dan “password” saja. Hanya informasi yang dicuri. Sementara itu orang yang kecurian tidak merasakan hilangnya “benda” yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini, penggunan dibebani biaya penggunaan acocunt tersebut. Kasus ini banyak terjadi di ISP. Namun yang pernah diangkat adalah penggunaan account curian oleh dua Warnet di Bandung.
2. **Membajak situs web**. Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman web, yang dikenal dengan istilah deface. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan.
3. **Probing dan port scanning**. Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan “port scanning” atau “probing” untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan firewall atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan. Berbagai program yang digunakan untuk melakukan probing atau portscanning ini dapat diperoleh secara gratis di Internet. Salah satu program yang paling populer adalah “nmap” (untuk sistem yang berbasis UNIX, Linux) dan “Superscan” (untuk sistem yang berbasis Microsoft Windows). Selain mengidentifikasi port, nmap juga bahkan dapat mengidentifikasi jenis operating system yang digunakan.
4. **Virus**. Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia . Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Kasus virus ini sudah cukup banyak seperti virus Mellisa, I love you, dan SirCam.
5.**Denial of Service (DoS) dan Distributed DoS (DDos) attack**. DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari berberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja.
6.**Kejahatan yang berhubungan dengan nama domain**. Nama domain (domain name) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah cybersquatting. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama domain adalah membuat “domain plesetan”, yaitu domain yang mirip dengan nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat ini adalah typosquatting.
7. **IDCERT ( Indonesia Computer Emergency Response Team)**. Salah satu cara untuk mempermudah penanganan masalah keamanan adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya “sendmail worm” (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk sebuah Computer Emergency Response Team (CERT). Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi point of contact bagi orang untuk melaporkan masalah kemanan. IDCERT merupakan CERT Indonesia .
8. **Sertifikasi perangkat security**. Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia. Di Korea hal ini ditangani oleh Korea Information Security Agency.

**2.7 Etika Dalam Sistem Informasi**

Masalah etika juga mendapat perhatian dalam pengembangan dan pemakaian system informasi. Masalah ini diidentifikasi oleh Richard Mason pada tahun 1986 yang mencakup privasi, akurasi, properti, dan akses, yang dikenal dengan akronim PAPA.

**1. Privasi**

Privasi menyangkut hak individu untuk mempertahankan informasipribadi dari pengaksesan oleh orang lainyang tidak diberi izin unruk melakukannya.

Contoh isu mengenai privasi sehubungan diterapkannya system informasi adalah pada kasus seorang manajer pemasaran yang ingin mengamati e-mail yang dimiliki para bawahannya karena diperkirakan mereka lebih banyak berhubungan dengan e-mail pribadi daripada e-mail para pelanggan. Sekalipun sang manajer dengan kekuasaannya dapat melakukan hal seperti itu, tetapi ia telah melanggarprivasi bawahannya.

Privasi dibedakan menjadi privasi fisik dan privasi informasi (Alter, 2002). Privasi fidik adalah hak seseorang untk mencegah sseseorang yangtidak dikehendaki terhadap waktu, ruang, dan properti (hak milik), sedangkan privasi informasi adalah hak individu untuk menentukan kapan, bagaimana, dan apa saja informasi yang ingin dikomunikasikan dengan pihak lain.

Penggunaan teknologi informasi berkecenderungan membuat pelanggaran terhadap privasi jauh lebih mudah terjadi. Sebagai contoh, para pemakai e-mail sering kali jengkel dengan kiriman-kiriman e-mail yang tak dikehendaki dan berisi informasi yang tidak berguna (junk e-mail).

Di America Derikat, masalah privasi diatur oleh undang-undang privasi. Berkaitan dengan hal ini, maka:

· Rekaman-rekaman data tdak boleh digunakan untuk keperluan lain yang bukan merupakan tujuan aslinya tanpa sepengetauhna individu bersangkutan.

· Setiap individu memiliki hak untuk melihat datanya sendiri dan membetulkan rekaman-rekaman yang menyangkut dirinya.

**2. Akurasi**

Akurasi terhadap informasi merupakan factor yang harus dpenuhi oleh sebuah sistem informasi. Ketidak akurasian informasi dapat menimbulkan hal yang mengganggu, merugikan, dan bahkan membahayakan.

Sebuah kasusakibat kesalahan penghapusan nomor keamanan social dialami oleh Edna Rismeller (Alter, 2002, hal.292). Akibatnya, kartu asuransinya tidak bias digunakan bahkan pemerintah menarik kembali cek pension sebesar $672 dari rekening banknya. Kisah lain dialami oleh para penyewa apartemen di Amerika yang karena sesuatu hal pernah bertengkar dengan pemiliki apartemen. Dampaknya, terdapat tanda tidak baik dalam basis data dan halini membuat mereka sulit untuk mendapatkan apartemen lain.

Mengingat data dalam sistem informasi menjadi bahan dalam pengambilan keputusan, keakurasiannya benar-benar harus diperhatikan.

**3. Properti**

Perlindungan terhadap hak properti yangsedang figalakkan saat ini yaitu dikenaldengan sebutan HAKI(hak atas kekayaan intelektual). Di Amerika Serikat, kekayaan intelektual diatur melalui tiga mekanisme, yaitu hak cipta (copyright), paten, dan rahasia perdagangan (trade secret).

· Hak cipta, adalah hak yang dijamin oleh kekuatan hokum yang melarang penduplikasian kekayaanintelektual tanpa seizing pemegangnya. Hak ini mudah untuk didapatkan dan diberikab kepada pemegangnya selamamasa hidup penciptanya plus 70 tahun.

· Paten, merupakan bentuk perlindungan terhadap kekayaan intelektual yang paling sulitdidapatkan karena hanyadiberikan pada penemuan-penemuaninovatif dan sangat berguna. Hukum paten memberikanperlindungan selama 20 tahun.

· Rahasia perdagangan, hokum rahasia perdagangan melindingi kekayaan intelektual melalui lisensi atau kontrak. Pada lisensi perangkat lunak, seseorang yang menandatanganikontrak menyetujui untuktidak menyalin perangkat lunak tersebut untuk diserahkan kepada oranglain atau dijual.

Masalah kekayaan intelektual merupakan faktor pentingyang perlu diperhatikan dalam sistem informasi untuk menghindari tuntutan dari pihak lain di kemudian hari. Isu pelanggaran kekayaan intelektual yangcukup seru pernah terjadi ketika terdapat gugatan bahwa sistem windows itu meniru sistem Mac. Begitu juga timbul perseteruan ketika muncul perangkat-perangkat lunak lain yang menyerupai spreadsheet Lotus 123. Kasus ini menimbulkan pertanyaan, “Apakah tampilan nuasa dari suatu perangkat lunak memang butuh perlindungan hak cipta?”.

Berkaitan dengan masalah intelektual, banyak masalah yang belum terpecahkan (Zwass, 1998), antara lain:

· Pada level apa informasi dapat dianggap sebagai properti?

· Apa yang harus membedakan antara satu produk dengan produk lain?

· Akankah pekerjaan yang dihasilkan oleh komputer memiliki manusia penciptanya? Jika tidak, lalu hak properti apa yang dilindunginya?

Isu yang juga marak sampai saat ini adalah banyaknya penyali perangkat lunak secara ilegal dengan sebutan pembajakan perangkat lunak (software privacy). Beberapa solusi untuk mengatasi hal ini telah banyak ditawarkan, namun belum memiliki penyelesaian, seperti sebaiknya software – terutana yang bias dijual massak – dijual dengan harga yang relative murah. Solusi yang mengkin bias figunakan untukperusahaan-perusahaan yang memiliki dana yangterbatas untukmemberli perangkat lunak yang tergolong sebagai open source.

**4. Akses**

Fokus dari masalah akses adalah pada penyediaanakses untuk semua kalangan. Teknologi informasi diharapkan tidak menjadi halangan dalam melakukan pengaksesan terhadap informasi bagi kelompok orang tertentu, tetapi justru untuk mendukung pengaksesan untuk semuapihak. Sebagai contoh, untuk mendukunf pengaksesan informasi Web bagi orang buta, TheProducivity Works ([www.prodworks.com](http://www.prodworks.com/)) menyediakan Web Broser khusus diberi nama pw WebSpeak. Browser ini memiliki prosesor percakapan dan dapat (Zwass, 1998).

**Perlunya Etika Dalam Pemanfaatan Teknologi Informasi**

Perlindungan atas hak individu di internet dan membangun hak informasi merupakan sebagian dari permasalahan etika dan sosial dengan penggunaan sistem informasi yang berkembang luas. Permasalahan etika dan sosial lainnya, di antaranya adalah: perlindungan hak kepemilikan intelektual, membangun akuntabilitas sebagai dampak pemanfaatan sistem informasi, menetapkan standar untuk pengamanan kualitas sistem informasi yang mampu melindungi keselamatan individu dan masyarakat, mempertahankan nilai yang dipertimbangkan sangat penting untuk kualitas hidup di dalam suatu masyarakat informasi.

Dari berbagai permasalahan etika dan sosial yang berkembang berkaitan dengan pemanfaatan sistem informasi, dua hal penting yang menjadi tantangan manajemen untuk dihadapi, yaitu:

a. Memahami risiko-risiko moral dari teknologi baru. Perubahan teknologi yang cepat mengandung arti bahwa pilihan yang dihadapi setiap individu juga berubah dengan cepat begitu pula keseimbangan antara risiko dan hasil serta kekhawatiran kemungkinan terjadinya tindakan yang tidak benar. Perlindungan atas hak privasi individu telah menjadi permasalahan etika yang serius dewasa ini. Di samping itu, penting bagi manajemen untuk melakukan analisis mengenai dampak etika dan sosial dari perubahan teknologi. Mungkin tidak ada jawaban yang selalu tepat untuk bagaimana seharusnya perilaku, tetapi paling tidak ada perhatian atau manajemen tahu mengenai risiko-risiko moral dari teknologi baru.

b. Membangun kebijakan etika organisasi yang mencakup permasalahan etika dan sosial atas sistem informasi. Manajemen bertanggung jawab untuk mengembangkan, melaksanakan, dan menjelaskan kebijakan etika organisasi. Kebijakan etika organisasi berkaitan dengan sistem informasi meliputi, antara lain: privasi, kepemilikan, akuntabilitas, kualitas sistem, dan kualitas hidupnya. Hal yang menjadi tantangan adalah bagaimana memberikan program pendidikan atau pelatihan, termasuk penerapan permasalahan kebijakan etika yang dibutuhkan.

Etika merupakan prinsip-prinsip mengenai suatu yang benar dan salah yang dilakukan setiap orang dalam menentukan pilihan sebagai pedoman perilaku mereka. Perkembangan teknologi dan sistem informasi menimbulkan pertanyaan baik untuk individu maupun masyarakat pengguna karena perkembangan ini menciptakan peluang untuk adanya perubahan sosial yang hebat dan mengancam adanya distribusi kekuatan, uang, hak, dan kewajiban.

Dengan menggunakan sistem informasi, penting untuk dipertanyakan, bagaimana tanggung jawab secara etis dan sosial dapat ditempatkan dengan memadai dalam pemanfaatan sistem informasi. Etika, sosial, dan politik merupakan tiga hal yang berhubungan dekat sekali. Permasalahan etika yang dihadapi dalam perkembangan sistem informasi manajemen umumnya tercermin di dalam lingkungan sosial dan politik.

Untuk dapat memahami lebih baik hubungan ketiga hal tersebut di dalam pemanfaatan sistem informasi, diidentifikasi  lima dimensi moral dari era informasi yang sedang berkembang ini, yaitu:

* 1. Hak dan kewajiban informasi; apa hak informasi yang dimiliki oleh seorang individu atau organisasi atas informasi? Apa yang dapat mereka lindungi? Kewajiban apa yang dibebankan kepada setiap individu dan organisasi berkenaan dengan informasi?
	2. Hak milik dan kewajiban; bagaimana hak milik intelektual dilindungi di dalam suatu masyarakat digital di mana sulit sekali untuk masalah kepemilikan ini ditrasir dan ditetapkan akuntabilitasnya, dan begitu mudahnya hak milik untuk diabaikan?
	3. Akuntabilitas dan pengendalian; siapa bertanggung jawab terhadap kemungkinan adanya gangguan-gangguan yang dialami individu, informasi, dan hak kepemilikan?
	4. Kualitas sistem; standar data dan kualitas sistem apa yang diinginkan untuk melindungi hak individu dan keselamatan masyarakat?
	5. Kualitas hidup; nilai apa yang harus dipertahankan di dalam suatu informasi dan masyarakat  berbasis pengetahuan? Lembaga apa yang harus ada untuk melindungi dari  kemungkinan terjadinya pelanggaran informasi? Nilai budaya dan praktik-praktik apa yang diperlukan di dalam era teknologi informasi yang baru?

Perkembangan teknologi dan sistem informasi banyak membawa perubahan pada berbagai aspek kehidupan, khususnya yang mempengaruhi etika dan sosial masyarakat.  Beberapa organisasi telah mengembangkan kode etik sistem informasi. Namun demikian, tetap ada perdebatan berkaitan dengan kode etik yang dapat diterima secara umum dengan kode etik sistem informasi yang dibuat secara spesifik.  Sebagai manajer maupun pengguna sistem informasi, kita didorong untuk mengembangkan seperangkat standar etika untuk pengembangan kode etika sistem informasi, yaitu yang berbasiskan pada lima dimensi moral yang telah disampaikan di awal, yaitu:

* + 1. Hak dan kewajiban informasi; Kode etik sistem informasi harus mencakup topik-topik, seperti: privasi e-mail setiap karyawan, pemantauan tempat kerja, perlakuan informasi organisasi, dan kebijakan informasi untuk pengguna.
		2. Hak milik dan kewajiban; Kode etik sistem informasi harus mencakup topik-topik, seperti: lisensi penggunaan  perangkat lunak, kepemilikan data dan fasilitas organisasi, kepemilikan perangkat lunak yang buat oleh pegawai pada perangkat keras organisasi, masalah copyrights perangkat lunak. Pedoman tertentu untuk hubungan kontraktual dengan pihak ketiga juga harus menjadi bagian dari topik di sini.
		3. Akuntabilitas dan pengendalian; Kode etik harus menyebutkan individu yang bertanggung jawab untuk seluruh sistem informasi dan menggaris bawahi bahwa individu-individu inilah yang bertanggung jawab terhadap hak individu, perlindungan terhadap hak kepemilikan, kualitas sistem dan kualitas hidup.
		4. Kualitas sistem; Kode etik sistem informasi harus menggambarkan tingkatan yang umum dari kualitas data dan kesalahan sistem yang dapat ditoleransi. Kode etik juga harus dapat mensyaratkan bahwa semua sistem berusaha mengestimasi kualitas data dan kemungkinan kesalahan sistem.
		5. Kualitas hidup; Kode etik sistem informasi juga harus dapat menyatakan bahwa tujuan dari sistem adalah meningkatkan kualitas hidup dari pelanggan dan karyawan dengan cara mencapai tingkatan yang tinggi dari kualitas produk, pelayanan pelanggan, dan kepuasan karyawan.

BAB III

PENUTUP

3.1  Kesimpulan

Perkembangan teknologi informasi dan internet sangatlah pesat dan berpotensi untuk membantu mempermudah umat manusia mengarungi kehidupanya untuk mencapai keberhasilan dalam bermasyarakat.efek-efek negatif bisa dihindari dengan memberikan pedoman-pedoman etika yang jelas kepada para profesional dan pengguna teknologi ini.Mamfaat maksimal atau efek negatif dari teknologi informasi sangat tergantung pada manusia yang mengoperasikan.

DAFTAR PUSTAKA

<https://muhammadsaprudin.blogspot.co.id/2015/06/v-behaviorurldefaultvmlo.html>

<http://kentangbegadang.blogspot.co.id/2015/03/etika-profesi-teknologi-informasi.html>

<http://eptik3.blogspot.co.id/>

<http://wahyu-dewanto.blogspot.co.id/2015/11/etika-profesi-sistem-informasi.html>