APTIKOM
ASOSIASI PERGURUAN TINGGI INFORMATIKA DAN KOMPUTER

MODUL PJJ

Mata Ajar

MANAJEMEN KEAMANAN INFORMASI DAN INTERNET

Topik Bahasan

MENCERMATI FENOMENA KEBOCORAN DATA DAN INFORMASI RAHASIA

Versi

2013/1.0

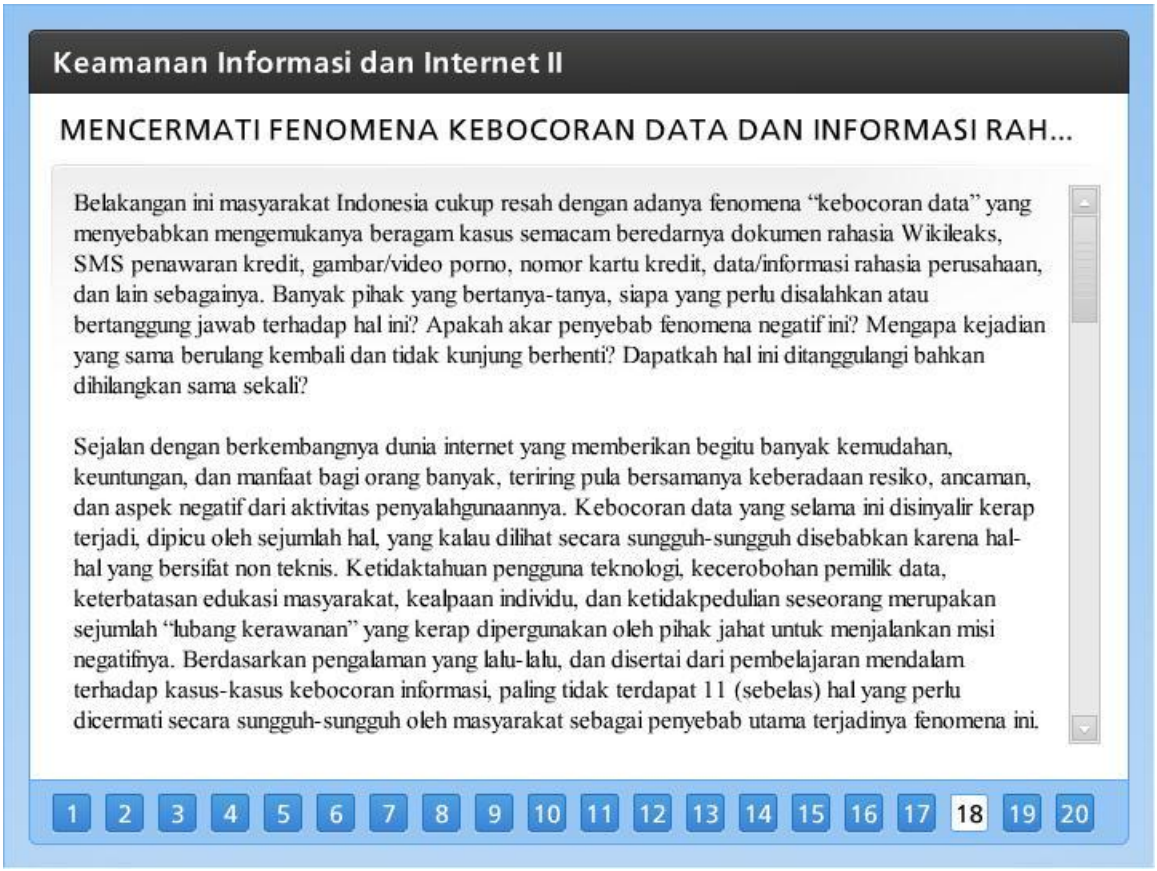
Nama File

MKIDI-12A-MencermatiFenomena.pdf

Referensi Pembelajaran

12-A

MENCERMATI FENOMENA KEBOCORAN DATA DAN INFORMASI RAHASIA



Belakangan ini masyarakat Indonesia cukup resah dengan adanya fenomena "kebocoran data" yang menyebabkan mengemukanya beragam kasus semacam beredarnya dokumen rahasia Wikileaks, SMS penawaran kredit, gambar/video porno, nomor kartu kredit, data/informasi rahasia perusahaan, dan lain sebagainya. Banyak pihak yang bertanya-tanya, siapa yang perlu disalahkan atau bertanggung jawab terhadap hal ini? Apakah akar penyebab fenomena negatif ini? Mengapa kejadian yang sama berulang kembali dan tidak kunjung berhenti? Dapatkah hal ini ditanggulangi bahkan dihilangkan sama sekali?

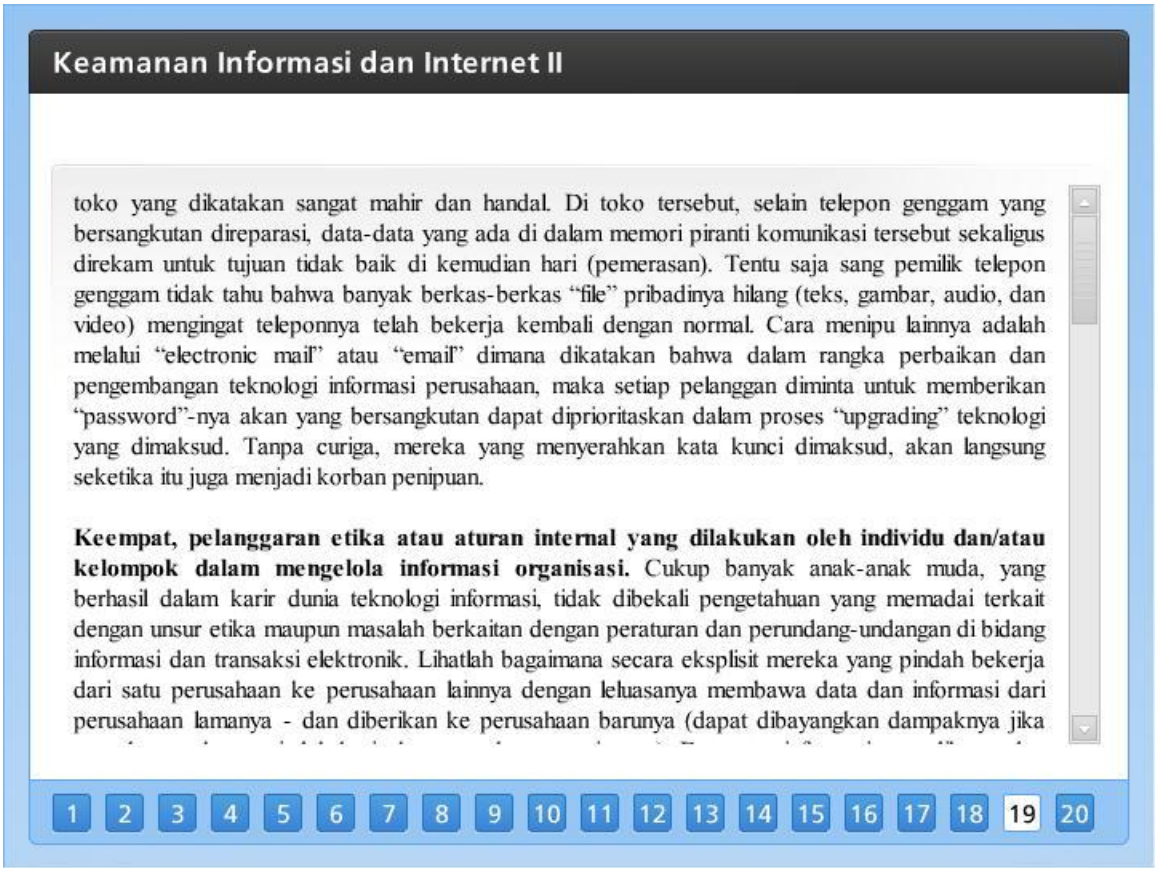
Sejalan dengan berkembangnya dunia internet yang memberikan begitu banyak kemudahan, keuntungan, dan manfaat bagi orang banyak, teriring pula bersamanya keberadaan resiko, ancaman, dan aspek negatif dari aktivitas penyalahgunaannya. Kebocoran data yang selama ini disinyalir kerap terjadi, dipicu oleh sejumlah hal, yang kalau dilihat secara sungguh-sungguh disebabkan karena hal-hal yang bersifat non teknis. Ketidaktahuan pengguna teknologi, kecerobohan pemilik data, keterbatasan edukasi masyarakat, kealpaan individu, dan ketidakpedulian seseorang merupakan sejumlah "lubang kerawanan" yang kerap dipergunakan oleh pihak jahat untuk menjalankan misi negatifnya. Berdasarkan pengalaman yang lalu-lalu, dan disertai dari pembelajaran mendalam terhadap kasus-kasus kebocoran informasi, paling tidak terdapat 11 (sebelas) hal yang perlu dicermati secara sungguh-sungguh oleh masyarakat sebagai penyebab utama terjadinya fenomena ini.

Pertama, perilaku atau budaya masyarakat Indonesia yang senang membagi-bagi data serta informasi mengenai kerabat dan teman dekatnya. Pernah ada suatu riset yang menarik, dimana jika dua orang Indonesia diambil secara acak (random), dan keduanya dibiarkan ngobrol, maka akan terungkap adanya hubungan langsung maupun tidak langsung di antara keduanya melalui pertalian keluarga atau teman paling banyak enam jarak titik hubungan (six degree of separation). Ramahnya dan senangnya masyarakat Indonesia dalam bersosialisasi menyebabkan setiap individu memiliki banyak teman. Didasari rasa saling percaya, maka kebiasaan atau perilaku saling tukar-menukar data atau informasi pribadi menjadi suatu hal yang biasa. Lihatlah bagaimana mudahnya dua orang yang baru berkenalan dalam sebuah seminar langsung tukar menukar PIN Blackberry-nya, atau kebiasaan mencantumkan nomor telepon genggam dalam kartu nama yang sering dibagikan dan dipertukarkan dalam berbagai kesempatan, atau secara sengaja memberitahukan alamat email maupun telepon pribadinya di seminar-seminar karena merupakan bagian dari pemasaran (marketing), atau bahkan di setiap profil pada akun jejaring sosial (seperti Facebook, Twitter, Friendster, MySpace, dan lain-lain) individu yang bersangkutan selalu mencantumkan data-data pribadinya secara relatif lengkap dan jujur. Tentu saja secara sengaja maupun tidak sengaja, dipicu dengan karakteristik internet yang terbuka dan bebas, data/informasi ini mudah sekali mengalir dari satu tempat ke tempat lainnya - tanpa terkendali. Oleh karena itu tidak mengherankan jika ada satu atau sekelompok orang yang rajin mengumpulkan data atau informasi tersebut (database) demi berbagai kepentingan di kemudian hari.

Kedua, kecerobohan pemilik data dalam mengelola data rahasia miliknya karena ketidaktahuan ataupun keteledoran. Hal yang paling mencolok terkait dengan aspek ini adalah mengenai cara seseorang mengelola kartu kredit yang dimilikinya. Perlu diketahui, bahwa seseorang dapat melakukan transaksi perdagangan via internet dengan mengetahui data atau informasi kartu kredit sebagai berikut: (i) 16 digit nomor kartu kredit yang tercantum di sisi muka; (ii) 3 digit nomor CCV yang ada di sisi belakang kartu kredit; (iii) tanggal akhir berlakunya kartu kredit; dan (iv) nama pemengang kartu kredit yang tercantum. Informasi ini dengan mudahnya dapat dicatat oleh siapa saja yang memperoleh kesempatan memegang kartu kredit orang lain selama beberapa menit, seperti misalnya dalam konteks: membayar makanan di restauran (kartu kredit dibawa pelayan untuk diserahkan ke kasir), membayar belanjaan di supermarket (pembeli tidak memperhatikan secara seksama apa yang dilakukan oleh kasir ketika transaksi berlangsung), membayar kamar di hotel (kartu kredit hilang dari pandangan selama beberapa menit untuk dikonfirmasi dan autentifikasi), membayar transaksi via e-commerce (tanpa melihat status "http" untuk mengetahui profil keamanan situs tempat berinteraksi), dan lain sebagainya. Hal ini bukan berarti ingin menuduh adanya modus kejahatan yang dilakukan para pelayan restauran, kasir, atau karyawan hotel, namun untuk menegaskan adanya resiko atau peluang melakukan tindakan kejahatan dimana-mana. Pengelolaan kartu ATM juga memiliki kerawanan tersendiri. Cukup banyak ditemukan seorang ayah atau ibu yang memperbolehkan anaknya mengambil uang melalui ATM milik orang tuanya tersebut dengan memberitahukan kata kunci atau "password"-nya (ada kemungkinan dalam kenyataan sang anak menyuruh orang lain seperti supir atau pembantu rumah tangganya yang melakukan pengambilan tunai via ATM). Keadaan makin bertambah runyam apabila sang orang tua, yang "password"-nya sudah diketahui orang lain tersebut menggunakan "password" yang sama untuk akun penting lainnya seperti "internet banking" atau "mobile banking" miliknya - termasuk akun email terkemuka di Yahoo atau GMail. Tentu saja dengan mengatahui kata kunci rahasia tersebut, dengan leluasa akun yang bersangkutan dapat dibajak oleh orang lain (sejumlah tokoh politik, pejabat publik, maupun aktor/artis terkemuka di Indonesia telah menjadi korban dari

pembajakan akun ini). Hal lain yang mengemuka adalah seringnya para pimpinan perusahaan menyerahkan atau memberitahu "password" akun miliknya ke sekretaris atau asisten pribadinya. Tujuannya sebenarnya baik, untuk membantu yang bersangkutan mengelola proses korespondensi dan komunikasi yang ada; namun yang bersangkutan lupa bahwa dengan memberitahukan "password" tersebut berarti sang pimpinan secara langsung menyerahkan seluruh "otoritas" yang dimilikinya untuk dapat dieksekusi oleh sekretaris atau asisten pribadinya tersebut (bisa dibayangkan apa yang akan terjadi jika dalam perusahaan tersebut menggunakan sistem "single log-in").

Ketiga, maraknya fenomena dengan menggunakan teknik "social engineering" dilakukan oleh pihak tak bertanggung jawab untuk menipu orang lain. "Social Engineering" atau "rekayasa sosial" adalah suatu teknik yang dipergunakan untuk mendapatkan kepercayaan orang lain melalui pendekatan interaksi sosial sehari-hari sehingga tidak menimbulkan kecurigaan. Contoh klasiknya adalah seseorang yang dikabarkan mendapatkan hadiah undian tertentu via SMS dimana hadiah tersebut dapat ditebus apabila yang bersangkutan segera mengirimkan biaya pembayaran pajaknya lewat ATM, atau berita buruk kepada seseorang mengenai adanya kecelakaan lalu lintas yang menimpa keluarga dekatnya sehingga yang bersangkutan diminta untuk segera mengirimkan uang untuk kebutuhan operasi yang harus segera dikirimkan untuk menyelamatkan nyawa sang korban, dan lain sebagainya. Bahkan saat ini modus tersebut sudah berkembang lebih jauh. Misalnya jika ada seorang tokoh politik yang telepon genggamnya rusak, disarankan oleh rekan lainnya



toko yang dikatakan sangat mahir dan handal. Di toko tersebut, selain telepon genggam yang bersangkutan direparasi, data-data yang ada di dalam memori piranti komunikasi tersebut sekaligus direkam untuk tujuan tidak baik di kemudian hari (pemerasan). Tentu saja sang

pemilik telepon genggam tidak tahu bahwa banyak berkas-berkas "file" pribadinya hilang (teks, gambar, audio, dan video) mengingat teleponnya telah bekerja kembali dengan normal. Cara menipu lainnya adalah melalui "electronic mail" atau "email" dimana dikatakan bahwa dalam rangka perbaikan dan pengembangan teknologi informasi perusahaan, maka setiap pelanggan diminta untuk memberikan "password"-nya akan yang bersangkutan dapat diprioritaskan dalam proses "upgrading" teknologi yang dimaksud. Tanpa curiga, mereka yang menyerahkan kata kunci dimaksud, akan langsung seketika itu juga menjadi korban penipuan.

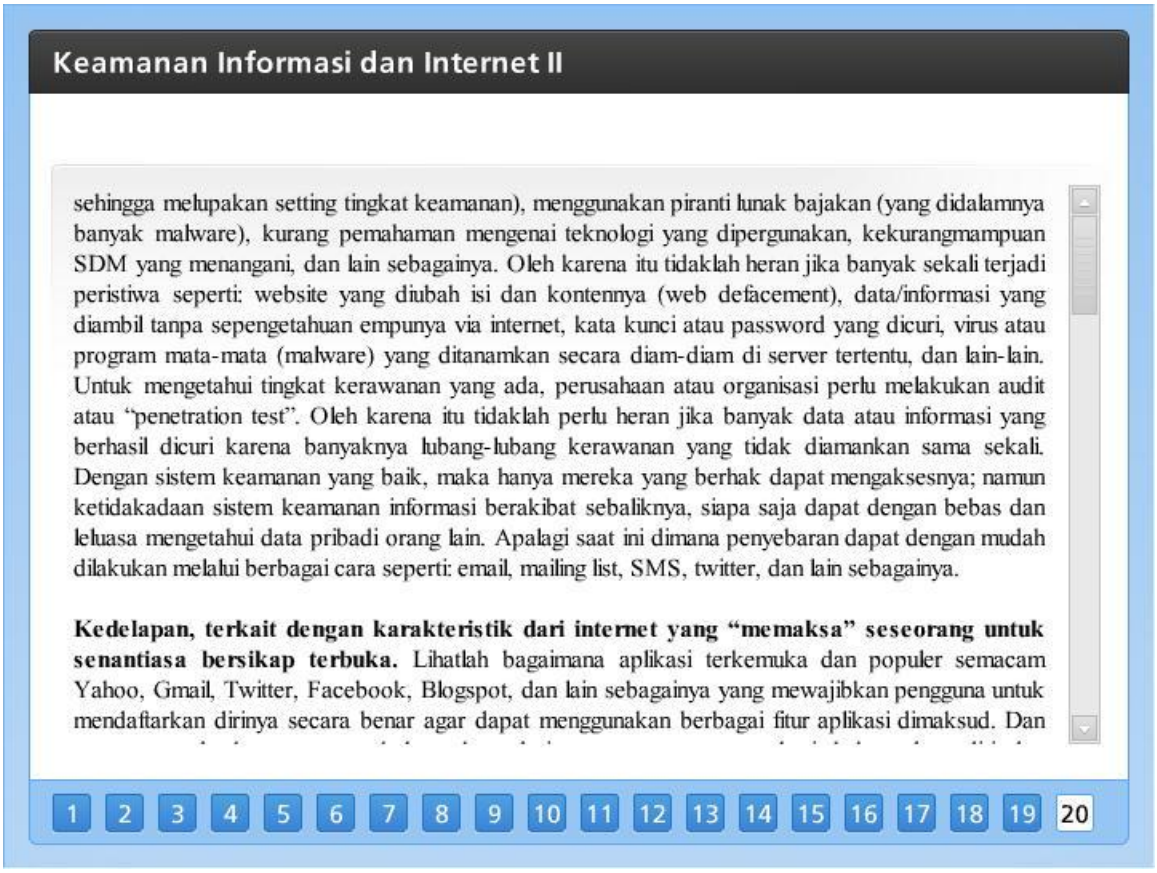
Keempat, pelanggaran etika atau aturan internal yang dilakukan oleh individu dan/atau kelompok dalam mengelola informasi organisasi. Cukup banyak anak-anak muda, yang berhasil dalam karir dunia teknologi informasi, tidak dibekali pengetahuan yang memadai terkait dengan unsur etika maupun masalah berkaitan dengan peraturan dan perundang-undangan di bidang informasi dan transaksi elektronik. Lihatlah bagaimana secara eksplisit mereka yang pindah bekerja dari satu perusahaan ke perusahaan lainnya dengan leluasanya membawa data dan informasi dari perusahaan lamanya - dan diberikan ke perusahaan barunya (dapat dibayangkan dampaknya jika yang bersangkutan pindah kerja ke perusahaan pesaingnya). Data atau informasi yang dibawa dan disampaikan itu dapat beraneka ragam rupanya, mulai dari profil pelanggan hingga detail transaksi yang terjadi. Hal ini belum termasuk unsur godaan yang selalu menghantui unit divisi teknologi informasi yang secara teknis dapat membaca hampir seluruh data yang berseliweran di sebuah perusahaan karena tidak adanya proses enkripsi atau penyandian yang diberlakukan (otoritas cukup tinggi dimiliki oleh seorang "super user"). Dengan berbekal dan beralasan menjalankan tugas teknis, seorang karyawan dari unit teknologi informasi dapat mengambil data apa saja dan dari mana saja - terutama jika pengguna yang bersangkutan berperilaku "pasrah" karena tidak memiliki pengetahuan teknis di bidang komputer atau teknologi informasi. Merubah konfigurasi, mengecek keberadaan virus, memperbaiki sistem yang "hang", meng-"upgrade" aplikasi lama ke yang baru, atau membantu instalasi program tertentu, merupakan sejumlah alasan yang dapat dipergunakan sebagai topeng untuk dapat masuk ke dalam sistem seseorang (ingat, dalam dunia digital, seseorang tidak akan merasa kehilangan aset elektronik yang dimilikinya, karena semuanya dapat diduplikasi dengan mudah dan bersifat identik).

Kelima, lemahnya manajemen informasi yang diberlakukan dan dipraktekan oleh organisasi. Di abad moderen ini, begitu banyak perusahaan dan organisasi yang memutuskan untuk memanfaatkan teknologi informasi dan internet dengan sebanyak-banyaknya dan sebaik-baiknya untuk meningkatkan kinerja dan performannya. Namun sayangnya kebanyakan usaha ini tidak dibarengi dengan sosialisasi dan edukasi mengenai penerapan manajemen informasi yang baik. Lihatlah contoh tidak diberlakukannya aturan untuk menyandikan atau mengenkripsi data atau informasi penting dan tergolong rahasia milik perusahaan; dimana ketika seorang Direktur atau General Manager kehilangan notebook atau laptopnya, dengan mudahnya sang pencuri akan memperoleh aset berharga tersebut (untuk kemudian diperdagangkan atau disebarkan ke pihak-pihak lain untuk mendapatkan keuntungan). Contoh lain dalam kasus promosi seorang pegawai atau karyawan. Biasanya, di posisinya yang baru, yang bersangkutan akan mendapatkan fasilitas komputer meja atau pun notebook/laptop yang baru pula - sehingga yang lama dapat ditinggalkan. Masalahnya adalah tidak ada prosedur yang mengharuskan komputer atau notebook/laptom yang lama tersebut dibersihkan dan diformat ulang sehingga orang baru yang menggantikan posisi yang ditinggalkan tersebut tidak dapat mengetahui isi dari file-file lama yang dimiliki oleh individu

yang dipromosi. Jika hal tersebut tidak dilakukan, bisa dibayangkan berapa banyak data individu maupun rahasia perusahaan yang akan diketahui yang bersaangkutan. Yang dapat dijadikan sebagai contoh klasik lainnya adalah masalah kebiasaan merekam isi pembicaraan sebuah rapat strategis dengan menggunakan perekam digital, agar nanti mempermudah proses pembuatan notulen rapat. Banyak hal yang terjadi dalam sebuah rapat, mulai dari yang bersifat rahasia hingga yang kritikal. Bayangkan dampak yang dapat terjadi, apabila sekretaris yang memiliki rekaman tersebut memiliki niat jahat dengan membeberkan rekaman dimaksud ke beberapa orang, maka hancurlah reputasi organisasi perusahaan yang dimaksud.

Keenam, adanya proses digitalisasi dari koleksi data/informasi sekunder yang dimiliki komunitas tertentu yang diunggah ke dunia siber (internet). Masyarakat Indonesia tumbuh dalam kelompok-kelompok, dimana setiap komunitas berusaha untuk memperlihatkan eksistensinya. Contohnya adalah sekelompok alumni dari SMA atau perguruan tinggi tertentu yang mengadakan pesta reuni. Sebagaimana layaknya komunitas alumni yang lain, mereka bersepakat membuat buku alumni dimana di dalamnya lengkap didaftarkan seluruh mantan pelajar atau mahasiswa, lengkap dengan alamat rumah, email, dan nomor telepon pribadi. Mereka yang punya hobi atau kesukaan seperti fitness, golf, fotografi, kuliner, atau filateli misalnya terdaftar sebagai anggota aktif klub-klub terkait, yang untuk menjadi anggotanya dibutuhkan sejumlah persyaratan administrasi ketika mendaftar - termasuk di dalamnya pengisian formulir menengai data pribadi. Klub ini kemudian menyimpan seluruh data anggotanya dalam sebuah buku induk keanggotaan. Hal yang sama berlaku pula untuk konteks seperti: kartu diskon anggota toko waralaba/retail, kartu anggota organisasi atau kelompok sosial, daftar pelanggan loyal jasa komersial, daftar pasien rumah sakit atau puskesmas, daftar penerima bantuan pemerintah, dan lain sebagainya. Berbeda dengan jaman dulu, saat ini hampir seluruh catatan tersebut telah diubah bentuknya menjadi file digital - dengan menggunakan program pengolah kata atau sejenisnya. Dan setelah menjadi berkas digital, maka untuk meningkatkan pelayanan pelanggan, data tersebut diunduh ke internet agar para pemangku kepentingan dapat mengaksesnya secara bebas.

Ketujuh, adanya kerawanan (vulnerabilities) dari kebanyakan sistem teknologi informasi yang dimiliki institusi. Sudah menjadi rahasia umum, bahwa kebanyakan situs atau "website" internet di Indonesia ini didesain dan dikembangkan secara sederhana (dan mungkin sedikit "asal-asalan"). Hasil pemantauan Komunitas Keamanan Informasi memperlihatkan betapa banyak dan umumnya lubang-lubang kerawanan serta kelemahan dari situs-situs internet di tanah air yang dapat dengan mudah dimanfaatkan dan dieksploitasi oleh pihak-pihak jahat yang tidak bertanggung jawab. Penyebabnya macam-macam, antara lain: ingin cepat-cepat instalasi sistem



sehingga melupakan setting tingkat keamanan), menggunakan piranti lunak bajakan (yang didalamnya banyak malware), kurang pemahaman mengenai teknologi yang dipergunakan, kekurangmampuan SDM yang menangani, dan lain sebagainya. Oleh karena itu tidaklah heran jika banyak sekali terjadi peristiwa seperti: website yang diubah isi dan kontennya (web defacement), data/informasi yang diambil tanpa sepengetahuan empunya via internet, kata kunci atau password yang dicuri, virus atau program mata-mata (malware) yang ditanamkan secara diam-diam di server tertentu, dan lain-lain. Untuk mengetahui tingkat kerawanan yang ada, perusahaan atau organisasi perlu melakukan audit atau "penetration test". Oleh karena itu tidaklah perlu heran jika banyak data atau informasi yang berhasil dicuri karena banyaknya lubang-lubang kerawanan yang tidak diamankan sama sekali. Dengan sistem keamanan yang baik, maka hanya mereka yang berhak dapat mengaksesnya; namun ketidakadaan sistem keamanan informasi berakibat sebaliknya, siapa saja dapat dengan bebas dan leluasa mengetahui data pribadi orang lain. Apalagi saat ini dimana penyebaran dapat dengan mudah dilakukan melalui berbagai cara seperti: email, mailing list, SMS, twitter, dan lain sebagainya.

Kedelapan, terkait dengan karakteristik dari internet yang "memaksa" seseorang untuk senantiasa bersikap terbuka. Lihatlah bagaimana aplikasi terkemuka dan populer semacam Yahoo, Gmail, Twitter, Facebook, Blogspot, dan lain sebagainya yang mewajibkan pengguna untuk mendaftarkan dirinya secara benar agar dapat menggunakan berbagai fitur aplikasi dimaksud. Dan memang pada kenyataannya kebanyakan dari para pengguna memberitahukan data diri dan lingkungannya secara benar karena selain berusaha untuk menerapkan etika yang baik dalam berinternet, tidak pernah terpikirkan oleh sang pengguna bahwa pemilik aplikasi tersebut akan menyalahgunakan data pelanggan yang dimilikinya. Situs-situs e-business atau e-commerce pun selalu didesain sedemikian rupa sehingga

senantiasa "memaksa" pegguna untuk membeberkan data dirinya seperti nama, tanggal lahir, alamat rumah/kantor, dan nomor telepon terkait agar barang yang dipesan dan dibelunya dapat dikirimkan atau diposkan ke rumah. Masalahnya adalah tidak semua penyedia jasa di internet memiliki etika dan profesionalisme yang baik. Banyak sekali terdapat situs-situs game, berita, perdagangan, dan lain-lain yang dibuat secara khusus sebagai "honeypot" atau umpan untuk mengumpulkan data pribadi individu-individu demi kepentingan jual-beli informasi di kemudian hari. Mereka tahu persis betapa mahal dan strategisnya memiliki data pribadi individu karena dapat dipergunakan untuk berbagai kepentingan - sehingga tidak segan-segan investasi untuk membuat aplikasi internet yang menarik. Oleh karena itu perlu berhati-hati setiap kali terdapat situs atau website yang meminta pengguna untuk mengisi sebanyak mungkin informasi detail karena berpotensi dapat disalahgunakan.

Kesembilan, menjamurnya para "pemulung data" di dunia siber (internet). Berbekal mesin pencari seperti Google.com, Yahoo.com, Altavista.com, atau MSNSearch.com, seseorang dapat dengan mudah melakukan berbagai jenis pencarian terhadap data atau informasi pribadi seseorang. Dengan ketekunan sedemikian rupa, seorang individu dapat dengan mudah mengumpulkan satu demi satu data pribadi seseorang dengan cara terencana (menggunakan teknik pencarian terfokus, artinya secara khusus mencari data individu tertentu) maupun dengan cara acak (memanfaatkan pola generik tertentu, mencari siapa saja yang dapat dikumpulkan datanya). Jika satu hari saja yang bersangkutan dapat mengumpulkan 100 data, berarti dalam satu bulan paling tidak 3,000 data individu dapat dikoleksi (apalagi jika yang melakukan pengumpulan adalah sekelompok orang). Pola ini jika dilakukan dengan benar dapat secara efektif digunakan untuk mengoleksi data pribadi berkualitas yang kelak dapat diperjualbelikan di pasar dunia siber.

Kesepuluh, perilaku piranti lunak (software) rancangan khusus yang diperuntukkan untuk mengoleksi beragam data dan informasi pribadi. Berbeda dengan teknik "pemulungan" sebelumnya, secara teknis dapat dikembangkan sebuah aplikasi, yang dapat secara otomatis melakukan pencarian terhadap data pribadi seseorang dengan memanfaatkan pendekatan algoritma tertentu (misalnya: crawling, filtering, profiling, dan lain sebagainya). Dengan berawal pada data email terkemuka seperti Yahoo atau Gmail misalnya, dapat ditelusuri kemudian profil seseorang melalui berbagai situs terkemuka jejaring sosial semacam Facebook, Twitter, Flickr, MySpace, Skype, dan lain-lain - bahkan terbuka kemungkinan untuk lebih jauh masuk ke dalam website "proprietary" organisasi tertentu seperti perguruan tinggi, pemerintahan, komunitas, perusahaan, dan lain sebagainya. Aplikasi semacam ini dapat tampil dalam dua rupa, yaitu yang bersifat legal formal maupun tergolong sebagai virus. Dikatakan legal formal karena memang dibuat, dirancang khusus, dan diperjual belikan untuk mereka yang bergerak di bidang pemasaran dan penjualan. Namun banyak pula piranti lunak "malware" yang dibuat untuk menyebarkan virus tertentu berbasis alamat email. Pada intinya adalah, sangat mudah dikembangkan sebuah program yang bertujuan untuk membantu seseorang dalam melakukan pengumpulan terhadap data tertentu untuk berbagai keperluan. Bahkan tidak jarang ditemukan sejumlah individu yang sengaja membuat program untuk mengoleksi berbagai dokumen dengan kategori "rahasia" atau informasi sensitif lainnya.

Kesebelas, memang ada kesengajaan dari pihak-pihak tertentu untuk melakukan kegiatan kriminal, baik melalui domain eksternal maupun internal. Yang terakhir dapat dikategorikan sebagai penyebab bocornya data atau informasi tertentu karena memang adanya pihak-pihak internal maupun eksternal organisasi yang memiliki niat dan agenda

melakukan tindakan kejahatan tertentu, seperti: pencurian data, penjebolan rekening, pengelabuan pelanggan, pengubahan informasi, pengambilalihan akses, pembohongan publik, dan lain sebagainya. Individu maupun komplotan yang mahir dalam melakukan kejahatan berbasis komputer maupun internet ini dapat berasal dari pihak luar maupun pihak dalam organisasi. Biasanya pihak luar melakukannya dengan berbekal pada teknik "hacking" yang dimilikinya, sementara pihak dalam melakukannya dengan berbekal pada teknik "social engineering" sebagai kuncinya. Secara karakteristik, kejahatan yang dilakukan oleh pihak internal organisasi lebih mudah dilakukan, mengingat yang bersangkutan tahu persis bagaimana cara kerja sebuah sistem dalam institusi terkait. Oleh karena itulah perlu adanya sistem keamanan informasi dalam rupa kebijakan, kendali teknis (kontrol), dan SOP (Standard Operating Procedure) yang ketat untuk mencegah terjadinya peristiwa yang tidak diinginkan tersebut.

Pada akhirnya, aspek edukasi merupakan kunci paling efektif dalam usaha untuk mencegah terjadinya peristiwa kebocoran data secara masal dan masif yang kerap terjadi belakangan ini. Setiap individu harus memiliki kesadaran, keperdulian, dan kemampuan - sesuai dengan kapasitas dan pekerjaannya sehari-hari - untuk mengelola keamanan informasi dalam lingkungannya sendiri. Prinsip "your security is my security" perlu ditanamkan secara mendalam ke seluruh insan pengguna komputer dan internet. Kebiasaan bersifat hati-hati atau "prudent" harus merupakan budaya yang perlahan-lahan perlu ditanamkan melalui pendekatan pendidikan kepasa semuar orang tanpa kecuali. Beragam organisasi dengan segala variasi dan karakteristiknya pun memiliki kewajiban dalam melakukan edukasi tiada henti kepada seluruh pemangku kepentingannya - mulai dari manajemen, karyawan, pelanggan, mitra, dan seluruh stakeholder terkait lainnya. Pepatah mengatakan "there is no patching for human stupidity" secara eksplisit mengatakan bahwa kerawanan teknis pada sistem dapat dengan mudah diperbaiki, namun lubang-lubang kerawanan pada manusia tidak ada obatnya kecuali pengetahuan, kemampuan, dan kemauan