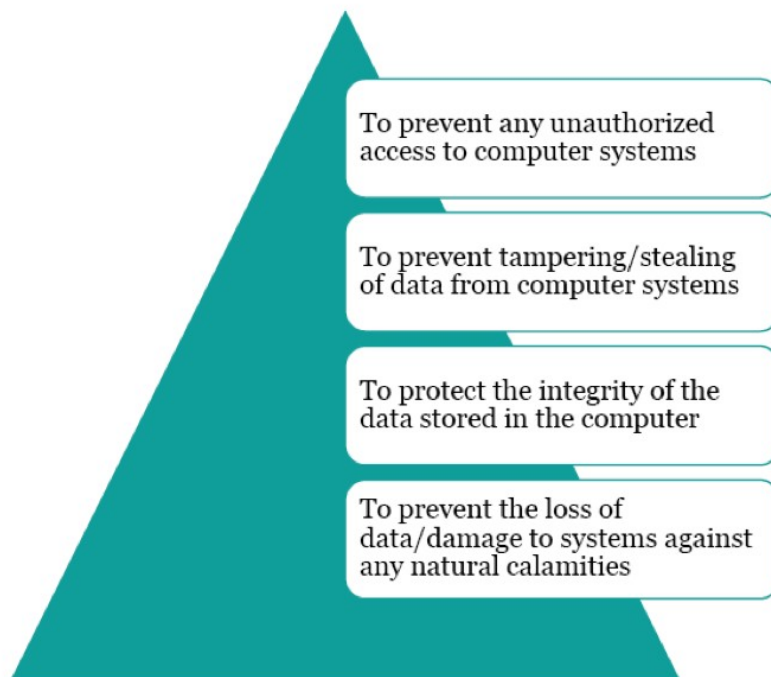


Strategi Korporat Mengamankan Diri

Prof. Richardus Eko Indrajit

“Budaya aman” belumlah menjadi suatu perilaku sehari-hari dari kebanyakan karyawan atau pegawai dalam sebuah perusahaan atau organisasi. Pengalaman membuktikan bahwa kebanyakan insiden keamanan informasi terjadi karena begitu banyaknya kecurobohan yang dilakukan oleh staf organisasi maupun karena kurangnya pengetahuan dari yang bersangkutan terkait dengan aspek-aspek keamanan yang dimaksud.



PHYSICAL SECURITY + INFORMATION SECURITY

Gambar: Tujuan Keamanan Informasi

Tujuan utama dari kebijakan keamanan informasi dari sebuah perusahaan atau organisasi secara prinsip ada 4 (empat) buah, yaitu masing-masing:

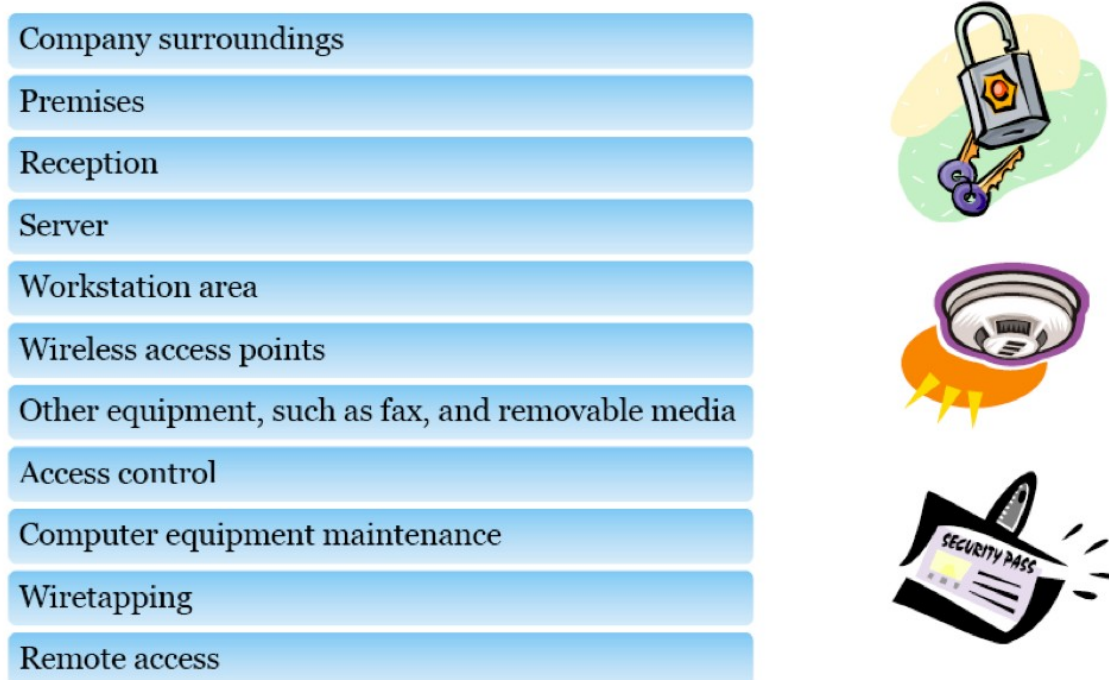
- Mencegah adanya pihak-pihak yang tidak berhak dan berwenang melakukan akses ke sistem komputer atau teknologi informasi milik organisasi;

- Mencegah terjadinya pencurian data dari sebuah sistem komputer atau media penyimpanan data yang ada dalam teritori organisasi;
- Melindungi keutuhan dan integritas data yang dimiliki organisasi agar tidak dirubah, diganti, atau diganggu keasliannya; dan
- Menghindari diri dari dirusaknya sistem komputer karena berbagai tindakan kerusakan yang dilakukan secara sengaja maupun tidak.

Untuk dapat mencapai tujuan ini, setiap individu dalam organisasi haruslah benar-benar mengimplementasikan “budaya aman”, yaitu suatu kebiasaan atau perilaku menjaga keamanan dengan memperhatikan dua aspek penting, yaitu: lingkungan fisik dan keamanan informasi.

Keamanan Lingkungan Fisik

Paling tidak ada 11 (sebelas) hal terkait dengan lingkungan fisik yang harus benar-benar diperhatikan oleh staf karyawan maupun manajemen yang bekerja dalam organisasi atau perusahaan. Berikut adalah penjelasan dari masing-masing aspek yang dimaksud.



Gambar: Menjaga Keamanan Lingkungan Fisik

Akses Masuk Organisasi

Hal pertama yang harus diperhatikan adalah memastikan diperhatikannya faktor keamanan pada seluruh pintu atau akses masuk ke dalam perusahaan, mulai dari pintu gerbang masuk ke dalam kompleks usaha sampai dengan seluruh jalan atau pintu masuk

ke setiap ruangan yang perlu dilindungi. Karena pintu-pintu ini merupakan jalan akses masuk ke dalam lingkungan perusahaan secara fisik, perlu dipastikan bahwa hanya mereka yang memiliki otoritas atau hak saja yang boleh masuk ke dalam lingkungan yang dimaksud. Oleh karena itu, perlu diterapkan sejumlah fasilitas dan prosedur keamanan di titik-titik ini, seperti: pemanfaatan kartu identitas elektronik untuk masuk melalui gerbang otomatis, pengecekan identitas individu oleh satuan petugas keamanan (satpam), penukaran kartu identitas dengan kartu akses teritori perusahaan, penggunaan sidik jari dan retina mata sebagai bukti identitas untuk membuka pintu, dan lain sebagainya.

Lingkungan Sekitar Organisasi

Walaupun sekilas nampak bahwa pintu masuk adalah satu-satunya jalan akses menuju perusahaan, namun pada kenyataannya terdapat sejumlah area yang dapat dimanfaatkan oleh pelaku kejahatan dalam menjalankan aksinya. Katakanlah akses masuk ke lingkungan perusahaan dapat melalui pagar yang dapat dipajut dan dilompati, atau melalui jendela yang dapat dibuka dengan mudah, atau melalui dinding kaca yang dapat dijebol, atau atap gedung yang mudah dirombak, atau lubang alat pendingin yang dapat dibongkar, dan lain sebagainya. Cara melindungi titik-titik penting ini antara lain dilakukan dengan menggunakan kamera CCTV, atau memasang sistem alarm, atau memelihara anjing pelacak, atau mengaliri pagar dengan tegangan listrik, dan cara-cara lainnya.

Daerah Pusat Informasi (Reception)

Banyak perusahaan tidak sadar, bahwa daerah “receptionist” merupakan sebuah titik rawan yang harus diperhatikan keamanannya. Ada sejumlah alasan dibalik pernyataan ini. Pertama, karena fungsi dan tugasnya sebagai sumber informasi, maka biasanya di meja seorang receptionist dapat ditemukan berbagai data dan informasi berharga, seperti: nama pegawai dan nomor telpon ekstensioennya, detail lokasi unit dan pimpinannya, daftar pengunjung individu atau unit tertentu, informasi kehadiran karyawan perusahaan, dan lain sebagainya. Kedua, daerah di sekitar receptionist adalah wilayah yang paling ramai dan sibuk karena yang bersangkutan harus berhadapan dengan tamu perusahaan yang keluar masuk. Tentu saja jumlah yang tidak imbang ini membuat sulitnya mengamati dan mengawasi perilaku semua tamu yang berada di sekitarnya. Ketiga, karena sifatnya sebagai “penerima tamu”, seorang receptionist biasanya cenderung memiliki perilaku yang ramah dan berfikir positif terhadap keberadaan semua tamu. Oleh karena itu, mudah sekali bagi pelaku kejahatan dalam melakukan tindakan social engineering terhadap seorang receptionist. Oleh karena itulah perlu dilakukan sejumlah tindakan pengamanan seperti: menghindari bercecernya catatan, dokumen, atau kertas-kertas berisi informasi di meja receptionist, mendesain meja receptionist agar tidak ada sisi yang memungkinkan kontak langsung dengan tamu, memposisikan monitor komputer sedemikian rupa agar tidak mudah diintip oleh orang lain, mengunci secara fisik seluruh peralatan yang dipergunakan dalam bertugas, dan lain sebagainya.

Ruang Server

Server adalah “jantung dan otaknya” perusahaan, karena selain terkoneksi dengan pusat-pusat penyimpanan data, entitas ini merupakan penggerak dan pengatur lalu

lintas data serta informasi yang ada di perusahaan. Oleh karena itulah maka secara fisik keberadaannya harus dijaga dengan sebaik-baiknya. Pertama adalah ruangan server harus tersedia dengan kondisi ruangan sesuai dengan persyaratan teknis yang berlaku. Kedua tidak boleh sembarang orang masuk ke ruang server tersebut, kecuali yang memiliki otoritas dan hak akses. Ketiga, pastikan server tersebut “terkunci” dan “terpasung” kuat di tempatnya, tidak berpindah-pindah dari satu tempat ke tempat lain. Keempat, set konfigurasi server dengan baik sehingga tidak memungkinkan adanya pintu akses ke dalamnya, misalnya dengan cara mematikan semua saluran atau port media eksternal, mempartisi sistem operasi sesuai dengan hak akses dan tingkat keamanan, dan lain sebagainya.

Area Workstation

Ini merupakan tempat dimana kebanyakan karyawan bekerja, yaitu terdiri dari sejumlah meja dengan komputer dan/atau notebook di atasnya. Dalam konteks ini, perusahaan perlu membuat kebijakan dan peraturan yang harus disosialisasikan kepada karyawannya, terutama terkait dengan masalah keamanan informasi ditinjau dari sisi keamanan fisik. Salah satu kebiasaan yang baik untuk disosialisasikan dan diterapkan adalah “clear table and clean monitor policy” – yaitu suatu kebiasaan membersihkan meja dan “mematikan” monitor komputer setiap kali karyawan sebagai pengguna hendak meninggalkan meja – baik sementara atau pun sebelum pulang ke rumah.

Wireless Access Points

Hampir semua lingkungan perusahaan sekarang diperlengkapi dengan Wireless Access Points atau Hot Spot. Selain murah dan praktis dalam penggunaannya, medium komunikasi “wireless” ini dianggap dapat menjawab berbagai kebutuhan berkomunikasi antar para pemangku kepentingan perusahaan. Yang perlu untuk diperhatikan adalah mengenai keamanannya, karena kerap kali perusahaan lalai dalam melakukannya. Bayangkan saja, jika seorang penyusup berhasil masuk via WAP atau Hot Spot ini, berarti yang bersangkutan berhasil masuk ke dalam sistem perusahaan. Oleh karena itulah perlu diperhatikan sejumlah hal terkait dengan keamanannya, seperti: terapkan enkripsi pada WEP, jangan memberitahu SSID kepada siapapun, untuk masuk ke WAP harus menggunakan password yang sulit, dan lain sebagainya.

Faksimili dan Media Elektronik Lainnya

Dalam satu hari, sebuah perusahaan biasanya menerima berpuluh-puluh fax dari berbagai tempat, dimana data atau informasi yang dikirimkan dapat mengandung sejumlah hal yang sangat penting dan bersifat rahasia. Oleh karena itulah perlu diperhatikan pengamanan terhadap mesin faksimili ini, terutama dalam proses penerimaan dan pendistribusiannya ke seluruh unit perusahaan terkait. Demikian pula dengan berbagai media elektronik terkait seperti: modem, printer, eksternal drive, flash disk, CD-ROM, dan lain sebagainya. Jangan sampai beragam media elektronik ini berserakan tanpa ada yang mengelola dan bertanggung jawab, karena jika berhasil diambil oleh yang tidak berhak dapat mengakibatkan berbagai insiden yang tidak diinginkan.

Entitas Kendali Akses

Di sebuah perusahaan moderen dewasa ini sering kali diterapkan manajemen identitas dengan menggunakan berbagai entitas yang sekaligus berfungsi sebagai kunci akses terhadap berbagai fasilitas perusahaan. Misalnya adalah kartu identitas, modul biometrik, token RFID, sensor wajah dan suara, dan lain sebagainya. Mengingat bahwa keseluruhan entitas ini adalah kunci akses ke berbagai sumber daya yang ada, maka keberadaan dan keamanannya harus dijaga sungguh-sungguh. Sebagai pemegang kartu identitas misalnya, jangan menaruh kartu tersebut di sembarang tempat sehingga dapat dicuri orang; atau untuk model token RFID, pastikan bahwa token yang ada selalu berada dalam posesi yang bersangkutan; dan lain sebagainya.

Pengelolaan Aset Komputer

Hal ini merupakan sesuatu yang sederhana namun jarang dilakukan oleh sebuah organisasi semacam perusahaan, yaitu pemeliharaan aset komputer. Seperti diketahui bersama, karyawan mengalami proses promosi, mutasi, dan demosi – dimana yang bersangkutan dapat berpindah-pindah unit kerjanya. Di setiap penugasannya, biasanya yang bersangkutan mendapatkan akses ke komputer tertentu. Permasalahan timbul ketika sebelum pindah jabatan, yang bersangkutan lupa menghapus seluruh file penting, baik milik pribadi maupun perusahaan. Akibat kelupaan tersebut, penggantinya dengan leluasa dapat mengakses file-file yang dimaksud. Masalah yang lebih besar lagi adalah ketika perusahaan berniat untuk mengganti seluruh komputer-komputer yang sudah usang dengan yang baru. Karena alasan biaya dan waktu, banyak perusahaan yang tidak melakukan proses format ulang atau bahkan pemusnahan terhadap data yang masih tersimpan di hard disk komputer usang tersebut. Perlu pula dijaga dengan hati-hati jika perusahaan menyerahkan kepada pihak ketiga untuk melakukan pemeliharaan sistem komputer yang dimaksud, misalnya dalam hal: pemutakhiran program anti virus, proses penataan ulang file dalam hard disk (defragmentation), dan lain sebagainya.

Penyadapan

Sudah bukan rahasia umum lagi, dengan dipicu oleh semakin berkembangnya kemajuan teknologi informasi dan komunikasi dewasa ini, harga peralatan untuk melakukan penyadapan terhadap media komunikasi menjadi sangat murah. Siapa saja dapat membelinya dan menginstalnya untuk keperluan positif maupun untuk tindakan kriminal. Perlu diingat bahwa di Indonesia, hanya penegak hukum yang boleh melakukan penyadapan; dalam arti kata, seluruh kegiatan penyadapan dalam bentuk apa pun tidaklah sah atau merupakan suatu tindakan kejahatan. Oleh karena itu, perusahaan perlu melakukan aktivitas untuk menyapu bersih kemungkinan adanya alat-alat sadap di sekitar daerah atau lokasi yang penting, seperti: telepon direktur, ruang rapat manajemen, koneksi ke/dari server pusat, dan lain sebagainya. Inspeksi dan audit yang teliti perlu dilakukan untuk memastikan tidak terjadi kegiatan penyadapan dalam perusahaan.

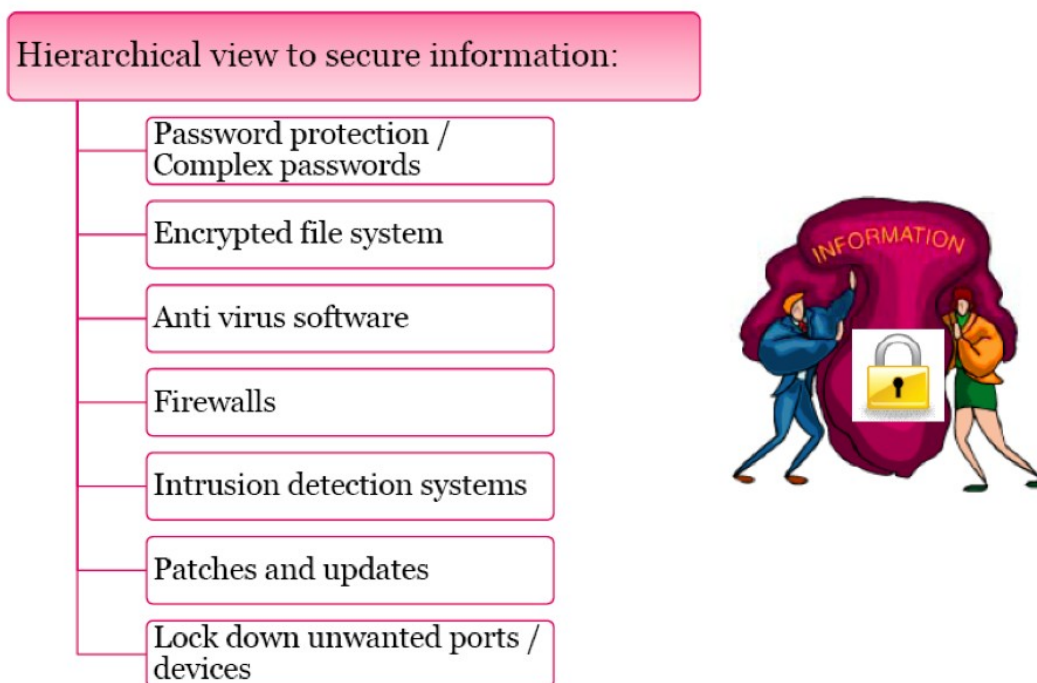
Remote Access

“Remote Access” adalah cara termudah bagi pegawai atau karyawan untuk bekerja di luar teritori perusahaan, seperti di rumah, di kendaraan, di tempat publik, dan lain-lain. Walaupun ditinjau dari segi bisnis hal tersebut sangatlah menguntungkan dan

memberikan nilai tambah, namun ditinjau dari aspek keamanan informasi hal tersebut mendatangkan sejumlah resiko baru. Karena sifatnya yang “remote” atau “kendali jauh”, maka terdapat banyak sekali titik-titik dimana pelaku kejahatan dapat melakukan aksi penetrasi dan eksploitasinya. Oleh karena itu saran yang baik untuk dilakukan adalah melakukan enkripsi atau penyandian terhadap data dan/atau informasi yang dikirimkan agar tidak dapat dibaca oleh mereka yang mencoba untuk menyadap atau memanipulasinya.

Keamanan Informasi

Setelah mengamankan lingkungan fisik, hal berikut yang disarankan untuk dilakukan adalah mengamankan konten dari data dan/atau informasi itu sendiri. Paling tidak ada 7 (tujuh) hal yang dapat dilakukan terkait dengan hal ini seperti yang dipaparkan di bawah ini.



Gambar: Menjaga Keamanan Lingkungan Fisik

Proteksi Password

Memproteksi akses ke beberapa file dan program dengan menggunakan password merupakan cara lumrah yang paling banyak dipergunakan. Dalam kaitan ini sang pengguna harus paham benar cara mengelola password yang baik, mulai dari menentukan password yang aman hingga memelihara dan memperbaharuinya. Password yang aman biasanya minimum terdiri dari 6 (enam) buah karakter yang merupakan campuran dari huruf besar dan kecil, angka, serta simbol. Dan paling tidak setiap 3 (tiga) bulan sekali password tersebut diganti dan diperbaharui.

Enkripsi File

Jika memang data dan/atau informasi yang dimiliki dan didistribusikan sedemikian pentingnya, ada baiknya file-file elektronik tersebut dienkripsi atau disandikan; sehingga jika ada pelaku kejahatan berhasil menyadap atau memperoleh data/informasi yang dimaksud, yang bersangkutan mengalami kesulitan dalam membacanya. Kebiasaan melakukan enkripsi terhadap file-file penting di perusahaan harus mulai disosialisasikan dan dibudayakan, terutama oleh kalangan manajemen yang berhubungan erat dengan informasi rahasia dan penting.

Software Anti Virus

Program anti virus ada baiknya diinstal pada server atau komputer yang di dalamnya terdapat data atau informasi penting. Perlu diperhatikan bahwa efektivitas sebuah program atau software anti virus terletak pada proses pemutakhiran atau “upgrading” file-file library terkait dengan jenis-jenis virus yang baru. Tanpa adanya aktivitas pemutakhiran, maka anti virus tidak akan banyak membantu karena begitu banyaknya virus-virus baru yang diperkenalkan setiap harinya. Dalam konteks ini jelas terlihat bahwa tidak ada gunanya menginstal program anti virus bajakan, karena selain bertentangan dengan HAKI, juga tidak bisa dilakukan aktivitas pemutakhiran. Banyak orang belakangan ini yang meremehkan kemampuan virus. Statistik memperlihatkan bahwa semakin banyak virus-virus baru yang bersifat destruktif terhadap file dan sistem komputer dewasa ini; belum lagi kemampuan virus dalam mengendalikan atau mengakses sistem komputer yang dapat menyebabkan perilaku kriminal dan dapat terjerat undang-undang terkait dengan “cyber law”.

Firewalls

Perangkat ini merupakan program atau piranti keras (baca: hardware) yang memiliki fungsi utama untuk melindungi jejaring sistem komputer internal dari lingkungan luar. Tugas utamanya adalah menjadi filter terhadap trafik data dari luar, dimana jika dipandang aman, data yang datang dari luar akan diteruskan ke dalam jejaring internal, namun jika ditemukan hal-hal yang mencurigakan atau yang tidak diinginkan, maka data yang dimaksud akan ditolak. Selain data, segala bentuk akses dari luar ke jejaring komputer juga dapat diseleksi oleh firewalls. Dengan diinstalasinya firewalls ini paling tidak data yang ada di dalam internal perusahaan dapat terlindung dari akses luar.

Intrusion Detection System

IDS atau Intrusion Detection System adalah sebuah piranti lunak atau keras yang memiliki fungsi utama untuk mendeteksi terjadinya aktivitas “penyusupan” pada jejaring sistem internal perusahaan. Cara kerja sistem ini adalah menganalisa paket-paket trafik data yang ada; jika terdapat jenis paket yang mencurigakan atau tidak normal, maka IDS akan memberikan peringatan kepada administrator sistem. Paket yang tidak normal dapat berisi macam-macam jenis serangan terhadap data maupun sistem yang ada, misalnya dalam bentuk DOS/DDOS, botnet, SQL injection, dan lain sebagainya.

Pemutakhiran Patches

Tidak ada program atau aplikasi yang dibangun dengan sempurna atau bebas dari kesalahan (baca: error). Untuk itu biasanya produsen yang bersangkutan menyediakan program tambalan atau “patches” untuk menutup lubang-lubang kesalahan atau

kerawanan yang ditemukan pada program, software, atau aplikasi tertentu. Dengan selalu dimutakhirkannya sistem dengan berbagai patches, maka paling tidak lubang-lubang kerawanan yang dapat dieksploitasi oleh pelaku kejahatan untuk mengambil dan merusak data dalam perusahaan dapat dihindari.

Penutupan Port dan Kanal Akses

Sistem komputer dihubungkan dengan entitas luar melalui port. Dengan kata lain, port merupakan jalan yang dapat dipergunakan oleh pihak luar untuk menyusup atau masuk ke dalam komputer. Seperti halnya pintu dan jendela dalam sebuah rumah, sistem komputer memiliki pula beberapa port; ada yang secara aktif dibuka untuk melayani berbagai kebutuhan input dan output, dan ada pula yang dibiarkan terbuka tanpa fungsi apa-apa. Sangatlah bijaksana untuk “menutup” saja seluruh port yang terbuka dan tanpa fungsi tersebut untuk mencegah adanya pihak yang tidak bertanggung jawab masuk ke sistem komputer melalui kanal tersebut.



Richardus Eko Indrajit, guru besar ilmu komputer ABFI Institute Perbanas,

dilahirkan di Jakarta pada tanggal 24 Januari 1969. Menyelesaikan studi program Sarjana Teknik Komputer dari Institut Teknologi Sepuluh Nopember (ITS) Surabaya dengan predikat Cum Laude, sebelum akhirnya menerima beasiswa dari Konsorsium Production Sharing Pertamina untuk melanjutkan studi di Amerika Serikat, dimana yang bersangkutan berhasil mendapatkan gelar Master of Science di bidang Applied Computer Science dari Harvard University (Massachusetts, USA) dengan fokus studi di bidang artificial intelligence. Adapun gelar Doctor of Business Administration diperolehnya dari University of the City of Manila (Intramuros, Phillipines) dengan disertasi di bidang Manajemen Sistem Informasi Rumah Sakit. Gelar akademis lain yang berhasil diraihinya adalah Master of Business Administration dari Leicester University (Leicester City, UK), Master of Arts dari the London School of Public Relations (Jakarta, Indonesia) dan Master of Philosophy dari Maastricht School of Management (Maastricht, the Netherlands). Selain itu, aktif pula berpartisipasi dalam berbagai program akademis maupun sertifikasi di sejumlah perguruan tinggi terkemuka dunia, seperti: Massachusetts Institute of Technology (MIT), Stanford University, Boston University, George Washington University, Carnegie-Mellon University, Curtin University of Technology, Monash University, Edith-Cowan University, dan Cambridge University. Saat ini menjabat sebagai Ketua Umum Asosiasi Perguruan Tinggi Informatika dan Komputer (APTIKOM) se-Indonesia dan Chairman dari International Association of Software Architect (IASA) untuk Indonesian Chapter. Selain di bidang akademik, karir profesionalnya sebagai konsultan sistem dan teknologi informasi diawali dari Price Waterhouse Indonesia, yang diikuti dengan berperan aktif sebagai konsultan senior maupun manajemen pada sejumlah perusahaan terkemuka di tanah air, antara lain: Renaissance Indonesia, Prosys Bangun Nusantara, Plasmedia, the Prime Consulting, the Jakarta Consulting Group, Soedarpo Informatika Group, dan IndoConsult Utama. Selama kurang lebih 15 tahun berkiprah di sektor swasta, terlibat langsung dalam berbagai proyek di beragam industri, seperti: bank dan keuangan, kesehatan, manufaktur, retail dan distribusi, transportasi, media, infrastruktur, pendidikan, telekomunikasi, pariwisata, dan jasa-jasa lainnya. Sementara itu, aktif pula membantu pemerintah dalam sejumlah penugasan. Dimulai dari penunjukan sebagai Widya Iswara Lembaga Ketahanan Nasional (Lemhannas), yang diikuti dengan berperan sebagai Staf Khusus Bidang Teknologi Informasi Sekretaris Jendral Badan Pemeriksa

Keuangan (BPK), Staf Khusus Balitbang Departemen Komunikasi dan Informatika, Staf Khusus Bidang Teknologi Informasi Badan Narkotika Nasional, dan Konsultan Ahli Direktorat Teknologi Informasi dan Unit Khusus Manajemen Informasi Bank Indonesia. Saat ini ditunjuk oleh pemerintah Republik Indonesia untuk menakhodai institusi pengawas internet Indonesia ID-SIRTII (Indonesia Security Incident Response Team on Internet Infrastructure). Seluruh pengalaman yang diperolehnya selama aktif mengajar sebagai akademisi, terlibat di dunia swasta, dan menjalani tugas pemerintahan dituliskan dalam sejumlah publikasi. Hingga menjelang akhir tahun 2008, telah lebih dari 25 buku hasil karyanya yang telah diterbitkan secara nasional dan menjadi referensi berbagai institusi pendidikan, sektor swasta, dan badan pemerintahan di Indonesia – diluar beragam artikel dan jurnal ilmiah yang telah ditulis untuk komunitas nasional, regional, dan internasional. Seluruh karyanya ini dapat dengan mudah diperoleh melalui situs pribadi <http://www.eko-indrajit.com> atau <http://www.eko-indrajit.info>. Sehari-hari dapat dihubungi melalui nomor telepon 0818-925-926 atau email indrajit@post.harvard.edu.