MODUL PERKULIAHAN

EDP Audit

Kebijakan, Standar, dan/atau Pedoman Keamanan Sistem Informasi

(*Information Systems Security Policies, Standards, and/or Guidelines*)

Modul ini berisi tentang pembahasan Salah satu elemen kunci dari lingkungan pengendalian internal dalam organisasi adalah kebijakan keamanan sistem informasi (SI). Kebijakan keamanan SI memberikan kerangka kerja tingkat tinggi dimana semua kontrol keamanan terkait SI lain berasal.

Mahasiswa mampu memahami tetang kebijakan keamanan sistem informasi dan penerpannya serta merncangnya kebijakan keamanan sistem informasi.

Pengantar

Salah satu elemen kunci dari lingkungan pengendalian internal dalam organisasi adalah kebijakan keamanan sistem informasi (SI) (Lihat Tampilan 1.1). Kebijakan keamanan SI memberikan kerangka kerja tingkat tinggi dimana semua kontrol keamanan terkait SI lain berasal. Banyak dari kita berasumsi bahwa hampir semua organisasi memiliki kebijakan keamanan SI atau sesuatu yang memenuhi syarat seperti itu. Secara mengejutkan, ini bukanlah kasus. Menurut survei Datapro Information Services Group pada tahun 1996 lebih dari 1.300 organisasi dari Amerika Serikat, Kanada, tengah dan Selatan Amerika, Eropa, dan Asia, hanya 54 persen yang memiliki kebijakan keamanan SI. Turun dari angka tertinggi yaitu 82 persen pada tahun 1992 dan merupakan angka terendah sejak Datapro memulai survei di tahun 1991.[1] Survei juga menunjukkan bahwa hanya 62 persen dari responden organisasi telah menetapkan orang tertentu untuk bertanggung jawab terhadap keamanan komputer, dan sebagian besar responden melaporkan bahwa kurang dari 5 persen anggaran teknologi informasi (TI) organisasi mereka dialokasikan untuk keamanan.

Sebuah survei di seluruh dunia yang terpisah oleh Xephon of England mengkonfirmasi temuan Datapro. Xephon menemukan bahwa kurang dari 60 persen menanggapi organisasi memiliki kebijakan keamanan SI. Dari mereka yang melakukannya, Xephon menemukan bahwa kebijakan pada dasarnya dibuat dalam ruang hampa, dengan hanya satu dari lima berdasarkan pada standar eksternal.[2]

Baru-baru ini, Juli 2000 industri survei yang dilakukan oleh majalah Information Security menemukan bahwa 22 persen dari organisasi tidak memiliki kebijakan keamanan dan 2 persen dari responden tidak tahu jika organisasi mereka telah memiliki kebijakan.[3] Demikian pula, sebuah survei Internet Week tahun 2000 terhadap IT dan manajer keamanan menemukan 25 persen tidak memiliki kemanan IT resmi.[4]

Hasil survei ini mengkhawatirkan. Mereka menunjukkan bahwa banyak organisasi yang terlena dengan keamanan informasi di zaman ketika komputer dan sistem informasi sedang bermunculan pada tingkat eksponensional dan risiko kritis. Jika organisasi tidak memiliki kebijakan keamanan SI, kelemahan pengendalian internal yang signifikan dapat diidentifikasi. Kebijakan keamanan harus dikembangkan dan diimplementasikan sesegera mungkin.

Selain itu, prosedur harus dilaksanakan untuk memastikan bahwa kebijakan dan standar pendukung diperbarui untuk menyertakan undang-undang dan peraturan serta sebagai perubahan dalam praktik teknologi dan bisnis. Kebijakan dan setiap pembaruan

harus disampaikan kepada semua karyawan secara teratur (setidaknya setiap tahun). Bagian-bagian yang berlaku dari kebijakan dan standar juga harus disampaikan kepada semua staf kontingen (vendor, konsultan, temps, dll.). Istilah kebijakan, standar, dan pedoman sering digunakan secara bergantian di banyak perusahaan. Hal ini juga terjadi ketika anggota organisasi membahas dokumen keamanan SI. Namun, perbedaan antara istilah ini penting untuk dipahami sebelum mengevaluasi kecukupan keamanan SI dalam sebuah organisasi. Bagian berikut mendefinisikan dan membahas masing-masing istilah untuk memperjelas perbedaan.

Kebijakan Keamanan Sistem Informasi

Kebijakan keamanan sistem informasi adalah pernyataan keseluruhan tingkat tinggi yang menggambarkan tujuan umum dari sebuah organisasi yang berkaitan dengan kontrol dan keamanan atas sistem informasi. Kebijakan harus menentukan siapa bertanggung jawab untuk implementasinya. Kebijakan biasanya dibuat oleh manajemen dan disetujui oleh Dewan Direksi. Karena kebanyakan Dewan bertemu hanya setiap bulan, perubahan kebijakan sering memakan waktu beberapa bulan agar menjadi resmi. Jika perubahannya signifikan, Dewan dapat meminta informasi tambahan atau penelitian sebelumnya yang akan memberikan suara pada perubahan. Jika perubahan relatif kecil, mungkin tidak ada waktu yang cukup dalam agenda mereka untuk mengatasi perubahan kebijakan kecil. Untuk alasan ini, penting bahwa kebijakan keamanan SI tidak akan terlalu spesifik. Misalnya, kebijakan harus mensyaratkan organisasi memberikan kontrol keamanan fisik dan logis yang memadai atas perangkat keras komputer, perangkat lunak, dan data untuk melindungi mereka terhadap akses yang tidak sah dan kerusakan yang disengaja atau tidak disengaja, kehancuran, atau perubahan. Namun, kebijakan tersebut tidak harus menentukan kontrol rinci, seperti jumlah minimal karakter yang diperlukan untuk password atau jumlah maksimum gagal masuk yang diperbolehkan sebelum menangguhkan ID pengguna. Jika ini terjadi, manajemen senior akan terus-menerus mengirimkan permintaan perubahan kebijakan pada Dewan. Seperti yang kita tahu, sering kontrol yang dianggap kuat telah diubah secara tidak memadai oleh kemajuan teknologi. Pada satu waktu, lima karakter password dianggap cukup untuk aplikasi bisnis. Dengan hacking software yang tersedia dengan sedikit atau tanpa biaya di internet, password delapan karakter atau lebih sekarang diperlukan di banyak organisasi. Oleh karena itu, lebih praktis untuk menyertakan persyaratan kontrol SI rinci dalam standar keamanan SI sebuah organisasi. Standar dibahas dalam bagian berikutnya.

Tampilan 4.1 ini memberikan contoh dari kebijakan keamanan SI. Kebijakan terbagi menjadi lima bagian:

1. Tujuan dan tanggung jawab
2. Sistem pengadaan dan pembangunan
3. Terminal akses
4. Keamanan peralatan dan informasi
5. Program biro jasa

Secara umum, kebijakan ini cukup memadai. Namun, ada sejumlah peluang dimana kebijakan dapat diubah untuk meningkatkan efektivitas keseluruhan. Setiap bagian dari kebijakan yang mengandung area yang dapat ditingkatkan akan dikritik untuk menunjukkan bagaimana auditor bisa menilai kecukupan kebijakan dan merumuskan rekomendasi untuk meningkatkan efektivitas keseluruhan.

Bagian 1: Tujuan Dan Tanggung Jawab

Perusahaan mengoperasikan berbagai bentuk sistem komputasi dan telekomunikasi di seluruh operasinya. Untuk tujuan kebijakan ini, istilah "sistem" mengacu pada semua operasi komputer (mainframe, mini, mikro, komputer pribadi dan telekomunikasi) dan setiap daerah fungsional lainnya dalam data yang ditransmisikan melalui media elektronik atau telekomunikasi.

Tujuan dari kebijakan keamanan sistem informasi perusahaan adalah untuk memberikan pedoman yang penting untuk memproses transaksi elektronik yang efisien dan pelaporan jasa, sistem informasi manajemen, dan kemampuan informasi yang tepat bagi manajemen dan Direksi untuk secara efektif mengoperasika perusahaan. Selain itu, kebijakan ini dirancang untuk memastikan dukungan terus-menerus dan perbaikan sistem komputer dan telekomunikasi perusahaan.

Itu harus menjadi tanggung jawab dari Presiden atau/individu yang ditunjuknya dan Komite Manajemen Senior untuk mengelola sistem komputer dan telekomunikasi perusahaan. Presiden harus membentuk struktur operasi yang mengoptimalkan kemampuan sistem perusahaan konsisten dengan praktik bisnis yang sehat. Berbagai sistem akan terus-menerus dipantau untuk memastikan kelayakan fungsinya dan kemampuan untuk memenuhi kebutuhan perusahaan saat ini dan di masa depan. Presiden dan Komite Manajemen Senior harus bertanggung jawab dan mengarahkan studi kelayakan mengenai pengembangan, implementasi, dan sistem konversi, serta kelanjutan sistem operasi komputasi dan telekomunikasi perusahaan.

Bagian 2: Sistem Pengadaan Dan Pembangunan

Pengadaan perusahaan, pengembangan dan pengoperasian sistem pengolahan data (hardware dan software) harus dikelola oleh Presiden atau individu yang ditunjuknya dan Komite Manajemen Senior. Sistem komputasi perusahaan akan terus-menerus dipantau, dan saat ini dan/atau kebutuhan masa depan untuk perubahan dapat teridentifikasi,

perusahaan harus mengikuti langkah-langkah evaluasi sistem siklus hidup yang disebutkan pada halaman berikutnya.

a. definisi lingkup—gambaran yang perlu diatasi
b. definisi persyaratan—gambaran persyaratan pengguna akhir dan tujuan pembangunan baru
c. review dari solusi alternatif
d. desain sistem
e. pengembangan sistem
f. pengujian sistem
g. pemantauan sistem

Bagian 3: Akses Terminal

Manajemen berwenang untuk menginstal akses dial-up terminal online lainnya yang mungkin diperlukan dalam operasi perusahaan.

Bagian 4: Keamanan Peralatan Dan Informasi

Pembentukan dan pemeliharaan program keamanan yang lengkap meliputi sistem komputasi adalah tanggung jawab Presiden atau/individu yang ditunjuknya. Sistem dan informasi terkait akan dilindungi dan diberikan lingkungan operasi yang aman. Kontrol dan keamanan yang harus ada termasuk, namun tidak terbatas pada, berikut:

a. **Peralatan Dan Ketahanan Lingkungan.** Keamanan yang tepat untuk sistem komputer dan telekomunikasi harus dibuat dan dirawat seperti yang diperlukan untuk melindungi peralatan dan data terkait. Tujuan utama dari sistem ini adalah untuk melindungi dari pelanggaran keamanan yang akan membatasi gangguan yang tidak perlu dalam waktu pengolahan sistem dan untuk mencegah korupsi data perusahaan. Ruang mainframe komputer perusahaan, serta sistem komputasi dan fasilitas telekomunikasi lainnya yang sesuai seperti yang ditetapkan oleh manajemen, harus didukung oleh catu daya tak terputus, yang juga akan berfungsi sebagai sumber daya sementara jika terjadi kegagalan daya. Lingkungan fisik untuk fasilitas sistem ini akan dilindungi dari api, asap dan air. Selain itu, perusahaan akan mempertahankan dan mendukung pemanasan, ventilasi, dan pendingin udara yang diperlukan oleh berbagai sistem. Akses ke sistem juga akan dipelihara dan dipantau oleh personil keamanan. Semua sistem perangkat keras dan biaya pembuatan kembali data yang hilang akan diasuransikan secara memadai.

b. **Keamanan Informasi Dan Komunikasi.** Perusahaan adalah untuk mempertahankan integritas dan kontrol keamanan untuk melindungi semua sistem komputasi dan telekomunikasi, yang dimaksudkan juga untuk mengatasi risiko yang timbul dari potensi penyalahgunaan sumber daya sistem komputasi. Pembentukan kontrol ini harus mencakup, namun tidak dibatasi untuk, langkah-langkah berikut:

i. Kontrol akses logis
ii. Metode klasifikasi sumber daya informasi
iii. Keamanan jaringan dan akses lokal
iv. Retensi dan pembuangan informasi
v. Sistem pelaporan insiden untuk menganalisis kesalahan dan pengembangan prosedur untuk mencegah kejadian di masa depan

Langkah-langkah yang digunakan untuk membangun dan/atau meningkatkan kontrol tersebut harus tepat dibenarkan sebagai biaya dan keuntungan finansial relatif terhadap kritis dan sensitivitas sumber daya informasi yang dilindungi.

c. **Kontingensi Dan Pemulihan.** Kontrak dukungan sistem cadangan dibuat untuk melindungi perusahaan apabila terjadi kerusakan yang tak terduga atau terjadi bencana. Perusahaan adalah untuk mengembangkan dan mempertahankan rencana yang dapat mengatasi resiko bahwa peristiwa semacam itu dapat terjadi. Ini akan memerlukan perencanaan untuk pilihan pengolahan sistem komputasi alternatif (fasilitas, peralatan, dll) dan bahwa prosedur yang diperlukan didirikan agar berhasil mencapai setiap alternatif ini. Ini adalah untuk memastikan bahwa perusahaan dapat membuat bisnis terus berlanjut. Persyaratan minimum kontinjensi harus mencakup, namun tidak terbatas pada, langkah-langkah berikut:

1) identifikasi aplikasi penting dalam menentukan prioritas mereka untuk pemulihan.
2) dokumentasikan pencadangan dan rencana pemulihan yang mencakup semua aset informasi terkait atau berpotensi terkena dampak (dan kemungkinan mereka/potensi efek pada setiap/semua bidang operasional).
3) menguji prosedur setidaknya setahun sekali untuk mengevaluasi efektivitas rencana aset informasi, personil dan semua hal lainnya yang berpotensi terkena dampak wilayah operasional.

4) perusahaan harus menjaga data cadangan di luar lokasi untuk membatasi risiko dan mengijinkan pemulihan data tepat waktu di tempat informasi yang hancur, rusak, atau untuk alasan apa pun dibuat tidak berguna.

Bagian 5: Program Biro Jasa

Perjanjian biro jasa perusahaan dirancang untuk mewajibkan biro tersebut yang ditunjuk perusahaan menunjukkan komitmen untuk mengembangkan dan memelihara perangkat lunak aplikasi komputer sedemikian rupa sehingga kemampuan sistem, sebagaimana ditentukan oleh perusahaan, dipaastikan dan sesuai dengan pembukuan cek dan saldo yang ada. Perjanjian harus mendetail tingkat dukungan biro jasa yang akan menyediakan program-program yang ada, program-program baru yang dikembangkan, dan program pembaruan. Akibatnya, langkah-langkah berikut dirancang untuk memfasilitasi interaksi yang positif dengan semua biro jasa yang sedang digunakan:

a. permintaan pemrograman oleh perusahaan akan dimonitor untuk ketepatan waktu respons oleh biro jasa, dan di mana ketepatan waktu atau kualitas kinerja dipertanyakan, Presiden atau orang yang ditunjuknya akan mengevaluasi alternatif untuk kinerja yang lebih baik.
b. perusahaan, melalui sendiri seperti sistem verifikasi biro jasa, akan memastikan bahwa sistem perangkat lunak baru beroperasi dengan benar sebelum konversi yang dibuat untuk penggunaan operasional standar.
c. sistem perangkat lunak biro jasa yang disediakan akan didukung oleh dokumentasi rinci yang menginstruksikan perusahaan dalam operasi dan prosedur kesalahan pencatatan.

Bagian 1: Tujuan dan tanggung jawab

Kalimat kedua dalam paragraf pertama memberikan sebuah definisi dari istilah sistem. Namun, definisi tersebut agak tanggal dengan tidak menjelaskan jenis komputer tertentu dan metode transmisi data yang sering digunakan hari ini. Untuk memberikan definisi yang lebih universal meliputi kemajuan teknologi terbaru, rekomendasi dapat disampaikan kepada manajemen untuk mengubah definisi sistem dalam membaca:

> Untuk tujuan kebijakan ini, istilah sistem menunjuk pada semua operasi komputer dalam perusahaan, termasuk, namun tidak terbatas pada, mainframe, midranges, mini, jaringan lokal dan wide area, desktop pribadi dan komputer laptop, telekomunikasi, setiap teknologi baru saat ini yang sedang dikembangkan, dan komputer khusus lainnya yang berada di bidang fungsional dimana data ditransmisikan atau diproses melalui elektronik, telekomunikasi, satelit, microwave, atau media lain.

Paragraph ketiga menentukan dengan tepat bahwa Presiden atau orang yang ditunjuknya dan Komite Manajemen Senior bertanggung jawab mengelola sistem komputasi dan telekomunikasi perusahaan. Pembaca harus mencatat bahwa dalam beberapa organisasi besar dengan lingkungan sistem komputasi yang kompleks, Komite Pengarah SI yang terdiri dari beberapa anggota manajemen senior dan manajer kunci lainnya diberikan tanggung jawab untuk mengelola dan mengarahkan semua sumber daya sistem komputasi. Pada kenyataannya, auditor eksternal organisasi ini mengajurkan agar Komite Pengarah SI dibuat. Ketika organisasi memutuskan untuk membuat suatu Komite Pengarah, kebijakan harus disesuaikan sebagaimana mestinya.

Bagian 2: Sistem pengadaan dan pembangunan

Bagian 2 menunjukkan langkah-langkah yang diperlukan ketika sistem informasi baru sedang dipertimbangkan dalam organisasi. Langkah-langkah ini mewakili pendekatan siklus hidup standar sistem pengembangan. Namun, salah satu langkah utama hilang antara sistem pengujian dan sistem pemantauan. Harus ada langkah yang disebut implementasi sistem. Implementasi sistem adalah puncak dari semua perencanaan sebelumnya dan tahap-tahap pengembangan. Ini adalah dimana sistem baru ditempatkan ke dalam produksi dan tim pengembangan proyek tahu seberapa baik sistem dilakukan di bawah beban data langsung yang terus-menerus. Efek dari penerapan sistem baru pada organisasi dapat bervariasi, tergantung pada jumlah komponen perangkat keras, program, dan jumlah data yang diproses pada sistem baru. Implementasi utama seringkali dilakukan selama akhir pekan untuk memberikan lebih banyak waktu timbul masalah tak terduga. Beberapa implementasi dapat berlangsung selama beberapa minggu atau bulan, sebagai bagian yang berbeda dari sistem yang dibawa secara online. Organisasi sering memilih untuk menjaga sistem lama beroperasi secara bersamaan dengan yang baru untuk memberikan jaminan tambahan bahwa sistem baru ini sepenuhnya mampu memproses data tanpa masalah yang signifikan. Karena pentingnya tahap implementasi dalam siklus hidup suatu sistem informasi baru, rekomendasi untuk menambahkan langkah implementasi sistem ke kebijakan keamanan SI akan dibenarkan.

Bagian 3: Akses terminal

Bagian 3 tidak mengandung informasi yang cukup untuk menjamin bagian terpisah. Oleh karena itu, bagian tersebut harus dihapus atau digabungkan ke dalam Bagian 4.

Bagian 4: Keamanan peralatan dan informasi

Bagian 4 membagi keamanan menjadi tiga subbagian:

a. peralatan dan ketahanan lingkungan
b. keamanan informasi dan komunikasi
c. kontingensi dan pemulihan

Subbagian b memerlukan setidaknya lima pembentukan kontrol tertentu (item i sampai v). Antara kontrol ini, item i (kontrol akses logis) dan item iii (keamanan jaringan dan akses lokal) sangat penting untuk dimasukkan dalam setiap kebijakan keamanan SI. Namun, ada kekurangan dalam kedua pernyataan ini yang pada dasarnya mengacu pada jenis kontrol yang sama. Pembaca kebijakan dalam Tampilan 4.1 akan menjadi bingung ketika mereka melihat keamanan logis dan jaringan serta keamanan akses lokal sebagai kontrol yang terpisah.

Seperti yang telah dibahas dalam Bab 1, kontrol keamanan logis adalah pembatasan kemampuan akses pengguna sistem dan pencegahan pengguna yang tidak sah dari pengaksesan sistem. Kontrol keamanan logis mungkin ada dalam sistem operasi, sistem manajemen database, program aplikasi, atau ketiganya. Karena sistem operasi dan program aplikasi yang ada di setiap komputer melakukan fungsi-fungsi khusus, keberadaan keamanan logis ini tidak bergantung pada ukuran atau jenis komputer. Keamanan logis harus ada di mainframe, midranges, mini, jaringan lokal, dan jenis peralatan yang membolehkan akses elektronik dengan data dalam sebuah organisasi.

Jaringan termasuk dalam definisi sistem dalam bagian 1 dari kebijakan, bersama dengan semua jenis sistem komputasi. Karena keamanan jaringan dapat dianggap sebagai bagian dari lingkungan keamanan logis organisasi, tidak boleh secara khusus disebutkan sebagai kontrol terpisah di bawah bagian 4, subbagian b.

Dalam referensi untuk keamanan akses lokal di item iii, tidak jelas apakah istilah lokal terkait. Akses ke sistem apapun dapat berlangsung dari berbagai lokasi, termasuk dimana ada unit pemroses Sentral (CPU), pada pengguna akhir di tempat kerja, atau dari lokasi terpencil melalui koneksi dial-in komunikasi. Tergantung pada salah satu sudut pandang, salah satu lokasi dapat dianggap lokal. Oleh karena itu, akan lebih baik untuk menggabungkan dua pernyataan kontrol dalam item i dan iii ke frase tunggal, bagian

menyeluruh, seperti " kontrol akses logis dalam sistem operasi, sistem manajemen database, dan aplikasi dari semua sistem komputasi dan telekomunikasi perusahaan."

Bagian 5: Program Biro Jasa

Bagian 5 mengatasi sebagian besar masalah yang berhubungan dengan kebijakan yang terkait dengan biro jasa. Namun, salah satu risiko penting yang tidak dibahas terkait dengan disposisi kode sumber aplikasi asli dalam acara operasi pemberhentian biro jasa atau sebaliknya gagal untuk memenuhi aspek penting dari kontraknya dengan organisasi klien.

Banyak perusahaan memerlukan kode sumber aplikasi versi yang digunakan saat ini yang akan berlangsung dalam perjanjian escrow oleh pihak ketiga yang independen. Pihak ketiga akan diotorisasi untuk melepaskan kode sumber ke organisasi klien jika aspek tertentu dari kontrak tidak terpenuhi. Jika dapat diterapkan, persyaratan kode dasar escrow juga harus diterapkan dalam kontrak dengan vendor perangkat lunak yang memasok dan memelihara program untuk organisasi tetapi yang tidak biro jasa. Dengan menetapkan persyaratan ini dalam kontrak, organisasi klien dapat mengurangi risiko gangguan bisnis jika biro jasa atau vendor perangkat lunak berhenti operasi. Organisasi akan dapat terus menjaga dan memodifikasi kode dasar aplikasi vendor sampai pengganti yang cocok bisa dikembangkan atau dibeli dari vendor lain.

Ide yang baik akan menambah langkah keempat dalam kebijakan Bagian 5 yang berbunyi: "Kontrak dengan organisasi biro jasa dan vendor perangkat lunak eksternal akan menentukan kode dasar asli yang diadakan dalam escrow oleh seorang pihak ketiga yang independen dan kode dasar akan dirilis ke perusahaan dalam acara biro jasa atau operasi teputus penjual perangkat lunak, berhenti mendukung perangkat lunak, atau jika melanggar syarat-syarat apapun yang signifikan dalam kontrak." (Catatan: Informasi lebih lanjut tentang item harus ditetapkan dalam kontrak dengan biro jasa dan vendor perangkat lunak luar harus dimasukkan dalam standar keamanan SI. Standar tersebut dibahas dalam bagian berikutnya.) Karena banyak risiko yang terkait dengan biro jasa yang juga berlaku untuk program perangkat lunak yang dibeli dari luar vendor, rekomendasi tambahan akan mengubah nama Bagian 5 untuk program biro jasa dan program perangkat lunak vendor di luar atau untuk menambahkan bagian kebijakan yang terpisah untuk mengatasi resiko unik apapun yang mungkin organisasi terkena sebagai bagian hasil dari program vendor perangkat lunak luar. Daftar berikut meringkas konsep-konsep umum yang dimasukkan dalam kebijakan keamanan di Tampilan 4.1 serta koreksi kekurangan pencatatan.

Masing-masing item dalam daftar harus disertakan dalam kebijakan keamanan SI semua organisasi. Jika organisasi tidak menggunakan biro jasa atau beberapa program vendor perangkat lunak, mereka dapat dikeluarkan dari kebijakan. Namun, termasuk mereka membuat kebijakan yang lebih fleksibel dengan mengurangi kebutuhan untuk memperbarui atau merevisinya ketika organisasi memutuskan untuk menggunakan layanan biro jasa atau beberapa vendor perangkat lunak. Item yang termasuk dalam kebijakan keamanan sistem informasi:

- Pernyataan tujuan dan tanggung jawab
- Sistem pengadaan dan pendekatan pengembangan
- Peralatan dan ketahanan lingkungan (yaitu, keamanan fisik)
- Keamanan informasi dan komunikasi (yaitu, keamanan logis)
- Kontingensi dan pemulihan (ini adalah bagian dari keamanan fisik, tetapi dapat diterima untuk memiliki bagian terpisah karena kepentingnya)
- Program biro jasa (jika diterapkan)
- Beberapa vendor program perangkat lunak (jika diterapkan)

Kebijakan keamanan SI organisasi harus diperiksa untuk memastikan bahwa itu mengandung setidaknya konsep-konsep yang disajikan dalam daftar ini. Tergantung pada sifat organisasi dan kompleksitas serta ukuran lingkungan sistem komputasinya, mungkin perlu untuk merekomendasikan penambahan atau penghapusan item tertentu dari kebijakan keamanan. Dalam beberapa kasus, bahkan mungkin tepat memiliki kebijakan terpisah dari masing-masing anak perusahaan, divisi atau unit operasi lain.

STANDAR KEAMANAN SISTEM INFORMASI

Standar keamanan sistem informasi adalah kriteria minimum, aturan dan prosedur yang didirikan oleh manajemen senior yang harus dilaksanakan untuk membantu memastikan pencapaian kebijakan keamanan SI. Mereka diimplementasikan oleh staf (misalnya, administrator keamanan sistem dan pengguna) di bawah arahan manajemen. Standar keamanan sistem informasi harus menentukan persyaratan rinci masing-masing kontrol SI. Beberapa contoh rinci kontrol yang harus ditentukan dalam standar adalah panjang sandi minimal delapan karakter, 30-hari masa kadaluarsa sandi, dan persyaratan sandi yang terdiri dari setidaknya dua alfa dan dua karakter numerik. Standar seharusnya tidak spesifik untuk platform komputer tertentu (misalnya, membuat, model, atau sistem operasi). Sebaliknya, sebaiknya cukup umum untuk menerapkan semua yang ada dan

mengusulkan sistem informasi yang memiliki beberapa bentuk keamanan logis dan/atau fisik. Setiap kali manajemen menganggap bahwa standar perlu diubah, perubahan dapat dikomunikasikan kepada staf dan dilaksanakan tanpa memerlukan persetujuan Dewan Direksi. Hal ini memungkinkan organisasi untuk bereaksi lebih cepat terhadap kemajuan teknologi yang mungkin telah melemahkan standar yang sudah ada.

Berkaitan dengan audit, standar keamanan SI memberikan sebuah tolak ukur persetujuan manajemen atau dasar terhadap kecukupan kontrol yang diterapkan pada sistem informasi individu yang dapat dinilai. Tampilan 4.2 memberikan contoh standar keamanan SI yang bisa diterapkan untuk banyak sistem informasi. Manajemen harus memastikan bahwa standar diterapkan untuk sistem yang ada, bahwa mereka merupakan bagian dari spesifikasi desain untuk sistem saat ini di bawah perkembangan secara internal, dan kontrak dengan vendor perangkat lunak eksternal dan biro jasa yang programnya harus sesuai dengan standar. Terkadang situasi mungkin timbul bahwa surat perintah menyimpang dari standar. Penyimpangan ini harus didokumentasikan dan disetujui oleh manajemen yang bertanggung jawab untuk sistem dan proses terkait.

Berikut adalah standar keamanan SI minimum yang telah disetujui oleh manajemen senior dan akan diterapkan pada sistem informasi yang berlaku dalam organisasi:

1. Setelah selesai instalasi awal perangkat lunak, sandi pertama akan diubah oleh administrator keamanan sistem.
2. Seorang administrator keamanan sistem cadangan harus ditunjuk dan dilatih untuk memastikan operasi lanjutan dari sistem, bahkan tanpa adanya administrator keamanan sistem utama.
3. Administrator keamanan sistem akan mengatur parameter untuk meminta sandi minimal 8 karakter alfa-numerik, karakter panjangnya.
4. Sistem harus dirancang sehingga sandi tersamar (yaitu, tak terlihat) pada layar tempat kerja seperti mereka dimasukkan oleh pengguna.
5. Sistem harus dirancang sehingga file kata sandi yang dienkripsi dengan algoritma yang aman agar tak seorang pun, termasuk administrator keamanan sistem, dapat melihat mereka.
6. Administrator keamanan sistem akan menetapkan sandi secara otomatis berakhir dalam waktu 60 hari atau kurang.
7. ID pengguna akan dibatalkan setelah upaya tiga kali berturut-turut gagal masuk. Pengguna akan diminta untuk menghubungi administrator keamanan sistem

untuk miliki ulang ID pengguna mereka. Hanya administrator keamanan sistem yang memiliki kewenangan untuk me-reset ID pengguna.

8. Sesi pengguna harus diakhiri setelah lima menit tanpa aktivitas.
9. Pengguna tidak akan diizinkan masuk (sign on) pada sesi yang bersamaan.
10. Administrator keamanan sistem harus menghapus ID pengguna dari pengguna yang dihentikan atau dialihkan segera setelah pemberitahuan dari manajer departemen pengguna dan/atau departemen sumber daya manusia. Prosedur harus mewajibkan manajer departemen untuk memberitahu semua administrator keamanan sistem yang berlaku ketika pengguna berhenti atau beralih.
11. Manajer departemen harus bertanggung jawab untuk pelatihan pengguna agar tidak membagi atau mengungkapkan sandi mereka kepada siapa pun, menuliskannya, mempostingnya dalam tempat kerja mereka, menyimpannya dalam sebuah file elektronik, atau melakukan tindakan lain yang dapat berpotensi menyebabkan sandi terungkap.
12. Administrator keamanan sistem akan meminta manajemen departemen pengguna untuk meninjau kemampuan akses pengguna dan menyatakan secara tertulis bahwa kemampuan akses pengguna di departemen mereka perlu melaksanakan tugas-tugas yang normal. Sertifikasi ini harus dilakukan setidaknya setiap tahunnya, atau lebih sering jika dianggap perlu oleh manajemen senior.
13. Keamanan logis terkait kejadian-kejadian akan dicatat oleh sistem, dan pencatatan akan terus-menerus dipantau oleh administrator keamanan sistem dari potensi tindakan akses yang tidak sah. Contoh keamanan logis yang berhubungan dengan kejadian-kejadian termasuk gagal masuk, penambahan/penghapusan pengguna dan perubahan kemampuan akses, menyetel ulang sandi, dan restart sistem. Ada banyak kemungkinan kejadian-kejadian lain yang bisa dicatat.

(Catatan: ada sebuah pertimbangan antara pengendalian dan efisiensi dalam standar ini. Semakin banyak kejadian yang dicatat, semkain banyak memori yang diperlukan untuk menyimpan kejadian-kejadian dalam file pencatatan. Pada beberapa sistem, "yang di atas" ini dapat menyebabkan penurunan yang signifikan dalam kinerja sistem atau bahkan kegagalan sistem jika file pencatatn tidak dibersihkan. Juga, administrator keamanan sistem harus menghabiskan lebih banyak waktu untuk meninjau file pencatatan. Oleh karena itu, administrator sistem keamanan harus bekerja dengan manajemen untuk menentukan kejadian paling penting yang sistem tertentu mereka dapat masuk dan dapat ditinjau dalam jumlah yang waktu tepat.)

14. Prosedur kembalinya bisnis harus sepenuhnya dikembangkan, diuji, dan didokumentasikan oleh manajemen bekerjasama dengan administrator keamanan sistem dan staf kunci lainnya. Rencana kembalinya bisnis harus memberikan backup sistem lengkap secara mingguan, backup data lengkap setiap hari, dan rotasi media cadangan ke fasilitas luar yang aman pada tiga generasi atau lebih siklus rotasi.
15. Cakupan asuransi yang memadai harus dapat memelihara perangkat keras, sistem operasi, aplikasi perangkat lunak dan data. Perangkat keras harus ditutupi dengan biaya penggantian. Sistem operasi, aplikasi perangkat lunak, dan data harus menutupi biaya penciptaan kembali. Pendapatan yang hilang akibat kegagalan perangkat keras dan/atau hilangnya sistem operasi, aplikasi perangkat lunak dan data selama peristiwa tertutup akan sepenuhnya ditutupi.
16. Untuk aplikasi khusus yang dikembangkan oleh vendor perangkat lunak eksternal, kontrak harus menentukan bahwa kode dasar asli harus ada di escrow oleh pihak ketiga yang independen dan bahwa kode dasar akan dirilis untuk pembeli dalam hal vendor berhenti mendukung perangkat lunak atau melanggar syaratan "signifikan" dalam kontrak. Hal lainnya yang termasuk dalam kontrak vendor termasuk kontrak periode, biaya pemeliharaan tahunan, jenis pemeliharaan yang disediakan, standar tingkat layanan (yaitu, persyaratan waktu respon), dan seterusnya.
17. Aplikasi vendor yang dikembangkan di kemudian hari secara kontrak diperlukan untuk menyertakan pemrograman yang memungkinkan standar digunakan setelah instalasi.
18. Informasi rahasia, termasuk sandi, akan dienkripsi oleh algoritma yang aman selama transmisi elektronik.
19. Administrator keamanan sistem akan menginstal perangkat lunak yang secara otomatis memeriksa virus menggunakan file pola virus saat ini. Parameter software virus harus ditetapkan untuk memeriksa semua sektor memori komputer, termasuk sektor boot, semua perangkat penyimpanan permanen, dan semua file masuk. Perangkat lunak juga ditetapkan untuk memberitahu administrator keamanan sistem atas virus yang teridentifikasi.

STANDAR OPSIONAL JIKA DIBENARKAN OLEH RISIKO (DAN JIKA SISTEM MAMPU)

20. Akses pengguna harus dibatasi untuk jam dan hari-hari kerja normal (misalnya, 6 A.M. hingga 6 P.M., Senin sampai Jumat). Akses malam dan akhir pekan harus memerlukan tambahan persetujuan tertulis dari manajemen yang bertanggung jawab atas sistem.
21. Akses pengguna harus dibatasi untuk tempat kerja tertentu. (Catatan: setiap tempat kerja diidentifikasi dengan sejumlah titik unik.)

Daftar di atas adalah standar keamanan SI yang didesain cukup umum. Tergantung pada sifat organisasi, mungkin perlu merekomendasikan standar tambahan yang akan membantu memperkuat lingkungan kontrol SI. Seperti kebijakan, mungkin perlu untuk merekomendasikan serangkaian standar yang berbeda untuk masing-masing anak perusahaan, divisi atau unit operasi.

PEDOMAN KEAMANAN SISTEM INFORMASI

Pedoman keamanan sistem informasi juga dibuat oleh manajemen senior dan dimaksudkan untuk membantu memastikan tercapainya kebijakan keamanan SI. Panduan tersebut serupa dengan format standar yang memberikan spesifikasi rinci untuk kontrol SI individu. Di mana keduanya berbeda dengan standar dalam implementasinya. Di beberapa perusahaan, manajemen dapat mengarahkan staf untuk menerapkan pedoman yang mereka nilai relevan atau bermanfaat. Di sisi lain, mereka mungkin paham dengan kesetaraan standar. Karena pedoman tidak selalu diperlukan oleh manajemen untuk diimplementasikan, mereka bisa membuktikan menjadi agak anomali ke auditor. Sebagai contoh, dalam sebuah perusahaan yang memiliki pedoman keamanan SI tetapi bukan standar, auditor dapat menggunakan pedoman sebagai tolok ukur kecukupan pengendalian dari sistem informasi tertentu yang dapat dinilai. Ketika merekomendasikan perbaikan dalam kontrol kepada manajemen lini yang bertanggung jawab atas sistem, menggunakan pedoman sebagai tolok ukur, auditor mungkin menghadapi perlawanan terhadap perubahan karena manajemen lini tidak mempertimbangkan pedoman menjadi persyaratan. Untuk alasan ini istilah penggunaan pedoman tidak pantas ketika mengacu pada kontrol keamanan SI. Semua perusahaan harus mengembangkan standar keamanan SI yang jelas didefinisikan dan dilaksanakan.

Seharusnya tidak mengejutkan ketika seseorang tidak dapat menemukan kebijakan, standar, atau pedoman keamanan SI yang memadai dalam sebuah organisasi. Berdasarkan pengalaman pribadi dan diskusi dengan banyak rekan dalam berbagai asosiasi professional audit, tampak bahwa banyak perusahaan yang tidak memiliki kebijakan, standar, atau pedoman keamanan SI apapun. Bahkan di perusahaan-perusahaan yang melakukan, kebijakan, standar, dan pedoman sering tidak memadai atau tidak membahas banyak risiko yang terkait dengan sistem informasi. Dalam banyak kasus, yang disebut kebijakan, standar, atau pedoman yang sebenarnya hanya konglomerasi prosedur di berbagai lokasi, masing-masing disiapkan secara independen dari yang lain (Lihat studi kasus 4.1, 4.2 dan 4.3).

STUDI KASUS 4.1

Standar keamanan sistem informasi yang memadai

Di satu organisasi yang diaudit, ada standar keamanan SI dalam buku pegangan karyawan, standar lainnya di mikrokomputer pengguna manual, dan masih ada standar lainnya yang berlaku untuk setiap platform komputer besar dalam organisasi. Ada juga satu lembar halaman pedoman sandi yang diserahkan kepada karyawan baru oleh departemen sumber daya manusia saat perekrutan. Setiap dokumen-dokumen tersebut disiapkan secara independen oleh departemen terpisah. Tidak ada tempat dengan seperangkat standar. Setelah mempekerjakan, karyawan tidak menerima pelatihan tambahan pada keamanan SI. Sebagian besar karyawan yang bahkan tidak menyadari adanya standar untuk platform komputer utama atau lokasi standar lainnya. Sebagai akibatnya, kesadaran keamanan SI tidak konsisten di seluruh organisasi. Dalam beberapa manajemen departemen sangat sadar akan adanya keamanan SI, sementara di departemen lain keamanan SI lebih dipandang sebagai ketidaknyamanan operasional.

Dianjurkan bahwa direksi masing-masing area pengolahan SI bersama-sama mengembangkan seperangkat standar keamanan SI yang akan memberikan konsistensi dalam aplikasi kontrol atas semua sistem informasi dalam organisasi. Hal ini juga dianjurkan bahwa, setelah selesai, standar dikomunikasikan ke semua anggota staf. Satu saran untuk mengkomunikasikan standar-standar baru adalah dengan mengembangkan sebuah brosur referensi atau pamflet yang merincikan standar dan kemudian mendistribusikan dokumen untuk semua anggota staf yang sudah ada. Lebih lanjut direkomendasikan bahwa standar-standar baru dimasukkan sebagai bagian dari pelatihan semua karyawan baru yang diwajibkan untuk hadir.

STUDI KASUS 4.2

Pengembangan program perlindungan informasi

Selama bertahun-tahun, sebuah organisasi perbankan telah memiliki standar keamanan sistem informasi yang memadai yang didasarkan pada jenis-jenis sistem komputasi yang ada dalam organisasi. Salah satu bagian dari standar mengatasi berbagai kontrol umum atas lingkungan mainframe, bagian lain mengatasi jaringan, bagian lain mengatasi komputer pribadi yang berdiri sendiri, bagian lain mengatasi sistem telekomunikasi, dan seterusnya. Setiap bagian dari standar pada dasarnya adalah salinan standar umum yang sama, dengan sedikit modifikasi kata-kata untuk menyesuaikannya dengan jenis sistem komputasi. Hal ini mengakibatkan tidak terlalu panjang serangkaian standar dengan informasi yang berlebihan. Selain itu, kontrol umum tidak menentukan setiap kontrol keamanan logis (password, enkripsi, administrasi keamanan sistem, dll), yang boleh dibilang standar yang paling penting. Standar umum hanya menutupi hal-hal seperti keamanan fisik dan pengadaan sistem. Seperti yang diharapkan, kurangnya standar keamanan logis yang mengakibatkan tidak konsistennya pelaksanaan kontrol keamanan logis seluruh organisasi, sehingga organisasi mendapat risiko yang berlebihan. Standar lain yang buruk mengatakan yang terbaik.

Auditor internal SI membuat rekomendasi yang konsisten mengenai keamanan logis dan kontrol lain selama audit setiap individu. Karena tidak ada standar internal yang dapat direferensi, auditor SI membela rekomendasi mereka sebagai praktek bisnis umum dalam industri. Selama beberapa tahun, manajer audit SI merekomendasikan beberapa kali ke kepala sistem informasi bahwa standar umum perusahaan harus dikembangkan. Upaya tersebut tidak berhasil. Setiap tahun manajer audit SI membahas masalah tersebut dengan auditor eksternal SI yang mendukung laporan keuangan audit tahunan. Akhirnya, manajer audit internal SI yakin auditor eksternal SI merekomendasikan kepada manajemen senior organisasi bahwa seperangkat standar keamanan SI harus dikembangkan. Sekitar 10 bulan kemudian, pada tahun 1997, manajemen senior menugaskan tim perwakilan dari berbagai bidang organisasi, termasuk audit SI, untuk merancang berbagai standar perusahaan yang mengatasi tidak hanya keamanan SI, tetapi juga perlindungan informasi secara umum, terlepas dari apakah informasi yang ada dalam elektronik, kertas, mikrofilm, atau bentuk lain. Manajemen senior khaawatir bahwa dengan meningkatkan prevalensi telekomunikasi dan keberadaan sejumlah besar informasi dalam bentuk non electronik, standar keamanan tidak cukup komprehensif. Tim juga menyewa konsultan dari perusahaan audit eksternal untuk memfasilitasi pengembangan standar.

Pada tahun 1998, produk akhir selesai. Tim telah mengembangkan program perlindungan informasi (IP) yang komprehensif dan satu set prosedur yang mengharuskan semua karyawan, terlepas dari apakah mereka bekerja dalam SI atau unit bisnis, melakukan praktik IP tersebut untuk lingkungan kerja mereka. Tim telah mengidentifikasi sekitar 125 standar IP umum. Ini dibagi menjadi tiga kategori: departemen, sistem administrasi, dan kemampuan sistem.

Standar departemen adalah standar yang dijalankan oleh semua karyawan di semua departemen. Mereka termasuk sekitar 25 standar nalar seperti mengunci tempat kerja ketika meninggalkan langsung, menyimpan informasi rahasia yang terlihat dan menguncinya bila diperlukan, tidak menuliskan sandi atau menggunakan sandi yang mudah ditebak, dan menutup jaringan pada akhir pergeseran. Masing-masing departemen juga diminta untuk mengklasifikasikan informasi yang diterima ke dalam tiga kategori umum: umum, terbatas dan rahasia. Informasi publik bisa dibagi oleh siapa pun. Contoh seperti hal-hal pemasaran dan bahan-bahan promosi. Informasi terbatas dapat dibagi di antara semua karyawan tetapi tidak dengan publik. Contoh buku telepon karyawan, informasi intranet, dan semua e-mail staf. Informasi rahasia dapat dibagi dengan orang-orang yang memiliki alasan bisnis yang sah untuk keperluan informasi. Sebagian besar informasi jatuh dalam kategori rahasia. Manajemen diminta untuk mengkomunikasikan klasifikasi informasi kepada karyawan dan melaksanakannya sesuai kontrol atas setiap jenis informasi.

Standar sistem administrasi adalah standar yang dijalankan oleh semua administrator sistem. Ada sekitar 50 standar, seperti: meninjau keamanan pencatatan peristiwa; memastikan bahwa informasi terbatas atau rahasia dienkripsi sambil mengirim secara elektronik; melindungi sistem hardware dari api, lonjakan listrik, dan pencurian; menunjuk dan melataih administrator sistem cadangan; dan menginstal perangkat lunak pemeriksa virus otomatis. Tergantung pada risiko dan signifikansi sistem, beberapa standar tidak akan diterapkan.

Standar kemampuan sistem adalah standar yang diinginkan dalam sistem. Ada sekitar 50 standar, seperti kemampuan untuk: membatasi akses ke informasi dan pemisahan tugas; menetapkan sandi panjang minimal delapan karakter dan kadaluarsa sandi 60 hari; menyimpan sandi dalam format terenkripsi; mengubah sandi awal pada sistem yang baru; dan membuat jejak audit.

Prosedur kritis yang dibangun dalam program IP untuk memastikan bahwa standar IP tidak hanya mengumpulkan debu: sertifikasi tahunan diselesaikan oleh 31 Maret. Manajer masing-masing departemen perlu meninjau daftar sertifikasi standar departemen

dengan staf. Daftar diperlukan para manajer dalam menentukan "ya," "tidak", atau "tidak dapat diterapkan" pada masing-masing standar. Ada ruang komentar singkat di sebelahnya untuk setiap tanggapan. Manajer harus menandatangani sertifikasi yang menunjukkan bahwa standar dikomunikasikan dan dibahas dengan staf dan mengaruskan manager divisi menyetujui sertifikasi. Demikian pula, para administrator dari setiap sistem unik di organisasi diperlukan untuk melengkapi sistem administrasi dan daftar pembanding penilaian kemampuan sistem. Daftar pembanding sertifikasi yang sudah selesai semua dikirim ke petugas keamanan untuk memastikan bahwa semua departemen dan administrator sistem telah menyelesaikannya. Selama satu bulan sebelum sertifikasi, seluruh tim organisasi, termasuk manajer audit SI, menyelenggarakan peninjauan dan memperbarui standar IP dan prosedur yang terkait.

Untuk beberapa sistem, terutama aplikasi yang kurang canggih, tidak semua sistem administrasi dan standar kemampuan sistem bisa bertemu. Begitu lama seperti risiko ketidakpatuhan yang dapat diterima manajemen, tidak ada tindakan yang diperlukan. Tindakan sertifikasi tahunan sebagai pengingat untuk manajemen untuk menilai kembali risiko sistem. Sertifikasi diperiksa untuk memastikan mereka telah selesai dan disetujui, dan tanggapan untuk setiap daftar standar ditinjau kewajaran dan akurasinya. Daftar tanggapan sering memberikan auditor SI ide atas tingkat pengetahuan para administrator sistem dan kecanggihan sistem yang diaudit.

Untungnya bagi organisasi, program IP baru ini memiliki kemajuan. Setelah penggunaan program IP pada tahun 1998, Gramm-Leach-Bliley (GLB) Financial Services Modernization Act pada tahun 1999 disahkan. Hal ini membutuhkan, antara lain, bahwa lembaga keuangan sepenuhnya mengungkapkan penjelasan praktiknya mengenai pembagian informasi keuangan pribadi kepada pelanggan mereka, mendistribusikan informasi pelanggan hanya jika pelanggan memberi mereka izin, dan melaksanakan praktik keamanan yang memadai untuk melindungi informasi pelanggan pribadi. Kepatuhan penuh sesuai dengan informasi pribadi GLB dan persyaratan perlindungan yang dibutuhkan pada tanggal 1 Juli 2001. Persyaratan GLB yang ditetapkan ke program IP, dan hanya segelintir standar baru atau penyesuaian yang harus dilakukan. Sementara kebanyakan organisasi perbankan harus mengembangkan program-program perlindungan informasi yang komprehensif dari awal, organisasi ini telah berkeinginan untuk mengembangkan praktik bisnisnya, terutama atas desakan manajer audit internal SI.

STUDI KASUS 4.3

Organisasi pemerintah tanpa kebijakan atau standar keamanan

Pemerintah kota besar AS tidak memiliki kebijakan dan standar keamanan sistem informasi. Sebagai hasilnya, keamanan yang dilaksanakan tidak konsisten dan tidak cukup di antara berbagai jaringan yang ada dan sistem aplikasi yang tersebar di seluruh banyak lembaga kota dan unit bisnis. Bahkan mainframe sistem operasi yang terpusat di pusat data kurangan konsisten dan keamanan yang kurang memadai. Kurangnya kebijakan dan standar juga terpengaruh pada sistem baru yang sedang dikembangkan. Selama audit dua perusahaan pada sistem proyek pembangunan aplikasi yang utama, telah ditemukan bahwa proposal permintaan proyek (RFPs) untuk vendor perangkat lunak tidak termasuk persyaratan rancangan keamanan logis tertentu yang dianggap perlu untuk melindungi informasi rahasia secara memadai. Tim proyek juga tidak mengidentifikasi prosedur pasca implementasi yang memadai untuk sistem keamanan administrasi sampai setelah auditor internal merekomendasikan mereka. Sementara beberapa jenis standar atau pedoman keamanan SI yang ada dalam sejumlah prosedur yang berbeda terletak di lembaga-lembaga kota yang berbeda, standar tidak dikomunikasikan dengan baik atau tidak dikomunikasikan sama sekali, dan dengan demikian biasanya terabaikan oleh semua kecuali lembaga yang mengembangkannya. Oleh karena itu, selama setiap audit pengembangan dua sistem aplikasi, internal auditor merekomendasikan bahwa manajemen senior SI membuat kebijakan keamanan informasi kota dengan standar pendukung.

Departemen pusat SI kota baru-baru ini menyewa kepala petugas keamanan informasi (CISO). Salah satu tantangan pertama CISO harus mengembangkan kebijakan dan standar keamanan SI seluruh kota. Tetapi CISO menghadapi banyak hambatan. Sebagai contoh, kepentingan politik sering mengalihkan sumber daya dari daerah dimana mereka paling dibutuhkan. Sistem sering dilaksanakan tanpa keamanan dalam pikiran, sering karena politisi lebih suka membuat layanan yang tersedia untuk umum daripada menunda layanan yang memadai sampai kontrol keamanan sistem dapat dijalankan. Juga, penyebaran keamanan meningkatkan biaya layanan. Kesulitan ketiga adalah laporan CISO kepada ketua SI dan akhirnya kepada walikota, sementara pemilik banyak sistem lainnya melaporkan kepada manajer senior yang berbeda dan dalam beberapa kasus untuk dewan kota. Dengan dua dasar struktur pelaporan, lembaga-lembaga kota sering beroperasi sebagai unit bisnis yang terpisah dan independen, dengan pelaporan dan struktur pendanaan terpisah. Hal ini membuat sulit untuk setuju pada standar keamanan SI kota atau bahkan mendanai upaya standar pengembangan pusat. Tantangan keempat adalah

CISO kekurangan staf dan perlu melobi pendanaan dalam kota dan dari negara serta pemerintah federal untuk dapat mengembangkan dan mengkomunikasikan kebijakan dan standar yang memadai.

CISO perlu menekankan bahwa meskipun terhambat, demi kepentingan kota terbaik dan warga negara untuk menyisihkan politik dan bekerja bersama sebagai sebuah tim dalam mengembangkan kebijakan dan standar keamanan SI yang dapat diimplementasikan oleh semua pekerja di kota, terutama administrator keamanan sistem. Masa depan keamanan dan reputasi kota beresiko jika standar keamanan SI tidak dikembangkan dan diterapkan. Sejauh ini kota telah beruntung tidak menderita kerugian besar dari pelanggaran keamanan.

Kebijakan, standar dan pedoman keamanan sistem informasi harus dirancang dalam hubungannya dengan satu sama lain untuk memastikan kontinuitas dan konsistensi dalam aplikasi mereka untuk semua sistem informasi di seluruh perusahaan. Mereka juga harus akan menjanjikan untuk membolehkan beberapa fleksibilitas dalam pengembangannya. Sebagai contoh, risiko yang rendah, sistem pengolahan non transaksi jelas tidak akan menjamin tingkat kontrol sistem transaksi keuangan yang berisiko tinggi seperti transfer. Untuk sistem rendah risiko, kepatuhan terhadap hal-hal tertentu dalam standar bisa dibebaskan dengan persetujuan tertulis dari manajemen senior.

Kebijakan, standar, dan pedoman sistem informasi harus didokumentasikan dan tersedia untuk semua karyawan organisasi baik bentuk tertulis ataupun elektronik. Mereka harus seringkas mungkin agar anggota staf tidak terintimidasi ketika mereka membacanya. Dokumen harus diperbarui setidaknya setahun sekali. Selain itu, semua staf harus dididik tentang isi dan lokasi dokumen-dokumen ini dan bagaimana mengaksesnya. Komunikasi tersebut harus dilakukan setidaknya setiap tahun.

Daftar Pustaka

1. "Policy Use Hits New Low." I*nfosecurity News* (January/February 1997): 14.

2. "Policies Made In a Vacuum, Survey Finds," *Infosecurity News* (January/February 1997): 14.

3. "Security Policies," *Information Security Magazine* (September 2000): 60.

4. "Do You Have an IT Security Policy?" Institute of Management and Administration *Newsletter* (October 2000): 9.