IT Risk Management

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan. Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

--- Selamat bekerja ----

Naurah Maryeifa
202420033 MTI 21B

UAS IT Risk Management

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan. Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

Jawaban :

1. Manajemen keamanan informasi bisa dilakukan dengan :
   - Mengidentifikasi threats (ancaman) yang dapat menyerang sumber daya informasi perusahaan,
   - Mendefinisikan resiko dari ancaman yang dapat memaksakan,
   - Penetapan kebijakan keamanan informasi,
   - Menerapkan controls yang tertuju pada resiko.

   Dan strategi yang bisa diterapkan yaitu :
   - Physical security adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman yang meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
   - Personal security adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup physical security.
   - Operasional security adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.

- Communication security adalah keamanan informasi yang bertujuan mengamankan media komunikasi, teknologi komunikasi serta apa yang masih ada didalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
- Network security adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringannya, data organisasi, jaringan dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

2. Dalam IT Risk Management pastinya ada ancaman terhadap sistem yang mungkin terjadi. Sumber ancaman meliputi bencana alam, kegagalan sistem, kerusakan hardware dan software, malware, virus komputer, dan human error.

   Contoh gangguan pada teknologi sistem informasi yaitu:

   a) Kesalahan teknis (*technical errors*),

      Kesalahan perangkat keras (*hardware problems*),

      Kesalahan di dalam penulisan sintak perangkat lunak (*syntax errors*),

      Kesalahan logika (*logical errors*).

   b) Gangguan lingkungan (*environmental hazards*) ,

      Kegagalan arus listrik karena petir.

   c) Kesalahan manusia (*human errors*).

3. Mengamankan asset IT yang saya kelola jika saya menjadi CIO (Chief Information Officer) dengan cara selalu mengidentifikasi area potensial yang rentan terhadap pelanggaran keamanan siber dan harus mempraktikkan metode pencegahan untuk memastikan bahwa intranet perusahaan tetap aman.

4. Salah satu contoh penerapan prinsip integritas dalam keamanan teknologi informasi yaitu salah satunya pada perangkat desktop malware disebarkan melalui perangkat lunak atau kode program. Saat menggunakan perangkat desktop dan ingin menginstal perangkat lunak Anda perlu berhati-hati dalam mengeksekusi kode programnya. Bisa jadi aplikasi yang Anda unduh merupakan aplikasi yang sudah disusupi malware di dalamnya. Ketika dieksekusi maka malware otomatis akan menyebar di dalam sistem. Tidak jarang di dalam kode program terdapat backdoor yang digunakan untuk memberikan hak akses kepada pembuat malware supaya dapat mengakses sistem dari jarak jauh.

5. *Risk Treatment* saling berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya dikarenakan sama-sama mengevaluasi pada penanggulangan resiko yang sudah dilakukan. Contohnya: Proses Manajemen Resiko ISO 31000:2009.

   - Proses pertama adalah ***Establishing The Context*** (Menetapkan Konteks).
   - Proses kedua adalah ***Risk Identification*** atau identifikasi risiko, yaitu melakukan identifikasi risiko-risiko yang dapat terjadi di masa yang akan datang (yaitu : risiko apa, kapan, di mana, bagaimana, mengapa suatu risiko bisa terjadi).
   - Proses ketiga adalah ***Risk Analysis*** atau analisis risiko-risiko, yaitu proses menentukan berapa besar dampak (***impact*** atau ***consequences***) dan kemungkinan (***frequency*** atau ***likelihood***) risiko-risiko yang akan terjadi, serta menghitung berapa besar level risikonya dengan mengalikan antara besar dampak dan besar kemungkinan (***Risk = Consequences x Likelihood***).
   - Proses keempat adalah ***Risk Evaluation*** atau membandingkan risiko-risiko yang sudah dihitung diatas dengan Kriteria Risiko yang sudah distandarkan (menempatkan posisi risiko-risiko pada gambar kriteria risiko), apakah risiko-risiko itu ***acceptable***/dapat diterima, menjadi ***issue***/diwaspadai, atau ***unacceptable***/tidak diterima, serta memprioritaskan mitigasi atau penangannya.
   - Proses kelima adalah ***Risk Treatment*** atau mitigasi risiko-risiko. Mitigasi risiko-risiko harus direncanakan sebaik-baiknya dan dipertimbangkan semua alternatif solusinya, sebelum dilaksanakan mitigasinya, agar mendapatkan hasil yang diharapkan secara efektif dan efisien.

Nama : Nurul Amalina Setyorini
NIM : 202420005
Jurusan : MTI Regular B

UAS IT Risk Management

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh.

   Strategi yang dapat diterapkan untuk manajemen resiko keamanan aset teknologi informasi dan komunikasi (TIK) demi kelancaran operasional suatu organisasi adalah sebagai berikut :

   - Mengidentifikasi Resiko (Risk Identification)
     Strategi awal untuk mengetahui resiko-resiko apa yang akan kita dapatkan yang kemudian dapat menimbulkan kerugian. Caranya adalah dengan mengumpulkan data-data atau mencari informasi lain yang dapat diperoleh sehubungan dengan resiko yang akan kita hadapi tersebut. Contohnya dalam pengembangan sebuah sistem absensi online menggunakan aplikasi, harus dianalisis resiko yang akan dihadapi misalnya terdapat pegawai gaptek (gagap teknologi).
   - Melakukan Penilaian Resiko (Risk Assessment)
     Risk Assessment adalah metode yang sistematis untuk menentukan apakah suatu kegiatan/aset mempunyai resiko yang dapat diterima atau tidak. Risk Assessment sangat penting karena membantu menciptakan kesadaran tentang bahaya dan resiko yang didapatkan dari aset yang dimiliki. Hal ini bertujuan untuk mengurangi kemungkinan bahaya dengan menambahkan langkah-langkah pengendalian yang diperlukan dan tindakan pencegahan. Penilaian juga memprioritaskan bahaya dan membantu menentukan apakah tindakan pengendalian yang ada memadai. Contohnya dalam pengembangan sistem absensi online, seluruh pegawai diberikan sosialisasi tentang penggunaan aplikasi tersebut, sehingga jika terdapat pegawai yang tidak menerima adanya sistem akan diberikan penjelasan mengapa sistem harus dijalankan.
   - Melakukan Penanganan Resiko (Risk Treatment)
     Risk treatment (penanganan resiko) bertujuan untuk menentukan tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara keseluruhan.

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya.

   Sumber ancaman yang mungkin terjadi terhadap sistem :

   1. Human error : terjadinya kelalaian.
      Contoh : kesalahan penginputan dan penghapusan data, serta kesalahan pengoperasian sistem.
   2. Bencana alam : merupakan faktor yang tak terduga yang bisa mengancam sistem informasi.
      Contoh : gangguan listrik, kegagalan peralatan dan fungsi perangkat lunak dapat menyebabkan data tidak konsisten , transaksi tidak lengkap atau bahkan data rusak. Selain itu variasi tegangan listrik yang terlalu tajam dapat membuat peralatan-peralatan terbakar.
   3. Hacker : orang-orang yang dapat dikategorikan sebagai programmer yang pandai dan senang mengutak-utik sesuatu yang dirasakan sebagai penghalang terhadap apa yang ingin dicapainya. Hacker akan mencari cara bagaimana bisa menembus password, firewall, access-key dan sebagainya.
      Contoh teknik yang digunakan untuk melakukan hacking :
      - Back Door : suatu serangan (biasanya bersumber dari suatu software yang baru di install) yang dengan sengaja membuka suatu “pintu belakang” bagi pengunjung tertentu, tanpa disadari oleh orang yang mgeinstall software, sehingga mereka dengan mudah masuk kedalam sistem jaringan.
      - Sniffer : Teknik ini diimplementasikan dengan membuat program yang dapat melacak paket data seseorang Ketika paket tersebut melintas internet, menangkap passeord atau isinya.
      - Spoofing : suatu usaha dari orang yang tidak berhak misalnya dengan memalsukan identitas, untuk masuk ke suatu sistem jaringan, seakan-akan dia adalah user yang berhak.
      - DNS Poisoning : hacker merubah atau merusak isi DNS sehingga semua akses yang memakai DNS ini akan disalurkan ke alamat yang salah atau alamat yang dituju tidak bisa diakses.
   4. Virus : program computer yang masuk kedalam sistem untuk melakukan sesuatu, misalnya meng-interupsi proses yang sedang berjalan di CPU, memperlambat kinerja computer, memenuhi memory computer sehingga kegiatan CPU berhenti, memenuhi hard disk, menghapus file-file, merusak sistem operasi dan sebagainya.

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

   Jika saya seorang CIO, ada tiga cara mengamankan asset IT yaitu :

   1. Mengamankan jaringan : selalu beri password dalam seluruh jaringan data computer serta hidden seluruh sistem adalah cara untuk mencegah cyber crime serta mempersulit hacker memperoleh akses menuju jaringan.
   2. Memperhatikan phishing : selalu berhati-hati dalam memberikan informasi. Jangan pernah membuka halaman dari link yang dikirimkan melalui surat, email, sms atau media lain yang sumbernya tidak jelas. Selalu menjaga kerahasiaan user id, password, serta data pribadi lain. Jangan pernah memberikan atau memasukkan data tersebut ke program aplikasi yang tidak terpercaya.
      Phising adalah suatu metode yang di gunakan hacker untuk mencuri password dengan cara mengelabui target menggunakan fake form login pada situs palsu yang menyerupai situs aslinya.
   3. Membackup data : melakukan backup berkala untuk jaga-jaga seandainya suatu waktu terjadi kehilangan data. Sehingga data masih tersimpan aman.

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi.

   Integritas merupakan bagian penting dari amannya suatu sistem berbasis teknologi karena integritas adalah prinsip yang bertujuan untuk melindungi keutuhan data dan informasi organisasi dari modifikasi yang tidak sah, penekanannya adalah sebuah informasi tidak boleh diubah kecuali oleh pemilik informasi.
   Contohnya disubbagian perencanaan dan keuangan sebuah kantor (kantor regional VII BKN Palembang) setiap bulan harus menginput laporan emonev (monitoring dan evaluasi) smartdja dari kemenkeu dan emonev bappenas, laporan emonev ini harus diinput sesuai dengan nilai realisasi atas pagu yang dianggarkan negara. Dalam penginputan emonev ini ada admin khusus yang bisa mengakses dan memberi data sebenarnya atas realisasi anggaran tersebut. Integritasnya admin mempunyai tanggungjawab secara penuh atas pelaporan data dan informasi yang diberikan, serta menjaga kerahasiaan, kebenaran dan keaslian data tersebut.

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

   Risk treatment (penanganan resiko) adalah suatu proses untuk mengembangkan dan memilih alternatif-alternatif untuk menangani resiko serta pelaksanaannya, bisa dikatakan juga bahwa risk treatment merupakan tindakan spesifik yang dilakukan dengan tujuan untuk menurunkan tingkat risiko dalam rangka menghindari atau mengurangi kerugian perusahaan. Sedangkan risk evaluation (evaluasi resiko) adalah suatu proses untuk membantu dalam membuat keputusan, sehingga adanya hasil evaluasi resiko untuk menentukan resiko mana yang memerlukan perbaikan dan prioritas untuk dilakukan lebih awal.
   Risk treatment (penanganan resiko) sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya bisa dilihat dari contoh berikut :
   Dalam tes seleksi ASN menggunakan sistem CAT (Computer Assisted Test) dengan server windows yang diinstall dari kantor regional kemudian dibawa ke masing-masing titik lokasi tes, telah di analisis bahwa resiko yang dihadapi seperti laptop server mengalami kerusakan saat dalam perjalanan dengan penyebab kelalaian, bencana alam bahkan tindakan kriminal. Sehingga untuk meminimalisir resiko tersebut, tim seleksi ASN membuat sebuah penanganan resiko (risk treatment) dengan mengembangkan alternatif server online yang terpusat pada kantor pusat BKN untuk mengelola seluruh data pada sistem CAT sehingga tim seleksi yang bertugas di titik lokasi daerah tidak perlu membawa server windows pada saat perjalanan menuju titik lokasi.

NAMA : OKTARIANSYAH
KELAS : MTI2B
NIM : 202420006

UAS IT RISK MANAGEMENT

- **Pengendalian Akses Fisik**

  Perusahaan telah memiliki pengendalian yang baik terhadap akses fisik, seperti adanya prosedur dan rencana fasilitas keamanan dalam menjaga lokasi, bangunan, namun belum didokumentasikan dan diuji. Perusahaan telah memiliki prosedur terutama dalam mengelola pengunjung dan pengendalian akses fisik ke tempat kerja, perangkat keras, dan perangkat lunak. Area kerja yang banyak menggunakan komputer dan komponen lainnya yang memungkinkan akses ke informasi yang sensitif dan secara fisik menjamin untuk mencegah akses yang tidak sah.

- **Pemantauan dan Audit Keamanan Fisik**

  Saat ini perusahaan telah memiliki catatan pemeliharaan yang disimpan kedalam dokumen perbaikan dan modifikasi dari komponen fasilitas fisik. Tindakan individu atau kelompok yang berkaitan dengan semua media yang dikontrol secara fisik, dapat dipertanggungjawabkan. Pemeriksaan dan pemantauan dilakukan secara rutin, memeriksa catatan dan melihat kejanggalankejanggalan yang ada, dan mengambil tindakan korektif (perbaikan) jika diperlukan.

- **Manajemen jaringan dan sistem**

  Perusahaan telah mengelola sistem dan jaringan dengan baik, hal tersebut dapat dilihat dari adanya penggunaan sistem wireless di dalam jaringan LAN. Perusahaan telah melindungi informasi sensitif di tempat yang aman. Dan pihak yang tidak mempunyai wewenang yang berkaitan dengan informasi tersebut tidak dapat mengaksesnya.

- **Pemantauan dan Audit Keamanan TI**

  Perusahaan telah melakukan pemantauan dan mengaudit sistem dan jaringan perusahaan secara baik. Perusahaan mengaktifkan firewall yang berfungsi sebagai sistem keamanan yang melindungi sistem komputer yang berjalan.

- **Pengesahan dan Otorisasi**

  Perusahaan telah melakukan pengontrolan yang baik sesuai dengan akses yang tepat dan pengesahan yang konsisten di dalam hal perizinan file dan konfigurasi jaringan. Perusahaan juga telah melakukan pembatasan akses terhadap informasi ataupun sistem sensitif.

  Perusahaan memiliki dokumentasi kebijakan dan prosedur yang mengatur hak akses secara individu maupun kelompok. Hal ini akan mengatur jaminan keamanan terhadap informasi yang bersifat sensitif. Informasi tidak dapat diakses ataupun diubah ke dalam bentuk apapun oleh pihak yang tidak memiliki wewenang.

- **Manajemen Kerentanan**

  Perusahaan belum memiliki manajemen kerentanan dengan baik karena perusahan tidak meninjau atau menilai sumber informasi mengenai kerentanan informasi, peringatan dan keamanan informasi dan pemberitahuan. Hal lainnya adalah perusahaan tidak mengidentifikasi komponen infrastruktur untuk dievaluasi serta tidak memberikan penafsiran dan menanggapi hasilnya.

- **Enkripsi**

  Perusahaan telah melakukan pengendalian keamanan yang sesuai dengan kebutuhan perusahaan untuk melindungi informasi yang sensitif, selama dalam penyimpanan dan transmisi data. Protokol enkripsi juga digunakan ketika mengelola sistem, router, dan firewall.

- **Desain dan Arsitektur Keamanan**

  Perusahaan sudah mempunyai sistem desain dan arsitektur keamanan yang baik terhadap sistem yang akan digunakan di perusahaan dan sistem tersebut akan direvisi dengan mempertimbangan hal-hal seperti: strategi keamanan, kebijakan dan prosedur. Namun, perusahaan belum mempunyai aplikasi yang up-to-date untuk menunjukkan arsitektur keamanan dari perusahaan dan topologi jaringan.

- **Manajemen Insiden**

  Dalam mengelola insiden di dalam perusahaan, perusahaan memiliki prosedur yang didokumentasikan untuk mengidentifikasi, melaporkan dan menanggapi dugaan pelanggaran keamanan dan insiden. Namun dalam penanganannya, perusahaan belum melakukan verifikasi dan diperbaharui secara periodik.

- **Profil Ancaman**

  Adapun aset-aset kritis yang terdapat di perusahaan, yaitu: (a) Aplikasi Group health insurance, (b) Database Server, (c) Jaringan, dan (d) PC.

- **Kebutuhan Keamanan pada Aset Kritis**

  Kebutuhan keamanan terhadap seluruh aset-aset penting yang ada di perusahaan terdiri dari tiga hal, yaitu: kerahasiaan informasi, integritas data, dan adanya ketersediaaan data dan informasi saat dibutuhkan. Kebutuhan keamanan yang paling penting dalam perusahaan terletak pada ketersediaan data atau informasi, karena jika data atau informasi yang dibutuhkan tidak tersedia maka aktivitas proses bisnis perusahaan tidak dapat berjalan dengan lancar.

- **Ancaman pada Aset Kritis Ancaman pada aset kritis**

  perusahaan dapat terjadi melalui dua akses, yaitu: akses fisik maupun akses jaringan, dan setiap akses mempunyai dua aktor, yaitu: aktor yang berasal dari dalam perusahaan dan aktor yang berasal dari luar perusahaan. Motif pelaku dalam melakukan ancaman dibagi menjadi dua, yaitu: ancaman yang dilakukan dengan sengaja dan ancaman yang dilakukan dengan tidak sengaja. Dari motif pelaku tersebut, mengakibatkan kemungkinan terjadinya penyingkapan, modifikasi, penghancuran dan gangguan.

- **Infrastruktur yang berhubungan dengan Aset Kritis**

  Sistem dan komponen yang berkaitan dengan aset kritikal perusahaan (group health insurance) yaitu: PC, jaringan, dan database server. PC, sangat berkaitan dalam penggunaan group health insurance untuk menginput data klien serta memilih bentuk proteksi yang akan digunakan. Database server (MS SQL Server) juga digunakan oleh perusahaan untuk menunjang penggunaan aplikasi group health insurance.

- **Kriteria Kemungkinan**

  Frekuensi terjadinya ancaman pada perusahaan masih tergolong rendah karena ancaman yang terjadi masih di bawah tiga kali dalam setahun. Saat ini, ancaman-ancaman yang terjadi pada perusahaan masih dapat diatasi oleh pihak dalam perusahaan. Pengukuran ini berlaku untuk semua ancaman pada aset penting, baik yang disengaja maupun yang tidak sengaja.

- **Peluang dari Ancaman**

  Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak dalam perusahaan melalui akses jaringan, yaitu: Besarnya motif pihak dalam perusahaan yang secara tidak sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang.

  Besarnya motif pihak dalam perusahaan yang secara tidak sengaja melakukan penghancuran tergolong rendah dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara tidak sengaja menyebabkan gangguan tergolong rendah dengan tingkat keyakinan sedang.

  Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak dalam perusahaan melalui akses jaringan, yaitu: Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang.

  Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan penghancuran tergolong rendah dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

  Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan, yaitu: Besarnya motif pihak luar perusahaan yang secara tidak sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak luar perusahaan yang secara tidak sengaja melakukan penghancuran tergolong sedang dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara tidak sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak luar perusahaan melalui akses jaringan, yaitu: Besarnya motif pihak luar perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang.

Besarnya motif pihak luar perusahaan yang secara sengaja melakukan penghancuran tergolong sedang dengan tingkat keyakinan sedang dan besarnya motif pihak luar perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang. Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak dalam perusahaan melalui akses fisik, yaitu: Besarnya motif pihak dalam perusahaan yang secara tidak sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang.

Besarnya motif pihak dalam perusahaan yang secara tidak sengaja melakukan penghancuran tergolong rendah dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara tidak sengaja menyebabkan gangguan tergolong rendah dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak dalam perusahaan melalui akses fisik, yaitu: Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan penghancuran tergolong rendah dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara tidak sengaja disebabkan oleh pihak luar perusahaan melalui akses fisik, yaitu: Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak dalam perusahaan yang secara sengaja melakukan penghancuran tergolong sedang dengan tingkat keyakinan sedang dan besarnya motif pihak dalam perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

Peluang terjadinya ancaman yang secara sengaja disebabkan oleh pihak luar perusahaan melalui akses fisik, yaitu: Besarnya motif pihak luar perusahaan yang secara sengaja melakukan modifikasi tergolong sedang dengan tingkat keyakinan sedang. Besarnya motif pihak luar perusahaan yang secara sengaja melakukan penghancuran tergolong sedang dengan tingkat keyakinan sedang. dan besarnya motif pihak luar perusahaan yang secara sengaja menyebabkan gangguan tergolong sedang dengan tingkat keyakinan sedang.

- **Strategi Perlindungan**

  Dari penelitian yang dilakukan pada Perusahaan dengan menggunakan pendekatan OCTAVES, ditemukan beberapa risiko dari penerapan teknologi informasi yang berkaitan dengan praktik keamanan yang ada pada perusahaan. Risiko-risiko yang ditemukan berfokus pada manajemen keamanan, rencana kemungkinan, manajemen kerentanan, serta desain dan arsitektur keamanan. Strategi perlindungan yang akan direncanakan dalam perusahaan, yaitu: manajemen keamanan, rencana kemungkinan, manajemen kerentanan, dan desain dan arsitektur keamanan.

- **Manajemen Keamanan**

  Saat ini perusahaan belum melakukan penilaian risiko terhadap keamanan informasi. Jika terjadi risiko maka divisi IT yang akan langsung mengambil langkah-langkah dalam meminimalisir risiko keamanan informasi tersebut. Selain itu perusahaan juga tidak memiliki kebijakan dan prosedur mengenai penghentian kerja terhadap pihak karyawan yang terlibat dalam permasalahan keamanan informasi.

- **Rencana Kemungkinan**

  Saat ini perusahaan belum melakukan operasi analisis terhadap operasi, aset-aset dan data penting yang dianggap dapat memberikan kontinuitas bisnis pada saat bencana telah terjadi. Perusahaan ini pun belum memiliki rencana pemulihan bencana dan mempertimbangkan rencana fisik untuk keberlangsungan bisnis.

- **Manajemen Kerentanan**

  Perusahaan belum meninjau atau menilai sumber informasi mengenai kerentanan informasi, peringatan akan keamanan informasi dan pemberitahuan. Selain itu perusahaan juga tidak melakukan identifikasi terhadap komponen infrastruktur untuk di evaluasi secara periodik. Dan prosedur manajemen kerentanan belum dimonitori dan ditinjau serta di-update secara berkala.

- **Desain dan Arsitektur Keamanan**

  Perusahaan belum memiliki hasil penilaian risiko keamanan yang dijadikan pertimbangan sebagai pertimbangan dalam membentuk sistem arsitektur dan desain baru maupun sistem yang direvisi. Perusahaan juga belum memilik aplikasi yang up-to-date yang menunjukkan arsitektur keamanan dari perusahaan dan topologi jaringan.

- **Pendekatan Mitigasi**

  Berdasarkan kertas kerja profil risiko yang terdapat pada langkah OCTAVE-S, ada pendekatan mitigasi yang dilakukan oleh perusahaan atas ancaman yang terjadi di perusahaan, baik ancaman yang bermotif sengaja maupun yang tidak disengaja pada pihak internal perusahaan dan pihak eksternal perusahaan melalui akses jaringan dan akses fisik.

  Perusahaan akan mengambil tindakan mitigasi risiko pada praktik keamanan melalui akses jaringan yang dilakukan oleh pihak dalam perusahaan. Kegiatan mitigasi berfokus pada satu aktivitas praktik keamanan, yaitu: (1) manajemen keamanan dan (2) arsitektur dan desain keamanan. Sedangkan untuk pihak luar, perusahaan belum melakukan mitigasi. dan tindakan mitigasi risiko pada akses fisik yang diakibatkan oleh pihak dalam dan pihak luar perusahaan berfokus pada (3) rencana kemungkinan dan (4) manajemen kerentanan rencana mitigasi risiko.

- **Rencana Mitigasi Risiko**

  Rencana mitigasi risiko yang berkaitan dengan manajemen keamanan untuk praktik keamanan, meliputi: (1) dibentuknya suatu tim manajemen risiko untuk melakukan penilaian risiko, sehingga dapat meminimalisir risiko sejak awal; (2)

mendokumentasikan mengenai tugas dan tanggung jawab keamanan informasi untuk semua karyawan dalam perusahaan; (3) melaksanakan program pelatihan kesadaran keamanan perusahaan yang mencakup informasi tentang proses manajemen keamanan perusahaan. Pelatihan ini disediakan untuk semua karyawan (tidak hanya karyawan baru) dalam kurun waktu tertentu.

Rencana mitigasi risiko yang berkaitan dengan rencana kemungkinan, meliputi: (1) melakukan analisis terhadap operasional, aplikasi-aplikasi, dan data penting yang dianggap dapat memberikan kontinuitas bisnis untuk penanggulangan bencana; (2) mendokumentasikan pengujian dan peninjauan terhadap kontinuitas bisnis, rencana pemulihan bencana, dan kemungkinan rencana untuk menanggulangi keadaan darurat.

Rencana mitigasi risiko yang berkaitan dengan manajemen kerentanan, meliputi: (1) mendokumentasikan prosedur yang digunakan untuk mengelola kerentanan, seperti: memilih alat evaluasi kerentanan, menjaga serangan dan pengetahuan tentang kerentanan secara up-to-date, serta menilai sumber informasi yang berkaitan dengan kerentanan informasi; (2) mengidentifikasikan komponen infrastruktur untuk dievaluasi; (3) mengelola tempat penyimpanan yang paling aman dan menjaga kerentanan data; (3) penilaian kerentanan teknologi dilakukan secara periodik.

Rencana mitigasi risiko yang berkaitan dengan desain dan arsitektur keamanan, meliputi: memiliki hasil penilaian risiko keamanan yang akan menjadi pertimbangan terhadap pembangunan sistem arsitektur dan desain baru, maupun sistem yang direvisi.

Perubahan Strategi Perlindungan Perubahan strategi perlindungan yang berkaitan dengan manajemen keamanan untuk praktik keamanan, meliputi: (1) melakukan penilaian risiko dilakukan secara rutin; (2) mengadakan pelatihan mengenai kesadaran keamanan perusahaan yang mencakup informasi tentang proses manajemen keamanan perusahaan. Pelatihan ini disediakan untuk semua karyawan (tidak hanya karyawan baru) dalam kurun waktu tertentu; (3) mendokumentasikan tugas dan tanggung jawab keamanan informasi untuk semua karyawan dalam perusahaan.

Perubahan strategi perlindungan yang berkaitan dengan rencana contigency, meliputi: (1) melakukan analisis terhadap operasional, aplikasi-aplikasi dan data penting yang dianggap dapat Manajemen Risiko Teknologi, memberikan kontinuitas bisnis untuk penanggulangan bencana; (2) memiliki rencana pemulihan bencana yang ditinjau, diuji dan didokumentasikan.

Perubahan strategi perlindungan yang berkaitan dengan manajemen kerentanan, meliputi: (1) mengidentifikasikan komponen infrastruktur untuk dievaluasi; (2) melakukan penilaian kerentanan teknologi yang dilakukan secara periodik; (3) memiliki prosedur manajemen kerentanan data yang didokumentasikan.

Perubahan strategi perlindungan yang berkaitan dengan desain dan arsitektur kemananan, meliputi: memiliki hasil penilaian risiko keamanan yang akan menjadi pertimbangan terhadap pembangunan sistem arsitektur dan desain baru, maupun sistem yang direvisi.

- **Identifikasi Langkah Selanjutnya**

  Dalam mendukung pelaksanaan hasil pengukuran risiko teknologi informasi OCTAVE-S, ada beberapa hal yang menjadi pertimbangan perusahaan, di mana manajemen perusahaan harus membuat suatu strategi bisnis sebagai prioritas bagi keamanan perusahaan dan melakukan evaluasi secara berkala agar dapat disusun rencana stategi untuk penangulangan risiko. Serta perusahaan dapat mempertimbangan apakah metode OCTAVE-S merupakan metode terbaik dalam melakukan pengukuran risiko guna menjaga aset-aset perusahaan.

- **KESIMPULAN**

  Dari hasil analisis yang dilakukan, diperoleh beberapa simpulan, yaitu: (1) perusahaan belum menerapkan manajemen risiko TI secara menyeluruh. Hal ini dapat dilihat dengan tidak adanya rencana contigency dan disaster recovery plan; (2) tidak memiliki alokasi dana untuk melakukan pelatihan kesadaran dan keamanan secara berkala; (3) perusahaan telah mengelola sistem keamanan dan jaringan dengan baik, dapat dilihat dari adanya akses terbatas terhadap informasi yang bersifat sensitive.

NAMA : RACHMAD IQBAL

NIM : 202420002

IT Risk Management

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

Jawaban :

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin

muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

- Mengidentifikasi risiko
- Menilai risiko
- Mengurangi risiko
- Mengembangkan rencana respon
- Mengkaji prosedur manajemen risiko.

Assessment, merujuk pada pencarian risiko dan penilaian tingkat keparahan risiko.

Mitigation, yaitu penanggulanan yang dilakukan untuk mengurangi dampat risiko.

Evaluation and Assessment, merujuk pada evaluasi terhadap penanggulangan yang sudah dilakukan.

2. Ancaman terhadap system terbagi menjadi dua yaitu ancaman aktif dan passif.
    1. Ancaman aktif
    2. Ancaman pasif

➢ Ancaman aktif

Merupakan ancaman yang sengaja dilakukan oleh manusia

Contoh :

- Pencurian data

Jika informasi penting yang terdapat dalam database dapat diakses oleh orang yang tidak berwenang maka hasilnya dapat kehilangan informasi atau harta. Misalnya mata-mata industry yang memperoleh informasi persaingan berharga, penjahat computer yang dapat mencuri uang di bank.

- Penggunaan system secara illegal

Orang yang tidak berhak mengakses informasi pada suatu system yang bukan menjadi haknya dapat mengakses system tersebut. Contohnya hacker yang menembus system keamanan dengan tujuan mendapatkan data atau informasi

penting yang diperlukan, memperoleh akses ke system telepon, dan membuat sambungan telepon jarak jauh.

- Penghacuran data secara illegal

Orang yang dapat merusak atau menghancurkan data atau informasi dan membuat berhentinya suatu system computer. Penjahat dengan cara ini tidak perlu berada ditempat kejadian. Ia dapat masuk ke jaringan computer suatu terminal dan menyebabkan kerusakan pada semua system dan hilangnya data atau informasi penting. Penjahat seperti ini biasa disebut cracker yaitu penjebol system computer yang bertujuan melakukan pencurian data atau merusak system.

- Modifikasi secara illegal

Perubahan data informasi dan perangkat lunak secara tidak disadari. Perubahan tersebut disebabkan oleh program aplikasi yang merusak (*malicious software*).

- Ancaman Pasif

Merupakan suatu ancaman yang diakibatkan ketidaksengajaan

Contoh

- Kegagalan Sistem

Kegagalan system yang menyebabkan data tidak konsisten, transaksi tidak berjalan lancar sehingga data menjadi tidak lengkap atau bahkan menjadi rusak atau hal lain seperti tegangan listrik yang tidak stabil.

- Kesalahan Manusia

Kesalahan dalam hal penginputan data atau informasi yang dpat mengancam integritas system dan data.

- Bencana Alam

Seperti gempa bumi, banjir, kebakaran, hujan, badai yang merupakan factor yang tidak terduga.

3. Karena itulah diperlukan penjagaan ekstra ketat dari pihak jaringan teknologi Apabila perusahaan Anda memakai sistem jaringan nirkabel, maka pastikan Anda memiliki teknisi yang mampu mengamankan jaringan Apalagi *hacker* yang berpengalaman pasti bisa memperoleh berbagai akses menuju jaringan dalam jangka waktu yang cepat Semakin canggih *hacker,* maka data perusahaan Anda akan langsung terbuka bahkan tanpa Anda

sadari pastikan perusahaan selalu mengunci *router* dan juga mengenkripsi seluruh informasi dari mata-mata. Bila perlu, selalu beri pasword dalam seluruh jaringan data komputer dan bila perlu cobalah untuk hidden seluruh system dengan menyembunyikan data, maka setidaknya Anda telah mencegah kejahatan dalam perusahaan Anda. Bila perlu, jangan ada orang lain yang mengakses komputer orang lain dengan sembarangan meskipun dalam satu perusahaan.

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

    - Keamanan informasi merupakan bagian integral dari praktik manajemen yang baik
    - Seorang manajer harus mampu menilai tingkat resiko keamanan yang cukup pantas untuk diterima sesuai dengan kontrol yang diberlakukan.
    - Keamanan informasi harus efektif dalam hal biaya
    - Tanggung jawab dan kewenangan keamanan informasi harus dijelaskan secara eksplisit
    - Pemilik sistem memiliki tanggung jawab keamanan diluar organisasinya.
    - Keamanan informasi memerlukan pendekatan yang komprehensif dan terintegrasi
    - Keamanan informasi harus dievaluasi ulang secara periodik
    - Keamanan informasi dibatasi oleh faktor social

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

    Hasil evaluasi risiko yang digunakan untuk membuat keputusan harus konsisten dengan konteks manajemen risiko keamanan informasi eksternal dan internal yang ditetapkan dan mempertimbangkan tujuan organisasi dan pandangan pemangku kepentingan, dll.

    Pertimbangan harus mencakup:

    Properti keamanan informasi: jika satu kriteria tidak relevan untuk organisasi (kehilangan kerahasiaan), Pentingnya proses bisnis atau aktivitas yang didukung oleh aset atau kumpulan aset tertentu.

Ini berarti hasil evaluasi resiko sebelumnya akan mengurangi impact dari dari risk treatment yang di lakukan selanjutnya

Nama : Ribhan Mandala
NIM. : 202420035

UAS IT Risk Management

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

Jawab

1. Untuk mengurangi Risiko keamanan akan aset Teknology Informasi dan Komunikasi (TIK) maka trdapat strategi yang dilakukan diantara lain.
   - Faktor Human Resource
     Terjadi dikarenakan kelalaian pengguna misal rusaknya perangkat atau pencurian perangkat.
   - Perangkat IT
     Seperti rentannya pengguna terkena virus komputer.

2. Dalam IT Risk Management pastinya ada ancaman terhadap sistem yang mungkin terjadi.

Nama : Ribhan Mandala
NIM. : 202420035

Sumber ancaman meliputi bencana alam, kegagalan sistem, kerusakan hardware dan software, malware, virus komputer, dan human error.
Contoh gangguan pada teknologi sistem informasi yaitu:

a) Kesalahan teknis (technical errors)

   Kesalahan perangkat keras (hardware problems)

   Kesalahan di dalam penulisan sintak perangkat lunak (syntax errors)

   Kesalahan logika (logical errors)

b) Gangguan lingkungan (environmental hazards)

   Kegagalan arus listrik karena petir

c) Kesalahan manusia (human errors)

3. Mengamankan asset IT yang saya kelola jika saya menjadi CIO (Chief InformationOfficer) dengan cara selalu mengidentifikasi area potensial yang rentan terhadap pelanggaran keamanan cyber dan harus mempraktikkan metode pencegahan untuk memastikan bahwa intranet perusahaan tetap aman.

4. Faktor yang mempengaruhi intergritas yaitu jujur, disiplin dan konsisten. Jika disamakan dengan pengaman sistem informasi, pengelola IT harus disiplin mulai dari pengecekan berkala sistem dari server router dan perangkat IT lainnya.

5. Treat Risk yaitu cara kita untuk memperlakukan sistem dan gejala yang brhubungan dengan risiko IT, hubungan dengan evaluasi IT yaitu sama-sama mengevaluasi kejadian yang berkaitan dengan kekurangan dalam sistem IT.

Nama : **Yusria Lenitasari**

NIM : **202420003**

Jurusan : **Magister Teknologi Informatika**

UAS ***: IT Risk Management and Disaster Recovery***

IT Risk Management

Pertanyaan :

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

Jawaban :

1. Strategy yang dapat diterapkan untuk mengamankan asset Teknology Informasi dan komunikasi (TIK) :
    a. Melakukan audit TI, karena audit TI merupakan proses pengujian infrastruktur teknologi informasi yang dimiliki oleh organisasi/perusahaan dan melalui audit TI, organisasi/perusahaan dapat mengetahui peran aset teknologi informasi yang dimilikinya dalam mencapai tujuan organisasi/perusahaan, serta mengetahui solusi yang tepat atau perbaikan apa saja yang harus dilakukan agar aset yang dimiliki oleh teknologi informasi tersebut dapat sesuai dengan yang diharapkan.

       Contohnya : Dalam suatu organisasi dilakukan audit TI per periode untuk mengamankan asset TIK untuk memastikan kebijakan yang dibuat sesuai dengan kondisi di lapangan.
    b. Harus tersedianya kebijakan yang menjadi panduan dalam melakukan pengelolaan aset. Kebijakan yang dibuat harus selaras dengan visi dan misi, tujuan, sasaran yang dijabarkan secara jelas dan terdokumentasi mengenai sasaran pengembangan TIK di lingkungan organisasi. Produk hukum terkait TIK dalam bentuk surat keputusan, peraturan, regulasi, kebijakan dan pedoman terkait pemanfaatan dan pengelolaan aset TIK harus tersedia dan dapat diakses oleh stakeholder.

       Contoh : Dalam suatu organisasi, dibuat suatu kebijakan untuk menginventaris asset TIK maka petugas yang berwenang harus menginventarisasi asset TIK dan diawasi oleh atasan petugas yang bertugas.
    c. Melabeling dan monitoring asset Teknologi Informasi dan Komunikasi yang dilakukan petugas.
    d. Adanya komitmen pimpinan dan staf untuk mendukung pengelolaan aset di lingkungan TIK.
    e. Membuat kebijakan yang terdokumentasi untuk menjadi panduan petugas
    f. Mengembangkan kemampuan petugas dalam hal mengamankan asset IT

2. Sumber ancaman IT yang terjadi saat ini pada suatu organisasi atau lembaga yang ungkin terjadi misalnya pada industry perbankan adalah :

1. Kelalaian pegawai yang tidak melakukan pekerjaan sesuai dengan fungsinya mengetahui, memahami, dampak dan arti sebuah ancaman IT yang akan terjadi pada perusahaannya misalnya tidak melakukan monitoring terhadap suhu ruangan yang mengakibatkan suhu udara ruangan server menjadi panas sehingga perangkat IT yang terdapat didalamnya tidak dapat berfungsi, kesalahan pengoperasian sistem oleh manusia juga dapat merusak integritas sistem dan data
2. Kegagalan sumber daya yang dikendalikan perbankan misalnya kabel listrik yang dipergunaka tidak sesuai standar atau kapasitas serta berkualitas buruk yang dapat mengakibatkan kegagalan proses system. Antivirus yang tidak berstandar atau tidak update pada perangkat hardware atau computer.
3. Bencana alam yang tidak dapat diprediksi misalnya banjir bandang sehingga membuat ruangan server terendam yang mengakibatkan tidak beroperasionalnya perusahaan perbankan tersebut.
4. Serangan cyber merupakan sumber ancaman aktif yang dilakukan oleh manusia misalnya melakukan peretasan system perbankan yang dapat merugikan perusahaan. Peretasan system bisa dilakukan hacker atau cracker dengan cara menembus pertahanan dan keamanan system computer dengan mencari keuntungan pribadi
5. Mengeksploitasi kerentanan (*vulnarebility*) misalnya Pencurian data yang dilakukan oleh "orang dalam" untuk dijual,
6. Situasi dan metode yang mungkin tidak disengaja misalnya Penginputan data yang salah dapat mengacaukan sistem
7. Maksud dan metode yang ditargetkan pada eksploitasi kerentanan (*vulnarebility*) misalnya Penyadapan oleh orang dalam, Pengubahan data secara langsung umum dilakukan oleh orang yang punya akses secara langsung terhadap basis data.

3. CIO (*Chief Information officer*) adalah jabatan eksekutif yang bertanggung jawab atas perencanaan, penyelarasan, penyiapan, implementasi, dan evaluasi teknologi informasi dan komunikasi (TIK) di dalam suatu organisasi. Cara CIO mengamankan asset IT adalah membuat kebijakan keamanan informasi. yang memberikan pedoman mengenai prosedur, aturan dan hal-hal lain yang berhubungan dengan pengelolaan informasi. prinsip dasar yang dapat digunakan sebagai panduan bagi pengambilan keputusan untuk membuat kebijakan, prosedur dan aturan lain yang berhubungan dengan keamanan informasi dengan contoh sebagai berikut :

1. Melakukan sosialisasi dan pelatihan secara berkala kepada petugas terkait
2. Membuat pedoman mengenai prosedur, aturan dan hal-hal lain yang berhubungan dengan pengelolaan informasi.
3. Mencatat semua insiden yang terjadi pada system. Pencatatan lengkap dengan menceritakan tanggal kejadian, jam dan kronologi kejadian dan hal yang telah dilakukan untuk penanganan kejadian insiden tersebut
4. Melakukan pencatatan atau register keluar masuk ruangan server dengan akses elektronik, sehingga bila mereka melakukan akses ke pintu ang server akan selalu tercatat dengan baik. Masuk dan luar kapan saja tercatat dalam log. access code ke pintu-pintu mangan server dan catatan log elektronik sangat sulit untuk dikelabui karena menggunakan peralatan berbasis authentication yang kuat seperti smart card, pemindai iometric (seperti sidik jari), retina dan iris, pengenal wajah, pengenal suara bahkan sampai dengan pengenal bentuk dan ukuran tubuh. Meletakan Kamera dan beberapa sensor yang diletakkan di ruang dan sudut-sudut server akan mempersulit gerakan orang asing tersebut untuk melakukan akses yang tidak diinginkan. Kamera dan hard disk akan merekam segala perbuatan detik per detik (terus-menerus) tanpa terlewatkan
5. Monitoring kondisi ruang server
6. Mengunci dan mengamankan ruang server dengan baik
7. Melakukan pelabelan atas asset IT yang dimiliki perusahaan
8. Memasang antivirus yang tervalidasi, terpercaya dan update pada perangkat computer
9. Pemblokiran instal aplikasi diluar ketentuan perusahaan
10. Melakukan penghindaran terhadap penggunaan flashdisk, harddisk yang dapat menyebabkan virus pada computer
11. Pemblokiran akses internet kepada pegawai
12. Dilarang membuka spam dari yang pengirim yang tidak dikenal
13. Memastikan tidak ada celah di peralatan yang tidak terkunci

4. Prinsip integritas dalam keamanan teknologi yaitu melindungi keutuhan data dan informasi organisasi dari modifikasi yang tidak sah. Keamanan informasi menjadi bernilai karena keamanan informasi memastikan bisnis dapat terus berjalan, meminimalisir turunnya pendapatan perusahaan, mengoptimalkan investasi, membuat bisnis berjalan dengan aman, dan mengatur privasi. Ada empat hal yang perlu diperhatikan dalam keamanan informasi yaitu :

1. *Confidentiality* (kerahasiaan). Hal ini menjamin bahwa data atau informasi hanya diakses oleh orang yang berwenang saja.
2. *Integrity* (integritas). Hal ini menjamin bahwa data atau informasi dikirim dengan akurat dan secara lengkap, tanpa ada perubahan apapun didalamnya.
3. *Availability* (ketersediaan). Data atau informasi tersedia pada saat dibutuhkan.
4. *Accountability.* (pertanggungjawaban). Data atau informasi yang ada dapat dipertanggungjawabkan

Contoh :

Suatu perbankan yang memiliki sekumpulan data pribadi nasabah, data keuangan, perbankan wajib menyimpan data nasabahnya dengan baik dan menjaga kerahasaiannya tanpa adanya kebocoran data yang dapat menguntungkan pihak tertentu. Data tersebut disimpan dan dan dikirm dengan akurat dan lengkap tanpa adanya perubahan didalamnya. Data tersebut dapay diambil atau tersedia pada saat kapanpun dibutuhkan serta data yang tersimpan dapat dipertanggungjawabkan.

5. Risk treatment merupakan bagaimana penanganan resiko yang perlu ditangani. Terhadap kendala yang terjadi bagaimana manajemen harus memberikan pilihan penangan atas kendala atau resiko tersebut. Oleh karena setiap keputusan penanganan yang diberikan manajemen harus dievaluasi untuk meminimalisir terjadinya kerugian suatu organisasi. Pilihan yang dipilih untuk penanganan tersebut dipilih berdasarkan hasil penilaian risiko, biaya yang diharapkan untuk menerapkan pilihan tersebut, dan manfaat yang diharapkan dari pilihan tersebut.. pilihan dari penanggulangan resiko tersebut adalah sebagai berikut :
    1. Pengurangan Resiko *(Risk Reduction)* misalnya suatu organisai yang dihadapakan dengan kendala keuangan yang menimbul
    2. Retensi Resiko (*Risk Retention)* misalnya resiko itu sudah diketahui oleh pengguna namun tetap tidak mematuhi system keamanan dengan mendownload film, atau lagu secara gratis pada website yang tidak terpercaya dengan menggunakan perangkat hadware yang tidak terpasang antivirus sehingga mengakibatkan perangkat hardware yang digunakan menjadi rusak atau terkena virus.
    3. Penghindaran Resiko *(Risk Avoidence)* misalnya pengguna menginstal antivirus terpercaya dan terupdate kepada perangkat yang digunakan, menginstal aplikasi original, tidak membuka situs website berbahaya,

4. Transfer Resiko *(Risk Transfer)* misalnya organisasi bekerjasama dengan pihak ketiga atau asuransi untuk menghindari kerugian yang terjadi dalam suatu organisasi.

IT Risk Management

MTI REG B

Aldo Fajarino

202420004

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan. Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

   IT Risk Management adalah penerapan dari prinsip-prinisip manajemen risiko terhadap perusahaan yang memanfaatkan teknologi informasi dengan tujuan untuk dapat mengelola risiko-risiko yang berhubungan dengan perusahaan tersebut. Risiko-risiko yang dikelola meliputi kepemilikan, operasional, keterkaitan, dampak, dan penggunaan dari teknologi informasi pada sebuah perusahaan.

   IT Risk Management tidak hanya berfokus tentang penanganan terhadap risiko dan dampak negative dari hambatan-hambatan terhadap operasional perusahaan dalam hal value sebuah perusahaan, tetapi juga dapat memberikan keuntungan potensial. langkah-langkah yang dilakukan untuk mengelola risiko teknologi informasi dalam sebuah perusahaan:

   - Assessment, merujuk pada pencarian risiko dan penilaian tingkat keparahan risiko.
   - Mitigation, yaitu penanggulanan yang dilakukan untuk mengurangi dampak risiko.
   - Evaluation and Assessment, merujuk pada evaluasi terhadap penanggulangan yang sudah dilakukan.

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

   Ancaman terhadap sistem yang biasa terjadi yaitu kerusakan perangkat, baik itu perangkat keras komputer maupun perangkat lunak, contohnya kerusakan pada harddisk yang dapat mengakibatkan kehilangan data-data penting di suatu perusahaan, karena seperti yang kita tahu, bahwa harddisk itu memiliki rentang usia, semakin tua usia harddisk, maka semakin besar resiko kerusakan pada harddisk tersebut. Ada ancaman human error atau kesalahan manusia maupun serangan secara fisik ke perangkat, untuk human error biasanya terjadi pada operator yang salah memasukkan kode inputan ke dalam komputer ataupun lalai dalam mengoperasikan komputer. Kemudian ada ancaman lain yang sering kita temui di internet contohnya berupa virus, malware, phishing, scam, dan fraud atau manipulasi data untuk kepentingan yang melanggar hukum, beberapa pihak dengan sengaja membuat suatu program yang sifatnya merusak ataupun mencuri data pada komputer yang terinfeksi. Ada

juga ancaman dari dalam atau internal perusahaan dimana terjadi pencurian data oleh karyawan dari perusahaan itu sendiri.

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

   Menurut saya, dalam mengamankan aset IT yang dikelola, seorang CIO bertanggung jawab merencanakan teknologi informasi secara matang, perencanaan infrastruktur yang baik adalah kunci penting dalam dunia IT, pengelolaan dan perhitungan budget yang tepat juga harus dilakukan, dengan tetap memperhatikan performa dari komponen keamanan informasi. Keputusan yang diambil oleh seorang CIO harus berdasarkan Risk Management Program.

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

   Aspek Integrity adalah aspek yang berkaitan dengan keakuratan dan kelengkapan sebuah informasi dan metode pemrosesannya. Hal ini menjamin bahwa data atau informasi dikirim dengan akurat dan secara lengkap, tanpa ada perubahan apapun didalamnya.

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

   Hasil evaluasi resiko akan dapat menentukan Langkah yang akan diambil dalam Risk Treatment. Risk treatment bertujuan untuk menentukan Tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara Keseluruhan. Risk treatment merubah analisis sebelumnya, risk identification dan risk assessment, menjadi tindakan substantif untuk mengurangi risiko. Terdapat beberapa risk treatment yang umumnya digunakan, yaitu; risk prevention (pencegahan risiko) dengan tujuan untuk mengurangi secara substansial kemungkinan terjadinya risiko, risk mitigation (mitigasi risiko) dengan tujuan untuk meminimalkan konsekuansi dari risiko, risk sharing (berbagi risiko) dengan tujuan untuk memindahkan risiko tidak hanya ke organisasi lain namun juga ke entitas bisnis ataupin individu, dan risk retention (retensi risiko) atau dikenal juga sebagai penyerapan, toleransi, atau penerimaan risiko.

IT Risk Management

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

--- Selamat bekerja ---

Jawab:

1. Misalnya saya bekerja di sebuah SMA yang akan mengadaptasi TI pada managemen SMA tersebut. Adapun strategi yang akan saya terapkan:
   A. Mengidentifikasi seluruh resiko yang akan terjadi, kemudian menganalisis resiko yang telah diidentifikasi agar dapat memahami lebih lanjut tentang resiko tersebut, yaitu

bagaimana resiko tersebut akan mempengaruhi proyek dan tujuan perusahaan. Misalnya dalam pendataan siswa. Beberapa resiko yang saya identifikasi adalah:

- Human Error
- Kebocoran data
- Bencana Alam (Kebakaran, Banjir, Tersambar Petir, dll.)

Berdasarkan dari 3 contoh diatas, saya mendapat beberapa kejelasan mengenai bagaimana resiko-resiko tersebut dapat mengganggu pendataan siswa, diantaranya:

- Human Error pada masalah kesalahan input data, yang akan berakibat pada beberapa hal seperti: Pendataan Ujian Nasional, Pendataan Pusat, Pendataan Dana PIP, Turunnya kepercayaan masyarakat, rugi waktu karena harus merevisi data yang telah diinput.
- Bencana alam, jika data siswa tidak di back-up atau disimpan di tempat lain, maka akan terjadi kerugian waktu dan kepercayaan yang besar, ketertinggalan waktu pendataan dapat menghambat sebagian besar operasional sekolah, belum lagi harus mempertanggungjawabkan hal tersebut pada pihak-pihak terkait seperti, para orang tua siswa, dinas pendidikan, bahkan hukum.

B. Berdasarkan beberapa analisis di atas, dilakukan mitigasi resiko untuk menanggulangi resiko tersebut sebelum terjadi, yaitu:
   - Untuk masalah human error, maka dicari tenaga professional yang sudah berpengalaman lebih dari 3-4 tahun dalam dunia administrasi pendataan. Tenaga yang belum berpengalaman sangat tidak dianjurkan untuk ditugaskan pada penanggungjawaban pendataan tersebut karena mereka cenderung memiliki tingkat human error yang lebih besar, seperti tidak tahu harus bagaimana jika ada suatu masalah yang muncul, bagaimana melakukan pendataan yang efektif dan efisien, dll.
   - Untuk masalah bencana alam dapat ditanggulangi dengan melakukan back-up data secara rutin 1x24 jam ke beberapa tempat penyimpanan berbeda, minimal 2 buah tempat penyimpanan, dengan begitu, jika terjadi bencana alam, data yang hilang dapat segera diganti dengan data back-up yang sama seperti hari sebelumnya.

C. Setelah dilakukan mitigasi resiko, dilakukan pemantauan resiko untuk melihat apakah ada resiko lain yang dapat mengancam, juga melakukan pemantauan pada resiko yang telah diketahui.

Tentunya asesmen dan solusi tersebut harus didiskusikan bersama para stakeholder, baik internal maupun eksternal, internal misalnya kepala sekolah, para guru, eksternal misalnya

komite sekolah. Bisa saja asesmen dan solusi yang saya berikan kurang disetujui oleh para stakeholder dan mereka memiliki masukan yang lebih baik.

2. Beberapa dari sumber ancaman yang dimaksud adalah:
   A. Properti yang bocor
      - Pembajakan

        Pembajakan adalah kegiatan penyalinan atau distribusi suatu perangkat lunak yang dilakukan secara illegal atau tidak sah.

      - Pelanggaran Hak Cipta

        Pelanggaran hak cipta adalah penggunaan suatu materi yang masih dilindungi hukum hak cipta tanpa seizin pencipta atau pemegang haknya.

   B. Serangan Software
      - Virus

        Virus adalah sebuah program komputer perusak yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinannya ke dalam program atau dokumen lain pada sebuah system.

      - Worm

        Worm adalah sebuah program computer perusak yang dapat menggandakan dirinya dengan memanfaatkan suatu jaringan tanpa perlu campur tangan dari user itu sendiri. Tidak seperti virus, worm memanfaatkan vulnerability dari suatu sistem untuk menyisipkan dirinya.

      - Macro

        Macro adalah sebuah fungsi yang memungkinkan penggunanya untuk melakukan banyak hal dalam waktu yang singkat. Dalam game, macro ini sangat merugikan pemain lain yang tidak menggunakan macro, dikarenakan pengguna macro akan mendapat kemenangan dalam waktu yang sangat singkat tanpa harus bersusah payah seperti pemain yang tidak menggunakan macro.

      - DoS

Denial of Services atau DoS adalah jenis serangan cyber yang menyerang suatu sistem dengan memanfaatkan jaringan internet dengan cara menghabiskan resource yang dimiliki oleh suatu sistem sehingga sistem tersebut tidak dapat menjalankan fungsinya dengan benar, sehingga pengguna dari sistem tersebut tidak akan dapat mengakses sistem yang terkena serangan DoS.

C. Bencana Alam

Bencana alam dapat merusak perangkat keras secara fatal, seperti kabel terbakar, kehancuran server, server terpanggang, listrik arus pendek, dan kehancuran infrastruktur lain yang Sebagian besar bersifat tidak dapat diperbaiki. Selain itu bencana alam dapat berpotensi membunuh individual yang penting pada keberlangsungan suatu sistem.

D. Sabotase atau Vandalisme

Sabotase atau Vandalisme adalah sebuah kegiatan yang dilakukan dengan tujuan untuk merubah data dari sebuah sistem. Misalnya seorang hacker/peretas yang mengubah desain grafis dari suatu sistem sehingga tampilan dari sistem tersebut tidak sesuai/menyimpang dari yang seharusnya.

3. Dengan cara membuat kerja sama secara hukum dengan pihak ke-3 yang terpercaya terkait keamanan informasi sistem, berupa keamanan server dan jaringan nirkabel. Selain itu saya juga akan membentuk sebuah tim khusus agar dapat terus memonitor pihak ke-3 agar tidak terjadi pelanggaran kerja sama.

4. Integrity artinya melindungi keutuhan data dan informasi organisasi dari modifikasi yang tidak sah. Misalnya dalam hal keuangan negara, Data penerimaan negara harus benar, tidak ada modifikasi, bila data tersebut sengaja dimodifikasi baik besar maupun kecil, maka ada kemungkinan akan terjadi beberapa dampak ganggungan dari keamanan informasi tersebut seperti: kerugian finansial, rusaknya reputasi, bocornya rahasia negara, dll. Oleh karena itu pengiriman data penerimaan negara harus sesuai sehingga dapat dicocokan dan dikontrol secara tepat.

5. Risk Treatment/penanganan resiko dan evaluasi resiko adalah proses yang saling bergantung satu sama lain, kedua proses ini memungkinkan manajer untuk menyeimbangkan biaya operasional dari tindakan perlindungan resiko dan meraih peningkatan dalam melindungi

sistem yang ada pada perusahaan/organisasi. Evaluasi resiko memungkinkan manajer untuk mengidentifikasi resiko dan menilai kemungkinan resiko tersebut, mengeksploitasi beberapa kerentanan perusahaan serta dampak potensial dari peristiwa tersebut terjadi. Setelah resiko diidentifikasi dan dinilai, proses penilaian berhenti dan dilanjutkan ke tahap penanganan resiko, dimana resiko tersebut akan diproses sesuai dengan identifikasi yang telah dilakukan pada tahap sebelumnya.

Contoh, jika seorang manajer telah mengidentifikasi resiko yang didapat berupa resiko overheat yang akan dialami oleh sebuah server, namun karena keterbatasan ruang dan biaya, dilakukan penanganan berdasarkan identifikasi resiko sebelumnya, yaitu dengan meletakan server tersebut pada ruang kedap udara tanpa jendela yang telah dilengkapi dengan AC di dalamnya agar suhu ruangan dapat mengalahkan panas yang dihasilkan oleh server secara terus menerus.

Nama : Enggi Ardius

NIM : 202420007

MK : UAS "IT Risk Management"

IT Risk Management

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

--- Selamat bekerja ----

Jawaban :

1. Strategi yang dapat dilakukan sebagai berikut :

a. Meningkatkan keamanan dalam sistem IT seperti penambahan perangkat firewall dan selalu upgrade sistem yang terbaru supaya untuk mencegah dari hacker dan lain sebagainya.
b. Manajemen pengawasan dalam IT seperti melakukan pengecekan realtime terhadap IT serta penilaian dan evaluasi terhadap kendala-kendala yang di hadapai di lapangan. Contohnya suhu dalam ruangan server, pengecekan expired dalam penggunaan SSL dan memonitor serangan-serangan virus dari pihak luar.
c. Manajemen dalam SDM dan perangkat IT seperti meninjau operasional server secara fisik melihat apakkah server masih bagus aau tidak, ada warning sistem di dislay server serta mengecek suhu ruangan panas atau tidak. Selain itu juga menilai dan mengawasi setiap karyawan atau staf dalam bekerja supaya untuk meminimalisir human eror bahkan serangan nyata di dalam perusahaan.
d. Peningkatan dalam pembuatan program pendukung IT seperti program pencegahan perusakan ruangan IT, program pengenal ID pegawai dll.

2. Sumber ancaman yang dapat terjadi banyak sekali contohnya : pertama dari manusia internal perusahaan yaitu sebuah prilaku yang dilakukan oleh manusia yang dilakukan secara fisik seperti menghancurkan, membakar, bahkan merusak komponen perangkat sebuah server. Kedua ancaman berasal dari virus yaitu merupakan sebuah aplikasi atau program yang dapat merusak sebuah pernagkat lunak atau software dengan cara menyebarkan virus kedalam sebuah sistem sehingga merusak semua file yang ada pada sebuah sistem tersebut seperti dokumen, aplikasi, bahkan sistem tersebut. Ketiga hackers adalah orang yang masuk dengan sengaja kedalam sebuah sistem komputer yang orang lain tidak ketahui yang merugikan karena mengambil atau mencuri data bahkan dapat merusak sistem komputer tersebut.

3. CIO merupakan sebuah jabatan yang bertanggung jawab untuk menjamin keakuratan data, ketepatan waktu, dan keamanan teknologi dan informasi yang dibutuhkan perusahaan untuk mencapai tujuan. Jika ini menjadi posisi saya yang akan dilakukan adalah :

a. Akan bertanggung jawab dalam mengamankan sebuah data atau aplikasi dalam perusahaan.
b. Akan bertanggung jawab dalam mengantisipasi berbagai macam serangan baik itu secara nyata maupun dunia maya
c. Akan bertanggung jawab dalam melakukan analisa dan perubahan teknologi yang sesuai dengan perkembangan zaman teknologi
d. Akan bertanggung jawab dalam melakukan strategi keamanan dan peluang bisnis dalam upaya meningkatkan infrastruktur teknologi.
e. Menjalin kerjasama tim dan melakukan pelayanan berbasis IT.

4. Integritas (integrity)

Aspek ini berkaitan dengan keakuratan dan kelengkapan sebuah informasi dan metode pemrosesannya. informasi dijaga agar selalu akurat, untuk menjaga informasi tersebut maka informasi hanya boleh diubah dengan izin pemilik informasi. Virus trojan merupakan contoh dari informasi yang integritasnya terganggu karena virus telah mengubah informasi tanpa izin. Integritas informasi ini dapat dijaga dengan melakukan enkripsi data atau membuat tanda tangan dijital (*digital signature*).

Contoh :

- Di dalam sebuah ruangan server harus menggunakan mesin finger door untuk masuk agar orang yang tidak berkepentingan tidak bisa masuk.
- Database yang ada didalam sebuah server agar di evaluasi dan dilakukan pengecekan realtime menggunakan sebuah program agar mengetahui virus atau malware yang dapat merusak sistem.
- Semua password harus menggunakan keamanan md5 atau kemanan yang lain.

5. Tujuan penilaian resiko adalah menetapkan kemunginan terjadinya dan dampak suatu suatu kejadian yang menghambat pencapaian tujuan atau sasaran organisasi supaya dapat dilakukan penanganan risiko secara tepat. Penilaian Risiko pada dasarnya merupakan kegiatan penilaian atas kemungkinan kejadian yang mengancam pencapaian tujuan dan sasaran organisasi.

Sebagai contoh adalah :

“Pembelian Server guna menunjang sistem informasi akademik pada Universitas”

Pada contoh kasus diatas kita dalam melakukan tahap penilaian resiko yaitu sebagai berikut:

1. Identifikasi Resiko
    a. Menentukan dimana lokasi pembelian server harus di toko yang akurat dan nyata.
    b. Berapa harga server tersebut apakah mahal atau tidak.
    c. Menentukan seperti apa spesifikasi server.
    d. Kapan waktu tepat harus membeli server, jangan sampai menganggu kegiatan akdemik.
    e. Harus menetukan perangkat pendukung server seperti firewall, ISP dll.

2. Analisis Resiko
    a. Spesifikasi yang besar atau kecil menentukan kualitas sistem informasi akademik.
    b. Lokasi toko pembelian server jauh maupun dekat berpengaruh pada waktu lama tidak barang sampai, berpengaruh pada harga semakin jauh maka harga mahal dan lain sebagainya.
    c. Spesifikasi server harus di perhitungkan untuk fungsi yang akan datang 5 atau 10 tahun kedepan masih layak pakai atau tidak.
    d. Untuk perangkat pendukung server seperti firewall, ISP harus di perhatikan dalam pembelian SSL, tempat berlangganan ISP dll.

3. Evaluasi Resiko
    a. Server yang dibeli harus sesuai dengan spesifikasi jika kemudian hari server tersebut bermasalah harus melakukan backup server atau mendatangkan teknisi dari toko tempat pembelian server
    b. Pembelian server pada lebih dari 2 toko yang sama2 jauh harus memilih toko yang dapat menjanjikan barang tersebut sesuai dengan estimasi waktu yang telah di sepakati.
    c. Server dan perangkat pendukung harus mencari yang keamanannya tinggi dan bahkan dari harga yang murah tapi kualitas tinggi.

Nama	**: KhadijahThahira**
NIM/ Kelas	**:202420027/ MTI 232**

IT Risk Management

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.
   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

   - Mengidentifikasi risiko
   - Menilai risiko
   - Mengurangi risiko
   - Mengembangkan rencana respon
   - Mengkaji prosedur manajemen risiko

   - *Assessment*, merujuk pada pencarian risiko dan penilaian tingkat keparahan risiko.
   - *Mitigation*, yaitu penanggulanan yang dilakukan untuk mengurangi dampat risiko.
   - *Evaluation and Assessment*, merujuk pada evaluasi terhadap penanggulangan yang sudah dilakukan.

   contoh:
   - Memasang antivirus pada setiap pc yang ada di perusahaan
   - Menggunakan pihak ketiga untuk keamanan asset yang dimiliki, kekurangan dari pihak ketiga adalah biaya yang di keluarkan besar
   - Jika terjadi ancaman yang tidak bisa dihindari/ *accidental* seperti bencana dan lain sebagainya sebaiknya data di setiap hari di backup
   - Jika permasalahannya adalah ruangan yang terlalu kecil sehingga membuat sirkulasi udara menjadi panas di tempat penyimpanan asset maka pasang pendingin udara AC
   - Jika kelalaian manusia yang terjadi maka sebaiknya di evaluasi lagi kinerja karyawan tersebut

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya
   Sumber – sumber ancaman :
   - Hacker & cracker, computer criminal, terrorist : Serangan dari pihak musuh atau diserang secara fisik oleh pihak lawan (rival) bisnis yang ada, contohnya: Ketika bulan mei 2021 palestina Kembali perang dengan israel, cyber indonesia dan Malaysia membantu dengan cara meretas beberapa situs, cctv, dan 300 nomor WhatsApp warga Israel, menurut komunitas cyber ini merupakan cara mereka untuk membantu warga palestina
   - Hardware : penyimpanan yang tidak terlindungi sehingga rentan terjadinya kerusakan, temperature yang tinggi dari hardware, pengaturan volt listrik yang salah,memori yang kecil, salah memilih spesifikasi hardware

- Software: memilih software yang salah, tidak adanya software testing, dokumentasi software yang buruk, salah memilih antivirus, tidak logout Ketika menggunakan aplikasi
- Jaringan : kegagalan dalam mengauntentikasi dan mengidentifikasi jaringan, manajemen password yang sala, firewall yang mudah di akses, pemasangan kabel dan alat jaringan yang salah
- Human error/ personal: tidak mengikuti pelatihan penggunaan aplikasi, kegagalan monitoring, banyak absence, kesalahan dalam ppenggunaan software dan hardware
- Terjadinya resiko dari kesalahan Situasi dan method yang di gunakan, contoh: perusahaan mengeluarkan banyak biaya menggunakan pihak ketiga (outsourcing) untuk mengamankan asset IT tetapi hasilnya ancaman dan resiko yang terjadi semakin banyak sehingga pemilihan pihak ketiga ini bukannya menguntungkan tapi malah merugikan perusahaan.
- Kesalahan manusia karena kelalain, contoh : kasus pembobolan rekening ilham bintang yang dilakukan oleh karyawan bank bekerja sama dengan hacker untuk mengambil uang di rekening ilham bintang. Hacker tersebut mendapatkan data pribadi ilham bintang melaui karyawa bank, karyawan bank mendapatkan data pribadi ilham bintang melalui Sistem Laporan Informasi Keuangan (SLIK).
- Kegagalan structural dari sumberdaya yang di Kelola oleh organisasi contoh: perangkat lunak dan perangkat keras yang di gunakan sudah ketinggalan zaman sehingga keamanan asset IT yang di miliki oleh perusahaan sangat minim
- Bencana alam, contoh: banjir/ gempa bumi/ kebakaran yang mengakibatkan rusak atau lenyapnya asset IT yang di miliki oleh perusahaan

Ancaman resiko di luar dari organisasi IT, contoh: serangan hacker.

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?
   - Memasang antivirus pada setiap pc yang ada di perusahaan
   - Menggunakan pihak ketiga untuk keamanan asset yang dimiliki, kekurangan dari pihak ketiga adalah biaya yang di keluarkan besar
   - Jika terjadi ancaman yang tidak bisa dihindari/ *accidental* seperti bencana dan lain sebagainya sebaiknya data di setiap hari di backup
   - Jika permasalahannya adalah ruangan yang terlalu kecil sehingga membuat sirkulasi udara menjadi panas di tempat penyimpanan asset maka pasang pendingin udara AC
   - Jika kelalaian manusia yang terjadi maka sebaiknya di evaluasi lagi kinerja karyawan tersebut

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

   - Keamanan informasi merupakan bagian integral dari praktik manajemen yang baik
   - Seorang manajer harus mampu menilai tingkat resiko keamanan yang cukup pantas untuk diterima sesuai dengan kontrol yang diberlakukan.
   - Keamanan informasi harus efektif dalam hal biaya
   - Tanggung jawab dan kewenangan keamanan informasi harus dijelaskan secara eksplisit
   - Pemilik sistem memiliki tanggung jawab keamanan diluar organisasinya.
   - Keamanan informasi memerlukan pendekatan yang komprehensif dan terintegrasi
   - Keamanan informasi harus dievaluasi ulang secara periodik

- Keamanan informasi dibatasi oleh faktor sosial

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

   Hasil evaluasi risiko yang digunakan untuk membuat keputusan harus konsisten dengan konteks manajemen risiko keamanan informasi eksternal dan internal yang ditetapkan dan mempertimbangkan tujuan organisasi dan pandangan pemangku kepentingan, dll.
   Pertimbangan harus mencakup:
   Properti keamanan informasi: jika satu kriteria tidak relevan untuk organisasi (kehilangan kerahasiaan), Pentingnya proses bisnis atau aktivitas yang didukung oleh aset atau kumpulan aset tertentu.

   Ini berarti hasil evaluasi resiko sebelumnya akan mengurangi impact dari dari risk treatment yang di lakukan selanjutnya

--- Selamat bekerja ----

IT Risk Management

Mirza Eka Putra

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat di timbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatar belakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul di lingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan.

   Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?

4. Integrity merupakan bagian penting dari aman nya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!

--- Selamatbekerja ----

Jawab

1. Untuk mengurangi Resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK) maka terdapat strategi yang dilakukan di antaranya yaitu

   -**Perangkat IT**

   Penanggulangan di perangkat IT sendiri seperti rentannya pengguna terkena virus komputer, pencurian data oleh hacker dan penyadapan yang dilakukan oleh hacker dapat di cegah

dengan pemasangan anti virus kemudian melakukan edukasi kepada pengguna agar tidak mendownload file yang sembarang. Kemudian dari sisi teknologi instansi harus menyediakan perangkat berupa firewall yang baik untuk mencegah dari kegiatan dari luar yang mencoba mencuri data. Dan selalu melihat / monitoring arus data yang terjadi.

sedangkan yang kedua yaitu faktor Human Resource

-Faktor Human Resource

Faktor eksternal bisa terjadi dikarenakan kelalaian pengguna misalnya rusaknya perangkat / pencurian perangkat, Kesalahan juga terjadi dikarenakan lemahnya sistem seperti operasional perangkat seperti pihak mana saja yang diizinkan melihat server dan mengkakses server hal ini sering digunakan hacker / cracker sebagai sisi lemah untuk mencoba merusak sistem. Hal ini bisa di cegah dengan pelatihan secara berkala akan penggunaan perangkat IT dari sisi pengguna biasa dan pengelola IT

2 Beberapa Sumber ancaman terhadap system informasi yaitu

Sumber ancaman terhadap sistem informasi yaitu dapat terjadi dikarenakan berbagai faktor

1. Bencana Alam

Bencana Alama merupakan suatu hal yang tidak dapat di prediksi, misal gempa bumi, banjir, dan yang lainnya. Oleh karena itu kita harus mengamankan perangkat penting IT yang kita kelola misalnya memindahkan server ke cloud server sebagai file backup cadangan

2. Kesalahan Manusia

Manusia tidak terlepas juga dari kelasahan misal mendownload file sembarangan sehingga terdapat virus komputer. Manusia yang sembarangan memfoto perangkat dan mengupload nya ke sosial media sehingga mengundang hacker/cracker untuk men pentesting sistem berdasar info yang didapat dari orang yang dengan sengaja atau tanpa sengaja mengupload file foto pereangkat server, router dan sebagainya

3. Kesalahan Perangkat

Kesalahan akan perangkat hardware yang tidak mensupport sistem ataupun kesalahan program bisa menjadi ancaman terhadap sistem informasi

3 Pengamanan terhadap asset IT yaitu

1. Back up data berkala
2. Pengecekan perangkat rutin
3. Edukasi terhadap karyawan yang menggunakan perangkat IT
4. Mencatat semua kesalahat yang terjadi sebagai rujukan jika error dikemudian hari
5. Disaster recovery dengan mengupload file ke cloud server

4 Faktor yang mempengaruhi intergritas yaitu disiplin, jujur dan konsisten. JIka dikaitkan dalam pengamanan sistem informasi, pengelola IT harus disiplin mulai dari ceking berkala sistem dari server router dan perangkat IT lainnya kemudian pengelola yang memegang sistem harus jujur

agar terhindar dari pencurian data dan pembobolan sistem, kemudian konsisten dalam pengerjaan di dunia IT

5 Treat Risk yaitu cara kita untuk memperlakukan sistem dan gejala yang berhubungan dengan resiko IT hubungan dengan evaluasi IT yaitu sama sama mengevalusi kejadian yang berhubungan dengan kekurangan kekurangan dalam sistem IT. Misal JIka terjadi sesuatu kejadian kita harus mencatat hal tersebut dan jika

Nama: Mustakim

Nim: 202420028

IT Risk Management

Pertanyaan:

1. Mengingat seriusnya resiko keamanan akan asset Teknology Informasi dan komunikasi (TIK), managemen resiko secara efektif menjadi bagian penting untuk mengurangi dampak buruk yang dapat ditimbulkannya. Ditambah lagi, penggunaan TI semakin menjadi bagian integral dari proses bisnis dimana gangguan dengan TIK berdampak langsung terhadap kelancaran operasional organisasi. Berlatarbelakang hal tersebut maka menjadi penting baik bagi pihak manajemen maupun seluruh staff memahami resiko apa yang mungkin muncul dilingkungan IT mereka dan bagaimana resiko tersebut dapat dikurangi atau bahkan dihilangkan. Sehubungan dengan hal ini bagaimana strategy yang dapat diterapkan untuk memanajemen resiko ini…? Jelaskan dengan contoh

   Jawaban:

   a. Mengidentifikasi resiko: yaitu mengetahui dan mengenali resiko-siko yang muncul kemudian menggambarkan resiko itu. Contoh: dalam sebuah perusahaan resiko-resiko yg mungkin dihadapi oleh dari segi IT adalah malware, spam, scam. Virus dan kerusakan perangkat lunak dan keras computer.
   b. Menganalisis resiko: yaitu menentukan kemungkinan dan dari setiap resiko-resiko yg ada. Contoh: kerusakan pd perangkat lunak dpt mengakibatkan computer tenaga IT tidak dpt digunakan dan diperlukannya backup computer bukan hanya satu computer.
   c. Mengevaluasi resiko: lalu kita dapat menentukan besarnya dapat dr resiko-resiko tersebut. Contoh jika compute/laptop bagian IT rusak maka proses TIK dlm perusahaan itu dpt berhenti atau bahkan tertunda.
   d. Memantau dan mempertibangkan resiko: disinilah kita akan dapat mempertimbangkan resiko-resiko baik yg terburuk maupun termudah. Contoh jika banyak virus computer diperlukannya antivirus.

2. Di era sekarang ini banyak ancaman terhadap system yang mungkin terjadi. Jelaskan sumber ancaman tersebut, beri contoh dan diskusikan masing-masingnya.

   Jawab:

   1. Hacker: orang yang dapat menerobos system computer dengan cara yg salah/ tidak sah,
   2. Fraud: yaitu orang memanipulasi data untuk kepentingan melanggar hukum dan merugikan Organisasi/perusahaan.
   3. Malware/Virus computer: sebuah program computer yg masuk kedalam system untuk mempengaruhi kinerjabahkan merusak sebuah system/computer.
   4. Spam, scams, and phishing: Penipuan melalui media teknologi informasi yaitu contohnya email yang dapat mencuri informasi seperti nomor rekening bank, kata sandi, dan nomor kartu kredit baik pribadi, organisasi maupun perusahaan.

5. Human Error: yaitu sebuah kesalahan atau yang dapat terjadi yang diakibatkan minimnya pengetahuan tentang IT pada sebuah organisasi/perusahaan.
Contoh: https://www.cnbcindonesia.com/tech/20210609131452-37-251746/ngeri-miliaran-password-bocor-di-forum-hacker
Kumpulan miliaran kata sandi diduga bocor di forum peretas populer. Hal ini diketahui dari pengguna forum yang menggugah file TXT 100GB berisi 8,4 miliar entri password. Jumlah itu nampaknya telah digabungkan dari kebocoran data dan pelanggaran yang telah terjadi di masa lalu. Menurut orang yang mengunggah, seluruh password memiliki panjang 6-20 karakter, dengan karakter non-ASCII dan tanpa spasi.Menurut saya dalam contoh kasus diatas tetap akan terjadi karna semakin canggihnya sebuah system pasti tetap akan ada celah. Maka dari itu pentingnya update password berjangka seperti password email yg dapat diganti agar tidak mudah dikases dan menghindari hal-hal diatas.

3. Jika anda seorang CIO, jelaskan bagaimana anda mengamankan asset IT yang anda kelola?
Jawaban: yang akan saya lakukan adalah menerapkan IT Risk Management pada perusahaan dan mencari pihak yang dapat menjamin keamanan IT perusahaan berjalan dengan baik. Dengan kemudian akan mengamankan jaringan untuh mencegah cyber crime, lalu memperhatikan phishing yang dapat mencuri informasi yg digunakan hacker dalam menjalankan aksi kriminalnya, dan membackup data atau file penting/ yg berkaitan dengan perusahaan secara berkala.

4. Integrity merupakan bagian penting dari amannya suatu system berbasis teknologi. Jelaskan dengan menggunakan contoh, penerapan prinsip integritas dalam keamanan teknologi informasi
Jawaban: Pada dasarnya Informasi yang baik adalah informasi yang diberikan sesuai dengan kebutuhannya, baik pada kelengkapan materinya, waktu pemberian informasinya, keakuratan datanya, dan sebagainya. Misalkan saja, manajer pemasaran membutuhkan informasi mengenai kondisi pasar, kondisi pesaing, kondisi ekonomi makro, kekuatan perusahaan, kemampuan finansial perusahaan, dan sebagainya. Agar informasi dapat dilakukan secara cepat dan akurat, maka pada masa kini, tak ada pilihan lain selain memanfaatkan komputer yang di dalamnya dibentuk sistem basis data. SIM adalah kerjasama yang harmonis antara manusia dan mesin (komputer). Sedapat mungkin semua alat-alat kantor dibuat berangkaian dengan komputer (*office automation*), misalkan pemanfaatan *e-mail, tele- conference, e-voice, internet, facs,* dan sebagainya.

5. Risk Treatment sangat berhubungan erat dengan hasil evaluasi resiko yang dilakukan sebelumnya. Anda diminta untuk menjelaskan hubungan keduanya. Agar lebih mengena, silakan jelaskan dengan contoh!
Jawaban: Risk Treatment adalah tindakan spesifik yang dilakukan dengan tujuan untuk menurunkan tingkat risiko dalam upaya menghindari atau mengurangi kerugian perusahaan. Maka dari itu jika risk treatment diterapkan maka akan mudah mendapatkan evaluasi resiko dimana setiap resiko yg sudah dievaluasi dpt segera diperbaiki lagi. Contoh saat kehilang e-KTP kita hanya perlu membuat laporan kehilangan kemudian akan mendapatkan surat dimana akan dapat digunakan dlm proses pembuatan e-ktp baru dengan menggunkan data lama sehingga tidak perlu lg membuat pengajuan dan mengisi persyarata-persyaratan lain.

--- Selamat bekerja ----