Seri Artikel “Integrated Risk Management”

“Mengelola Risiko Teknologi Informasi”

Pengantar untuk RiskWorkshop / Lokakarya / Seminar tentang Mengelola Risiko Teknologi Informasi *(Managing Information Technology Risk)* dalam lingkungan bisnis di Indonesia.

Oleh: Antonius Alijoyo, June 2011, Jakarta - Indonesia

SEPULUH HAL UMUM YANG DAPAT DIHINDARI UNTUK MENGURANGI TERJADINYA RISIKO TEKNOLOGI INFORMASI DI PERUSAHAAN

Artikel ini membahas sepuluh hal umum yang sebenarnya mudah untuk dihindari, tetapi dapat menjadi sumber risiko teknologi informasi yang serius bagi perusahaan. Kesepuluh risiko tersebut tidak hanya bersumber dari teknologi semata tetapi juga dapat terjadi karena strategi sistem informasi yang tidak mendukung keamanan dan pengamanan aset informasi perusahaan, atau karena permasalahan individu yang dihadapi oleh karyawan perusahaan yang berdampak terhadap bocornya aset informasi berharga perusahaan ke pihak lain.

Artikel ini hanya sekedar pengantar dan atau bekal bagi calon peserta dalam mengikuti suatu ‘riskworkshop’ atau ‘lokakarya manajemen risiko’ yang mengupas tentang bagaimana mengelola risiko teknologi informasi atau ‘managing IT risks’ di Indonesia.

Risiko #1: Menunda siklus penyegaran/penggantian PC (Personal Computer) baik ‘desktop PC’ maupun ‘notebook PC’

Kejadian atau permasalahan yang dapat timbul	• Pada saat anggaran sangat ketat, perusahaan umumnya menunda program penggantian PC bagi para karyawan. Padahal, semakin lama PC usang berada dalam infrastruktur TI perusahaan, semakin besar biaya tersembunyi akan terjadi, misal turunnya produktivitas pengguna PC dan semakin besarnya ‘downtime’ yang dialami oleh perusahaan.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun,** karena karyawan membutuhkan waktu lebih lama dalam manyelesaikan pekerjaan mereka, terutama dalam menyelesaikan suatu tugas yang bersifat ‘multitasking’. Hal tersebut terjadi karena semakin tua suatu PC semakin kecil kemampuan atau teknologi mereka untuk mendukung lingkungan bisnis yang menuntut adanya ‘multitasking’ tersebut. • **Keamanan jaringan informasi perusahaan dapat terganggu**, karena PC yang sudah tua tidak dapat melakukan pemantauan dan enkripsi akan adanya virus secara berkesinambungan atau terus-menerus. Hal ini akan membuat/menjadi suatu titik lemah dalam solusi keamanan perusahaan secara menyeluruh yang disebabkan tidak adanya jalur keamanan bagi PC lama tersebut – terutama yang menggunakan sistem operasi yang sudah usang. • **Profitabilitas perusahaan dapat terganggu,** karena biasanya setelah tiga tahun penggunaan ‘desktop PC’ dan dua tahun ‘Notebook PC’, biaya tersembunyi akan meningkat misal naiknya biaya perawatan dan dukungan TI, hilang atau berkurangnya laba karena produktivitas karyawan menjadi rendah dan naiknya ‘system downtime’.

Risiko #2: Menggunakan ‘desktop PC’ sebagai ‘server’.

Kejadian atau permasalahan yang dapat timbul	• Perusahaan kadang masih menggunakan ‘desk-top PC’ sebagai ‘server’ dengan memasukkan piranti lunak ‘server’, dan menambahkan ‘hard drives’ serta kartu memori ke PC tersebut. Padahal, suatu desktop PC dirancang hanya untuk mengakomodasi satu pengguna saja (single user) dan tidak dapat menyediakan hal-hal yang ‘server’ mampu lakukan misal pengembangan kapasitas (expandability) dan kinerjanya (performance) atau tingkat keandalan (reliability) untuk pelaksanaan kerja sebagai ‘server’.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun,** karena penggunaan PC sebagai ‘server’ dapat menimbulkan kemungkinan terjadinya ‘crash’ lebih besar dalam sistem informasi perusahaan, sehingga karyawan sering harus menghadapi adanya arsip atau catatan yang hilang secara digital, serta email yang tidak tercatat, dan perlu waktu berjam-jam bahkan berhari-hari untuk mengatasi hal tersebut. • **Keamanan jaringan informasi perusahaan dapat terganggu**, karena sebuah PC kurang aman dibandingkan dengan ‘server’, yang berarti dokumen sensitif dan email perusahaan dapat lebih mudah jatuh ke pihak yang tidak diinginkan. • **Profitabilitas perusahaan dapat terganggu,** karena ‘crash’ dari suatu PC server akan menyebabkan operasi bisnis perusahaan terganggu, sehingga perusahaan kehilangan transaksi yang tadinya atau seharusnya menghasilkan pendapatan bagi perusahaan. Selain itu, ‘crash’ juga dapat menyebabkan naiknya biaya pendukung operasional TI di perusahaan.

Risiko #3: Adanya instalasi ‘unauthorized wireless access points’ di dalam perusahaan.

Kejadian atau permasalahan yang dapat timbul	• Ketika karyawan butuh fasilitas akses ‘wireless LAN’ dalam gedung perusahaan dan ternyata tidak disediakan atau belum disediakan oleh perusahaan, mereka cenderung untuk menyelesaikannya sendiri sehingga dapat terjadi adanya beberapa instalasi ‘wireless access points’ yang tidak terotorisasi secara patut atau sempurna dari departemen TI perusahaan.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun,** terutama bagi karyawan yang menggunakan ‘unauthorized wireless access points’ karena kinerja fasilitas yang digunakan dapat jauh lebih lambat dari yang ‘authorized access points’, yang pada akhirnya akan menyebabkan waktu pengerjaan tugas mereka menjadi lebih lama, dan otomatis produktivitas mereka sendiri akan turun. • **Keamanan jaringan informasi perusahaan dapat terganggu**, karena ‘unauthorized wireless access points’ dapat menjadi titik lemah terhadap penyusup untuk masuk ke dalam jaringan sistem informasi keseluruhan perusahaan. • **Profitabilitas perusahaan dapat terganggu,** karena penggunaan ‘unauthorized wireless access points’ dapat menyebabkan interfensi terhadap ‘wireless access points’ yang sudah dibangun oleh departemen TI perusahaan, sehingga akan mengurangi kualitas dan kinerja ‘Wide Local Area Network’ yang ada, dan itu berarti pemborosan sumber daya perusahaan.

Risiko #4: Penggunaan metode manual atau teknologi usang untuk ‘data storage’ sebagai solusi utama ‘data-backup’ perusahaan.

Kejadian atau permasalahan yang dapat timbul	• Banyak perusahaan terutama kelas medium ke bawah yang tidak memiliki solusi memadai untuk ‘data-backup’ terhadap aset informasi yang dimiliki. Kebanyakan dari mereka masih menggunakan metode manual misal: ‘burning CD’ dan menggunakan ‘storage’ portabel. Ada juga yang menggunakan satu mesin yang sama untuk aplikasi yang digunakan dan sekaligus untuk ‘bakc-up data’.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun,** terutama bagi karyawan departemen TI yang harus menyediakan jumlah karyawan yang cukup banyak dengan keterampilan khusus dalam memastikan proses ‘back-up’ data yang masih dilaksanakan secara manual atau dengan teknologi yang sudah usang. • **Keamanan jaringan informasi perusahaan dapat terganggu**, karena tanpa suatu solusi ‘back-up data’ yang komprehensif dan dapat diandalkan, informasi bisnis yang kritikal dapat hilang selamanya bila terjadi bencana alam atau adanya tindakan sabotase karyawan. Dan tanpa adanya solusi penyimpanan yang aman, arsip elektronik tentang informasi bisnis perusahaan dapat lebih mudah untuk jatuh ke pihak yang tidak diinginkan. • **Profitabilitas perusahaan dapat terganggu,** karena penggunaan metode manual atau tertinggal jaman dapat jauh lebih mahal dibandingkan dengan menggunakan solusi berbasis ‘server’. ‘Data-backup’ secara manual membutuhkan tenaga kerja yang lebih banyak, media penyimpanan yang lebih mahal dibandingkan dengan kebutuhan akan keterampilan dan perawatan TI solusi masa kini.

Risiko #5: Menyediakan perangkat komputer yang tidak sesuai dengan kebutuhan karyawan.

Kejadian atau permasalahan yang dapat timbul	• Dalam rangka menyederhanakan dan menstandarisasi penggunaan PCs atau kadangkala dalam rangka melakukan penghematan, perusahaan tidak memberikan PCs yang layak kepada para karyawan untuk melakukan pekerjaan mereka.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun,** terutama bagi karyawan yang mobilitasnya tinggi tetapi tidak memperoleh 'mobile PC', sehingga mereka harus bekerja dengan 'desktop PC' yang membutuhkan waktu lebih lama karena keterbatasan tempat kerja. Selain itu, bagi karyawan yang membutuhkan PC dengan kemampuan 'multitasking' tetapi tidak memperolehnya, akan butuh waktu sangat lama bila harus bekerja di PC yang tidak menyediakan kemampuan 'multitasking' tersebut. • **Keamanan jaringan informasi perusahaan dapat terganggu**, bukan karena permasalahan fisik infrastruktur TI, tetapi karena karyawan dapat beranggapan bahwa perusahaan atau departemen TI tidak benar-benar serius melengkapi kebutuhan kerja mereka, sehingga mereka juga tidak terlalu serius atau mengalami demotivasi dalam menanggapi bagaimana seharusnya tingkat keamanan penggunaan TI dilakukan di tingkat karyawan. Lebih jauh lagi, hal ini dapat menyebabkan karyawan terdorong untuk melaksanakan pekerjaannya di jaringan internet umum atau melakukan 'upgrading' piranti keras dan piranti lunak tanpa memberitahukan kepada pihak manajemen perusahaan atau departemen TI mereka. Bila hal-hal tersebut terjadi, akan menyebabkan perusahaan mengalami paparan risiko TI yang sangat besar karena membuka celah untuk masuknya peretas ke dalam jaringan perusahaan atau terjadinya inkonsistensi tingkat keamanan TI perusahaan yang berakibat rapuhnya pertahanan TI perusahaan secara keseluruhan. • **Profitabilitas perusahaan dapat terganggu,** karena semakin banyaknya waktu karyawan yang seharusnya dapat dihemat bila mereka memiliki jenis PC yang sesuai dengan pekerjaan mereka.

Risiko #6: Menggunakan ‘multiple images’ dalam lingkungan ‘client PC base’.

Kejadian atau permasalahan yang dapat timbul	• Walaupun para manajer TI ingin membatasi ‘software images’ dan membuat suatu platform yang menggunakan ‘standardized image’, seringkali hal ini tidak mudah untuk dijaga, terutama pada saat vendor membuat suatu perubahan piranti keras untuk PC baru mereka yang tidak sama atau agak berbeda dengan kualifikasi platform dari PC lama mereka. Hal ini membuat perusahaan harus melakukan pengkinian terhadap PC yang diubah atau diperbaharui tersebut agar dapat jalan dalam platform yang sama. Bila hal ini sering terjadi, maka proses pengkinian akan semakin sering dilakukan yang akhirnya dapat berdampak pada meningkatnya biaya perawatan TI yang tinggi dan juga terhadap ketahanan keamanan jaringan TI perusahaan.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun,** karena semakin banyaknya konfigurasi piranti keras di perusahaan akan meningkatkan prasyarat dan cakupan dukungan TI, yang pada akhirnya akan menimbulkan kebutuhan untuk pelatihan yang lebih banyak, dokumentasi yang lebih masif, dan prasyarat-prasyarat beberapa proses unik yang harus diketahui oleh pengguna. Hal ini akan mengurangi waktu karyawan untuk berkontribusi pada pelaksanaan kerja yang langsung berhubungan dengan pencapai sasaran bisnis perusahaan. • **Keamanan jaringan informasi perusahaan dapat terganggu**, karena kebutuhan akan kemampuan TI dalam melakukan respon terhadap pembuatan jalur keamanan untuk piranti lunak baru, pelaksanaan ‘upgrading’, dan penanganan ‘bug’ akan sejalan dengan tingkat kompleksitas dari infrastruktur. Oleh karena itu, dengan bertambahnya waktu yang diperlukan dalam melakukan kualifikasi dan pelaksanaan jalur keamanan mutakhir ke dalam PC yang sudah ada, akan membuat kerentanan (vunerability) perusahaan semakin besar, sehingga membukapeluang bagi para peretas (Hacker) untuk masuk ke dalam jaringan TI perusahaan. • **Profitabilitas perusahaan dapat terganggu,** karena semakin banyaknya konfigurasi platform akan membuat perusahaan mengeluarkan biaya dan waktu lebih banyak untuk melakukan uji kompatibilitas terhadap piranti lunak baru atau ‘upgrading’, penanganan ‘bug’, dan pemastian jalur ‘keamanan/security’ dari piranti baru ke dalam dasar dan standard lingkungan keamanan TI dari platform yang sudah dipakai sebelumnya.

Risiko #7: Menggunakan atau berbagi piranti lunak hasil bajakan, ilegal, atau tidak berotorisasi walaupun legal.

Kejadian atau permasalahan yang dapat timbul	• Seringkali terjadi karyawan perusahaan menggunakan piranti lunak versi bajakan atau ilegal dari pihak luar atau meminjamnya dari teman sejawat. Yang lebih buruk lagi, adalah mereka menggunakan piranti lunak yang legal tetapi tidak memiliki otoritas untuk penggunaan tersebut.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun,** karena penggunaan piranti lunak yang tidak resmi dapat menyebabkan karyawan perusahaan harus menghadapi berbagai permasalahan dalam instalasi, dan kadang tidak dapat bekerja karena piranti keras komputer mereka macet, dan terpaksa harus menunggu sampai selesai direparasi. Hal itu semua akan menyebabkan waktu karyawan terbuang untuk penanganan hal-hal yang tidak diharapkan tersebut. • **Keamanan jaringan informasi perusahaan dapat terganggu**, karena piranti lunak hasil bajakan atau yang tidak memiliki otoritisasi dapat tidak cocok (not-compatible) untuk beroperasi dalam 'platform' dan lingkungan keamanan TI yang sudah ditetapkan oleh perusahaan, sehingga dapat menjadi gerbang masuknya penetrasi pihak luar yang tidak diinginkan. • **Profitabilitas perusahaan dapat terganggu,** karena tuntutan hukum pelanggaran 'hak cipta' penggunaan piranti lunak akan dapat menyebabkan kerugian finansial yang besar bagi perusahaan, tidak hanya denda tetapi juga biaya litigasi yang besar. Selain itu, reputasi perusahaan juga akan terciderai.

Risiko #8: Mengoperasikan dan merawat penggunaan beberapa ‘servers’ tanpa mempertimbangkan adanya konsolidasi.

Kejadian atau permasalahan yang dapat timbul	• Seringkali perusahaan tidak mempertimbangkan penggunaan beberapa tingkatan konsolidasi untuk pengoperasian dan perawatan dari penggunaan beberapa ‘servers’ di dalam perusahaan, misal: konsolidasi aplikasi,konsolidasi data, penggunaan virtualisasi server, dan sentralisasi lokasi server.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun,** karena karyawan pendukung Ti perusahaan harus menangani beberapa aplikasi yang sama di berbagai daerah sehingga perlu melakukan perjalanan jauh dari satu tempat ke tempat lain. • **Keamanan jaringan informasi perusahaan dapat terganggu**, karena kompleksitas dan jumlah fisik ‘servers’ bertambah yang secara inheren akan membuat jauh lebih sulit untuk dapat menerapkan praktik-praktik pengelolaan TI yang baik secara konsisten termasuk pelaksanaan kebijakan-kebijakan, serta proses-proses baku yang sudah ditetapkan sebelumnya. • **Profitabilitas perusahaan dapat terganggu,** karena dapat terjadi redundansi yang disebabkan adanya banyak server di berbagai daerah, atau karena adanya server-server untuk aplikasi yang bersifat identik. Redundansi tersebut mengakibatkan terjadinya kompleksitas yang lebih tinggi sehingga penanganan infrastruktur TI akan lebih sulit dan membutuhkan biaya besar untuk merawatnya.

Risiko #9: Memodifikasi atau mengganti komponen internal komputer (Komputer personal atau laptop atau notebook).

Kejadian atau permasalahan yang dapat timbul	• Untuk memenuhi kebutuhan spesifik beberapa pengguna komputer, kadangkala perusahaan perlu melakukan 'upgrade' beberapa komponen piranti lunak di dalam komputer perusahaan. Untuk hal ini, beberapa karyawan perusahaan (bahkan dapat juga terjadi, departemen TI sendiri yang melakukan) melakukan 'overclocking' atau 'penukaran komponen' (component swapping) yang dapat membuat komputer bekerja lebih cepat atau umurnya menjadi lebih panjang. Akan tetapi (seringkali tidak disadari) hal ini dapat memicu permasalahan yang lebih besar yaitu timbulnya kebutuhan baru bagi semua pengguna akhir (end-users) akan komputer personal/ Lap Top/ Note Book yang lebih kuat dan tinggi spesifikasinya.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun** karena para karyawan yang sibuk mengutak-ngutik komputer akan kehilangan waktu yang seharusnya dapat mereka gunakan untuk melakukan kegiatan atau proses bisnis yang lebih fokus kepada pencapaian hasil atau kinerja bisnis dari fungsi atau peran mereka. • **Keamanan jaringan informasi perusahaan dapat terganggu**, karena teknik-teknik 'overclocking' dan 'component swapping' dapat menjadi celah atau titik lemah, yang akhirnya akan memperlemah platform keamanan TI perusahaan secara keseluruhan. • **Profitabilitas perusahaan dapat terganggu,** karena semakin banyak variasi dari jenis piranti keras dan lunak digunakan oleh perusahaan, semakin tinggi biaya yang diperlukan dalam melakukan penanganan permasalahan dan reparasi TI yang diperlukan. Selain itu, biaya untuk melakukan modifikasi suatu komputer dan merawatnya tidak selalu lebih murah daripada membeli yang baru.

Risiko #10: Membuka alamat email dan beberapa informasi tentang perusahaan melalui jaringan internet publik

Kejadian atau permasalahan yang dapat timbul	• Pada saat seorang karyawan menggunakan alamat email perusahaan mereka melalui jaringan internet publik, alamat email karyawan tersebut akan dengan sangat mudah dicuri oleh perusahaan-perusahaan penghasil SPAM. Lebih buruk lagi, alamat email tersebut juga dapat dicuri oleh individu atau golongan tertentu yang memiliki maksud jahat terhadap perusahaan kita.
Risiko – Dampak terhadap perusahaan	• **Produktivitas karyawan dapat turun** karena kecepatan pengiriman dan pengolahan data dapat terganggu oleh adanya SPAM yang timbul dari adanya jaringan koneksi dengan internet publik. • **Keamanan jaringan informasi perusahaan dapat terganggu**, karena SPAM dapat membuat lingkungan keamanan fasilitas pengolahan informasi menjadi lemah dan dapat diterobos melalui email dari karyawan yang pernah menggunakan fasilitas publik tersebut. Selain itu, email karyawan yang sudah terinfeksi virus dari SPAM akan berpotensi menjadi sumber penyebaran virus ke dalam jaringan teknologi informasi perusahaan secara khusus dan sistem informasi perusahaan secara umum. • **Profitabilitas perusahaan dapat terganggu,** karena perusahaan terpaksa harus menerapkan program anti-spam yang masif dan berbiaya tinggi terutama dalam menghadapi serangan SPAM yang serius dan bertubi-tubi dalam jumlah besar serta dalam frekuensi yang sangat sering.

-oOo-