Implementasi Keamanan Pemanfaatan Teknologi Informasi untuk Usaha Kecil dan Menengah

Hari Murti
Fakultas Teknologi Informasi, Universitas Stikubank Semarang
email : harimurti@unisbank.ac.id

ABSTRAK : Pemakaian perangkat teknologi informasi atau komputer pada UKM bukan tanpa resiko, apalagi jika perangkat tersebut terpasang dalam basis jaringan dan internet. Operasi pemanfaatan teknologi informasi pada UKM dimungkinkan terdapat perbedaan dibanding dengan bisnis dengan skala besar (*enterprise*). Perbedaan pendekatan penerapan TI dilatarbelakangi oleh keterbatasan sumber daya yang dimiliki oleh UKM. Namun keamanan komputer memiliki standar yang harus dipenuhi untuk menjamin keamanannya. Data atau informasi dianggap aman jika memenuhi persyaratan berupa kerahasiaan (*confidentiality*), integrasi (*integraty*), dan Otentikasi (*othentication*). Persyaratan tersebut merupakan bagian dari aspek keamanan yang harus dipenuhi. Model pengendalian resiko dan pembebasan dari bahaya ancaman keamanan terhadap sumber daya informasi dapat dilakukan dengan dua cara yaitu pencegahan (*preventive*) dan penyembuahan atau perbaikan (*recovery/corrective*). Model pengendalian tersebut harus dapat diimplementasikan oleh UKM baik pada bagian *front-office* maupun *back-office*. Upaya perlindungan terhadap perangkat teknologi ionformasi harus dimulai dari atasan (*top manjemen*). Tanpa danya kemauan dari top manajemen maka tidak mungkin system keamanan dapat diimplementasikan. Top manajemen pada UKM dapat memutuskan prioritas manajemen atau manfaat keamanan sistem informasi. Setiap ukuran keamanan yang dirancang manajer usaha kecil dan menengah untuk menjaga keamanan komputer dan sistem informasi UKM harus diterapkan system keamanan secara yang komprehensif terhadap semua system yang berpotensi terhadap hilangnya keamanan computer. Langkah-langkah yang dapat ditempuh untuk pengendalian keamanan berupa pengendalian dan proteksi, melakukan monitoring dan auditing, serta selalu memahami masalah-masalah yang muncul terhadap ancaman dan serangan.

Kata kunci : UKM, implementasi, keamanan, dan pengendalian

PENDAHULUAN

Teknologi informasi (TI) saat ini penggunaanya sudah begitu menyebar dikalangan masyarakat, termasuk pelaku usaha kecil dan menengah (UKM). Pemakaian perangkat teknologi informasi atau komputer bukan tanpa resiko, apalagi jika perangkat tersebut terpasang dalam basis jaringan dan internet. Operasi pemanfaatan teknologi informasi pada UKM dimungkinkan terdapat perbedaan dibanding dengan bisnis dengan skala besar (*enterprise*). Perbedaan pendekatan penerapan TI dilatarbelakangi oleh keterbatasan sumber daya yang dimiliki oleh UKM, terutama terkait dengan kondisi keuangan yang tidak memungkinkan untuk menginvestasikan sejumlah besar modalnya untuk membangun infrastruktur dan aplikasi TI yang canggih termasuk implementasi keamanannya. Berbagai studi tentang pemanfaatan TI pada UKM di Indonesia terdapat temuan-temuan sebagai berikut :

- Kurangnya memperdulikan keamanan sistem informasi, hal ini diakibatkan karena terbatasnya kemampuan sumber daya manusia (SDM) yang menangani bidang tersebut.
- Atau sudah memiliki keamanan, namun masih minimal misalnya bersikap reaktif terhadap masalah keamanan sistem informasi yang muncul.
- Masih belum banyaknya perangkat yang terhubung (jaringan) baik secara local maupun berbasis internet, untuk memperlanjar dan meningkatkan usahanya. Sehingga anggapan bahwa ancaman keamanan sering berasal dari luar organisasi tidak dapat masuk pada system mereka.

- Menganggap bahwa ancaman keamanan semata-mata berupa virus computer.

Sikap-sikap seperti ini justru memicu semakin maraknya masalah-masalah keamanan sistem informasi yang ada pada UKM dan semakin kompleks. Untuk itu perlu adanya pemahaman tentang konsep keamanan secara umum terhadap pemanfaatan teknologi informasi, dan selanjutnya tentang penerapannya terhadap UKM.

Tujuan Keamanan

Tujuan keamanan komputer secara umum adalah mengamankan sumber daya (*resources*) komputer seperti hardware, software, jaringan komunikasi, dan yang paling penting adalah dokumen (data/ informasi). Data atau informasi dianggap aman jika memenuhi persyaratan berupa kerahasiaan (*confidentiality*), integrasi (*integraty*), dan Otentikasi (*othentication*). Persyaratan tersebut merupakan bagian dari aspek keamanan yang harus dipenuhi. Aspek keamanan komputer adalah bentuk pertimbangan yang menyatakan sebuah komputer bisa dinyatakan aman. Begitu pentingnya aspek keamanan dalam teknologi informasi sehingga beberapa perusahaan pengembang software menjadikan keamanan sebagai prioritas bisnisnya.

Syarat keamanan tersebut sangat berkaitan dengan aspek keamanan lain seperti tidak dapat menyangkal (*non-repudatiun*), otoritas (*autority*),ketersediaan (availability), dan kendali akses (*access-control*).

Fungsi Keamanan TI dalam Organisasi

Fungsi keamanan TI dalam organiasi UKM, secara umum hampir sama dengan organisasi perusahaan atau organisasi institusi lainnya, namun dalam implementasi pada skala yang lebih kecil. Untuk beberapa tugas dan fungsi pada organisasi keamanan TI bisanya dilakukan oleh seorang staff. Karena dalam kenyataannya diberbagai organisasi dengan beragam tugas dari tim keamanan TI sering dihadapkan pada kekurangan sumberdaya atau prioritas beban kerja untuk menyelesaikan hanya tugas-tugas yang penting. Namun secara ideal fungsi-fungsi keamanan dalam TI yang dibutuhkan antara lain:

a. Auditor. Auditor bertanggungjawab dalam memeriksa sistem untuk melihat apakah sistem tersebut telah memenuhi kebutuhan keamanan TI. termasuk sistem dan kebijakan organisasi, dan apakah kontrol keamanan TI telah dijalankan dengan benar.

b. Keamanan Fisik. Bagian kemanan fisik biasanya bertanggungjawab untuk mengembangkan dan menjalankan kontrol keamanan fisik yang baik, dengan konsultasi dengan manajemen keamanan komputer.

c. Recovery. Staff keamanan TI harus memiliki *disaster recovery/contingency planning team*. Tim ini bertanggungjawab pada aktifitas *contingency planning* organisasi tersebut dan bekerjasama dengan dengan bagian keamanan fisik, telekomunikasi, IRM, pengadaan barang dan pegawai lainnya.

d. Pengadaan. Bagian pengadaan bertanggungjawab untuk memastikan pengadaan barang dalam organisasi telah ditinjau oleh petugas yang berwenang.

e. Pelatihan. Pelatihan mengenai keamanan TI termasuk dalam kebutuhan keamanan TI. Staff keamanan TI memiliki salah satu tanggung jawab utama untuk memberikan pelatihan kepada user, operator, dan manajer mengenai keamanan komputer.

f. Personalia. Bagian personalia dan staff keamanan TI harus bekerjasama dalam lekaukan investigasi terhadap latar belakang dan, prosedur pemberhentian kerja dari seorang pegawai yang hendak mengundurkan diri. Staff keamanan TI harus familiar terhadap istilah “least privilege access” dan “separation of duties.”

g. Risk Management/Planning**.** Beberapa organisasi memiliki staff yang bertugas mempelajari berbagai tipe resiko yang mungkin dihadapi oleh organisasi. Staff keamanan TI harus mengembangkan proses untuk mengenali resiko yang ada dalam siklus hidup organisasi. Ketika sebuah kelemahan (vulnerabilities) terdeteksi, tim keamanan harus menganalisa resiko dan jumlah sumberdaya yang dibutuhkan untuk menurunkan resiko (mitigate the risk).

h. Building Operations. Bagian pemeliharaan gedung bertanggungjawab dalam memastikan bahwa setiap fasilitas keamanan gedung, daya listrik dan kontrol lingkungan gedung, aman digunakan selama masa operasional organisasi. Staff keamanan TI harus berkoordinasi dengan mereka untuk memastikan bahwa kebutuhan pengamanan lingkungan sistem dan gedung telah terpenuhi.

i. System Management / System Administrators**.** Pegawai ini adalah manajer dan teknisi yang merancang dan mengoperasikan suatu sistem, jaringan komputer dan LAN dari organisasi. Mereka bertanggungjawab dalam mengimplementasikan kemanan teknis dan harus paham terhadap teknologi pengamanan TI yang berhubungan dengan sistem mereka.

j. Telekomunikasi**.** Bagian telekomunikasi bertanggungjawab untuk menyediakan layanan telekomunikasi termasuk telekomunikasi suara, data, video dan layanan faks. Tim harus berkoordinasi dengan bagian ini untuk memenuhi kebutuhan keamanan TI dan meneliti teknologi baru yang berhubungan dengan telekomunikasi serta bentuk-bentuk serangan pada jaringan telekomunikasi.

k. Telekomunikasi**.** Bagian telekomunikasi bertanggungjawab untuk menyediakan layanan telekomunikasi termasuk telekomunikasi suara, data, video dan layanan faks. Tim harus berkoordinasi dengan bagian ini untuk memenuhi kebutuhan keamanan TI dan meneliti teknologi baru yang berhubungan dengan telekomunikasi serta bentuk-bentuk serangan pada jaringan telekomunikasi.

l. Maintenance of Security Program. Yaitu bertugas untuk melakukan backup data secara berkala, melakukan diagnosa seperti defragmentasi, dan sebagainya.

Model Pengendalian Keamanan

Pengendalian resiko dan pembebasan dari bahaya ancaman keamanan terhadap sumber daya informasi dapat dilakukan dengan dua cara yaitu pencegahan (*preventive*) dan penyembuahan atau perbaikan (*recovery/corrective*). Usaha pencegahan adalah usaha yang dilakukan dengan cara memberikan atau memasang tool atau utilitas baik berupa software dan hardware yang dapat terhindar atau kebal terhadap adanya serangan baik yang disengaja maupun tidak disengaja. Misalnya dengan memasang antivirus yang selalu ter-*updating*, pemakaian sistem dan aplikasi dengan pemberian otoritas yang jelas (pemberian *password login*), penyandian dan mengotentikasi dokumen, pemasangan *firewall*, melakukan *backup*, defragmentasi dan sebagainya. Usaha pencegahan tersebut dapat dianalogikan seperti manusia yang ketika baru lahir langsung diberikan berbagai macam imunisasi untuk mencegah atau memperoleh kekebalan terhadap suatu penyakit.

Model pengendalian keamanan juga dapat ditinjau berdasarkan lingkupnya. Lingkup keamanan komputer merupakan tindakan pengamanan komputer yang dilakukan dengan melakukan tinjauan dari sumbar asalnya, dan klasifikasi wujudnya. Ditinjau dari sumber asalnya ancaman keamanan komputer dapat dibagi menjadi ancaman yang berasal dari dalam organisasi (*internal/local attack*), ancaman interface pemakai (*user interface*), dan ancaman keamanan yang berasal dari luar (*eksternal attack*). Sedangkan berdasarkan lubang atau celah keamanan, wujud keamanan dapat diklasifikasikan menjadi empat, yaitu: keamanan fisik, keamanan personal, keamanan akses, dan keamanan jaringan komunikasi.

Manfaat Teknologi Informasi Bagi UKM

Saat ini banyak vendor yang memberikan perhatian kepada UKM terhadap implementasi teknologi Informasi. Perhatian dan optimisme itu tidak saja berhenti sebatas wacana. Mereka bekerja nyata dengan mengeluarkan solusi teknologi informasi untuk perusahaan skala kecil dan menengah. Hampir semua vendor mulai dari penyedia perangkat keras seperti server, komputer, jaringan dan vendor software untuk aplikasi bisnis mempunyai produk yang ditujukan pada UKM. Internal, langkah yang dilakukan para vendor teknologi informasi ini menunjukkan bahwa UKM merupakan pasar yang potensial bagi mereka. Sedangkan secara

umum, langkah ini sekaligus menjadi menjadi bukti optimisme mereka pada eksistensi dan prospek UKM.

Tujuan sekaligus keuntungan utama pemanfaatan teknologi informasi oleh UKM untuk mendapatkan pasar yang lebih luas, bahkan setara dengan perusahaan besar lainnya. Kesempatan ini akan membuat UKM bisa bersaing dalam pasar yang sama dengan perusahaan besar. Selain itu dengan teknologi informasi, UKM juga dapat mempunyai kesempatan beroperasi lebih efisien.

Pemanfaatan TI pada UKM dapat diimplementasikan secara *front-office* maupun *back-office*. *P*enerapan solusi *Customer Relationship Management* (CRM) sebagai fungsi front office, sangat membantu hubungan yang lebih cepat dan lebih baik dengan pelanggan. Pengalaman komunikasi menyenangkan yang diperoleh pelanggan pada saat kontak dengan perusahaan menjadi nilai tambah. Pada banyak kasus, CRM membantu meningkatkan loyalitas pelanggan.

Untuk back office, teknologi informasi meningkatkan efisiensi dalam biaya, alur pekerjaan serta menekan tanggung jawab administrasi yang mesti dilakukan sumber daya manusianya. Dengan dukungan local area network (LAN), wide area network (WAN), dan virtual private network (VPN), tanggung jawab administrasi serta manajemen renumerasi karyawan bisa dilakukan secara online. Karyawan bisa lebih berkonsentrasi pada tanggung jawab pekerjaan yang lebih bersifat strategis, sehingga UKM mempunyai peluang membuat lompatan dalam hal produktivitas.

IMPLEMENTASI KEAMANAN PADA UKM

Motivasi Implementasi Keamanan

Upaya perlindungan terhadap perangkat teknologi ionformasi harus dimulai dari atasan (*top manjemen*). Tanpa danya kemauan dari top manajemen maka tidak mungkin system keamanan dapat diimplementasikan. Top manajemen pada UKM dapat memutuskan prioritas manajemen atau manfaat keamanan sistem informasi dengan mempertanyakan beberapa pertanyaan sebagai berikut berikut:

- Apa manfaatnya menggunakan komputer atau sistem informasi? Apakah untuk kegiatan transaksi pemesanan (pembelian dan penjualan) secara *online*? *Electronic banking*? *Electronic trading*? *E-mail* perusahaan? Apakah anda tahu bagaimana tingkat kematangan keamanan layanan-layanan ini? Apa artinya bagi manajer usaha kecil dan menengah bila akses menggunakan fungsi-fungsi ini diambil alih oleh pihak-pihak yang tidak berwenang? Harus tetap diingat bahwa terdapat faktor-faktor bukan finansial yang dimiliki tiap gangguan atau masalah keamanan sistem informasi. Penyalahgunaan identitas dimanfaatkan oleh *hacker* untuk merusak reputasi pengguna sesungguhnya.
- Bagaimana keterhubungan informasi yang dibangun ? Banyak orang menghubungkan komputer mereka ke internet, selain beberapa orang yang menghubungkan komputer dengan jaringan pribadi seperti akses jarak jauh korporat yang dimiliki perusahaan tempat bekerja.
- Bagaimana komputer-komputer pada UKM terhubung dengan jaringan? Apa komputer tersambung terus menerus pada jaringan atau anda mengendalikan koneksi (dan pemutusan koneksi) komputer anda ke jaringan? Hubungan komputer melalui modem analog telah menjadi satu-satu metode yang tersedia bagi banyak pengguna layanan internet, namun teknologi yang lebih baru seperti DSL dan modem kabel memberikan kemudahan bagi banyak pengguna layanan internet untuk terhubungkan melalui jaringan dengan kecepatan akses lebih tinggi. Penggunaan teknologi-teknologi baru ini memberikan pertimbangan keamanan tertentu.
- Siapa saja yang memiliki akses fisik terhadap komputer pada usaha kecil dan menengah? Apakah manajer memberikan kewenangan bagi orang-orang yang memiliki akses fisik terhadap komputer pada usaha kecil dan menengah untuk menggunakan komputer pada usaha kecil

dan menengah tersebut? Apakah manajer ingin mengendalikan akses yang dimiliki orang-orang ini terhadap komputer pada usaha kecil dan menengah atau layanan-layanan pada jaringan lokal yang dimanfaatkan usaha kecil menengah?

- Siapa yang bertanggungjawab dalam masing-masing tugas yang ada pada implementasi TI pada UKM? karyawan dan manajer usaha kecil dan menengah? Dalam komunikasi data komputer atau saling menukarkan informasi? Apakah karyawan dan manajer membuka *attachment* pada sebuah *e-mail* dari teman? Atau dari seseorang yang tidak dikenal? Bagaimana karyawan dan manajer memilih situs *web* yang aman untuk berbelanja secara *online*?

Motivasi organisasi terhadap keamanan teknologi informasi pada UKM menjadi tanggung jawab bersama sesuai dengan peran masing-masing yaitu :

- Pemilik, merupakan peran yang membuat suatu data pada sistem informasi pada usaha kecil dan menengah.
- Penanggung jawab, merupakan peran yang bertanggung jawab untuk menjaga dan merawat integritas data sistem informasi pada usaha kecil dan menengah.
- Pengguna, merupakan peran yang memanfaatkan data untuk melaksanakan suatu proses bisnis di usaha kecil dan menengah.

Tujuan Perlindungan keamanan UKM

Keamanan sistem informasi merupakan upaya manajemen. Manajemen keamanan sistem informasi dapat diterapkan dengan baik bila top manjemen UKM mengetahui beberapa hal dasar keamanan sistem informasi UKM, kebijakan keamanan yang perlu dikembangkan dan perbedaan metode terutama digunakan untuk menganalisa resiko keamanan sistem informasi. Upaya perlindungan terhadap keamanan teknologi informasi harus diketahui terlebih dahulu tentang tujuan dari keamanan pada UKM.

Tujuan keamanan komputer dan perlindungan sistem informasi pada usaha kecil dan menengah adalah:

1. Memberikan pengetahuan tentang manfaat implementasi keamanan computer pada perangkat teknologi informasi yang digunakan pada UKM
2. Menumbuhkan tingkat kesadaran tentang pentingnya implementasi keamanan kepada UKM.
3. Memberikan metode praktis upaya memperoleh keamanan komputer dan system nformasi bagi UKM, termasuk pertimbangan ekonomi upaya keamanan komputer.
4. Membimbing pelaksanaan upaya memperoleh keamanan komputer dan system informasi pada usaha kecil dan menengah.
5. Terciptanya system teknologi informasi yang andal, terbebas dari masalah keamanan pada UKM.

Kebijakan Implementasi Keamanan pada UKM

Setiap ukuran keamanan yang dirancang manajer usaha kecil dan menengah untuk menjaga keamanan komputer dan sistem informasi UKM harus diterapkan system keamanan secara yang komprehensif terhadap semua system yang berpotensi terhadap hilangnya keamanan computer. Penerapan system keamanan berlapis tersebut harus sesuai dengan standar operasi keamanan yang ada agar prinsip kemanan dapat berlangsung secara optimal.

Untuk menjamin keamanan operasional tidak hanya bicara teknologi pelindungnya, tetapi kebijakan yang jelas dalam melakukan kemanan operasional adalah sangat penting untuk dapat dijalankan dengan baik karena ancaman yang paling tinggi pada prakteknya adalah dari sumber daya internal sendiri. Hal ini adalah ancaman yang sebenarnya sangat mengancam dan sulit untuk diperkirakan, karena internal sumber daya sudah ada di dalam sistem itu sendiri. Dalam rangka meminimalisasi ancaman ini maka kebijakan untuk keamana operasional harus dibuat dengan sedetail mungkin

memperkirakan hal-hal yang dapat menjadi ancaman, dan melakukan prosedur – prosedur keamanan dengan konsekwen. Jadi tanpa kebijakan dan prosedur yang baik maka tidak hanya ancaman dari luar yang menakutkan tetapi juga lebih menakutkan ancaman dari dalam. Untuk itu setiap divisi teknoogi informasi harus punya kebijakan untuk *corporate user* dalam menggunakan sumber daya teknologi informasi yang dipunyai.

Operasional yang baik dengan teknologi yang canggih dan sumber daya yang handal tanpa adanya keamanan yang maksimal menjadi sesuatu yang tidak begitu berarti karena tanpa keamanan berarti hanya membuka pintu untuk bencana bagi informasi dan asset yang dimiliki. Untuk itu system keamanan harus diterapkan sesuai dengan standar operasi berupa pengendalian dan proteksi (*control and protection*), monitoring dan auditing, serta pemahaman tentang ancaman dan *vulnerability*.

Pengendalian dan Proteksi

Tujuan dari kontrol dan proteksi dalam *operations security* adalah menjamin terlaksananya *Confidentiality*, *Intergity*, dan *Avaibility*. Tujuan tersebut dapat dilakukan sebagai berikut :

- *Preventive control* dirancang untuk menekan tingkat kesalahan dan tingkat kerusakan dari kesalahan-kesalahan yang tidak disengaja yang masuk ke dalam sistem. Ini juga dilakukan untuk mencegah masuknya *intruder* (yang tidak berhak) baik dari dalam maupun dari luar untuk menggunakan sistem.
- *Corrective control* memulihkan keadaan yang diakibatkan oleh aktivitas yang tidak berwenang atau mengembalikan kondisi ke keadaan semula sebelum pelanggaran terjadi. Tindakan ini juga digunakan untuk membantu mengurangi dampak yang terjadi dari waktu kejadian kesalahan sampai dengan data prosedur perbaikannya. Kegiatan ini dapat digunakan untuk melakukan pemulihan setelah terjadinya kerusakan.
- *Detective control* digunakan untuk mendeteksi suatu kesalahan pada saat ketika akan terjadi. *Detective control* dapat menggunakan fakta-fakta yang sudah terjadi untuk melakukan pelacakan terhadap transaksi yang tidak berhak yang dapat digunakan sebagai alat penahan. Kegiatan ini bertujuan pula untuk menekan dampak dari kesalahan karena dapat mengindetifikasikan suatu kesalahan dengan cepat. Contoh: *Audit trail*, jika terjadi sebuah kejahatan melalui sistem, maka proses investigasi dapat dilakukan melalui penelusuran sistem log. Temuan yang didapat dapat digunakan sebagai barang bukti untuk diproses lebih lanjut.
- *Deterrent control* digunakan untuk merujuk kepada suatu kepatuhan (*compliance*) dengan peraturan-peraturan eksternal maupun regulasi-regulasi yang ada. Contoh: penerapan standar *business practice* yang berlaku secara internasional, yaitu penerapan SWIFT (*Society for the Worldwide Interbank Financial Telecommunication*) pada dunia perbankan, dimana semua bank koresponden SWIFT harus menerapkan standar yang telah ada untuk menjamin *interoperability* antar bank.
- *Application control* adalah pemindaian secara terus menerus terhadap sistem operasi dan aplikasi untuk mendeteksi perilaku tidak normal. Perilaku tidak normal ini berkaitan dengan penyalahgunaan dari karyawan, penyusup dari luar, virus, dan *worm*. Sebagian besar kontrol ini dilakukan dengan memonitor *software* yang melakukan *call* ke kernel sistem operasi dari *host computer* dan memungkinkannya untuk "melihat" serangan ketika serangan tersebut terjadi pada *host computer*.
- *Transaction control* digunakan dalam melakukan kegiatan kontrol dalam setiap tahap transaksi yang dimulai dari inisiasi, dokumentasi, *testing* dan manajemen perubahan.
- Separation and Rotation of Duties. *Separation and rotation of duties* merupakan kegiatan yang membedakan suatu tugas dengan pemisahan orang sehingga diharapkan tidak ada orang yang menguasai sistem secara keseluruhan. Kegiatan ini

berhubungan dengan konsep *least privilege*. Sedangkan rotasi dilakukan untuk meminimalkan terjadinya KKN dalam pelaksanaan kegiatan operasional.

Monitoring and Auditing

Setelah dilakukan pengaturan dan proteksi yang baik maka tidak bisa hanya berhenti untuk bisa melakukan proteksi tetapi tetap diperlukan monitoring and auditing untuk bisa mengetahui dan menjamin sejauh mana keamanan yang sudah dicapai, faktor yang harus diperhatikan adalah *Change management*, *Escalation management*, *Record retention*, *Due dilligince*, dan *Logging monitoring*.Dengan melakukan hal-hal diatas yang lebih bersifat prosedur maka pengawasan keamanan dapat lebih ditingkatkan.

- *Change Management.* Sebuah proses untuk mengelola perubahan proses bisnis atau *policy* organisasi yang memberikan dampak langsung kepada Sistem Informasi dimana terdapat kebutuhan untuk melakukan perubahan pada sistem yang sudah ada. Untuk melakukan manajemen perubahan maka dibentuk suatu tim dari perwakilan pengguna, *business line* manager dan *Infromation Technology admin* untuk mengotorisasi tiap perubahan.
- *Escalation Management.* Sebuah tahapan yang dibutuhkan untuk menangani sebuah keputusan/masalah secara berjenjang sesuai dengan kompleksitas dari keputusan /masalah yang dihadapi. Eskalasi dilakukan mulai dari struktur organisasi yang paling rendah, untuk kemudian dibawa ke struktur yang lebih tinggi. Jika masalah belum dapat ditangani, ataupun jika dibutuhkan sebuah proses otorisasi dari orang yang mempunyai wewenang lebih tinggi.
- *Record retention* adalah suatu catatan yang berupa daftar yang berisi informasi tentang berapa lama suatu dokumen dipertahankan. Beberapa dokumen dipertahankan untuk waktu tertentu karena alasan hukum, sementara yang lainnya berdasarkan pertimbangan-pertimbangan praktis.
- *Due Dilligince.* Memastikan langkah-langkah tertentu sudah dilakukan untuk melakukan operasional dengan baik. Proses investigasi dilakukan oleh pihak yang tidak berkepentingan/netral atas nama pihak yang akan melakukan transaksi bisnis.
- *Logging Monitoring*. Sistem yang baik menggunakan suatu cara untuk melakukan pencatatan terhadap aktifitas baik dalam sistem maupun *checklist* operasional. Pencatatan ini berlangsung secara terus menerus dan tersimpan dalam sistem.

Thread and Vulnerabilties

Berisi pemahaman tentang jenis ancaman dan kelemahan yang dapat mengancam operasional keamanan yang sudah dilakukan. Untuk *threat* dan *vulnerability* beberapa hal yang akan dibahas adalah *Accidental Loss*, *Inappropriate Activities*, *Illegal computer operations*, *Account maintenance*, *Data Scavenging Attacks*, *IPL/rebooting*, dan *Network highjacking*.

- *Accidental Loss. Accidental threats* terkait dengan kesalahan dan penghilangan, kesalahan, dan penghilangan yang dilakukan oleh karyawan atau orang dalam adalah penyebab utama dari masalah keamanan informasi.
- *Inappropriate activity* adalah aktivitas dalam pemakaian komputer yang sekedar penyalahgunaan biasa sampai yang termasuk tindak kriminal. Penggunaan yang tidak sesuai mencakup aktivitas yang luas. Sebagai contoh adalah pada sisi yang satu karyawan melakukan belanja *online* pada jam kerja, dan pada sisi lainnya, bisa terjadi aktivitas kriminal seperti menjual rahasia perusahaan.
- *Illegal Computer Operations*. Aktifitas komputer yang diangap sebagai kesengajaan dan ketidaksahan aktivitas komputer untuk keuntungan keuangan pribadi dan untuk penghancuran.
- *Data Scavenging Attacks. Data scavenging* adalah teknik penambahan data infromasi dari bit data yang ditemukan.
- *Maintenance Account*. Biasanya dalam sistem ada *account* untuk *maintenance* seperti *administrator* atau *root*, seringkali pengguna sistem lupa untuk mengubah *account* ini dari *default* yang ada pertama

kali, sehingga dapat mudah sekali ditebak oleh user yang tidak terotorisasi atau pun orang luar sangat memungkinkan sekali masuk dalam sistem.

- *IPL/Rebooting*. Permulaan setiap sistem selalu dapat memberikan kelemahan, pada saat IPL (*Initial Program Load*), seorang operator dapat saja menjalankan program, data yang tidak terotorisasi, bahkan mereset sistem.
- *Network Address Hijacking. Intruder* selalu saja dapat merubah *route* dari *traffic data* dari server, jaringan ke *personal machine*, baik dengan modifikasi alamat perangkat ataupun *network address "hijacking"*, dengan melakukan ini *intruder* dapat saja melakukan analisis data ataupun modifikasi atau mencuri *password* dari server.

KESIMPULAN

Perangkat teknologi informasi sangat mendukung peningkatan usaha pada usaha kecil dan menengah (UKM). Permasalahan utama yang selama ini ada pada UKM dalam memanfaatkan perangkat teknologi informasi adalah diabaikannyan pengendalian keamanannya. Untuk itu perlu diterapkan system keamanan yang memadai pada UKM, yaitu system keamanan yang memenuhi standar keamanan yang ada agar system dapat dilakukan pengendalian keamanan secara optimal. Dalam sebuah organisasi termasuk UKM standar yang perlu diimplementasikan dalam system keamanan komputernya meliputi pengendalian dan proteksi, monitoring dan auditing, serta mengetahui bentuk ancman dan lubang kemananan yang lemah terhadap serangan, sehingga proses pengendalian keamanan dapat diterapkan secara maksimal.

DAFTAR PUSTAKA

1. Argabudhi S, dkk, 2005, "*Operation Security*", UI Jakarta
2. Brenton C., dan Hunt C., 2003, "*Network Security*", Elex Media, Jakarta.
3. http://www.korantempo.com/news/2002/8/16/Ekonomi/
4. Praharja A.P, dan Jeffry O.A.A, 2005, "*Praktek Manajemen Keamanan Komputer Pada UKM*", UI, Jakarta
5. Supriyanto A., 2003, "*Analisis Keamanan Pada jaringan Komputer PT. Texmaco Kaliwungu Kendal*, Unisbank Semarang
6. Supriyanto A., 2005, "*Pengantar Teknologi Informasi*", Salemba, Jakarta