AUDIT KEAMANAN INFORMASI
(Studi Kasus Perusahaan Manufaktur)

Eddy Setiawan Wibowo

Teknik Informatika, Fakultas Teknologi Industri
Universitas Langlangbuana
eddy@informatika.unla.ac.id, eswibowo@gmail.com,

ABSTRAK

Saat ini mayoritas proses pengelolaan administrasi dan bisnis di perusahaan telah menggunakan sistem elektronik yang menyimpan begitu besar informasi secara digital dan menggunakan jalur atau jaringan teknologi informasi dalam berkomunikasi. Kegiatan bisnis dan administrasi begitu bergantung pada teknologi informasi yang digunakan. Oleh karena itu, suatu hal yang penting untuk memahami dan mengimplementasikan keamanan sumberdaya informasi pada sistem informasi yang digunakan perusahaan. Penerapan keamanan sumberdaya informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun non-teknis seperti faktor ketersediaan (*availability*), kerahasiaan (*confidentiality*), dan kesatuan (*integrity*).

Penelitian ini membahas mengenai suatu aktifitas audit keamanan informasi pada suatu perusahaan berbasis manufakturing teknologi tinggi

Kata Kunci : audit, keamanan informasi

1. PENDAHULUAN

Pada saat ini sebagian besar proses pengelolaan administrasi dan bisnis di perusahaan telah menggunakan sistem elektronik yang menyimpan begitu besar informasi secara digital dan menggunakan jalur atau jaringan teknologi informasi dalam berkomunikasi. Dengan kata lain, kegiatan bisnis, administrasi bergantung pada teknologi informasi yang digunakan. Oleh karena itu, suatu hal yang penting untuk memahami dan mengimplementasikan keamanan sumberdaya informasi pada sistem informasi yang digunakan perusahaan. Penerapan keamanan sumberdaya informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun non-teknis seperti faktor ketersediaan (*availability*), kerahasiaan (*confidentiality*), dan kesatuan (*integrity*).

Perusahaan memiliki sederetan tujuan dengan diadakannya sistem informasi yang berbasis komputer. Oleh karena itu, perusahaan menuntut agar diciptakannya sistem keamanan terhadap *hardware* maupun *software*-nya. Tujuan dari pengamanan adalah untuk meyakinkan integritas, kelanjutan, dan kerahasiaan dari pengolahan data. Keuntungan dengan meminimalkan risiko harus diimbangi dengan biaya yang

dikeluarkan untuk tujuan pengamanan ini. Biaya untuk pengamanan terhadap keamanan sistem komputer harus wajar. Perusahaan harus dapat mengurangi risiko dan memelihara keamanan sistem komputerisasi pada suatu tingkatan/ level yang dapat diterima.

Audit keamanan informasi merupakan bagian dari setiap manajemen keamanan informasi yang sukses. Audit keamanan informasi merupakan suatu alat atau perangkat dalam menentukan, mendapatkan, dan mengelola setiap level keamanan dalam organisasi.

2. SASARAN DAN TUJUAN

Sasaran dari kegiatan audit ini adalah :

1. Menilai sistem / prosedur serta pengendalian internal
2. Menilai kepatuhan terhadap ketentuan yang berlaku
3. Tujuan dari kegiatan audit Keamanan Sumberdaya Informasi adalah:
4. Menilai sistem pengendalian intern terhadap keamanan informasi;
5. Memeriksa kesesuaian dari mulai kebijakan, bakuan, pedoman, dan prosedur keamanan yang ada;
6. Mengidentifikasi kekurangan dan memeriksa efektifitas dari kebijakan, bakuan, pedoman, dan prosedur keamanan yang ada;
7. Mengidentifikasi dan memahami kelemahan (*vulnerability*) yang ada;
8. Mengkaji kendala keamanan yang ada terhadap permasalahan operasional, administrasi, dan manajerial, dan memastikan kesesuaian dengan bakuan keamanan minimum;
9. Memberikan rekomendasi dan aksi perbaikan/koreksi untuk peningkatan.

3. METODOLOGI

Metodologi audit yang digunakan selama audit Keamanan Sumberdaya Informasi adalah:

1. Wawancara (pertanyaan verbal)
2. Inspeksi visual suatu sistem, lokasi, ruang, dan objek
3. Observasi
4. Analisis file/berkas (termasuk data elektronik)
5. Pemeriksaan teknis (misal menguji sistem alarm, sistem kontrol akses, aplikasi)

6. Analisis Data (misal *log files*, evaluasi database, dll)
7. Pertanyaan tertulis (misal, kuesioner).

Kegiatan ini dilakukan dengan tujuan utamanya untuk membandingkan seberapa jauh persyaratan klausul-klausul pada Prosedur Administrasi Nomor: 85-AP-001 dan pada ISO 27001 telah dipenuhi, baik pada aspek kerangka kerja (kebijakan dan prosedur) maupun aspek penerapannya.

Pertimbangan digunakannya ISO 27001 terkait dengan rencana Unit Pengelola IT yang akan menerapkan standar ini dalam IT Master Plannya dan standar ini fleksibel dikembangkan sesuai dengan kebutuhan organisasi, tujuan organisasi, persyaratan kemananan. Untuk implementasi di Indonesia sudah diadopsi ke SNI ISO 27001 dan menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara nasional dan internasional.

Kriteria dan standar yang dipergunakan sebagai acuan dalam audit adalah:

1. Prosedur Administrasi Nomor: 85-AP-001 tanggal 28 September 2014 perihal Pengamanan Sumberdaya Informasi; (Prosedur Internal)
2. International Standard ISO/IEC 27002:2005. Information Technology - Security Techniques - Code of Practice for Information Security Controls.

4. TEMUAN

Secara ringkas, temuan pada aktifitas audit ini adalah sebagai berikut:

1. Perusahaan telah menetapkan kebijakan dan prosedur pengamanan sumberdaya informasi, namun sosialisasinya masih terbatas pada karyawan baru
2. Belum adanya klausul penekanan keamanan informasi pada perjanjian kontrak dengan pihak ketiga
3. Belum dilakukan pengujian *restore and recovery procedure* menggunakan data hasil backup dari media backup secara berkala
4. Belum adanya prosedur pembuangan atau penggunaan kembali peralatan secara aman
5. Belum ada dokumen kajian kebutuhan lisensi *software* untuk masing-masing unit kerja
6. Fasilitas email publik seperti Yahoo Mail dan GMail digunakan untuk korespondensi kedinasan

7. Belum ada anti virus, update anti virus maupun *update operating system* (OS) secara periodik pada *computer client*
8. Komputer *client* yang masuk jaringan komunikasi data internal tidak harus terdaftar
9. Audit Trail/Log SAP belum diamankan dengan baik
10. Potensi kebocoran informasi maupun penyerangan dari jalur internet lain di luar yang sudah disediakan oleh Unit Pengelola IT

5. TEMUAN DETIL

Berdasarkan hasil audit, ada sejumlah temuan yang cukup penting untuk ditindak lanjuti. Temuan-temuan tersebut yaitu sebagai berikut.

1. Perusahaan telah menetapkan kebijakan dan prosedur pengamanan sumberdaya informasi, namun sosialisasinya masih terbatas pada karyawan baru

   Perusahaan telah menetapkan kebijakan dan prosedur pengamanan sumberdaya informasi, yaitu:

   a. Kebijakan Perusahaan Nomor: 00-PTD-15B perihal Teknologi Informasi;
   b. Kebijakan Perusahaan Nomor: 00-PTD-20B perihal Pengamanan;
   c. Kebijakan Perusahaan Nomor: 85-KP-002 perihal Pelayanan Informasi Publik
   d. Prosedur Administrasi Nomor: 85-AP-001 tentang Pengamanan Sumberdaya Informasi.

   Dokumen kebijakan keamanan informasi yang telah disetujui oleh manajemen sebaiknya dipublikasikan serta dikomunikasikan kepada semua pekerja dan pihak-pihak yang terkait. Saat ini program pelatihan dan sosialisasi untuk meningkatkan kesadaran dan komitmen terhadap keamanan informasi terbatas pada karyawan baru.

   Karyawan diwajibkan “melek” keamanan sistem informasi. Mereka harus mengetahui dan dapat membayangkan dampak apabila peraturan keamanan sistem informasi diabaikan.

   Semua manajer bertanggungjawab untuk mengkomunikasikan kepada semua bawahannya mengenai pengamanan yang dilakukan di perusahaan dan meyakinkan bahwa mereka mengetahui dan memahami semua peraturan yang diterapkan di perusahaan dan bagiannya.

Di lain pihak setiap pegawai bertanggungjawab dan harus mematuhi peraturan keamanan informasi yang diterapkan dan dianut oleh perusahaan.

Sosialisasi terkait keamanan informasi dapat mencakup dan tidak terbatas pada :

a. Kebijakan terkait keamanan informasi
b. Prosedur dan peraturan tentang keamanan informasi
c. Pengamanan fisik sumber daya informasi
d. Pengklasifikasian informasi
e. Informasi yang disediakan untuk Publik
f. Peraturan disiplin dan tata tertib karyawan
g. Pengamanan data oleh setiap karyawan, misalnya:
    - Tanggung jawab pemakaian user id dan pengamanannya
    - *File sharing*
    - Anti virus dan penanganan virus
    - Transmisi informasi yang sensitif dalam keadaan terenkripsi
    - *Setting timeout pada screen saver*
    - Pengembalian seluruh hak milik perusahaan yang berkaitan dengan data pada saat putusnya hubungan kerja
    - Tidak menginstal S/W yang tidak berhubungan dengan pekerjaan
    - Melaporkan kelemahan sistem yang diketahui

Rekomendasi:

Divisi Human Development (HD), Divisi Pengamanan, Sekretaris Perusahaan dan Divisi Information Technology (IT) agar merencanakan dan mengadakan program pelatihan serta sosialisasi keamanan informasi ke seluruh karyawan untuk meningkatkan kesadaran dan komitmen terhadap keamanan informasi.

2. Belum adanya klausul penekanan keamanan informasi pada perjanjian kontrak dengan pihak ketiga.

Dalam kegiatannya, perusahaan dapat melakukan kerjasama atau mempekerjakan pihak lain di luar karyawan tetap perusahaan. Pihak lain ini, yang sering disebut sebagai pihak ketiga, mencakup tapi tidak terbatas pada perusahaan lain, tenaga ahli / technical assistant, dan mahasiswa kerja praktek (KP) / penelitian.

Apabila ada pihak ketiga yang melakukan pekerjaan di perusahaan, maka perusahaan maupun informasi milik perusahaan harus dilindungi keamanannya. Di dalam kontrak harus didefinisikan agar pihak ketiga mematuhi peraturan dan keamanan informasi perusahaan. Manajemen harus bertanggungjawab agar pihak ketiga mematuhi dan mengikuti peraturan keamanan yang telah dirumuskan.

Perjanjian dengan pihak ketiga yang meliputi pengaksesan, pengolahan, pengkomunikasi, pengelolaan dan penyebaran informasi perusahaan harus memenuhi persyaratan keamanan informasi perusahaan``.

Dari beberapa kontrak yang dipelajari oleh auditor, belum ada klausul penekanan keamanan informasi. Ketiadaan klausul penekanan keamanan informasi mengakibatkan rentannya keamanan informasi/rahasia perusahaan dari pihak lain.

Rekomendasi:

Divisi Pengadaan dan Fasilitas berkoordinasi dengan Sekretariat Perusahaan, agar dalam membuat perjanjian kontrak dengan pihak ketiga, juga memasukkan klausul tentang keamanan informasi.

3. Belum dilakukan pengujian restore and recovery procedure menggunakan data hasil backup dari media backup.

Dari prosedur dan aktifitas backup yang diperiksa oleh auditor, saat ini proses backup sudah dilakukan secara rutin / setiap hari. Backup disimpan pada media backup yang berlokasi di dua lokasi yang berbeda (gedung PKN dan strong room gedung GPM). Keberhasilan proses backup dan integritas file backup ditandai dengan munculnya icon centang hijau pada tools backup yang digunakan.

Walaupun begitu, auditor belum melihat adanya dokumentasi untuk menguji kelengkapan file maupun prosedur restore. Ketiadaan dokumentasi pengujian seperti ini berpotensi kurang suksesnya proses restore pada saat timbulnya permasalahan di kemudian hari.

Rekomendasi:

Unit Pengelola IT agar membuatkan dokumentasi pengujian secara berkala prosedur recovery menggunakan data hasil backup dari media backup.

4. Belum adanya prosedur pembuangan atau penggunaan kembali peralatan secara aman

   Seluruh item atau peralatan yang memuat media penyimpanan harus diperiksa untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa (overwritten) secara aman sebelum dibuang.

   Saat ini belum ada prosedur pembuangan atau penggunaan kembali peralatan secara aman. Ketiadaan prosedur pembuangan atau penggunaan kembali peralatan ini berpotensi mengakibatkan adanya informasi pada media penyimpanan tersebut yang bisa diakses oleh pihak yang tidak berhak.

   Rekomendasi:

   Unit Pengelola IT agar membuatkan prosedur pembuangan atau penggunaan kembali peralatan informasi secara aman.

5. Belum ada kajian kebutuhan lisensi software

   Berdasarkan ISO27000 tentang kesesuaian dengan persyaratan hukum, prosedur yang sesuai harus diterapkan untuk memastikan kesesuaian dengan peraturan hukum, peraturan perundang-undangan dan persyaratan kontrak tentang penggunaan materi berkenaan dengan HAKI di mana mungkin terdapat hak kekayaan intelektual dan tentang penggunaan produk perangkat lunak yang memiliki. Setiap software yang diinstal pada perangkat perusahaan harus memiliki lisensi yang sah.

   Dari hasil audit yang dilakukan Microsoft tanggal 2 — 5 Februari 2015, ditemukan instalasi sofware pada sejumlah PC dan laptop milik perusahaan tanpa dilengkapi dengan lisensi yang sah. Hal ini terjadi walaupun direksi telah mengeluarkan surat edaran Nomor SE/016/030.02/DU0000/PTD/12/2014 tertanggal 15 Desember 2014 tentang Kewajiban Menggunakan Software Legal pada Computer Client milik perusahaan.

   Tidak lengkapnya lisensi atas software-software yang telah diinstal pada perangkat perusahaan dapat mengakibatkan denda lisensi dari prinsipal software maupun ancaman hukuman pidana berdasarkan Undang-undang HAKI.

Saat ini tidak diketahui kebutuhan riil lisensi software di perusahaan. Hal ini disebabkan karena belum adanya dokumentasi kajian kebutuhan lisensi software untuk masing-masing unit kerja.

Belum adanya dokumen kajian ini dapat mengakibatkan perusahaan merencanakan pembelian lisensi software secara tidak tepat.

Rekomendasi:

Unit Pengelola IT mengkoordinir pembuatan kajian kebutuhan lisensi software di masing-masing unit kerja di perusahaan.

6. Fasilitas email publik seperti Yahoo Mail dan Google Mail digunakan untuk korespondensi kedinasan.

   Fasilitas email publik seperti Yahoo Mail dan Google Mail memiliki sejumlah resiko keamanan namun masih digunakan untuk korespondensi kedinasan. Sejumlah vulnerabilities yang telah ditemukan diantaranya pada :

   a. Paparan email; sumber :
      - http://www.tripwire.com/state-of-security/latest-security-news/gmail-vulnerability-could-have-exposed-every-email-address/
      - Credential untuk login; sumber :
      - http://www.tripwire.com/state-of-security/latest-security-news/researcher-discovers-serious-gmail-account-recovery-vulnerability/
      - http://thenextweb.com/insider/2013/03/06/despite-its-efforts-to-fix-vulnerabilities-yahoos-mail-users-continue-reporting-hacking-incidents/

   b. *Reset Password*; sumber :
      - http://www.hackersnewsbulletin.com/2013/11/vulnerability-gmail-allows-reset-password-account.html

   c. XSS Vulnerabilities; sumber :
      - http://www.acunetix.com/blog/articles/xss-vulnerability-injected-google-analytics-executed-ioss-gmail-application/

- http://thenextweb.com/insider/2013/01/31/yahoo-mail-users-still-seeing-accounts-hacked-via-xss-exploit-amid-reports-yahoo-failed-to-fix-old-flaw/

d. Pemalsuan Identitas Nama; sumber : http://www.gohacking.com/closer-look-at-vulnerability-in-gmail/

Penggunaan email publik dan bukannya fasilitas perusahaan disebabkan diantaranya karena :

a. *Space* email perusahaan terbatas.
   Space email perusahaan yang disediakan tidak sebesar space pada email publik. Saat ini email perusahaan dialokasikan terbatas 350 MB per akun email untuk keseluruhan folder email seperti inbox, sent, draft, saved, dll.
b. Batasan ukuran *attachment* email.
   Attachment yang bisa disertakan pada email di email perusahaan tidak sebesar attachment pada layanan email publik. Saat ini limit attachement email perusahaan adalah 10MB.
c. Belum ada sosialisasi penggunaan email perusahaan untuk korespondensi kedinasan.
   Saat ini juga tidak ada *disclaimer standard* pada *footer* email yang dikirim menggunakan fasilitas email perusahaan.

Rekomendasi:
Unit Pengelola IT agar :

a. mensosialisasikan penggunaan email perusahaan untuk korespondensi kedinasan
b. memberikan secara otomatis disclaimer pada footer email perusahaan
c. memperbesar space email dan limit attachment

7. Belum ada anti virus, update anti virus maupun update operating system (OS) secara periodik pada computer client.

Saat ini belum ada software anti virus, update anti virus maupun update operating system yang disediakan oleh perusahaan untuk PC atau laptop perusahaan.

Ketiadaan software anti virus, update anti virus maupun operating system update yang disediakan perusahaan berpotensi menyulitkan pengguna dalam mengamankan peralatan kerja komputernya dari serangan virus, hacking, maupun vulnerability lainnya

Rekomendasi:

Unit Pengelola IT agar menyediakan di salah satu portal perusahaan, software anti virus, update anti virus dan update operating system, serta menyosialisasikan aplikasi updatenya ini.

8. Komputer client yang masuk jaringan komunikasi data internal tidak harus terdaftar.

Dalam Prosedur Administrasi 85-AP-001 dinyatakan bahwa semua komputer client yang akan masuk ke jaringan komunikasi perusahaan harus terdaftar sebelumnya.

Saat ini komputer client tidak harus terdaftar terlebih hulu di Unit Pengelola IT sebelum dapat masuk pada jaringan komunikasi data internal perusahaan. Dengan menggunakan laptop pribadi, setiap orang dapat menghubungkan laptopnya dengan kabel jaringan perusahan untuk langsung mengakses jaringan perusahaan.

Digunakannya teknologi Dynamic Host Configuration Protocol (DHCP) lebih memudahkan proses akses jaringan perusahaan karena laptop/perangkat baru tersebut langsung mendapatkan IP Address tanpa perlu mendaftar dahulu ke Helpdesk Unit Pengelola IT.

Kondisi saat ini tidak sesuai dengan apa yang tertulis di Prosedur Administrasinya.

Rekomendasi:

Unit Pengelola IT agar mereview Prosedur Administrasi ini, khususnya relevansi klausul ini terhadap teknologi yang digunakan saat ini.

9. Audit Trail/Log SAP belum diamankan dengan baik.

Berdasarkan Prosedur Administrasi 85-AP-001 tentang Pengamanan Sumber Daya Informasi, point 5.e., dinyatakan bahwa "Setiap aktivitas user (pengguna) dicatat dalam Log Trail Field".

Dari observasi didapatkan bahwa Log aktifitas user SAP untuk bulan Desember 2014 dan Januari 2015 tidak ada.

Menurut penjelasan dari pengelola sistem SAP, ketiadaan Log untuk kedua bulan tadi disebabkan oleh Log Service yang terlewat dinyalakan pada saat maintenance rutin sistem.

Hilang atau ketiadaan suatu Log Aktifitas merupakan kelemahan sistem/prosedur serta tidak diketahuinya aktifitas user pada waktu yang bersangkutan.

Rekomendasi:

Unit Pengelola IT agar melakukan :

a. Pembuatan Manual Instruksi *Maintenance* Sistem SAP
b. Pemantauan rutin aktifitas pengamanan Audit Trail agar hal seperti ini tidak terjadi lagi.

10. Potensi kebocoran informasi maupun penyerangan dari jalur internet lain di luar yang sudah disediakan oleh Unit Pengelola IT

Keluar masuknya data sebaiknya difilter atau dimonitor. Data yang tidak difilter atau dimonitor berpotensi menjadi titik kelemahan / kebocoran informasi atau menjadi asal penyerangan .

Saat ini terdapat sejumlah jalur internet di luar yang disediakan oleh Unit Pengelola IT. Belum ada standar pengamanan jalur internet. Pengamanan bergantung pada kemampuan masing-masing individu sysadmin.

Rekomendasi:

Unit Pengelola IT agar membuat prosedur administrasi untuk pengamanan jalur internet lain.

6. SARAN UMUM

Ada beberapa saran yang diusulkan yang berhubungan dengan keamanan sumber daya informasi sebagai berikut.

Pertama, saat ini di perusahaan terdapat layanan email, portal internal, SAP, fasilitas informasi maupun aplikasi lainnya. Sementara itu hingga saat ini belum ada fasilitas Single Sign On (SSO) maupun Directory Service.

Teknologi SSO adalah teknologi yang mengizinkan pengguna jaringan agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja. Teknologi ini sangat diminati, khususnya dalam jaringan yang sangat besar dan bersifat heterogen (di saat sistem operasi serta aplikasi yang digunakan oleh komputer adalah berasal dari banyak vendor, dan pengguna dimintai untuk mengisi informasi dirinya ke dalam setiap platform yang berbeda tersebut yang hendak diakses oleh pengguna). Dengan menggunakan SSO, seorang pengguna hanya cukup melakukan proses autentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan yang terdapat di dalam jaringan.

SSO mempunyai sejumlah manfaat diantaranya:

1. Mengurangi kesulitan user dalam mengingat user ID dan password-nya untuk setiap situs/aplikasi
2. Mengurangi banyaknya entrian login untuk masuk ke masing-masing situs/aplikasi
3. Mengurangi kerumitan layanan TI dalam mengelola, khususnya mereset, password user

Unit Pengelola IT sebaiknya mulai mengkaji dan mengimplementasikan penggunaan Single Sign On maupun Directory Service untuk mempermudah pengelolaan dan meningkatkan pengamanan sistem perusahaan.

Kedua, sebaiknya ada contingency plan yang dituangkan dalam bentuk Dokumen Contingency Plan. Contingency Plan merupakan suatu perencanaan yang dibuat untuk mengantisipasi hal-hal/ musibah yang kemungkinan jarang terjadi tetapi memiliki konsekuensi yang besar jika sampai terjadi. Contingency Plan memungkinkan organisasi untuk menyelaraskan usahanya dalam merespon suatu keadaan darurat.

7. DAFTAR PUSTAKA

J.A. Hall, “Information Technology Auditing,” Cengage Learning, 2010

A. Trennery, “Principles of Internal Control”, UNSW Press, 1999

D. N. Chorafas, “Implementing and Auditing the Internal Control System”, Palgrave MacMillan, 2001