Chapter #2

Struktur Program Keamanan Informasi

AIK21363 (3 sks)

Keamanan dan Jaminan Informasi

Information Assurance and Security

Nurdin Bahtiar, M.T

Materi

1. Overview
2. Business Unit Responsibilities
3. Information Security Awareness Program
4. Information Security Program Infrastructure

1. Overview

- Struktur program keamanan informasi menunjukkan kinerja dari setiap tingkatan organisasi.
- Jangkauan program, bagaimana setiap unit bisnis mendukung program, dan bagaimana setiap individu menjalankan tugasnya sebagaimana ditentukan dalam program, semuanya **menentukan seberapa efektif** program tersebut dilaksanakan.
- Tujuan dari praktisi keamanan informasi harus memiliki program keamanan informasi yang seragam yang mencakup seluruh perusahaan.

1. Overview

- Beberapa perusahaan memiliki area yang kuat dan area lemah;
- Misalnya, perusahaan jasa keuangan di mana setiap orang (kecuali pedagang saham) mematuhi standar keamanan informasi yang kuat.
- Kebalikannya, para pedagang saham merasa dirinya selalu bekerja di bawah tekanan yang besar sehingga mematuhi standar keamanan informasi akan menghambat pekerjaan mereka.
- Dalam hal ini, manajemen pedagang saham mungkin memiliki pengaruh yang cukup untuk menunda upaya dalam menegakkan kepatuhan.

1. Overview

- Oleh karena itu, diperlukan suatu program keamanan perusahaan untuk memastikan bahwa semua orang mengetahui aturan tersebut dan mematuhinya.
- Dengan demikian, dapat dipastikan bahwa informasi perusahaan diberikan perlindungan yang diinginkan oleh manajemen senior perusahaan.
- Struktur organisasi harus dibentuk untuk memastikan disampaikan secara tepat, baik kebijakan maupun standar, ke seluruh organisasi maupun masalah dari seluruh organisasi kepada para pembuat keputusan.

1. Overview

Struktur organisasi sebaiknya melibatkan:

- ✓ **Pihak manajemen keamanan informasi**, yang memberikan arahan untuk program keamanan, saran pada organisasi, dan fokus pada penyelesaian isu-isu keamanan.
- ✓ **Auditor internal**, yang memberikan laporan seputar praktek keamanan informasi kepada komite audit. Kemudian diteruskan ke para direktur dan manajemen senior.
- ✓ **Komite pengarah**, yang terdiri dari kepala semua unit bisnis, yang salah satu tugasnya mengambil arahan dari manajemen senior dan memastikannya diterjemahkan secara praktis.
- ✓ **Koordinator keamanan di setiap unit bisnis**, bersama manajemen keamanan informasi mengimplementasikan instruksi dari komite pengarah.
- ✓ **Administrator keamanan di setiap unit bisnis**, yang menjaga akses dan alat lainnya sebagai kontrol untuk melindungi informasi.
- ✓ **Tim kerja keamanan**, yang berfokus pada rencana untuk menerapkan proses dan perangkat keamanan informasi (baik yang baru maupun yang diamandemen) sehingga implementasinya memiliki dampak serendah mungkin pada organisasi.

1. Overview

- Sudah tentu tidak ada praktisi keamanan informasi yang boleh memaksakan struktur ini pada organisasi yang jelas-jelas berbeda (tidak cocok), tetapi tanggung jawab luas harus dilakukan agar program keamanan informasi mendapat dukungan kuat dalam organisasi.

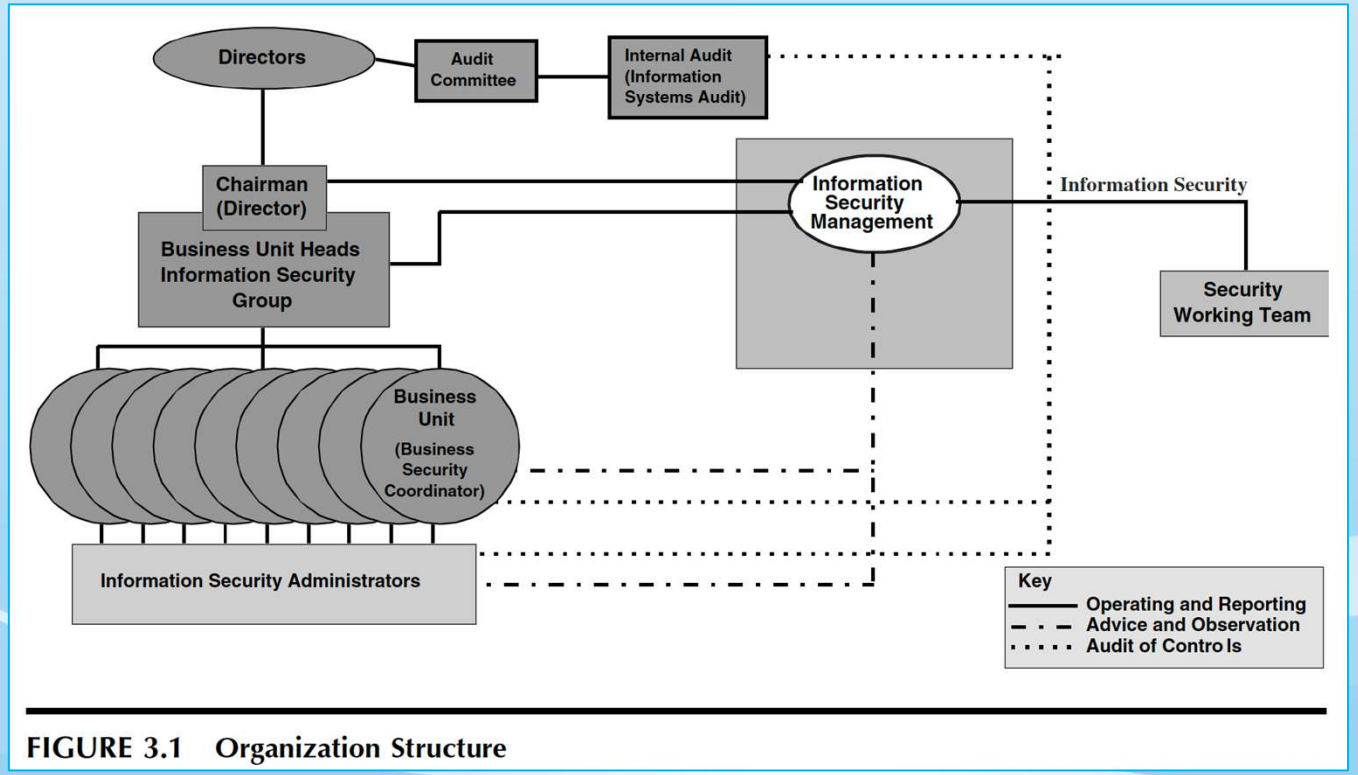

FIGURE 3.1 Organization Structure

2. Business Unit Responsibilities

- Tanggung jawab unit bisnis, terbagi dalam dua area:

1. Pembuatan dan implementasi dari kebijakan dan standar

   Pengembangan kebijakan dan standar membutuhkan keterlibatan dari setiap unit bisnis.

   Setiap unit bisnis harus terwakili dalam proses peninjauan dan persetujuan kebijakan.

2. Kepatuhan terhadap kebijakan dan standar

   Setiap unit bisnis memiliki tanggung jawab untuk memastikan kepatuhan yang konstan terhadap kebijakan dan standar.

   Bentuk tanggung jawab lain dalam unit bisnis, adalah penegakan kepatuhan.

   Kepatuhan dapat dilihat sebagai praktik normal dan **penegakan kepatuhan** dilihat sebagai tindakan yang harus diambil ketika seseorang menemukan pelanggaran.

3. Information Security Awareness Prog.

- Tujuan dari **program kesadaran keamanan** adalah untuk menunjukkan secara jelas “siapa, apa, dan mengapa” dari suatu kebijakan dan standar perusahaan.
- Hanya dengan cara membaca bukanlah metode yang paling efektif untuk menyerap informasi, karena begitu selesai membaca, pesan kebijakan dan standar dapat mudah terlupakan akibat tekanan kerja sehari-hari.
- Jika sebuah organisasi menginginkan kebijakan dan standarnya memiliki efek panjang dan berkesinambungan, organisasi harus berkomitmen pada program penguatan dan informasi yang panjang pula – yaitu program kesadaran keamanan.

3. Information Security Awareness Prog.

- Permasalahan keuangan dapat menghalangi program kesadaran keamanan informasi pegawai sebelum dimulai dengan benar.
- Pihak pengendali keuangan harus menunjukkan uji tuntas dengan menunjukkan efek atau potensi pengembalian investasi untuk setiap dolar yang dihabiskan. Sedangkan program kesadaran keamanan informasi terkenal sulit untuk diukur dengan cara ini.
- Pengembalian investasi, peningkatan kesadaran pekerja, dan bagaimana kedua hal tsb berkontribusi pada profitabilitas perusahaan, merupakan angka yang sulit untuk ditunjukkan.

4. Information Security Program Infrast.

- Infrastruktur yang dimaksud di sini adalah mekanisme dalam organisasi yang mendukung praktek keamanan informasi.
- Mulai dari peran manajemen senior hingga kebiasaan para pekerja, yang harus tangguh dan memiliki pengetahuan agar program keamanan informasi ini membawa manfaat kepada organisasi secara penuh.

4. Information Security Program Infrast.

- Keamanan organisasi merupakan tanggung jawab seluruh organisasi yang menyentuh setiap individu.
- Program keamanan informasi hanya dapat berhasil jika semua pihak dalam organisasi tersebut mengakui tanggung jawab mereka untuk melindungi informasi dan menjalankan tanggung jawab itu.
- Perlindungan dari informasi lebih dari sekedar bagian dari menjalankan bisnis. Seperti halnya memastikan bahwa banyak aset berwujud, misalnya uang di bank atau produk yang dibuat oleh perusahaan manufaktur, yang harus dilindungi secara fisik.

4. Information Security Program Infrast...

- Unsur-unsur yang bertanggung jawab program keamanan informasi:

1. Senior manajement
2. Information Security Management
3. Business Unit Managers
4. First Line Supervisors
5. Employees
6. Third Parties

4. Information Security Program Infrast.

1. Senior Management

Bertugas:

- Memastikan bahwa rekomendasi audit yang berkaitan dengan perlindungan informasi ditangani secara tepat waktu dan memadai
- Berpartisipasi dalam kegiatan Komite Pengarah Keamanan Informasi untuk memandu kegiatan upaya keamanan informasi
- Mengawasi pembentukan, pengelolaan, dan kinerja dari unit keamanan informasi (termasuk menyediakan sumber dayanya)
- Berpartisipasi dalam upaya untuk mendidik staf organisasi tentang tanggung jawab mereka untuk melindungi informasi
- Meninjau dan menyetujui kebijakan dan strategi keamanan informasi
- Memberikan resolusi untuk masalah keamanan informasi yang besar atau urgent untuk diatasi berdasarkan basis organisasi.

4. Information Security Program Infrast.

2. Information Security Management

Bertugas:

- Mendorong upaya untuk membuat, menerbitkan, dan menerapkan kebijakan dan standar keamanan informasi
- Mengkoordinasikan pembuatan dan pengujian rencana bisnis kesinambungan
- Mengelola upaya keamanan informasi di dalam unit keamanan informasi
- Mengelola perangkat lunak keamanan informasi atas nama organisasi
- Memberikan program pendidikan dan kesadaran yang cukup untuk organisasi.

4. Information Security Program Infrast.

3. Business Unit Managers

Bertugas:

- Berpartisipasi dalam proses peninjauan kebijakan
- Memberi masukan untuk standar keamanan informasi
- Mengukur keamanan informasi di dalam unit
- Menegakkan kepatuhan dengan kebijakan dan standar
- Mendukung pendidikan dan kesadaran keamanan informasi
- Memastikan sumber daya tersedia untuk menyusun, menguji, dan memelihara rencana bisnis kesinambungan di bawah koordinasi manajer Keamanan Informasi atau yang ditunjuk oleh manajer IS.

4. Information Security Program Infrast.

4. First Line Supervisors

Bertugas:

- Memantau aktivitas pekerja mereka sehubungan dengan kebijakan dan standar keamanan informasi organisasi
- Mengomunikasikan masalah keamanan kepada Keamanan Informasi dan manajemen senior (melalui manajer unit bisnis)
- Memberi komentar tentang kinerja masing-masing pekerja sehubungan dengan keamanan informasi saat penilaian kinerja
- Mendukung kebijakan keamanan informasi dengan memperkuat pesan yang terkandung dalam elemen pendidikan dan kesadaran program.

4. Information Security Program Infrast.

5. Employees

- Bagaimanapun, program keamanan informasi hanya berfungsi dengan baik jika semua pekerja berpartisipasi, dan pekerja berpartisipasi dengan sukarela karena mereka merasa mereka memiliki peran nyata untuk dilakukan.
- Sayangnya, jarang terdapat pekerja yang “melaporkan pelanggaran keamanan” kepada penyelia mereka, karena pekerja tidak merasa nyaman menceritakan tentang rekan kerja mereka.

6. Third Parties

- Bertanggung jawab mematuhi kebijakan dan standar keamanan informasi dari pihak organisasi yang berkontrak atau pihak mereka berikan layanan. Hal ini secara jelas harus dinyatakan dalam kontrak apa pun yang mengikat kedua pihak.

End of File

Tugas 01

- Bentuk kelompok (2 – 5 mahasiswa)
- Diskusikan sebuah organisasi (apa saja) yang memiliki nilai yang penting dalam suatu organisasi.
- Pastikan bahwa nilai tersebut sangat membutuhkan pengamanan informasi.
- Jelaskan peran apa saja yang bisa dilakukan oleh 6 elemen pelaksana program keamanan informasi untuk mendukung program tersebut (dengan studi kasus dan contoh yang konkrit)
- Outline:
  - ✓ Nama organisasi (termasuk penjelasannya)
  - ✓ Nilai yang penting bagi organisasi
  - ✓ Upaya yang dilakukan PIC keamanan informasi
- Dikumpulkan minggu depan dalam bentuk PDF ke koordinator MK.

Tugas 01

- Misal:
  - ✓ Perusahaan XYZ Cargo
    - Penyedia layanan pengantar paket yang melayani …
  - ✓ Nilai yang penting bagi organisasi ini adalah:
    - Kecepatan layanan antar
    - Kerahasiaan isi paket yang diantar
    - Jaminan keutuhan paket, dsb…
  - ✓ Upaya yang dilakukan PIC keamanan informasi
    - …
    - First Line Supervisors:
      a) Memberikan pengawasan agar …
      b) Memastikan …
    - …