JILS
Journal of Information and Library Studies **Vol.1 No.1, Juni 2018**

KEAMANAN INFORMASI

Aditya Ramadhani[1]

[1]Pustakawan, Perpustakaan Universitas PGRI Adi Buana, Surabaya

armadha31@gmail.com

ABSTRAK

Informasi sebagai aset yang sangat berharga karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha dan kepercayaan publik. Sejalan dengan perkembangan informasi maka keamanan informasi juga harus diperhatikan. Keamanan informasi adalah bagaimana kita dapat mencegah penipuan *(cheating)* atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Dalam ISO-17799, Keamanan informasi ini terdiri dari 3 aspek penting, dapat menghafalnya dengan nama CIA yang berarti Confidentiality, Integrity dan Availability. Terdapat berbagai ancaman dalam system keamanan informasi diantaranya virus, worm, Trojan horse, serta ancaman dari dalam maupun dari luar, disengaja maupun tidak disengaja. Langkah-langkah untuk memastikan bahwa sistem benar-benar mampu menjamin keamanan data dan informasi dapat dilakukan dengan menerapkan kunci-kunci pengendalian yang teridentifikasi dalam standar ISO 17799 tentang keamanan informasi diantaranya terdapat 10 kontrol clouse.

Kata kunci: Keamanan informasi, Ancaman, ISO-17799

ABSTRACT

Information become a valuable asset because it is one of the strategic resources in increasing business value and public trust. In line with the development of information, information security must also be considered. Information security is how we can prevent cheating or, at the very least, detect fraud in an information-based system, where the information itself has no physical meaning. In ISO-17799, this information security consists of 3 important aspects, it can memorize it with the name CIA which means Confidentiality, Integrity and Availability. There are various threats in the information security system including viruses, worms, Trojan horses, as well as internal and external threats, intentional or unintentional. Steps to ensure that the system is truly capable of ensuring data and information security can be carried out by applying the control keys identified in the ISO 17799 standard regarding information security including 10 clouse controls.

Keywords: Information security, threats, ISO-17799

I. PENDAHULUAN

Dengan era kemajuan teknologi informasi dan komunikasi yang berkembang sangat pesat sangat berpengaruh terhadap perkembangan informasi yang beredar di masyarakat. Berbagai kegiatan komunikasi secara elektronik salah satunya dalam bidang seperti perdagangan pendidikan dan perbankan. Dengan teknologi informasi khususnya dengan jaringan komputer yang luas seperti internet. Barang dan jasa dapat dipromosikan secara luas dalam skala global. Semua orang dapat dengan mudah memperoleh informasi dari berbagai sumber secara cepat, tepat, mudah, dan murah. Informasi sebagai aset yang sangat berharga karena merupakan salah satu sumber daya strategis dalam meningkatkan nilai usaha dan kepercayaan publik.

Pemberian kemudahan kemudahan yang memungkinkan konsumen mengakses dan membeli produk dan jasa secara praktis, misalnya pada pelayanan kartu kredit. Perkembangan ini rupanya membawa serta dampak negatif dalam hal keamanan. Maka diperlukan perlindungan terhadap informasi atau kemanan informasi yang harus diperhatikan dengan sungguh-sungguh oleh perseorangan maupun segenap organisasi yang bersangkutan.

Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Keamanan informasi adalah upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Secara tidak langsung keamanan informasi menjamin kontinuitas bisnis, mengurangi risiko-risiko yang terjadi, mengoptimalkan pengembalian investasi.

Semakin banyak informasi perusahaan yang disimpan dan dikelola maka semakin besar pula risiko terjadi kerusakan, kehilangan atau terekspos nya ke pihak yang tidak diinginkan. Dalam ISO-17799, Keamanan informasi ini terdiri dari 3 aspek penting, dapat menghafalnya dengan nama CIA yang berarti Confidentiality, Integrity dan Availability.

Gambar 1. Keamanan Informasi

Confidentiality (kerahasiaan) aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan. *Integrity* (integritas) aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang *(authorized)*, harus terjaga keakuratan dan keutuhan informasi serta *Availability* (ketersediaan) aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait bilamana diperlukan.

Manajemen Keamanan Informasi.

Seperti halnya cakupan keamanan informasi telah meluas, demikian juga pandangan akan tanggung jawab manajemen. Manajemen tidak hanya diharapkan untuk menjaga agar sumber daya informasi aman, namun juga diharapkan untuk menjaga perusahaaan tersebut agar tetap berfungsi setelah suatu bencana atau jebolnya sistem keamanan. Aktivitas untuk menjaga agar sumber daya informasi tetap aman disebut manajemen keamanan informasi *(information security Management – ISM)*, sedangkan aktivitas untuk menjaga agar perusahaan dan sumber daya informasinya tetap berfungsi setelah adanya bencana disebut manajemen keberlangsungan bisnis *(Business continuity Management-BCM)*. CIO adalah orang yang tepat untuk memikul tanggung jawab atas keamanan informasi, namun kebanyakan organisasi mulai menunjuk orang-orang tertentu yang dapat mencurahkan perhatian penuh terhadap aktivitas ini.

Jabatan direktur keamanan sistem informasi perusahaan *(Corporate information system security Office-CISSO)* digunakan untuk individu di dalam organisasi, biasanya anggota dari unit sistem informasi, yang bertanggung jawab atas keamanan sistem informasi perusahaan tersebut. Namun saat ini, perubahan sedang dibuat untuk mencapai tingkat informasi yang lebih tinggi lagi di dalam suatu perusahaan dengan cara menunjuk seorang direktur *Assurances* informasi perusahaan (Corporate information Assurances Office-CIAO) yang akan melapor kepada CEO dan mengelola unit penjagaan informasi.

Pada bentuknya yang paling dasar, manajemen keamanan informasi ISM terdiri atas empat tahap:

1. Mengidentifikasi ancaman yang dapat menyerang sumber daya informasi perusahaan.

2. Mengidentifikasi risiko yang dapat disebabkan oleh ancaman-ancaman tersebut.
3. Menentukan kebijakan keamanan informasi.
4. Mengimplementasikan pengendalian untuk mengatasi risiko-risiko tersebut.

Ancaman menghasilkan risiko, yang harus dikendalikan.

Istilah manajemen risiko *(risk Management)* dibuat untuk menggambarkan pendekatan ini di mana tingkat kemanan sumber daya informasi perusahaan dibandingkan dengan risiko yang dihadapinya. Terdapat pilihan lain untuk merumuskan kebijakan keamanan informasi suatu perusahaan, yaitu tolok ukur keamanan informasi.

Tolok ukur keamanan informasi *(information security benchmark)* adalah tingkat keamanan yang disarankan yang dalam keadaan normal harus menawarkan perlindungan yang cukup terhadap gangguan yang tidak terotorisasi. Tolak ukur semacam ini ditentukan oleh pemerintah dan asosiasi industri. Ketika perusahaan mengikuti pendekatan ini, yang disebut kepatuhan terhadap tolok ukur *(benchmark compliance)*, dapat diasumsikan bahwa pemerintah dan otoritas industri telah melakukan pekerjaan yang baik dalam mempertimbangkan berbagai ancaman serta risiko dan tolok ukur tersebut menawarkan perlindungan yang baik.

Ancaman

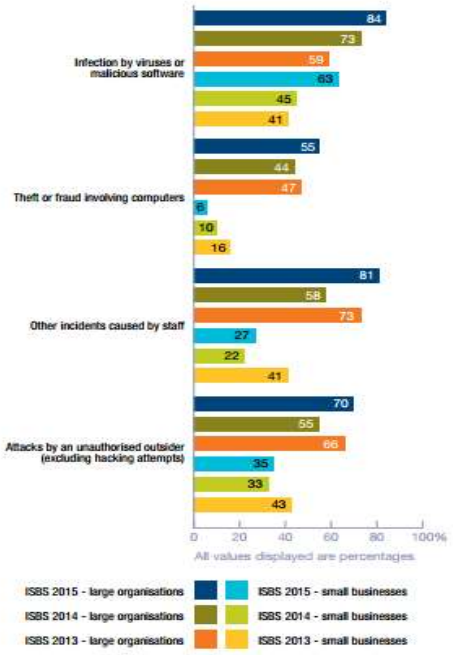
Ancaman keamanan informasi adalah seseorang, organisasi, mekanisme, atau peristiwa yang dapat berpotensi menimbulkan kejahatan pada sumber daya informasi perusahaan. Ancaman dapat berupa internal atau external, disengaja atau tidak disengaja.

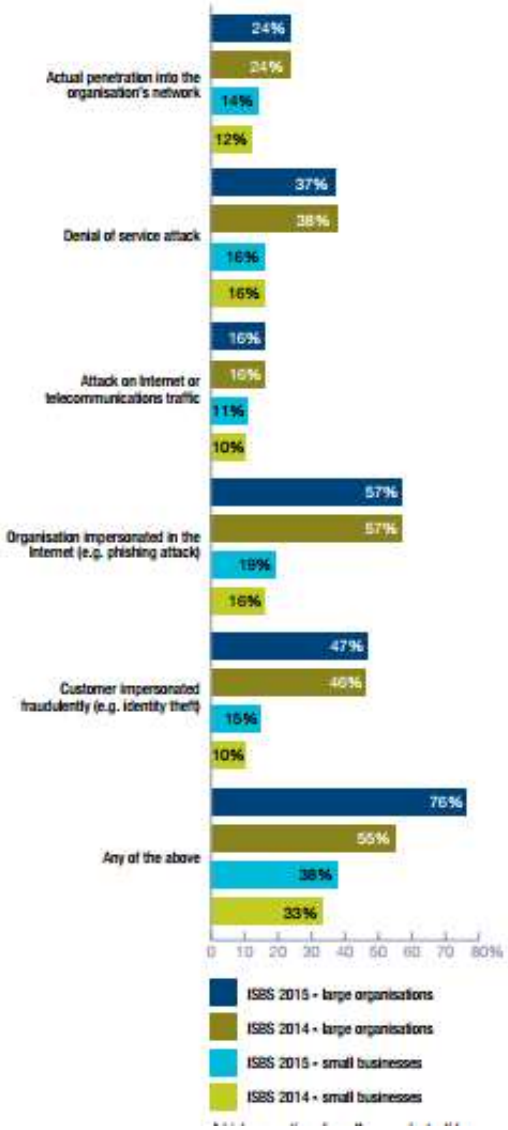
Ancaman yang paling terkenal

Sebuah virus adalah sebuah program komputer yang dapat mereplikasi dirinya sendiri tanpa pengetahuan pengguna Sebuah worm tidak dapat mereplikasi dirinya sendiri tanpa sebuah sistem tapi dapat memancarkan salinan dengan sendirinya oleh e-mail Sebuah Trojan horse tidak dapat mereplikasi maupun mendstribusikan dirinya sendiri. Distribusi terpenuhi oleh para pemakai yang mendistribusikannya sebagai utilitas, maka ketika digunakan menghasilkan sesuatu perubahan yang tidak dikehendaki dalam kemampuan system.

Mengapa diperlukan keamanan informasi

Keamanan informasi memproteksi informasi dari ancaman yang luas untuk memastikan kelanjutan usaha, memperkecil rugi perusahaan dan memaksimalkan laba atas investasi dan kesempatan usaha. Manajemen sistem informasi memungkinkan data untuk terdistribusi secara elektronis, sehingga diperlukan sistem untuk memastikan data telah terkirim dan diterima oleh user yang benar. Hasil survey ISBS (Information Security Breaches Survey) pada tahun 2015 menunjukkan bahwa sebagian besar data atau informasi tidak cukup terpelihara atau terlindungi sehingga beralasan kerawanan. Hasil survey yang terkait dengan hal ini dapat dilihat dalam gambar berikut:





Gambar 2. Hasil Survey

Data survey terbaru diatas menunjukkan bahwa banyak organisasi menderita infeksi oleh malware, dengan organisasi besar menunjukkan angka (84%) pada ISBS 2015. Sedangkan pada organisasi kecil (63%) pada ISBS 2015. Hal tersebut menunjukkan adanya peningkatan sebesar 15% angka minimal pada tahun 2014. (81%) dari organisasi besar menyatakan bahwa ada

unsur staf terlibat dalam pelanggaran yang mereka derita dengan peningkatan hampir (40%) selama satu tahun. Untuk organisasi kecil angka itu naik menjadi (27%) dari tahun lalu yang hanya (22%). Pelanggaran terkait staf akan diperiksa secara lebih rinci nanti dalam laporan.

Untuk organisasi besar, proporsi insiden terburuk yang disebabkan oleh malware, insiden terkait telah dibelah dua, tren yang selanjutnya dikurangi dalam organisasi kecil. Sebaliknya, pencurian atau pengungkapan informasi yang tidak sah atau informasi rahasia, dan serangan atau akses yang tidak sah oleh pihak luar adalah sama-sama mencetak nilai tertinggi. Langkah-langkah untuk memastikan bahwa sistem benar-benar mampu menjamin keamanan data dan informasi dapat dilakukan dengan menerapkan kunci-kunci pengendalian yang teridentifikasi dalam standar ini.

II. PEMBAHASAN

Standar ISO 17799 tentang keamanan informasi.

Berikut adalah objek pengamatan/pengawasan keamanan merupakan uraian dari aspek 10 control clouse tersebut.

Gambar 3. Aspek 10 control clouse

Security Policy *(kebijakan keamanan)***,** mengarahkan visi dan misi manajemen agar kontinuitas bisnis dapat dipertahankan dengan mengamankan dan menjaga integritas/keutuhan informasi-informasi krusial yang dimiliki oleh perusahaan. *Security Policy* sangat diperlukan mengingat banyak ditemuinya masalah-masalah non teknis salah satunya penggunaan *password* oleh lebih dari satu orang. Hal ini menunjukan tidak adanya kepatuhan dalam menerapkan sistem keamanan informasi. Harus dilakukan inventarisasi data-data perusahaan. Selanjutnya dibuat peraturan yang melibatkan semua departemen sehingga peraturan yang dibuat dapat diterima oleh semua pihak. Setelah itu rancangan peraturan tersebut diajukan ke pihak direksi. Setelah disetujui, peraturan tersebut dapat diterapkan. *Security Policy* meliputi berbagai aspek, yaitu:

a. Information security infrastructure

b. *Information security policy*

System Access Control *(sistem kontrol akses)***,** mengendalikan/membatasi akses user terhadap informasi-informasi yang telah diatur kewenangannya, termasuk pengendalian secara mobile-computing ataupun tele-networking. Mengontrol tata cara akses terhadap informasi dan sumber daya yang ada meliputi berbagai aspek, yaitu:

a. *Access control.*
b. *User Access Management.*
c. *User Responsibilities.*
d. *Network Access Control*
e. *Operation System Access Control*
f. *Application Access Control.*
g. *Monitor system Access and use.*
h. *Mobile Computing and Telenetworking.*

Communication and Operations Management *(manajemen komunikasi dan operasi)***,** menyediakan perlindungan terhadap infrastruktur sistem informasi melalui perawatan dan pemeriksaan berkala, serta memastikan ketersediaan panduan sistem yang terdokumentasi dan dikomunikasikan guna menghindari kesalahan operasional. Pengaturan tentang alur komunikasi dan operasi yang terjadi meliputi berbagai aspek, yaitu:

a. *Operational procedures and reponsibilities.*
b. *System Planning and acceptance.*
c. *Protection against malicious software.*
d. *Housekeeping*
e. *Network Management.*
f. *Media handling and security.*
g. *Exchange of Information and software.*

System Development and Maintenance *(pengembangan sistem dan pemeliharaan)***,** memastikan bahwa sistem operasi maupun aplikasi yang baru diimplementasikan mampu bersinergi melalui verifikasi/validasi terlebih dahulu sebelum diluncurkan ke live environment. Penelitian untuk pengembangan dan perawatan sistem yang ada meliputi berbagai aspek, yaitu:

a. *Security requirements of system.*
b. *Security in application system.*
c. *Cryptographic Control*
d. *Security of system files*
e. *Security in development and support process.*

Physical and Environmental Security *(keamanan fisik dan lingkungan)***,** membahas keamanan dari segi fisik dan lingkungan jaringan, untuk mencegah kehilangan atau

kerusakan data yang diakibatkan oleh lingkungan, termasuk bencana alam dan pencurian data dalam media penyimpanan atau fasilitas informasi yang lain. Aspek yang dibahas antara lain:

a. *Secure Areas*
b. *Equipment security*
c. *General Control*

Compliance *(penyesuaian)***,** memastikan implementasi kebijakan-kebijakan keamanan selaras dengan peraturan dan perundangan yang berlaku, termasuk persyaratan kontraktual melalui audit sistem secara berkala. Kepatuhan yang mengarah kepada pembentukan prosedur dan aturan-aturan sesuai dengan hukum yang berlaku meliputi berbagai aspek, yaitu :

a. *Compliance with legal requirements*
b. *Reviews of security policy and technical comliance.*
c. *System audit and consideration*

Personnel Security (*keamanan perorangan)***,** mengatur tentang pengurangan resiko dari penyalahgunaan fungsi penggunaan atau wewenang akibat kesalahan manusia (human error), sehingga mampu mengurangi human error dan manipulasi data dalam pengoperasian sistem serta aplikasi oleh user, melalui pelatihan-pelatihan mengenai security awareness agar setiap user mampu menjaga keamanan informasi dan data dalam lingkup kerja masing-masing. *Personnel Security* meliputi berbagai aspek, yaitu:

a. Security in Job Definition and Resourcing.
b. User Training.
c. Responding to Security Incidens and Malfunction.

Security Organization *(organisasi keamanan)***,** mengatur tentang keamanan secara global pada suatu organisasi atau instansi, mengatur dan menjaga integritas sistem informasi internal terhadap keperluan pihak eksternal termasuk pengendalian terhadap pengolahan informasi yang dilakukan oleh pihak ketiga (outsourcing). Aspek yang terlingkupi, yaitu:

a. Security of third party access
b. Outsourcing

Asset Classification and Control *(klasifikasi dan kontrol aset)***,** memberikan perlindungan terhadap aset perusahaan dan aset informasi berdasarkan level proteksi yang ditentukan. Membahas tentang penjagaan aset yang ada meliputi berbagai aspek, diantaranya:

a. Accountability for Assets.

b. Information Classification.

Business Continuity Management *(manajemen kelanjutan usaha)***,** siap menghadapi resiko yang akan ditemui didalam aktivitas lingkungan bisnis yang bisa mengakibatkan "*major failure*" atau resiko kegagalan yang utama ataupun "disaster" atau kejadian buruk yang tak terduga, sehingga diperlukan pengaturan dan manajemen untuk kelangsungan proses bisnis, dengan mempertimbangkan:

a. Aspects of business continuity management

Membangun dan menjaga keamanan sistem manajemen informasi akan terasa jauh lebih mudah dan sederhana dibandingkan dengan memperbaiki sistem yang telah terdisintegrasi. Penerapan standar ISO 17799 akan memberikan benefit yang lebih nyata bagi organisasi bila didukung oleh kerangka kerja manajemen yang baik dan terstruktur serta pengukuran kinerja sistem keamanan informasi, sehingga sistem informasi akan bekerja lebih efektif dan efisien.

Contoh Kasus

Modus pembobolan rekening lewat *e-banking*

Selasa, 14 April 2015 / 19:18 WIB

JAKARTA. Penyidik Bareskrim Polri saat ini sedang mengusut pembobolan beberapa dana nasabah di tiga bank besar di Indonesia dengan modus menggunakan software internet banking. Modus kejahatan ini diklaim telah menimbulkan kerugian mencapai Rp 130 miliar. Kepala Badan Reserse Kriminal (Bareskrim) Polri, Komjen Budi Waseso ketika dihubungi KONTAN membenarkan kabar ini. Ia menuturkan polisi telah berhasil mengendus dugaan pembobolan dana nasabah tiga bank yang dilakukan oleh sindikat kejahatan dunia maya.

Menurutnya, pelaku menggunakan malware untuk muncuri data nasabah bank yang ditanamkan melalui jaringan internet.

> "Pada Senin (13/4) kemarin kami telah berhasil membongkar sindikat pembobolan uang nasabah dengan menggunakan internet. Saat ini kasus masih didalami oleh penyidik," ujar Budi, Selasa, (14/4).

Modus dari pencurian dana nasabah ini menurut Direktur Tindak Pidana Ekonomi Khusus (Dirtipideksus) Bareskrim Polri, Brigjen Victor Simanjuntak adalah dengan membajak akun internet banking milik nasabah bank sehingga ketika nasabah akan menyetorkan uang ke rekeningnya, aliran uang tersebut akan dibelokkan ke rekening pelaku. Ia menjelaskan pelaku utama bukanlah warga negara Indonesia karena berdasarkan penyelidikan Bareskrim ternyata aliran dana tersebut menuju ke sebuah rekening di negara Ukraina.

> "Pelaku bukan warga negara Indonesia. Ia menggunakan jasa kurir yang merupakan WNI. Sehingga dana

nasabah dibelokkan masuk ke rekening kurir, kemudian langsung diteruskan ke rekening pelaku," ujar Victor ketika dihubungi KONTAN.

Modus kejahatan ini bermula saat pelaku menawarkan perangkat aplikasi antivirus melalui pesan layanan di internet kepada korban pengguna e-banking. Setelah korban mengunduh software palsu tersebut, malware akan secara otomatis masuk ke komputer dan memanipulasi tampilan laman internet banking seolah-olah laman tersebut merupakan milik bank. Dengan begitu, pelaku dapat dengan mudah mengendalikan akun e-banking nasabah setelah mengetahui password korban.

"Namun, pelaku tidak menguras rekening korban, hanya membelokkan ke rekening kurir jika korban melakukan transaksi keuangan melalui e-banking," tutur Victor.

Dalam aksi kejahatannya tersebut, pelaku merekrut WNI sebagai kurir dengan kedok kerjasama bisnis sehingga kurir sendiri tidak mengetahui bahwa uang yang masuk ke rekening mereka merupakan hasil pembobolan. Victor menjelaskan pelaku menjanjikan kurir dapat mengambil 10% dari dana yang masuk dan sisanya dikirimkan ke rekening di Ukraina melalui Western Union.

Perekrutan kurir ini dilakukan secara acak dengan mengaku kerjasama bisnis perdagangan seperti kayu, kain, dan mesin.

"Pelaku menjalin kerjasama dengan kurir di Indonesia. Pelaku mengatakan kalau dirinya akan berusaha di Indonesia tapi tidak memiliki rekening untuk menerima pembayaran dalam bentuk rupiah. Para kurir cuma diminta membuka rekening dan mentrasferkan uang yang masuk ke rekeningnya tersebut," jelas Victor.

Saat ini Bareskrim Polri tengah mendalami kasus ini dengan memeriksa keterangan dari enam orang kurir yang telah ditahan sebagai saksi. Penyidik, ujar Victor, telah mengantongi identitas pelaku dan akan bekerja sama dengan Interpol untuk mengungkap jaringan sindikat pencurian uang nasabah ini. Berdasarkan hasil pemeriksaan sementara, jumlah kurir diduga berjumlah ratusan orang yang tersebar diseluruh penjuru tanah air.

"Pelaku adalah penjahat profesional yang memahami betul IT. Semua kurir yang telah diperiksa sama sekali tidak menyadari jika mereka terlibat dalam pembobolan bank. Pelaku ada di luar negeri, kami telah mengontak interpol untuk membantu kami," tutur Victor.

Namun, Victor enggan menyebutkan nama maupun inisial dari tiga bank tersebut karena masih dalam penyelidikan oleh Polri. Ia hanya menyebutkan ketiga bank tersebut ada yang berasal dari BUMN dan swasta. Ia mengungkapkan terdapat sekitar 300 nasabah dari ketiga bank tersebut yang menjadi korban dengan total kerugian mencapai Rp 130 miliar yang berhasil dicuri pelaku.

"Nanti bank akan kita panggil untuk melengkapi laporan. Karena ada pihak bank yang telah mengembalikan uang nasabahnya ada yang belum," ujarnya.

Menurutnya, Indonesia dengan salah satu jumlah pengguna internet terbesar di dunia akan menjadi sasaran empuk dari tindak kejahatan dengan media online, terutama banyak masyarakat yang masih menggunakan software palsu sehingga rentan diretas. Deputi Komisioner Pengawasan Perbankan Otoritas Jasa Keuangan (OJK), Irwan Lubis, mengaku pihaknya belum menerima laporan dari pihak bank, Bareskrim Polri, maupun institusi lainnya

terkait kasus pembobolan dana nasabah di tiga bank ini. Meskipun begitu, Ia menegaskan bahwa OJK telah meminta kepada bank untuk meningkatkan pengamanan teknologi informasi pada sistem internet banking.

> "OJK belum menerima laporan baik dari bank maupun dari pihak atau intitusi lain. Pada 9 Maret 2015 yang lalu, OJK sudah meminta kewaspadaan bank dan meningkatkan IT security pada layanan internet banking mereka," tuturnya kepada KONTAN.

Selain meminta kepada pihak bank, Irwan juga menekankan kepada para nasabah untuk selalu berhati-hati dan waspada dalam bertransaksi dengan menggunakan internet banking terutama dengan menggunakan komputer yang rentan terserah virus. Ia memberi saran kepada para nasabah jika terdapat instruksi yang tidak lazim dan meragukan pada saat transaksi harap segera menghubungi call center bank masing-masing.

> "Nasabah juga diminta untuk selalu waspada dalam bertransaksi via internet. Kalau ada instruksi yang tidak lazim segera hubungi call center bank," ujar Irwan.

Sesuai dengan Undang-undang No 21 Tahun 2011 tentang Otoritas Jasa Keuangan, OJK merupakan lembaga negara yang memiliki fungsi pengaturan dan pengawasan terhadap individual bank (mikroprudensial). OJK diberikan kewenangan memberikan izin, mengatur, mengenakan sanksi, dan mengawasi setiap aktivitas perbankan di Indonesia.

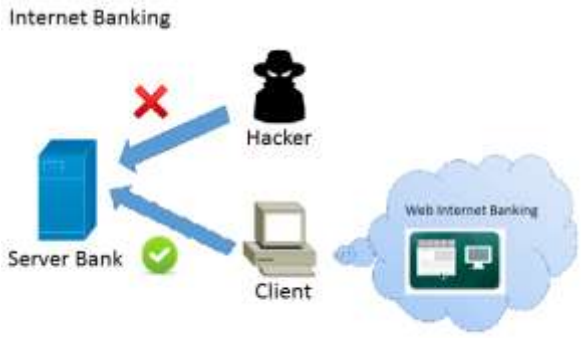
Analisis

Melihat data survey terbaru diatas menunjukkan bahwa banyak organisasi menderita infeksi oleh malware, dengan organisasi besar menunjukkan angka (84%) pada ISBS 2015. Sedangkan pada organisasi kecil (63%) pada ISBS 2015. Dan contoh kasus diatas serangan dari hacker tertuju pada program malware untuk mengelabuhi korban. Misalkan pada kasus internet banking, yang dimaksud *confidentiality* adalah hacker tidak dapat mengakses informasi jumlah saldo klien karena informasi saldo hanya boleh dilihat oleh klien pemilik account bank tersebut. Sebaliknya, saat klien ingin mengetahui informasi saldo di rekeningnya menggunakan internet banking, maka fasilitas tersebut sebaiknya tersedia 24 jam dan inilah yang dimaksud *availability*. Kemudian yang dimaksud *integrity* adalah informasi saldo milik klien haruslah memiliki jumlah yang sesuai dengan yang disetor oleh klien.

Jadi dapat dikatakan apa yang dilakukan tersangka dan termasuk jasa kurir tersebut adalah tindakan yang tidak benar dan melanggar etik karena tindakannya sangat merugikan privasi orang lain. Orang tidak akan sadar bahwa dirinya telah menggunakan situs palsu tersebut karena tampilan yang disajikan serupa dengan situs aslinya. *Hacker* tersebut mampu mendapatkan *User ID* dan *password* dari pengguna yang memasuki situs palsu tersebut, tindakan yang dilakukan

oleh tersangka termasuk *black-hat hacker* karena membuat virus malware dan juga dengan diam-diam mengambil data milik pihak lain serta mengambil dana milik nasabah bank.

Dengan modus kejahatan dari perangkat aplikasi antivirus melalui pesan layanan di internet kepada korban pengguna e-banking. Setelah korban mengunduh software palsu tersebut, malware akan secara otomatis masuk ke komputer dan memanipulasi tampilan laman internet banking seolah-olah laman tersebut merupakan milik bank. Dengan begitu, pelaku dapat dengan mudah mengendalikan akun e-banking nasabah setelah mengetahui password korban. Namun juga menimbulkan sisi positif dimana pihak perbankan dapat belajar dari kasus tersebut. Perbankan menggunakan internet banking yang dapat dipakai pengambilan keputusan atau yang disebut *decision support system*, dimana data para nasabah yang bertransakasi serta aktivitas lainnya melalui internet banking merupakan database milik perbankan secara privasi yang tidak boleh disebarluaskan ataupun disalahgunakan karena internet banking tersebut merupakan salah satu layanan yang menguntungkan baik bagi nasabah maupun pihak perbankan. Database para nasabah internet banking dapat digunakan oleh pihak perbankan untuk membuat keputusan dalam berbagai bidang perbankan.



Gambar 4. Model e-banking

III. KESIMPULAN

Keamanan informasi adalah bagaimana kita mencegah penipuan (cheating) atau paling tidak mendeteksi adanya penipuan di sebuah system yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Keamanan informasi adalah upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Secara tidak langsung keamanan informasi menjamin kontinuitas bisnis, mengurangi risiko-risiko yang terjadi, mengoptimalkan pengembalian investasi. Aspek penting dalam keamanan informasi adalah kerahasiaan, integritas, dan ketersediaan.

Seperti halnya cakupan keamanan informasi telah meluas, demikian juga pandangan akan tanggung jawab manajemen.

Manajemen tidak hanya diharapkan untuk menjaga agar sumber daya informasi aman, namun juga diharapkan untuk menjaga perusahaaan tersebut agar tetap berfungsi setelah suatu bencana atau jebolnya sistem keamanan.

Ancaman keamanan informasi adalah seseorang, organisasi, mekanisme, atau peristiwa yang dapat berpotensi menimbulkan kejahatan pada sumber daya informasi perusahaan. Ancaman dapat berupa internal atau external, disengaja atau tidak disengaja. Langkah-langkah untuk memastikan bahwa sistem benar-benar mampu menjamin keamanan data dan informasi dapat dilakukan dengan menerapkan kunci-kunci pengendalian yang teridentifikasi dalam standar ISO 17799 tentang keamanan informasi diantaranya terdapat 10 kontrol clouse yaitu kebijakan keamanan, system control akses, manajemen komunikasi dan operasi, pengembangan system dan pemeliharaan, keamanan fisik dan lingkungan, penyesuaian, keamanan perorangan, organisasi keamanan, klasifikasi dan control aset, manajemen kelanjutan usaha.

DAFTAR PUSTAKA

Belsis, Petros; Kokolakis, Spyros; Kiountouzis, Evangelos. 2005. *Information systems security from a knowledge management perspective*. Information Management & Computer Security; 2005; 13, 2/3; ProQuest, pg. 189.

Nnolim, Anene L. 2007. *A Framework and Methodology for Information Security Management*. Lawrence Technological University.

Saint-Germain, René. 2005. *Information Security Management Best Practice Based on ISO/IEC 17799*. Information Management Journal; Jul/Aug 2005; 39, 4; ProQuest. pg. 60.

Http://nasional.kontan.co.id/news/ini-modus-pembobolan-rekening-lewat-e-banking diakses pada 7 Mei 2016 pada pukul 21.00 WIB.

Sumber Internet

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf diakses pada 7 Mei 2016 pada pukul 20.00 WIB

https://www.academia.edu/5082000/ISO_17799_Standar_Sistem_Manajemen_Keamanan_Informasi artikel berjudul ISO 17799: Standar Sistem Manajemen Keamanan Informasi Penulis: Melwin Syafrizal, S.Kom. Diakses pada 7 Mei 2016 pada pukul 20.00 WIB.

https://www.academia.edu/4761474/Keamanan_Informasi_ISO17799 artikel ini berjudul Kajian ISO 17799 Pada Organisasi Oleh Yudi Herdianan. Diakses pada 7 Mei 2016 pukul 20.30 WIB.