Kesadaran Keamanan Informasi pada Pegawai Bank X di Bandung Indonesia

Awareness Information Security Employees X Bank in Bandung Indonesia

Dian Chisva Islami, Khodijah Bunga I.H, Candiwan
Universitas Telkom, Jl. Telekomunikasi No.1, DayeuhKolot, Bandung
Email:dianchisva@students.telkomuniversity.ac.id

Abstract

The development of technology coupled with the increasing number of internet users in Indonesia increase the number of cyber crime. Low levels of information security (InfoSec) in the banking sector, such as the ATM burglary, skimming, phishing and malware also experienced by X Bank an international bank located in Bandung. Therefore, this needs for InfoSec awareness actions. The importance of maintaining an InfoSec awareness in the Bank is influenced by several factors namely compliance with the law (regulation) and guard the integrity of the data bank. In raising the awareness of the employees, researchers used a theoretical approach to verification that includes three employee's behaviors at work. This is to measure employee understanding of awareness of information security through knowledge, attitudes and behavior. Researchers used qualitative research with description by using purposive sampling method, where the data collection is obtained through interviews. The Results of this research showed that the implementation of information security policy at X Bank Bandung was good , and the employees of X Bank had a high level of awareness for information security.

Keywords: *Awareness, Information Security , Information Management System, Verification Theory*

Abstrak

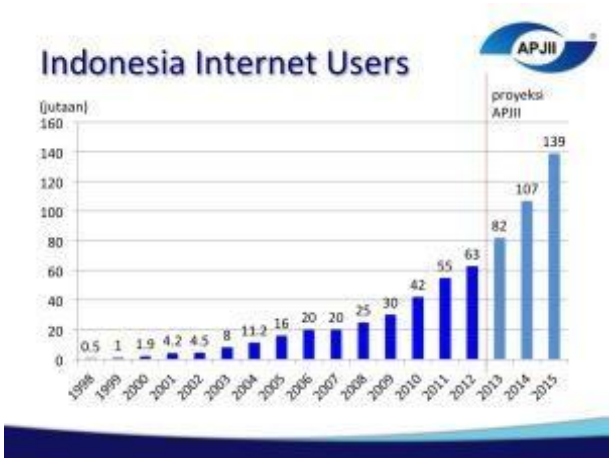
Berkembangnya teknologi diiringi dengan semakin meningkatnya jumlah pengguna internet di Indonesia, hal inilah yang membuat jumlah kejahatan di dunia maya bertambah. Rendahnya tingkat keamanan informasi di bidang perbankan, seperti adanya pembobolan ATM, *skimming*, *phising* dan *malware* juga dialami oleh Bank X yang merupakan Bank internasional dan berlokasi di Bandung. Sehingga perlu adanya tindakan kesadaran keamanan informasi (*information security awareness).* Kesadaran akan pentingnya menjaga keamanan informasi di Bank dipengaruhi oleh beberapa faktor yakni kepatuhan hukum (regulasi) danpenjagaan integritas data bank. Dalam meningkatkan kesadaran pegawai Bank X tersebut, peneliti menggunakan pendekatan teori verifikasi yang meliputi tiga hal perilaku pegawai dalam bekerja. Hal ini untuk mengukur pemahaman pegawai tentang kesadaran keamanan informasi melalui pengetahuan, sikap dan perilaku. Peneliti menggunakan metode penelitian kualitatif secara deskriptif dengan teknik *purposive sampling*, dimana pengumpulan datanya melalui wawancara. Hasil penelitian ini menunjukan bahwa pelaksanaan kebijakan keamanan informasi pada Bank X Bandung berjalan dengan baik, serta pegawai Bank X Bandung rata-rata telah mempunyai tingkat kesadaran yang tinggi terhadap keamanan informasi.

Kata kunci: Kesadaran, Keamanan Informasi, Manajemen Sistem Informasi, Teori Verifikasi

1. Pendahuluan

Berdasarkan data statistik dari APJII tahun 2015 yang tersedia pada situs kominfo.go.id, pertumbuhan pengguna internet di Indonesia meningkat sangat tajam.

Received: 20 Nov 2015; Revised: 17 Juni 2016; Accepted: 06 Juni 2016; Published online: 21 Nov 2016 ©2016 INKOM 2016/16-NO428 DOI: http://dx.doi.org/10.14203/j.inkom.428



Gambar 1. Pengguna Internet di Indonesia [1]

Gambar 1 menunjukan grafik pengguna internet di Indonesia dari tahun 1998 hingga 2015. Pada tahun 2013 pengguna internet sebanyak 82 juta, meningkat pada tahun 2014 sebanyak 107 juta kemudian meningkat kembali pada tahun 2015 sebanyak 139 juta [1]. Selain itu, trend penguna internet via mobile di Indonesia juga tumbuh pesat. Berdasarkan survei terbaru baidu, mesin pencari dari china yang merupakan rival dari google. Sebanyak 59,9% pengguna internet di Indonesia mengakses dunia maya melalui *smartphone*. Angka tersebut mengalahkan persentase pengguna yang mengakses internet melalui laptop atau netbook[2][3]. Dengan semakin banyaknya pengguna internet, maka semakin banyak pula kejahatan dalam dunia maya, khususnya pada sektor perbankan [3]. Berdasarkan rekap berita yang tercantum dari beberapa website, peneliti merangkumkan kejahatan yang biasa terjadi di sektor perbankan sebagai berikut :

Terdapat empat kejahatan yang biasa terjadi pada sektor perbankan, yaitu :

1. *Pembobolan ATM*. Berikut adalah cuplikan kasus mengenai pembobolan ATM.
- Pada tahun 2011 silam, terjadi pembobolan ATM senilai Rp. 250.000.000 pada Bank X di Indonesia yang berlokasi di Serang. Kejadian tersebut merupakan tindak kejahatan secara fisik yang merugikan pihak Bank dan pihak lainnya yang bersangkutan seperti pelanggan Bank tersebut [4].
- Kasus pembobolan ATM Bank X juga terjadi pada kompleks Green Ville, Kebon Jeruk, Jakarta Barat pada 20 Maret 2011.
- Tidak diketahui kerugian yang ditanggung oleh pihak Bank, hanya saja penyebab dari pembobolan tersebut adalah tidak adanya CCTV yang terpasang dan tidak ada satpam yang menjaga ATM tersebut [5].
- Pembobolan ATM pada pusat perbelanjaan [6].

2. *Skimming*. Terjadinya kejahatan *skimming* di daerah Jakarta Selatan, kejahatan tersebut dengan memanfaatkan alat *cam spy* dan *router*. Sekitar 560 nasabah menjadi korban [7][8].
3. *Phising* dan *Malware*. Terjadi kasus pembobolan tiga bank besar di Indonesia melalui penyebaran virus dan *phising*, total kerugian mencapai 130 miliar [8].

Dengan semakin banyaknya kasus kejahatan perbankan, diperlukan peningkatan kesadaran terhadap perlindungan informasi dari internal dan eksternal perusahaan. Kesadaran keamanan informasi ("*Information Security Awareness*") sangat penting karena dapat mengurangi ancaman – ancaman yang berasal dari internal perusahan. Ancaman kejahatan yang ada pada perusahaan berskala besar adalah kejahatan yang dilakukan oleh staff [8]. Untuk itu tujuan penelitian ini adalah untuk mengetahui kesadaran keamanan informasi pada pegawai Bank.

Gambar 2. Kejahatan dalam Sektor Perbankan[4][5][6][7][8]

2. Dasar Teori

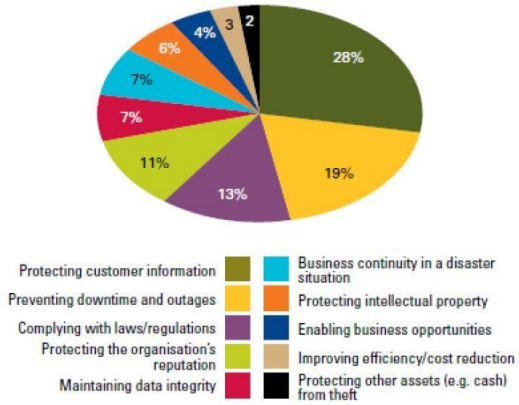
2.1. Keamanan Informasi

Informasi yang merupakan aset yang harus dilindungi keamanannya. Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, serta mempercepat kembalinya investasi dan peluang usaha [10][11][12]. Setiap individu dalam organisasi memiliki peran yang berbeda-beda terhadap informasi. Merupakan hal yang penting bagi seluruh anggota organisasi untuk memahami bagaimana peran dan tanggung jawab mereka terhadap informasi. Unsur utama yang menjadi subyek dari informasi adalah peran

pengguna, pemilik, atau *custodian* terhadap informasi [13].

1. *Owner*/Pemilik. Pemilik bertanggung jawab atas informasi yang harus dilindungi [13].
2. *Custodian*. *Custodian* adalah pihak yang bertanggung jawab untuk melindungi informasi yang diberikan oleh pemiliknya [13].
3. *User*/Pengguna. Pengguna adalah pihak yang dianggap secara rutin menggunakan informasi sebagai bagian dari pekerjaannya [13].

InfoSecurity Europe telah mengklasifikasikan 10 faktor pemicu pentingnya diterapkan sistem keamanan informasi. Berdasarkan laporan teknis survei pelanggaran keamanan informasi tahun 2010 terhadap 539 perusahaan (besar dan kecil), diperoleh diagram komposisi tingkat urgensi dari ke-10 faktor tersebut seperti yang tertera di Gambar 3 [13] Dari gambar terlihat bahwa tiga besar faktor utama perlu diterapkanya keamanan informasi adalah untuk mengamankan informasi pelanggan, faktor kepatuhan hukum (regulasi) serta menjaga integritas data. Sementara faktor lainnya tidak terlalu signifikan.



Gambar 3.Diagram komposisi faktor pemicu Pentingnya kemanan informasi [13]

Dari grafik di atas, dipaparkan bahwa 10 faktor pemicu sistem keamanan informasi adalah sebagai berikut: faktor perlindungan informasi customer sebesar 28%, faktor pencegahan *downtime* dan pemadaman 19%, Sebesar 13% faktor tentang mematuhi peraturan perundang-undangan, faktor perlindungan reputasi perusahaan sebesar 11%, faktor tentang menjaga integritas data sebesar 7%, faktor keberlangsungan bisnis dalam situasi bencana sebesar 7%, faktor perlindungan kekayaan intelektual sebesar 6%, faktor memungkinkan adanya peluang bisnis sebesar 4%, faktor peningkatan efisiensi atau pengurangan biaya sebesar 3%, faktor perlindungan asset lainnya (misalnya uang tunai) dari pencurian sebesar 2%. Selanjutnya, didapatkan bahwa tiga faktor pemicu terbesar yang harus lebih ditingkatkan lagi keamanan informasinya adalah perlindungan informasi *customer*, pencegahan *down time* dan pemadaman, serta faktor tentang mematuhi peraturan perundang-undangan, sementara faktor lainnya tidak terlalu signifikan.

2.2. Sistem Manajemen Keamanan Informasi / Information Security Management System (ISMS)

Sistem Manajemen Keamanan Informasi atau *"information security management system"* (ISMS) saat ini memainkan peran penting dalam implementasi keamanan organisasi. Sistem Keamanan Informasi sebagai jangka pandang yang luas mengenai keamanan komputer, adalah sistem yang menggabungkan analisis dan metode desain, informasi pengguna sistem, masalah manajerial masyarakat dan masalah etika [1]. Definisi di atas jelas menunjukkan bahwa IS keamanan meliputi perspektif yang lebih luas dibandingkan dengan keamanan komputer (berorientasi teknis). Namun dalam praktek yang sebenarnya, pelaksanaan ISMS masih sangat rendah. Dalam laporan tahunan *Deloitte's technology* baru-baru ini, perusahaan media dan telekomunikasi (TMT) tentang survei keamanan menemukan bahwa 32% responden mengurangi anggaran keamanan informasi mereka dalam satu tahun terakhir [14]. Sehingga perlu adanya peningkatan keamanan informasi.

Berdasarkan uraian di atas, maka rencana keamanan akan berisi tentang penentuan kombinasi kontrol keamanan informasi yang digunakan, serta prioritas dalam melakukan implementasinya. Isi atau konten dasar pada dokumen rencana keamanan informasi (*information security plan*), antara lain [15]:

1. Ancaman dan kelemahan. Merupakan proses untuk mereview hasil tahapan penilaian risiko, dengan mengambil informasi mengenai sesuatu yang dapat menganggu kegiatan organisasi.
2. Tujuan dan sasaran. Merupakan proses menentukan target dan lingkup keamanan informasi yang ingin dicapai, sehingga dapat fokus pada aspek keamanan yang akan diselesaikan. Sasaran keamanan informasi menggambarkan spesifik hasil, kejadian atau manfaat yang ingin dicapai sesuai dengan tujuan keamanan yang ditetapkan.
3. Aturan dan tanggung jawab. Merupakan proses menyusun aturan dan penanggung jawab, yang mengatur kegiatan sebagai upaya untuk menurunkan risiko keamanan informasi yang bersumber dari ancaman dan kelemahan.

4. Strategi dan kontrol keamanan. Merupakan proses untuk memberikan prioritas aksi yang akan dilakukan untuk mencapai tujuan dan sasaran keamanan informasi yang telah ditetapkan. Prioritas aksi tersebut sebagai pengaman untuk menjaga kerahasiaan, keutuhan dan ketersediaan informasi, dengan penentuan kontrol keamanan yang sesuai dengan tujuan dan sasaran yang diinginkan.

2.3. Kesadaran Keamanan Informasi (Information Security Awareness)

Kesadaran merupakan poin atau titik awal untuk seluruh pegawai suatu organisasi dalam mengejar atau memahami pengetahuan mengenai keamanan teknologi informasi. Dengan adanya kesadaran pengamanan, seorang pegawai dapat memfokuskan perhatiannya pada sebuah atau sejumlah permasalahan atau ancaman-ancaman yang mungkin terjadi [13]. Tujuan kesadaran keamanan informasi adalah untuk meningkatkan keamanan dengan melakukan hal berikut:[13]

1. Pemilik. Pengguna maupun custodian dari informasi paham akan tanggung jawab mereka terhadap sistem keamanan informasi dan mengajar mereka bagaimana bentuk pengamanan yang tepat sehingga membantu untuk mengubah perilaku mereka menjadi lebih sadar akan keamanan.
2. Mengembangkan kemampuan dan pengetahuan sehingga pemilik, pengguna maupun custodian informasi dapat melakukan pekerjaan mereka dengan lebih aman.
3. Membangun pemahaman akan pengetahuan yang diperlukan untuk merancang, mengimplementasikan, atau mengoperasikan program pembinaan kesadaran keamanan informasi untuk organisasi.

"Information Security" akan selalu mempunyai hambatan dalam pelaksanaannya. Untuk itu terdapat beberapa teknik yang digunakan oleh para ahli dalam menangani hambatan yang terjadi pada *InfoSec*, diantaranya [16] : Memanfaatkan teknik secara natural dengan fokus pada pengembangan perangkat keras dan perangkat lunak serta fokus pada perkembangan jaringan. Akan tetapi *InfoSec* bukan hanya mencangkup masalah teknis tetapi juga "pelaku" atau people. Pada dasarnya *InfoSec* selain mempunyai *hardware*, *software* dan jaringan yang bagus, harus mempunyai pelaku *"people"* yang kompeten dalam memanfaatkan teknologi tersebut [16]. Melindungi organisasi dari ancaman *cyber* hampir sama fungsinya dengan *security* yang berjaga pada malam hari. Semakin dia tidak mengantuk dan tetap berjaga maka, tidak akan ada kesempatan pencurian terjadi [17]. *Information Security Awareness* dibagi menjadi dua sektor, yaitu sektor publik dan sektor swasta *(private)*. Yang mencangkup sektor publik yaitu, *"Government awareness"* dan *"educational institutions awareness".Government awareness* merupakan sektor kesadaran tentang keamanan informasi yang terjadi di pemerintahan [17]. Di Indonesia *Government awareness* nya adalah dengan adanya ID-CERT dan ID SIRTI [15]. *Educational institutions awareness* pemberian pelajaran kepada institusi perguruan tinggi tentang pentingnya keamanan informasi. Beberapa hal yang harus disampaikan kepada mahasiswa di universitasnya adalah *security awareness, security policy,procedures,and guidelines,disaster recovery planning support*, dan *system monitoring and response*[17]. Yang mencangkup *private sector* adalah *financial institutions awareness*, *manufacturing industry's awareness*. Dalam institusi keuangan, seperti Bank dan Broker harus mempunyai sistem keamanan informasi yang canggih contohnya penggunaan *secure socket layers* (SSL), *data encryption*, dan *digital certificates provide decent protection to financial institutions*[17]. Kemudian untuk bagian manufacturing adalah penggunaan *Virtual Private Network (VPN)* yang melindungi mereka ketika berhubungan dengan *supplier* [17]. Penelitian ini menggunakan pendekatan teori verifikasi. Ada beberapa tipe perilaku yang dijadikan sebagai referensi peneliti dalam penelitian ini, dapat dilihat pada Tabel1 [16].

Dari literature tersebut , penelitian ini berhipotesis bahwa pengguna teknologi di suatu perusahaan yang memiliki pengetahuan tentang *InfoSec*, akan lebih mempunyai sikap positif dan berhati-hati terhadap pengelolaan *InfoSec* daripada pengguna teknologi yang tidak memiliki pengetahuan tentang *InfoSec*. Oleh karena itu, peneliti menggunakan tiga dimensi utama untuk mengukur pemahaman pelaku tentang *InfoSec*, yaitu pengetahuan, sikap dan perilaku [17].

3. Metode Penelitian

Penelitian ini menggunakan metode penelitian kualitatif deskriptif, kata kualitatif menyiratkan penekanan pada proses dan makna yang tidak dikaji secara ketat atau sebelum diukur dari sisi kuantitas, jumlah, intensitas atau frekuensinya. Secara garis besar, teknik pengumpulan data kualitatif menggunakan teknik wawancara dan survei[18]. Penelitian deksriptif adalah penelitian yang berusaha mendeksripsikan suatu gejala, peristiwa, kejadian yang terjadi saat sekarang. Penelitian deskriptif memusatkan perhatian pada

masalah aktual sebagaimana adanya pada saat penelitian berlangsung [18]. Teknik pengumpulan data yang peneliti gunakan adalah teknik wawancara. Wawancara merupakan salah satu teknik pengumpulan data yang dilakukan dengan berhadapan secara langsung dengan yang diwawancarai. Jenis wawancara yang digunakan adalah wawancara terstruktur. Wawancara terstruktur adalah wawancara yang pewawancaranya menetapkan sendiri masalah dan pertanyaan – pertanyaan yang akan diajukan. Pokok–pokok yang dijadikan dasar pertanyaan diatur secara sangat struktur [18]. Dalam proses pengambilan sampel peneliti menggunakan teknik *purposive sampling*, yaitu teknik penentuan sampel dengan pertimbangan khusus sehingga layak dijadikan sampel [18]. Pertimbangan khusus pada penelitian ini adalah :

- Responden merupakan salah satu pegawai pada Bank X di Bandung.
- Responden ahli dalam bidang IT dan *Information Security Management*.

Responden paham akan implementasi kebijakan keamanan informasi yang ada pada Bank X. Responden kami merupakan Kabag IT pada Bank X, peneliti memberikan beberapa pertanyaan dengan susunan pertanyaan sebagai berikut :

3.1. Jumlah Pegawai dan Jenis Kelamin

Jumlah pegawai merupakan pertanyaan yang bertujuan mengidentifikasi karakteristik objek yang akan kami teliti, dari jumlah dapat diketahui tingkat kesulitan pihak manajemen, semakin banyak jumlah pegawai maka semakin sulit untuk memberikan kesadaran bagi pegawai [16]. Selain itu komponen yang lainnya adalah jenis kelamin. Jenis kelamin menentukan sikap dan etika ketika sedang beroperasi dengan menggunakan internet, karena laki-laki lebih rasional dalam menggunakan internet dibandingkan wanita yang cenderung mengikuti suasana hati [2].

3.2. Mengukur Pengetahuan

Pengetahuan dari pegawai Bank X diukur dengan mengajukan pernyataan kepada responden, kemudian responden menanggapi dengan memberikan jawaban "YA" atau "TIDAK" tentang kondisi dari pegawai selama kurun waktu satu tahun terakhir. Responden juga dipersilahkan untuk memberikan argumen tentang pernyataan yang diajukan peneliti., dimana responden merupakan kepala bagian *Information and Technology* yang bertanggung jawab atas seluruh keamanan informasi di Bank X. Komponen pernyataan yang peneliti ajukan adalah sebagai berikut [19] :

3.2.1 Manajemen Keamanan Informasi
3.2.2 Manajemen Risiko
3.2.3 Manajemen Insiden
3.2.4 Manajemen Asset
3.2.5 *Access Control*

Mengacu pada Dokumen KOMINFO tahun 2011, kelima komponen pernyataan tersebut dianggap oleh peneliti cukup mewakili dasar-dasar ilmu *InfoSec* yang harus dimiliki oleh pegawai perbankan [19]. Terdapat dua pernyataan yang diajukan peneliti untuk masing – masing komponen, sehingga total pernyataan yang diajukan pada bagian pengukuran pengetahuan karyawan sebanyak sepuluh pernyataan. Penilaian yang digunakan peneliti adalah [16]:

- Penilaian baik, apabila rata–rata jawaban responden adalah "YA" untuk masing - masing pernyataan yang diajukan.
- Penilaian buruk, apabila rata–rata jawaban responden adalah "TIDAK" untuk masing – masing pernyataan yang diajukan.

3.3. Mengukur Sikap dan Perilaku

Untuk mengukur sikap dan perilaku pegawai Bank X, peneliti memberikan pernyataan yang berhubungan dengan tingkah laku pegawai Bank X. Dengan kriteria pengukuran sebagai berikut [16]:

3.3.1 Perilaku Pegawai Baik

Pegawai Bank X dapat dikatakan berperilaku baik apabila pegawai Bank X mengikuti setiap kebijakan yang telah ditetapkan oleh perusahan, dengan kriteria sebagai berikut [16][20] :

- Selalu log-off saat komputer tidak digunakan.
- Menolak email dari sumber yang tidak diketahui.
- Menggunakan hanya *software* yang *authorized.*
- Tidak mengakses media sosial selama waktu kerja.
- Pengiriman email, hanya dilakukan menggunakan jaringan yang aman.
- Dokumen penting yang tidak dibutuhkan lagi harus dimusnahkan dan dihancurkan.
- Selalu waspada dalam mengenali dan mendekati pengguna yang tidak sah *(unauthorized).*

3.3.2 Perilaku Pegawai Netral

Perilaku pegawai netral digambarkan dengan pernyataan "meninggalkan laptop kerja tanpa pengawasan, tidak melaporkan insiden

keamanan". Kriteria lebih lanjut terdapat pada Tabel 1 [16][20].

3.3.3 Perilaku Pegawai Tidak Baik

Perilaku pegawai tidak baik digambarkan dengan pernyataan "hack account orang lain, membuat dan menyebarkan email spam". Kriteria pegawai tidak baik terdapat pada Tabel 1 [16][21]. Untuk mengukur jenis perilaku pegawai, peneliti menggunakan teori Pattinson and Anderson (2007) [16]. Lihat Tabel 1 pada literature.

Tabel 1. Tipe Perilaku Pegawai dalam Bekerja [16]

Perilaku yang baik (deliberate)	Perilaku Netral (accidental)	Perilaku Buruk (deliberate)
Selalu log-off saat komputer tidak sedang digunakan	Berbagi nama pengguna dan password	Meng-hack akun orang lain
Menolak email dari sumber yang tidak diketahui	Membuka email yang tidak jelas sumbernya	Membuat dan mengirim email spam
Menggunakan software yang telah *authorized*	Mengakses situs yang meragukan	Mengunduh konten video ke komputer kerja melalui *peer-to-peer file sharing*
Tidak mengakses media sosial selama waktu kerja	Tidak mempertimbangkan konsekuensi negatif sebelum posting sesuatu di jejaring sosial	Memposting informasi sensitif mengenai tempat kerja di jejaring sosial
Pengiriman email, hanya menggunakan jaringan yang aman	Meninggalkan laptop kerja tanpa pengawasan	Konfigurasi nirkabel gerbang yang memberikan akses tidak sah ke jaringan perusahaan
Dokumen penting yang tidak dibutuhkan lagi harus di musnahkan dan dihancurkan	Meninggalkan DVD atau dokumen yang mengandung informasi sensitif pada meja kerja semalaman	Menulis dan menyebarkan kode berbahaya *(Malicious Code)*
Selalu waspada dalam mengenali dan mendekati pengguna yang tidak sah *(unauthorized)*	Tidak melaporkan insiden keamanan	Memberikan hak akses ke orang sembarangan

3.4. Mengukur Keberhasilan Kebijakan Keamanan Informasi di Perusahaan Bank X

Pada bagian ini, peneliti memberikan pertanyaan yang akan dijawab oleh responden secara jelas dan singkat mengenai kebijakan yang ada didalam perusahaan Bank X. Mengukur keberhasilan kebijakan keamanan informasi pada perusahaan dapat dilakukan dengan menganalisis ketepatan penempatan diterapkannya suatu kebijakan, dan apabila prosedur kebijakan belum diterapkan secara tepat. Terdapat dua faktor penyebabnya yaitu, sosialisasi kebijakan yang terlalu singkat atau prosedur yang terlalu rumit atau kurang praktis [19].

4. Hasil Penelitian

4.1. Tingkat Kesulitan Bank X dalam Mengelola Manajemen Keamanan Informasi Berdasarkan Jumlah dan Jenis Kelamin Pegawai.

Jumlah pegawai Bank X di Indonesia saat ini memiliki lebih dari 6.500 pegawai. Jumlah itu tersebar di lebih dari 330 kantor yang terdapat di 59 kota di seluruh Indonesia [21]. Di Bandung terdapat 130 orang pegawai dengan rincian jumlah pegawai laki-laki 80 orang dan jumlah pegawai perempuan adalah 50 orang. Hal ini seperti yang ada di Tabel 2 .

Tabel 2. Pengelompokan jumlah pegawai Bank X berdasarkan jenis kelamin

Jenis Kelamin	Jumlah Pegawai
Laki-laki	80
Perempuan	50
Total	130

Dari data diatas didapatkan hasil bahwa semakin banyak jumlah pegawai yang ada di Bank, maka tingkat kesulitan dalam mengelola manajemen keamanan informasi semakin sulit [16]. Namun karena data jumlah pegawai laki-laki pada Bank X Bandung lebih banyak dari perempuan, maka tingkat kesulitan mengelola keamanan informasi lebih rendah atau tergolong medium. Hal ini dikarenakan laki-laki lebih rasional dibandingkan perempuan dalam menggunakan internet [2].

4.2. Tingkat Pengetahuan Pegawai Bank X

Berdasarkan hasil wawancara peneliti dengan responden, didapatkan hasil sebagai berikut : hasil tentang mengukur tingkat pemahaman pegawai mengenai manajemen keamanan informasi, manajemen risiko, manajemen insiden, manajemen asset dan *access control*. Responden memberikan respon positif dengan memberikan jawaban "YA" yang berarti bahwa pegawai pada

perusahan Bank X rata-rata mempunyai pengetahuan dasar tentang manajemen keamanan informasi, manajemen risiko, manajemen insiden, manajemen asset dan *access control*. Responden juga menambahkan argumen bahwa pegawai di Bank X mampu membedakan subjek penting dalam sistem keamanan informasi yang berupa, *owner*, *user* dan pihak ketiga [13]. Selain itu, pegawai telah mengetahui faktor pemicu keamanan informasi [13]. Dengan demikian, peneliti menyimpulkan tingkat pemahaman pegawai terhadap keamanan informasi tergolong baik.

4.3. Sikap dan Perilaku Pegawai Bank X

Pada pengukuran sikap dan perilaku pegawai Bank X, peneliti memberikan pernyataan sebanyak tujuh pernyataan untuk masing – masing jenis perilaku sehingga total pernyataan yang diajukan peneliti adalah 21 pernyataan (Tabel 1). Dari 21 pernyataan tersebut, hasilnya sebagai berikut :

Tabel 3. Rekap hasil wawancara

PERNYATAAN	JUMLAH	
	YA	TIDAK
BAIK	5	2
NETRAL	2	5
TIDAK BAIK	0	7

Berdasarkan tabel tersebut, responden memberikan jawaban TIDAK pada perilaku karyawan baik sebanyak dua pernyataan, yaitu pernyataan mengenai "karyawan yang tidak membuka media sosial pada waktu kerja serta karyawan yang tidak membuka email dari pengirim yang tidak diketahui asal usulnya". Kemudian, responden memberikan jawaban YA pada pernyataan karyawan netral sebanyak dua pernyataan yaitu pernyataan mengenai "pegawai berbagi nama pengguna dan password serta membuka email yang tidak jelas pengirimnya". Untuk pernyataan pegawai tidak baik, responden menjawab TIDAK untuk semua pernyataan. Dari hasil tersebut, maka peneliti menyimpulkan bahwa pegawai pada Bank X rata-rata mempunyai kombinasi sikap dan perilaku baik - netral.

4.4. Tingkat Keberhasilan Penerapan Kebijakan Keamanan Informasi

Pada bagian ini peneliti mengajukan empat pernyataan, jawaban responden untuk masing – masing pertanyaan adalah sebagai berikut :

4.4.1 Kebijakan Keamanan Informasi pada Bank X Bandung

Bank X merupakan Bank internasional dengan menggunakan standar audit COBIT, TOGAF, dan ITIL, sehingga sangat diwajibkan adanya kebijakan keamanan informasi. Bank X harus memberikan pelayanan yang baik kepada pelanggannya. Untuk itu, perlindungan data dan informasi, baik yang ada di internal perusahaan maupun eksternal perusahaan, harus terjaga dengan baik dan aman. Kebijakan keamanan informasi pada Bank X Bandung meliputi kebijakan hak akses, kebijakan perlindungan semua data penting Bank X, kebijakan kerjasama pihak ketiga, kebijakan keberlangsungan bisnis apabila terjadi suatu insiden, kebijakan pelaporan insiden serta kebijakan–kebijakan lain yang berhubungan dengan standar COBIT, TOGAF, dan ITIL.

4.4.2 Implementasi Kebijakan Keamanan Informasi

Pengimplementasian kebijakan keamanan informasi pada Bank X Bandung dilakukan secara bertahap dan disesuaikan berdasarkan kebutuhan perlindungan informasi dengan prosedur kebijakan yang tidak rumit sehingga mudah dipahami oleh pegawai. Prosedur kebijakan yang tidak terlalu rumit seperti, adanya penyebaran informasi tentang kebijakan *security awareness* dari manajemen atas ke bawah melalui kepala bagian masing–masing area fungsional manajemen. Dengan begitu pegawai dapat dengan mudah mengikuti kebijakan yang dibuat oleh manajemen puncak Bank X dengan baik.

4.4.3 Keuntungan Implementasi Kebijakan Keamanan Informasi

Terdapat banyak sekali keuntungan yang didapat dengan mengimplementasikan kebijakan keamanan informasi apabila keamanan tersebut sesuai dengan kebutuhan, penempatan yang sesuai serta prosedur kebijakan yang tidak terlalu rumit. Keuntungan yang paling mendasar yaitu Bank X terlindungi dari oknum kejahatan penyebaran informasi dari dalam perusahaan. Dengan terlindunginya data pegawai, maka kepercayaan pelanggan meningkat. Dengan meningkatnya kepercayaan pelanggan maka kualitas dan nama Bank X akan menjadi suatu Brand yang menarik di mata masyarakat.

4.4.4 Kegiatan pada Bank X Bandung untuk Meningkatkan Kesadaran Pegawainya tentang Keamanan Informasi

Pada Bank X Bandung, setiap pegawai diberikan training dan seminar tentang keamanan informasi. Sebelum training, pegawai diwajibkan mengisi pertanyaan yang telah disediakan oleh instruktur. Setelah masa training dan seminar, pegawai

kembali diberikan tes untuk mengetahui keberhasilan dari training dan seminar sebelumnya serta untuk mengukur pengetahuan pegawai terhadap keamanan informasi. Untuk menjaga kestabilan pengetahuan keamanan informasi yang dimiliki oleh pegawainya, Bank X melaksanakan evaluasi secara berkala setiap tiga bulan sekali dengan memberikan kuesioner kepada pegawai–pegawainya.

5. Kesimpulan

Pada Bank X Bandung, pelaksanaan kebijakan keamanan informasi berjalan dengan baik, serta pegawai Bank X Bandung rata–rata telah mempunyai tingkat kesadaran terhadap keamanan informasi. Bank X Bandung merupakan Bank dengan tingkat kesuksesan yang tinggi dan mempunyai prospek yang bagus dimasa depan, karena perusahaan tersebut mempunyai pegawai dengan tingkat pengetahuan tentang keamanan informasi yang bagus dan berperilaku baik. Kedepannya, Bank X Bandung harus lebih mampu mendefinisikan area terpenting yang harus dilindungi dari kejahatan informasi, dengan memberikan pendidikan tentang *information security awareness*, seperti mensosialilasisikan teknik pengelolaan password.

Daftar Pustaka

[1] Kementerian Kominfo (2014,3,Mei). Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta [Online]. Tersedia:http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_ satker [23 April 2015].

[2] Agung Prasetyo (2014, 11, 27) .59 Persen pengguna Internet Akses via smartphone [online]. Tersedia:http://www.tempo.co/read/news/2014/11/27/072624959/59-Persen-Pengguna-Internet-Akses-Via- Smartphone.

[3] Pembinaan Kesadaran Keamanan Informasi di Lingkungan Sekolah Tinggi Sandi Negara Berdasarkan Standar National Institute of Standard and Technology (NIST SP 800-100) Jumiati,Santi Indarjani, Dwi Destrya Sofiana Volume 2011, 1 (2011) Institut Teknologi Bandung.

[4] Kamis, 14 April 2011 Pembobol ATM Senilai Rp.250 juta Ditangkap (Sabtu, 18 April 2015) Wasi'ulUlum / www.tempo.co/.

[5] Paulus Yoga. 2013 BCA SIAP GANTI KERUGIAN NASABAH KORBAN PENCURIAN DATA KARTU. sabtu 18 april 2015. www.infobanknews.com.

[6] Rachmad Faisal Harahap (2015, 01,14). Pembobolan ATM Merajalela di Pusat Perbelanjaan [online] Tersedia: economy.okezone.com.

[7] Lukman Diah Sari (2015, 04, 20). Penyadapan ATM, Modus Baru Pencurian Uang Nasabah Bank [Online].Tersedia : news.metrotvnews.com.

[8] Fiki Ariyanti (2015, 04, 14). Bos OJK Belum Tahu soal Pembobolan 3 Bank Besar [Online].Tersedia : bisnis.liputan6.com.

[9] Arif Pitoyo.2014. Pencurian data M-banking bakal melonjak (sabtu 18 april 2015) www.merdeka.com.

[10] Hal Tipton and Micki Krause. 2005. Handbook of Information Security Management, CRC Press LLC.

[11] Undang-undang Republik Indonesia Nomor 14 tahun 2008 Tentang Keterbukaan Informasi Publik.

[12] Undang-undang Republik Indonesia Nomor 11 tahun 2008 Tentang Informasi dan Transaksi Elektronik.

[13] Jumiati, Santi Indarjani, Dwi Destrya Sofiana. 2011. Pembinaan Kesadaran Keamanan Informasi di Lingkungan Sekolah Tinggi Sandi Negara Berdasarkan Standar National Institute of Standard and Technology (NIST SP 800-100). Institut Teknologi Bandung

[14] Azah Anir Norman and Norizan Mohd Yasin. 2010. An Analysis of Information Systems Security Management (ISSM): The Hierarchical Organizations vs. Emergent Organization. International Journal of Digital Society (IJDS), Volume 1, Issue 3. Faculty of Computer Science and Information Technology, University of Malaya, Malaysia

[15] Aan AlBone. 2009. Pembuatan rencana keamanan informasi berdasarkan Analisis dan mitigasi risiko teknologi informasi. JURNAL INFORMATIKA VOL. 10, NO. 1, MEI 2009: 44 - 52 Jurusan Teknik Informatika, Universitas Pasundan : Bandung.

[16] Kathryn Parsons Agata McCormac Malcolm Pattinson Marcus Butavicius Cate Jerram , (2014),"A study of information security awareness in Australian.

[17] Steve Hawkins David C. Yen David C. Chou, (2000),"Awareness and challenges of Internet security", Information.

[18] Noor, Juliansyah. 2011. Metodologi Penelitian : Skripsi, Tesis, Disertasi, dan Karya Ilmiah. Jakarta : Kencana.

[19] Tim Direktorat Keamanan Informasi. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Dokumen Kominfo

[20] Hennie Kruger Lynette Drevin Tjaart Steyn, (2010),"A vocabulary test to assess information

[21] PT. Bank X, Tbk. 2014. " Sejarah Singkat". security awareness", Information Management & Computer Security, Vol. 18 Iss 5 pp. 316–327 [Online] Tersedia : http:// www.bank-x.com/