KAJIAN STANDAR BIDANG KEAMANAN

Eddy Herjanto dan Ellia Kristiningrum

Abstract

Many incidents have caused a big loss and death, due to either by nature or human interference. In order to reduce the loss, it is needed to develop references or guides, i.e. standards. The International Organization for Standardization (ISO), as a world organization on standardization, has paid enough attention to standards on security, as have been reflected in the use of security aspects as the main topic on 2005 ISO General Assembly. The purpose of this study is to know the development of international standards in the field of security as well as the development and the implementation of Indonesian national standards. The result of this study shows the importance to encourage the formulation of SNI in the field of security. This can be done by, among others, adoption to internasional standards, as well as the need to identify security standards priorities to be developed by the Technical Committees concerned.

Keywords: standard, security, technical committee

1. PENDAHULUAN

Gempa bumi, kecelakaan transportasi, kecelakaan industri, terorisme, dan bencana lainnya, baik yang disebabkan oleh alam secara langsung ataupun karena adanya campur tangan manusia, telah menimbulkan kematian dan kerugian yang sangat banyak di waktu yang sangat singkat. Keamanan menjadi faktor yang semakin menjadi perhatian manusia sebagai suatu kebutuhan yang diperlukan bagi semua pihak. Diperlukan suatu usaha agar manusia dapat merasa aman dalam bekerja, dalam perjalanan, maupun dalam aktivitas kehidupannya yang lain.

Diantara berbagai usaha tersebut ialah menyusun suatu acuan atau pedoman yang berbentuk standar bagaimana produk, peralatan kerja, sistem, dan proses harus dibangun agar tidak mengabaikan faktor keselamatan bagi pemakai dan manusia di sekitarnya. Standar keamanan juga dirumuskan tidak hanya untuk pencegahan kejadian-kejadian yang menyebabkan kematian dan kerugian manusia, misalnya gempa bumi, transportasi, wabah, banjir, kecelakaan industri, dan angin topan, tetapi juga untuk pencegahan terhadap bahaya terorisme dan serangan internet.

Sebagai organisasi standardisasi dunia, ISO telah mengembangkan agenda standardisasi keamanan internasional. Dalam General Assembly ISO tahun 2005 di Singapura, isu tentang standar keamanan dijadikan topik utama bersama standar tentang jasa. Dalam acara itu disebutkan bahwa tema untuk tahun 2005 adalah "*Global Trade in Services*" and "*Security and the Global Economy*". ISO juga telah menegaskan bahwa standardisasi keamanan harus dipertimbangkan dalam semua pengembangan standar.

Keamanan didefinisikan sebagai suatu kondisi dalam keadaan terlindung dari kerugian atau bahaya. Dalam pengertian yang umum, keamanan adalah suatu konsep yang serupa dengan keselamatan. Perbedaan tipis antara keduanya adalah tambahan penekanan pada hal yang dilindungi dari bahaya, yang datangnya dari luar. Sedangkan keselamatan berarti suatu kondisi selamat, baik secara fisik, sosial, spiritual, finansial, politik, emosional, jabatan, kejiwaan, atau keadaan lainnya, ataupun konsekuensi dari kegagalan, kerusakan, kesalahan, kecelakaan, kejahatan, dari suatu peristiwa tertentu yang menimbulkan bahaya (wikipedia, 2006)

Ruang lingkup standar keamanan sangat luas, standar keamanan juga dipergunakan dalam bidang informasi, yaitu untuk mengendalikan keamanan jaringan komputer, pengiriman dokumen dan barang-barang dari satu tempat ke tempat lain. Informasi merupakan salah satu sumber daya organisasi yang perlu dikelola seperti halnya sumber daya organisaasi yang lain. Informasi tidak berdaya guna atau bermanfaat jika tidak dikomunikasikan. Demikian pula halnya, informasi tidak bernilai jika tidak dimanfaatkan. Oleh karena itu, supaya informasi dapat dimanfaatkan atau dikomunikasikan, maka sudah sepantasnya dilakukan pengelolaan yang strategis. Pengelolaan ini mencakup program dan kegiatan akuisisi, pengorganisasian dan pendistribusian informasi dalam basis sistem yang terpadu dan terintegrasi yang dilakukan secara terus-menerus. Dalam pengelolaan ini

juga diperlukan suatu pengamanan yang layak. Keamanan informasi juga menjadi tantangan utama untuk sebagian besar organisasi. Sangat disayangkan, beberapa organisasi melupakan dengan cepat bahwa keamanan informasi tidak lebih dari sekedar masalah teknologi yang sederhana. Dalam kenyataannya, informasi merupakan bagian dari proses manajemen resiko yang bersambung, menyangkut semua informasi yang perlu untuk diproteksi.

Uraian di atas menggambarkan peran standar keamanan sangat diperlukan untuk mengendalikan kejadian-kejadian fatal yang menyangkut keselamatan manusia. Disamping itu, standar keamanan juga membantu menciptakan lingkungan yang lebih aman untuk melakukan bisnis dalam atau antar negara, karena dengan adanya standar keamanan, perpindahan barang dan jasa lebih terjamin. Keamanan juga merupakan urutan yang paling dasar yang harus dipenuhi terlebih dahulu dari sekian banyak kebutuhan manusia.

Permasalahan yang dihadapi di Indonesia mengenai standar keamanan, ialah:

a. Bagaimana perkembangan standar internasional di bidang keamanan?
b. Bagaimana perkembangan standar nasional Indonesia di bidang keamanan dan penerapannya?

Bertitik tolak dari permasalahan tersebut, penelitian ini bertujuan untuk mengetahui:

a. Perkembangan standar internasional bidang keamanan
b. Perkembangan standar keamanan di Indonesia dan penerapannya.

2. STANDAR BIDANG KEAMANAN

2.1 Standar internasional

Standar Internasional di bidang keamanan telah dikembangkan oleh ISO, melalui technical committee (TC) terkait. COPOLCO (2005) menyebutkan terdapat 35 TC yang telah merumuskan standar keamanan di bidangnya masing-masing. Sebagian dari 35 TC tersebut ditunjukkan dalam tabel berikut.

Tabel 1 Sebagian TC-ISO yang Telah Menyusun Standar Keamanan

No.	No. TC	Nama TC
1.	8	Ships and marine technology
2.	20	Aircraft and space vehicles
3.	21	Fire protection and fire safety
4.	34	Food products
5.	68	Financial services
6.	85	Nuclear energy
7.	94	Personal safety – protective clothing and equipment
8.	98	Design of structures
9.	104	Freight containers
10.	146	Air Quality
11.	204	Intelligent transportation systems
12.	207	Environmental management
13.	215	Health informatics
14.	147	Drinking water supply and water quality
15.	JTC 1/SC 17	Cards and personal identification
16.	JTC 1/SC 27	IT security
17.	JTC 1/SC 37	Biometrics
18.	JTC 1/SC 31	Automatic identification and data capture

Pada akhir 2005, standar bidang keamanan yang dipublikasikan ISO sebanyak 122 standar, yang antara lain berupa standar cara uji, sistem, dan spesifikasi seperti dilihat Lampiran A. Uraian selanjutnya menjelaskan secara singkat

perkembangan standar keamanan di beberapa TC-ISO.

TC 8 telah menghasilkan 3 standar di bidang keamanan, yang antara lain menyangkut spesifikasi sistem manajemen keamanan untuk rantai pasokan (*supply chain*), serta tentang keamanan transfer data untuk kapal dan teknologi kelautan. Standar terbaru yang dipublikasikan oleh TC 8 ialah ISO/PAS 28000:2005 tentang *Specification for security management systems for the supply chain*, yang akan membantu kelancaran dan keamanan perdagangan internasional. Menurut Bryden (2006), ISO/PAS 28000:2005 merupakan seri pertama dari beberapa dokumen yang berhubungan dengan keamanan manajemen. Dua dokumen lainnya sedang dalam perbaikan, yaitu ISO/PAS 28001 dan ISO/PAS 28004, yang kesemuanya akan dirangkum dalam satu *portfolio* sebagai standar ISO untuk keamanan rantai pasokan. Standar ini disusun oleh ISO/TC 8 berkolaborasi dengan komite teknis lainnya. Terdapat 14 negara yang berpartisipasi dalam penyusunan standar ini bersama-sama dengan badan organisasi internasional dan regional lainnya.

Standar ini memberikan beberapa prasyarat kepada organisasi untuk menetapkan, mengimplementasikan, memelihara, dan mengembangkan sistem manajemen keamanan rantai pasokan internasional yang menjadi pemikiran kelompok pemangku kepentingan, seperti pemerintah, pemilik barang (produsen), dan pelanggan. Untuk organisasi individu, penerapan ISO/PAS 28000:2005 menawarkan pendekatan sistematik untuk manajemen keamanan yang dapat meningkatkan kemampuan operasional dan meningkatkan kepercayaan mereka sebagai bagian dari pelanggan dan regulator. Sebagai tambahan, karena pendekatan tersebut merupakan hasil kesepakatan internasional, ISO/PAS 28000:2005 diharapkan dapat menghindari kesulitan dan perbedaan biaya yang mungkin berlawanan dengan kebutuhan nasional dan memfasilitasi perdagangan secara global untuk keuntungan bersama.

Standar keamanan yang dihasilkan oleh TC 204, antara lain menyangkut transportasi darat dan lalu lintas telematik, khususnya tentang petunjuk untuk keamanan pengumpulan pembayaran secara elektronik. Sementara, TC 215 mempublikasikan beberapa standar yang menyangkut tentang informatika di bidang kesehatan, yaitu tentang direktori jasa untuk keamanan, identifikasi dan komunikasi para profesional dan pasien.

JTC 1/SC 27 merupakan sub panitia teknis yang menyusun standar keamanan terbanyak yaitu 62 standar, yang berhubungan dengan keamanan jaringan sistem informasi. Hal ini menunjukkan begitu pentingnya standar bidang keamanan di bidang jaringan sistem informasi. Butir 2.2. akan membahas lebih lanjut tentang standar keamanan di bidang teknologi informasi.

Contoh-contoh di atas menunjukkan cakupan standar keamanan yang sangat luas, yang kesemuanya memang diperlukan bagi manusia untuk memperoleh keamanan dalam segala bidang. Tabel 1 juga menyiratkan bahwa faktor keamanan telah menjadi bagian penting dalam kegiatan standardisasi internasional. Jumlah TC yang telah merumuskan standar keamanan berkembang terus sejalan dengan meningkatnya kesadaran dan tuntutan akan keamanan internasional dan berkembangnya kompleksitas perdagangan global.

2.2 Standar Keamanan Bidang Teknologi Informasi

Teknologi informasi meliputi spesifikasi, disain, pengembangan sistem dan peralatan yang berhubungan dengan penangkapan, penyajian, pemrosesan, keamanan, pemindahan, pertukaran, presentasi, manajemen, organisasi, penyimpanan, dan perolehan kembali informasi (www.callio.com, 2006).

Berdasarkan kejadian-kejadian yang menyebabkan kerugian besar manusia, serangan terhadap sistem informasi merupakan ancaman yang perlu diwaspadai. Keamanan teknologi informasi telah dikembangkan ke dalam suatu industri terkemuka, sebagai pemenuhan kebutuhan, seperti identifikasi dan verifikasi.

Mengidentifikasi kebutuhan keamanan adalah sangat penting untuk suatu organisasi. Menurut ISO/IEC 17799:2005, terdapat tiga sumber pokok dari kebutuhan keamanan, yaitu:

1. Satu sumber yang diperoleh dengan cara menaksir resiko-resiko dari organisasi tersebut, mempertimbangkan strategi bisnis dan tujuan keseluruhan dari organisasi tersebut. Melalui penilaian resiko, perawatan untuk aset-aset organisasi bisa ditemukan.
2. Sumber lain ialah hukum/undang-undang, regulator dan kebutuhan kontrak, mitra perdagangan, dan layanan pelanggan serta lingkungan sosial ekonominya.
3. Sumber lain lagi ialah prinsip utama, tujuan dan kebutuhan bisnis untuk proses informasi dari organisasi yang telah dikembangkan untuk mendukung pengoperasian.

Sistem informasi saat ini merupakan sumber daya penting, mempunyai nilai strategis dan mempunyai peranan yang sangat penting sebagai daya saing, kompetensi utama dan dalam keberlangsungan hidup dari suatu organisasi. Kenyamanan, kemudahan dan keuntungan yang dijanjikan dalam setiap pengembangan dan implementasi suatu sistem informasi, disadari juga sebagai upaya yang menjadikan atau menempatkan sistem informasi semakin rentan akan potensi ancaman (*threats*). Sehingga menjadi suatu prinsip dasar bahwa dalam pengelolaan sistem informasi juga harus diimbangi dengan perhatian yang serius terhadap keamanan sistem informasi (*information system security*).

Keamanan sistem informasi disadari merupakan salah satu bagian yang penting dalam melakukan pengelolaan sistem informasi. Prinsip-prinsip kerahasiaan, integritas dan ketersediaan data dan informasi (*confidentiality*, *integrity and availability* - *CIA*) menjadi taruhan utama dalam setiap upaya-upaya pengamanan terhadap sistem informasi. Kebijakan, prosedur, teknik dan mekanisme keamanan harus mampu menjamin sistem informasi dapat terlindungi dari berbagai potensi ancaman yang mungkin timbul, atau setidaknya mampu mengurangi kerugian yang diderita apabila ancaman terhadap sistem informasi teraktualisasi.

Hasil penelitian *e-Criem Wacth Survey* (Kahardityo, et al, 2004) menunjukkan bahwa ancaman keamanan tidak saja berasal dari luar tetapi dapat berasal dari dalam lingkungan sendiri. Tabel 2 menunjukkan daftar ancaman keamanan pada sistem informasi. Jumlah data sebanyak 500 kejadian selama tahun 2003.

Tabel 2 Ancaman Keamanan pada Sistem Informasi

Sumber ancaman	Persentase
Hackers	40%
Karyawan baru	22%
Karyawan lama	6%
Pelayanan baru, kontraktor, konsultan	3%
Pelanggan	2%
Kesatuan asing	2%
Pesaing	2%
Teroris	1%
Pelayanan lama, kontraktor, konsultan	1%
Pemasok/rekan kerja	<1%
Tidak diketahui	20%

Sumber: Kahardityo, et al (2004)

Tabel 3 memperlihatkan adanya beberapa tipe kejahatan yang terjadi pada sistem informasi. Jumlah sampel yang digunakan sebanyak 342 kejadian. Kejahatan ini bisa dilakukan oleh pihak dari dalam sendiri ataupun pihak dari luar, yang tujuannya untuk menghancurkan atau menghilangkan data-data penting dalam sistem jaringan informasi. Virus yang menyerang sistem jaringan informasi merupakan tipe kejahatan yang paling banyak ditemukan. Virus seringkali dapat merusak semua sistem dalam komputer, bahkan menghilangkan data-data penting yang ada dalam jaringan informasi. Penipuan dan pencurian hak milik juga sering dilakukan lewat sistem informasi. Seringkali sabotase juga dilakukan oleh pihak-pihak tertentu baik dari dalam maupun dari luar untuk mendapatkan suatu informasi dengan cara yang ilegal.

Tabel 3 Tipe Kejahatan Elektronik

Tipe Kejadian	Persentase
Virus	77%
Pengingkaran serangan	44%
Generasi ilegal dari SPAM email	38%
Akses tanpa otorisasi oleh orang dalam	36%
Phishing (metode pengambilan hak milik)	31%
Penipuan	22%
Pencurian hak milik	20%
Pencurian atas kepemilikan info	16%
Pencurian identitaas karyawan	12%
Sabotase oleh orang dalam	11%
Sabotase oleh orang luar	11%
Pemerasan oleh orang dalam	3%
Pemerasan oleh orang luar	3%
Lain-lain	11%
Tidak diketahui	8%

Sumber: Kahardityo, et al (2004)

Upaya-upaya yang bersifat pencegahan terhadap potensi ancaman yang mungkin timbul menjadi sangat penting, selain upaya pendeteksian kejahatan terhadap sistem informasi,serta upaya pemulihan sistem informasi. Pencegahan menjadi penting karena pencegahan dapat menghindarkan pengelola dari timbulnya kejahatan, kerugian yang besar. Upaya pencegahan terhadap serangan kejahatan sistem informasi menurut penelitian *e-Criem Wacth Survey* (Kahardityo, et al, 2004) sebagai berikut:

Tabel 4. Upaya Pencegahan Kejahatan terhadap Sistem Informasi

Pencegahan	Persentase
Firewalls	98%
Keamanan sistem secara fisik (sistem akses kontrol elektronik, CCTV, dll)	94%
Manajemen penambalan secara manual	91%
Enkripsi tingkat kritis pada saat pengiriman	85%
Akses kendali (*Role-based*)	85%
Instruksi sistem pendeteksian yang dimonitor oleh personal	81%
Teknologi jaminan informasi (jalur akses yang digunakan)	76%
Managemen tambalan yang diotomatiskan	74%
Sistem perintah untuk penghapusan yang dimonitor oleh sistem alarm otomatis	74%
Enkripsi tingkat kritis pada saat penyimpanan	71%
Teknologi anti-fraud bekerjasama dengan sistem ERP	63%
Penggunaan biometrik, *smart card*, dll	56%
Pengawasan tanpa kawat	54%
Tombol yang dimonitor sistem individu	39%

Sumber: Kahardityo, et al (2004)

Komite teknis ISO yang menangani tentang keamanan teknologi informasi ialah JTC 1/SC 27 (IT Security) yang sekretariatnya ditangani oleh DIN, Jerman. ISO JTC 1 SC 27 mempunyai P member sebanyak 32 negara dan O member sebanyak 11 negara, Indonesia termasuk ke dalam O member.

Ruang lingkup dari ISO JTC 1 SC 27 ini meliputi:

1. identifikasi kebutuhan secara umum (termasuk metodologi requirement) untuk jasa keamanan sistem teknologi informasi.
2. pengembangan mekanisme dan teknik keamanan (termasuk prosedur pendaftaran dan hubungan antara komponen-komponen keamanan)
3. pengembangan petunjuk keamanan (dokumen-dokumen interpretatif dan analisis resiko)
4. pengembangan manajemen pendukung standar dan dokumentasi (istilah dan kriteria evaluasi keamanan).

Proyek baru yang sedang dikembangkan oleh SC ini adalah *WG study period* dengan topik Sistem Manajemen Keamanan Informasi (ISMS). Daftar standar yang masuk dalam program penyusunan oleh ISO JTC 1/SC 27 dapat dilihat pada Lampiran B, sedangkan Lampiran C menyajikan data standar yang telah dipublikasikan oleh ISO JTC 1/SC 27.

Dari sekian banyak standar bidang keamanan informasi yang telah dipublikasikan, terdapat dua standar baru, yaitu ISO 17799:2005 tentang "*Code of Practice for Information Security Management*", dan ISO/IEC 27001:2005 tentang *"Information Security Management System – Requirement*"

2.2.1 ISO 17799:2005

ISO 17799:2005 pada awalnya merupakan standar yang diadaptasi dari BS 7799, "*Code of practice for information security management",* pertama kali dipublikasikan sebagai standar UK pada tahun 1995, mengandung praktek kontrol keamanan terbaik untuk mendukung industri dan pemerintah dalam mengimplementasikan dan meningkatkan keamanan informasi. Pertama kali dipublikasikan, organisasi di seluruh dunia menyadari bahwa BS 7799 menyediakan satu bahasa umum untuk manajemen keamanan informasi.

Pada saat banyak organisasi di dunia mengimplementasikan BS 7799, negara lain memulai untuk menerbitkan standar nasional mereka, seperti Belanda (SPE 20003), Australia/New Zealand (AS/NZS 4444), Denmark dan Swedia (SS 627799). BS 7799 juga langsung diterjemahkan dalam berbagai macam bahasa, misalnya Perancis, Jerman, *Finish, Dutch*, Cina/Mandarin, Norwegia, *Danish*, Swedia, Portugal, Korea, dan Jepang.

BS 7799 yang dipublikasikan pada bulan Maret 1999 diadopsi dalam bentuk ISO 17799:2000, dibawah penanganan JTC 1 SC 27. Revisi terbaru dari ISO/IEC 17799:2000 ini telah dipublikasikan menjadi ISO/IEC 17799:2005 yang berjudul "*Code of Practice for Information Security Management*". Standar ini mengandung 134 grup kontrol dalam 11 area untuk mendukung keamanan informasi. Kontrol ini berdasarkan dari pengalaman perusahaan, tanpa tergantung pada ukuran atau bisnis perusahaan tersebut. Kesebelas area dalam standar ini antara lain kebijakan keamanan, organisasi keamanan informasi, aset menegemen, keamanan sumber daya masnusia, keamanan fisik dan lingkungan, manajemen komunikasi dan operasi, akses kontrol, didapatnya sistem informasi, pengembangan dan pemeliharaan, manajemen kecelakaan keamanan informasi, manajemen bisnis yang berkelanjutan, pemenuhan.

ISO 17799:2005 dapat digunakan oleh organisasi untuk menetapkan program manajemen sistem informasi secara menyeluruh ataupun untuk meningkatkan kegiatan keamanan sistem informasi secara langsung. Tujuan dari ISO 17799 adalah untuk menyediakan dasar yang umum untuk mengembangkan standar-standar keamanan organisasi dan manajemen praktek keamanan yang praktis dan untuk menyediakan rasa percaya diri dalam hubungan antar organisasi. ISO 17799:2005 ini akan menarik perhatian organisasi-organisasi yang menyimpan sistem-sistem dan informasi rahasia dalam sistem internal ataupun eksternal, organisasi tersebut bergantung pada informasi ini untuk menjalankan aktivitasnya.

2.2.2 ISO/IEC 27001:2005

ISO tentang *"Information Security Management System – Requirement*" diadopsi dari BS 7799:2002 bagian 2, yang mencakup isu keamanan informasi. Standar ini mengedepankan persyaratan untuk *Information Security Management System (ISMS),* dan mencakup 10 kontrol, antara lain kebijakan keamanan, aset organisasi dan sumber daya, pembagian dan kontrol aset, keamanan personel, keamanan fisik dan lingkungan, managemen komunikasi dan operasi, kontrol

akses, sistem pengembangan dan pemeliharaan, managemen bisnis yang berkelanjutan, pemenuhan.

Standar ini dipublikasikan pada Oktober 2005, merupakan standar sistem manajemen keamanan informasi. Standar ini dimaksudkan untuk menyediakan suatu model untuk menetapkan, menerapkan, mengoperasikan, monitoring, meninjau ulang, memelihara dan meningkatkan suatu sistem manajemen keamanan informasi.

3. SNI BIDANG KEAMANAN

3.1 Ketersediaan SNI

Standar Nasional Indonesia (SNI) merupakan satu-satunya standar yang berlaku secara nasional di Indonesia. Berdasarkan situs jaringan BSN 1 Februari 2006, SNI yang berhubungan dengan keamanan yang telah ditetapkan sebanyak 17 standar seperti ditunjukkan dalam Tabel 5.

Tabel 5 Daftar SNI Bidang Keamanan

NO SNI	JUDUL	NO ICS
SNI 16-4778-1998	Persyaratan khusus keamanan peralatan bedah frekuensi tinggi	11.040.30
SNI 04-3888.1-1995	Persyaratan keamanan untuk kipas angin listrik serta pengatur kecepatannya. Bagian 1 : Kipas angin serta pengatur kecepatannya untuk pemakaian rumah tangga dan sejenisnya	23.120
SNI 04-4516-1998	Persyaratan keamanan untuk kipas angin listrik serta pengatur kecepatannya	23.120
SNI 04-4517-1998	Pedoman dan prosedur pengoperasian dan keamanan pemasangan instrumen pneumatik yang digerakkan oleh gas proses asosiasi	23.140
SNI 04-1704-1989	Lampu berfilamen tungsten untuk penerangan rumah tangga dan penerangan umum yang sejenis, Persyaratan keamanan	29.140.20
SNI 06-6501.1-2000	Refrigeran kelompok A3: Keamanan pengisian penyimpanan dan transportasi	29.160.30
SNI 03-6460.3-2000	Tata cara keamanan penerowongan untuk konstruksi sipil. Bagian 3: Komunikasi, kebisingan dan transportasi	93.060
SNI 03-6460.1-2000	Tata cara keamanan penerowongan untuk konstruksi sipil. Bagian 1: Perencanaan dan organisasi	93.060
SNI 03-6460.2-2000	Tata cara keamanan penerowongan untuk konstruksi sipil. Bagian 2: Bahaya darurat dan lingkungan kerja	93.060
SNI 03-1731-1989	Pedoman keamanan bendungan	93.160
SNI 04-1921-1995	Keamanan pemanfaatan listrik rumah tangga dan sejenis. Bagian 2: Persyaratan khusus untuk lemari pendingin dan pembeku makanan	97.040.30
SNI 05-3061-1992	Peralatan pendinginan kecil, Keamanan	97.040.30
SNI 04-6292.2-2000	Keamanan pemanfaat listrik rumah tangga dan sejenisnya. Bagian 2: Persyaratan khusus untuk kukusan listrik (bains marie) komersial	97.040.50
SNI 12-6527.1-2001	Keamanan mainan. Bagian 1: Spesifikasi sifat fisis dan mekanis	97.200.50
SNI 12-6527.2-2001	Keamanan mainan. Bagian 2: Spesifikasi sifat mudah terbakar	97.200.50
SNI 12-6527.3-2001	Keamanan mainan. Bagian 3: Spesifikasi untuk perpindahan elemen-elemen tertentu	97.200.50
SNI 12-6527.4-2001	Keamanan mainan. Bagian 4: Spesifikasi untuk peralatan percobaan kimia dan aktivitas yang terkait	97.200.50

Sumber: www.bsn.or.id, 1 Februari 2006

Dari tabel dapat dilihat sebagian besar dari standar tersebut telah berusia lebih dari 5 tahun, yang memerlukan kaji ulang atas kelayakannya untuk dapat digunakan sebagai acuan dalam industri dan perdagangan. Dari 17 standar yang telah dipublikasikan tersebut, terdapat 15 standar yang memerlukan proses kaji ulang, yaitu proses yang diberlakukan untuk SNI yang sudah berumur lebih dari 5 tahun dan diragukan kelayakannya, karena tidak sesuai lagi dengan perkembangan ilmu pengetahuan dan teknologi maupun kebutuhan pasar.

Kecepatan perumusan SNI tersebut menggambarkan bahwa kesiapan SNI bidang keamanan sangat rentan. Perlu perbaikan terhadap kondisi standar nasional terkait jika akan dipergunakan instrumen dalam regulasi teknis.

3.2 Penerapan SNI Bidang Keamanan

SNI pada dasarnya merupakan standar sukarela yaitu penerapannya bersifat sukarela. SNI yang berkaitan dengan kepentingan keselamatan, keamanan, kesehatan, kelestarian fungsi lingkungan hidup, atas dasar pertimbangan tertentu dapat diberlakukan secara wajib oleh instansi teknis. SNI tersebut disebut sebagai SNI wajib.

Penerapan standar dimaksudkan untuk mendukung terwujudnya jaminan mutu barang, jasa, proses, sistem atau personel sehingga dapat memberikan kepercayaan kepada pelanggan dan pihak terkait bahwa suatu organisasi, individu, barang dan/atau jasa yang diberikan telah memenuhi persyaratan yang ditetapkan. Selain itu penerapan standar juga dimaksudkan untuk menjamin peningkatan produktivitas, daya guna dan hasil guna serta perlindungan terhadap konsumen, tenaga kerja, dan masyarakat dalam hal keselamatan, keamanan, kesehatan dan kelestarian fungsi lingkungan hidup. Sampai saat ini, standar bidang keamanan yang telah dipublikasikan oleh BSN belum ada yang diterapkan oleh pelaku usaha.

3.3 Jenis Standar Keamanan yang Diperlukan

Banyaknya standar di bidang keamanan yang dipublikasikan oleh ISO, menunjukkan bahwa ISO mempunyai perhatian khusus untuk bidang keamanan, termasuk jaringan sistem informasi. Namun sampai saat ini, belum ada standar yang mengatur tentang kerusakan keamanan yang disebabkan alam, misalnya banjir, gempa bumi, dan bencana alam lainnya.

Sedangkan SNI bidang keamanan yang telah dipublikasikan meliputi bidang peralatan medis, sistem fluida, kelistrikan, rekayasa sipil, rumah tangga, hiburan, dan olah raga. SNI yang telah dipublikasikan tersebut sebagian besar mengenai persyaratan keamanan, prosedur dan spesifikasi teknis untuk keamanan. Jika melihat perkembangan standar internasional bidang keamanan yang sudah dipublikasikan oleh ISO, maka SNI yang perlu dirumuskan antara lain meliputi bidang keamanan jaringan informasi, perkapalan dan teknologi kelautan, pesawat terbang dan saranan angkut penerbangan, proses serta elemen data dan dokumen di (dalam) perdagangan, administrasi dan industri; servis finansial, dll. Adanya perkembangan perumusan standar bidang keamanan yang dilakukan ISO dapat dijadikan acuan untuk perumusan SNI oleh Panitia Teknis perumusan SNI yang bersangkutan.

4. PENUTUP

4.1 Kesimpulan

Pentingnya keamanan disegala bidang telah menjadi perhatian dunia, khususnya ISO sebagai organisasi standar dunia. Hal ini disebabkan karena dengan adanya standar bidang keamanan dapat digunakan untuk mencegah kematian dan kerugian besar bagi manusia.

Dari hasil kajian, dapat disimpulkan bahwa:

a. Standar internasional bidang keamanan yang telah dipublikasikan oleh ISO melalui beberapa TC nya adalah sebanyak 122 standar yang antara lain berupa standar cara uji, spesifikasi dan sistem, dan jumlahnya terus berkembang. Standar terbaru yang dipublikasikan antara lain ISO/IEC 17799:2005 dan ISO/IEC 27001:2005, keduanya adalah standar di bidang keamanan untuk teknologi informasi. Sedangkan untuk perkapalan dan teknologi kelautan, standar terbaru yang dipublikasikan adalah ISO/PAS 28000:2005.

b. Indonesia telah mempublikasikan beberapa standar di bidang keamanan, namun melihat kondisi SNI bidang keamanan yang ada, masih banyak yang harus dilakukan pembenahan ataupun penambahan untuk pengembangan, agar konsumen bisa terlindungi dan dapat dilaksanakan secara efektif. Alternatif yang dapat diambil, antara lain dengan cara menginformasikan kepada Panitia Teknis perumusan SNI tentang data standar

internasional di bidang keamanan yang sedang dikembangkan ISO.

4.2 Saran

a. Indonesia sebaiknya melakukan pembenahan ataupun penambahan untuk pengembangan SNI di bidang keamanan, dengan melihat perkembangan perumusan standar internasional di bidang keamanan

b. Sebaiknya Indonesia dapat mengadopsi standar terbaru tentang keamanan jaringan informasi, yaitu ISO 17799:2005 tentang "*Code of Practice for Information Security Management*", ISO/IEC 27001:2005 tentang "*Information Security Management System – Requirement*" tersebut menjadi SNI, dan ISO/PAS 28000:2005 tentang *Spesification for Security Management System for Supply Chain*"

Selain daripada itu, perlu dikembangkan keberadaan Panitia Teknis yang berhubungan dengan bidang keamanan untuk proses perumusan SNI. Lampiran A juga dapat dijadikan pertimbangan sebagai acuan dalam mengadopsi standar bidang keamanan menjadi SNI.

DAFTAR PUSTAKA

1. Badan Standardisasi Nasional, www.bsn.or.id, 2006
2. Bryden, A. 2006. ISO/PAS 28000:2005. ISO Focus
3. Foo, Cedric. 2005. Opening Ceremony of the ISO Open Session *in* 2005 ISO General Assembly. Geneve: ISO Secretariat
4. George, A.W. 2005. The ISO Advisory Group on Security. 2005 COPOLCO Workshop
5. International Organisation for Standardization, www.iso.org, 2006
6. Kahardityo, Widagso, dan Wisnuaji. 2004. Keamanan Sistem Informasi untuk Usaha Kecil dan Menengah: Studi terhadap PT. IMT. Magister Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Indonesia
7. ISO/IEC 17799:2005
8. Siang, Yu Chien. 2005. Why Security Matters *in* 2005 ISO general Assembly. Geneve: ISO Secretariat
9. Sturgeon, Alice. 2005. Security as a Prime Mover in ISO's Work *in* 2005 ISO General Assembly. , www.iso.org.ch
10. www.callio.com, 2006
11. http://en.wikipedia.org/wiki/security, 2006

BIODATA

Eddy Herjanto, Alumni Program Studi Ekonomi Pertanian, Institut Pertanian Bogor, 2003 dan *Industrial & Systems Engineering Department,* Ohio University, 1991. Penulis bekerja di Badan Standardisasi Nasional.

Ellia Kristiningrum, menyelesaikan program S1 bidang Teknik Kimia UPN Veteran Yogyakarta, 2003. Penulis bekerja pada Pusat Penelitian dan Pengembangan Standardisasi, Badan Standardisasi Nasional.