Akademi
Esensi Teknologi Informasi dan Komunikasi untuk Pimpinan Pemerintahan

Modul 6

Keamanan Jaringan dan Keamanan Informasi dan Privasi

UNITED NATIONS ESCAP / APCICT
ASIAN AND PACIFIC TRAINING CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY FOR DEVELOPMENT

ECONOMIC AND SOCIAL COMMISSION FOR ASIA AND THE PACIFIC

ASIAN AND PACIFIC TRAINING CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY FOR DEVELOPMENT

Akademi Esensi Teknologi Informasi dan Komunikasi untuk Pimpinan Pemerintahan

Modul 6

Keamanan Jaringan dan Keamanan Informasi dan Privasi

Korea Information Security Agency

UNITED NATIONS ESCAP Economic and Social Commission for Asia and the Pacific / APCICT ASIAN AND PACIFIC TRAINING CENTRE FOR INFORMATION AND COMMUNICATION TECHNOLOGY FOR DEVELOPMENT

Seri Modul Akademi Esensi Teknologi Informasi dan Komunikasi untuk Pimpinan Pemerintahan

Modul 6: Keamanan Jaringan dan Keamanan Informasi dan Privasi

Kontak:

United Nations Asian and Pacific Training Centre for
Information and Communication Technology for Development
Bonbudong, 3rd Floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu-gu, Incheon City
Republic of Korea

Telepon: +82 32 245 1700-02
Fax: +82 32 245 7712
E-mail: info@unapcict.org

http://www.unapcict.org

ISBN: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Desain dan Tata Letak: Scandinavian Publishing Co., Ltd.
Dicetak di: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

SAMBUTAN

Abad 21 ditandai dengan bertumbuhnya saling ketergantungan antara orang-orang di dunia global. Sebuah dunia dimana peluang terbuka bagi jutaan orang melalui teknologi-teknologi baru, perluasan akses ke informasi dan pengetahuan esensial yang dapat mengembangkan kehidupan masyarakat secara signifikan dan membantu mengurangi kemiskinan. Namun hal ini hanya mungkin terjadi jika pertumbuhan saling ketergantungan diiringi dengan nilai-nilai, komitmen dan solidaritas bersama untuk pembangunan yang inklusif dan berkelanjutan, dimana kemajuan yang dicapai adalah untuk semua orang.

Dalam beberapa tahun terakhir, Asia dan Pasifik telah menjadi 'kawasan superlatif' jika dikaitkan dengan teknologi informasi dan komunikasi (TIK). Menurut *International Telecommunication Union*, terdapat dua miliar pelanggan telepon dan 1,4 miliar pelanggan telepon seluler di kawasan Asia Pasifik. India dan Cina sendiri mengambil porsi seperempat dari pengguna telepon seluler di dunia pada pertengahan 2008. Kawasan Asia Pasifik juga mewakili 40 persen pengguna Internet dan merupakan pasar *broadband* terbesar di dunia dengan porsi sebanyak 39 persen dari total dunia.

Seiring dengan kondisi kemajuan teknologi yang cepat tersebut, banyak yang bertanya-tanya apakah kesenjangan dijital akan hilang. Sayangnya, jawaban pertanyaan tersebut adalah 'belum'. Bahkan lima tahun sesudah *World Summit on the Information Society* (WSIS) diselenggarakan di Geneva pada tahun 2003, dan terlepas dari semua terobosan teknologi yang mengesankan dan komitmen pemain kunci di kawasan, akses ke komunikasi dasar masih belum terjangkau oleh sebagian besar masyarakat, terutama yang miskin.

Lebih dari 25 negara di kawasan, terutama negara berkembang kepulauan kecil (*small island*) dan negara berkembang tanpa perairan (*land-locked*), memiliki kurang dari 10 pengguna Internet per 100 orang, dan pengguna tersebut sebagian besar terkonsentrasi di kota-kota besar, sementara di sisi lain, beberapa negara maju di kawasan yang sama mempunyai rasio lebih dari 80 pengguna Internet per 100. Disparitas *broadband* antara negara maju dan negara berkembang bahkan lebih menyolok.

Untuk mengatasi kesenjangan dijital dan mewujudkan potensi TIK untuk pembangunan inklusif sosial-ekonomi di kawasan, penyusun kebijakan di negara berkembang perlu menentukan prioritas, menyusun kebijakan, memformulasikan kerangka kerja hukum dan peraturan, mengalokasikan dana, dan memfasilitasi kemitraan yang memajukan sektor industri TIK dan mengembangkan keterampilan TIK di masyarakat.

Seperti tertuang dalam Rencana Aksi WSIS, "... setiap orang semestinya mendapatkan kesempatan untuk memperoleh keterampilan dan pengetahuan yang diperlukan untuk memahami, berpartisipasi, dan merasakan manfaat dari Masyarakat Informasi (*Information Society*) dan Ekonomi Pengetahuan (*Knowledge Economy*)". Sampai saat ini, Rencana Aksi tersebut menyerukan kerjasama regional dan internasional untuk peningkatan kapasitas dengan menekankan kepada penyediaan besar-besaran akan ahli-ahli dan profesional TI.

Untuk merespon seruan tersebut, APCICT telah menyusun kurikulum pelatihan komprehensif tentang TIK untuk pembangunan (*ICT for Development*-ICTD) – yaitu Akademi Esensi TIK untuk Pimpinan Pemerintahan (*Academy of ICT Essentials for Government Leaders*) – yang saat ini terdiri dari delapan modul dengan tujuan untuk memberikan pengetahuan dan kepakaran esensial yang dapat membantu para penyusun kebijakan dalam merencanakan dan mengimplementasikan inisiatif TIK dengan lebih efektif.

APCICT adalah salah satu dari lima institusi regional dari *United Nations Economic and Social Commission of Asia and the Pacific* (ESCAP). ESCAP mengembangkan pembangunan sosio-ekonomi yang inklusif dan berkelanjutan di Asia dan Pasifik melalui analisis, usaha normatif, peningkatan kapasitas, kerjasama regional dan berbagi pengetahuan. Dalam kerjasamanya dengan lembaga PBB lainnya, organisasi internasional, mitra nasional dan *stakeholder*, ESCAP, melalui APCICT, berkomitmen untuk mendukung penggunaan, kustomisasi dan penerjemahan modul-modul *Akademi* ke berbagai negara, serta pengajarannya secara reguler di serangkaian *workshop* nasional dan regional untuk aparatur pemerintahan tingkat menengah dan atas, dengan tujuan bahwa kapasitas yang dibangun dan pengetahuan yang didapat akan diterjemahkan ke dalam bentuk peningkatan kesadaran akan manfaat TIK dan aksi-aksi nyata untuk mencapai tujuan-tujuan pembangunan.

Noeleen Heyzer
Under-Secretary-General of the United Nations
dan Sekretaris Eksekutif ESCAP

PENGANTAR

Perjalanan dalam menyusun *Seri Modul Akademi Esensi TIK untuk Pimpinan Pemerintahan* merupakan pengalaman yang menakjubkan dan inspirasional. Seri modul ini tidak hanya mengisi kekosongan dalam peningkatan kapasitas di bidang TIK, tapi juga membuka cara baru dalam pengembangan kurikulum – melalui partisipasi dan kepemilikan banyak pihak dalam prosesnya.

Akademi ini merupakan program utama dari APCICT, yang telah disusun melalui analisis dan penelitian yang mendalam akan kekuatan dan kelemahan materi-materi pelatihan yang telah ada serta proses mitra bestari diantara para ahli. Serangkaian *workshop Akademi* yang telah dilangsungkan di berbagai negara di kawasan telah memberikan kesempatan yang sangat berharga untuk bertukar pengalaman dan pengetahuan diantara peserta yang berasal dari berbagai negara, sebuah proses yang membuat para alumni *Akademi* menjadi pemain kunci dalam membentuk modul.

Peluncuran secara nasional delapan modul awal *Akademi* ini menandai awal dari proses sangat penting dalam memperkuat kerja sama yang telah ada dan membangun kerja sama baru untuk meningkatkan kapasitas pengambilan kebijakan terkait TIK untuk Pembangunan (*ICT for Development*-ICTD) di seluruh kawasan. APCICT berkomitmen untuk menyediakan dukungan teknis dalam peluncuran *Akademi Nasional* sebagai pendekatan kunci untuk memastikan bahwa *Akademi* menjangkau para pengambil kebijakan. APCICT telah bekerja sama erat dengan sejumlah institusi pelatihan nasional dan regional yang telah membangun jaringan dengan pemerintah lokal maupun pusat, untuk meningkatkan kapasitas mereka dalam ICTD dengan mengkustomisasi, menerjemahkan dan menyelenggarakan *Akademi* yang memperhitungkan kebutuhan dan prioritas nasional. APCICT juga merencanakan untuk lebih memperdalam dan memperluas cakupan dari modul-modul yang sudah ada dan juga mengembangkan modul-modul baru.

Selanjutnya, APCICT juga menggunakan pendekatan multi-kanal untuk memastikan bahwa konten dari *Akademi* menjangkau lebih banyak orang di kawasan. Selain disampaikan dengan cara tatap muka melalui *Akademi* yang diselenggarakan di level nasional dan regional, juga tersedia APCICT *Virtual Academy* (AVA), sebuah media *online* untuk pembelajaran jarak jauh, yang dirancang untuk memungkinkan peserta dapat mempelajari materi sesuai dengan kecepatan mereka masing-masing. Di dalam AVA tersedia semua modul *Akademi* dan materi pendampingnya, seperti *slide* presentasi dan studi kasus, yang dapat dengan mudah diakses secara *online* untuk diunduh, digunakan kembali, dikustomisasi dan di-*lokal*-kan. AVA juga menyediakan berbagai fasilitas seperti kuliah virtual, perangkat manajemen pembelajaran, perangkat pengembangan konten dan sertifikasi.

Kedelapan modul yang telah disusun dan disampaikan melalui serangkaian *workshop Akademi* baik di level nasional, sub-regional, maupun regional tidak akan mungkin ada tanpa komitmen, dedikasi, dan partisipasi proaktif dari banyak individu dan organisasi. Saya ingin menggunakan kesempatan ini untuk menyampaikan penghargaan atas semua usaha dan pencapaian oleh para alumni *Akademi* dan rekan-rekan dari departemen/kementerian pemerintah, institusi pelatihan, dan organisasi nasional dan regional yang telah berpartisipasi dalam *workshop Akademi*. Mereka tidak hanya

memberikan masukan yang berharga terhadap isi modul, tetapi yang lebih penting, mereka menjadi penganjur *Akademi* di negara mereka masing-masing, yang akhirnya menghasilkan perjanjian formal antara APCICT dengan sejumlah mitra insititusi nasional dan regional untuk melakukan kustomisasi dan menyelenggarakan *Akademi* secara reguler di negara mereka.

Saya juga ingin menyampaikan penghargaan khusus untuk dedikasi orang-orang luar biasa yang telah membuat perjalanan ini menjadi mungkin. Mereka adalah Shahid Akhtar, Penasihat Proyek dari *Akademi*; Patricia Arinto, Editor; Christine Apikul, Manajer Publikasi; semua pengarang modul *Akademi*; dan tim APCICT.

Saya sungguh berharap bahwa *Akademi* ini dapat membantu bangsa untuk mempersempit kesenjangan sumber daya TIK, menghilangkan rintangan adopsi TIK, dan turut mempromosikan penggunaan TIK untuk mempercepat pembangunan sosial-ekonomi dan pencapaian *Millennium Development Goals* (Tujuan Pembangunan Milenium).

Hyeun-Suk Rhee
Direktur, APCICT

TENTANG SERI MODUL

Di 'era informasi' ini, kemudahan akses informasi telah mengubah cara kita hidup, bekerja dan bermain. 'Ekonomi dijital' (*digital economy*), yang juga dikenal sebagai 'ekonomi pengetahuan' (*knowledge economy*), 'ekonomi jaringan' (*networked economy*) atau 'ekonomi baru' (*new economy*), ditandai dengan pergeseran dari produksi barang ke penciptaan ide. Pergeseran tersebut menunjukkan semakin pentingnya peran Teknologi Informasi dan Komunikasi (TIK) bagi ekonomi dan masyarakat secara keseluruhan.

Akibatnya, pemerintah di seluruh dunia semakin fokus kepada penggunaan TIK untuk Pembangunan (dikenal dengan *ICT for Development*-ICTD). TIK untuk Pembangunan tidak hanya berarti pengembangan industri atau sektor TIK, tetapi juga mencakup penggunaan TIK yang dapat meningkatkan pertumbuhan ekonomi, sosial, dan politik.

Namun demikian, salah satu kendala yang dihadapi pemerintah dalam penyusunan kebijakan TIK adalah para penyusun kebijakan seringkali kurang akrab dengan teknologi yang mereka manfaatkan untuk pembangunan nasional. Karena seseorang tidak mungkin mengatur sesuatu yang tidak dimengerti olehnya, banyak penyusun kebijakan yang akhirnya menghindar dari penyusunan kebijakan di bidang TIK. Akan tetapi melepaskan penyusunan kebijakan TIK kepada para teknolog juga kurang benar karena teknolog seringkali kurang mawas akan implikasi kebijakan atas teknologi yang mereka kembangkan dan gunakan.

Seri modul Akademi *Esensi Teknologi Informasi dan Komunikasi untuk Pimpinan Pemerintahan* telah dikembangkan oleh *United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development* (UN-APCICT) untuk:

1. Penyusun kebijakan baik di tingkat pemerintah pusat maupun daerah yang bertanggung-jawab akan penyusunan kebijakan bidang TIK.

2. Aparatur pemerintah yang bertanggung jawab terhadap pengembangan dan implementasi dari aplikasi berbasis TIK; serta

3. Para manajer di sektor publik yang ingin memanfaatkan perangkat TIK untuk manajemen proyek.

Seri modul ini bermaksud untuk meningkatkan pengetahuan akan isu-isu pokok terkait TIK untuk Pembangunan baik dari perspektif kebijakan maupun teknologi. Tujuannya bukan untuk menyusun manual teknis TIK, tetapi lebih kepada memberikan pemahaman yang baik akan kemampuan teknologi digital saat ini atau kemana teknologi mengarah, serta implikasinya terhadap penyusunan kebijakan. Topik-topik yang dibahas dalam modul telah diidentifikasi melalui analisis kebutuhan pelatihan dan survei terhadap materi-materi pelatihan lain di seluruh dunia.

Modul-modul telah dirancang sedemikan rupa agar dapat digunakan untuk pembelajaran mandiri oleh pembaca individu atau juga sebagai rujukan untuk program pelatihan. Modul-modul dibuat berdiri sendiri sekaligus saling berkaitan satu sama lain, dan telah diusahakan agar setiap modul berkaitan dengan tema dan diskusi pada modul-modul

lain. Tujuan jangka panjangnya ialah agar modul-modul ini dapat digunakan dalam pelatihan yang dapat disertifikasi.

Setiap modul diawali dengan tujuan modul dan target pembelajaran yang ingin dicapai sehingga pembaca dapat menilai kemajuan mereka. Isi modul terdiri dari bagian-bagian yang termasuk di dalamnya studi kasus dan latihan-latihan untuk memperdalam pemahaman terhadap konsep utamanya. Latihan dapat dikerjakan secara individual ataupun secara berkelompok. Gambar dan tabel disajikan untuk mengilustrasikan aspek-aspek spesifik dari diskusi. Referensi dan bahan-bahan *online* juga disertakan agar pembaca mendapatkan pengetahuan tambahan tentang materi yang diberikan.

Penggunaaan TIK untuk Pembangunan sangatlah beragam sehingga terkadang studi kasus dan contoh-contoh baik di dalam modul maupun antara satu modul dengan modul lainnya mungkin terlihat kontradiksi. Hal ini memang diharapkan. Ini adalah gairah dan tantangan dari disiplin ilmu baru yang saat ini terus berkembang dan sangat menjanjikan sehingga semua negara mulai menggali kemampuan TIK sebagai alat pembangunan.

Sebagai bentuk dukungan bagi seri modul *Pendidikan* ini, telah tersedia sebuah media pembelajaran jarak jauh — *the APCICT Virtual Academy* (AVA – http://www.unapcict.org/academy) — dengan ruang kelas virtual yang memuat presentasi dalam format video dan slide presentasi dari modul.

Sebagai tambahan, APCICT juga telah mengembangkan *e-Collaborative Hub for ICTD* (e-Co Hub – http://www.unapcict.org/ecohub), sebuah situs *online* bagi para praktisi dan penyusun kebijakan TIK untuk meningkatkan pengalaman pelatihan dan pembelajaran mereka. E-Co Hub memberikan akses ke sumber pengetahuan akan berbagai aspek TIK untuk Pembangunan dan menyediakan ruang interaktif untuk saling berbagi pengetahuan dan pengalaman, serta berkolaborasi dalam peningkatan TIK untuk Pembangunan.

MODUL 6

Di Era Informasi ini, informasi adalah aset yang harus dijaga dan penyusun kebijakan perlu mengetahui apa itu keamanan informasi dan tindakan apa saja yang perlu dilakukan untuk menghadapi kebocoran dan pelanggaran informasi. Modul ini memberikan gambaran atas kebutuhan, isu-isu, dan tren keamanan informasi, serta proses penyusunan strategi keamanan informasi.

TUJUAN MODUL

Modul ini bertujuan untuk:

1. Menjelaskan konsep keamanan informasi, privasi, dan konsep terkait lainnya;

2. Menjelaskan ancaman terhadap keamanan informasi dan bagaimana mengatasinya;

3. Membahas persyaratan dalam menyusun dan mengimplementasikan kebijakan keamanan informasi, serta daur hidup kebijakan keamanan informasi; dan

4. Memberikan gambaran standar keamanan informasi dan proteksi privasi yang digunakan di beberapa negara dan organisasi keamanan informasi internasional.

HASIL PEMBELAJARAN

Setelah menyelesaikan modul ini, pembaca diharapkan mampu untuk:

1. Menjelaskan keamanan informasi, privasi dan konsep terkait;

2. Mengidentifikasi ancaman terhadap keamanan informasi;

3. Menilai kebijakan keamanan informasi yang ada dikaitkan dengan standar internasional keamanan informasi dan proteksi privasi; dan

4. Menyusun atau membuat rekomendasi tentang kebijakan keamanan informasi yang cocok dengan konteks masing-masing.

DAFTAR ISI

DAFTAR STUDI KASUS

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

APCERT	Asia-Pacific Computer Emergency Response Team
APCICT	Asian and Pacific Training Centre for Information and Communication Technology for Development
APEC	Asia-Pacific Economic Cooperation
BPM	Baseline Protection Manual
BSI	British Standards Institutution
BSI	Bundesamt fűr Sicherheit in der Informationstechnik, Germany
CAP	Certificate Authorizing Participant
CC	Common Criteria
CCP	Certificate Consuming Participant
CCRA	Common Criteria Recognition Arrangement
CECC	Council of Europe Convention on Cybercrime
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team Coordination Center
CIIP	Critical Information Infrastructure Protection
CISA	Certified Information Systems Auditor
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CM	Configuration Management
CSEA	Cyber Security Enhancement Act
CSIRT	Computer Security Incident Response Team
DID	Defense-In-Depth
DNS	Domain Name Server
DoS	Denial-of-Service
ECPA	Electronic Communications Privacy Act
EGC	European Government Computer Emergency Response Team
ENISA	European Network and Information Security Agency
ERM	Enterprise Risk Management
ESCAP	Economic and Social Commission for Asia and the Pacific
ESM	Enterprise Security Management
EU	European Union
FEMA	Federal Emergency Management Agency
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
FOI	Freedom of Information
GCA	Global Cybersecurity Agenda
HTTP	Hypertext Transfer Protocol
ICT	Information and Communication Technology
ICTD	Information and Communication Technology for Development
IDS	Intrusion Detection System
IGF	Internet Governance Forum
IM	Instant-Messaging
IPS	Intrusion Prevention System

ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization and International Electrotechnical Commission
ISP	Internet Service Provider
ISP/NSP	Internet and Network Service Provider
IT	Information Technology
ITU	International Telecommunication Union
ITU-D	International Telecommunication Union Development Sector
ITU-R	International Telecommunication Union Radiocommunication Sector
ITU-T	International Telecommunication Union Standardization Sector
KISA	Korea Information Security Agency
MIC	Ministry of Information and Communication, Republic of Korea
NIS	Network and Information Security
NISC	National Information Security Center, Japan
NIST	National Institute of Standards and Technology, USA
OECD	Organisation for Economic Co-operation and Development
OMB	Office of Management and Budget, USA
OTP	One-Time Passwords
PC	Personal Computer
PP	Protection Profile
PSG	Permanent Stakeholders Group
RFID	Radio Frequency Identification
SAC	Security Assurance Component
SFR	Security Functional Requirement
SME	Small and Medium Enterprise
ST	Security Target
TEL	Telecommunication and Information Working Group
TOE	Target of Evaluation
TSF	TOE Security Functions
UK	United Kingdom
UN	United Nations
US	United States
WPISP	Working Party on information Security and Privacy
WSIS	World Summit on the Information Society

DAFTAR IKON

 Pertanyaan

 Latihan

 Studi Kasus

 Ujian

 Tujuan

1. KEBUTUHAN AKAN KEAMANAN INFORMASI

Bagian ini bertujuan untuk:
- Menjelaskan konsep informasi dan keamanan informasi; dan
- Menjelaskan standar yang digunakan untuk aktivitas keamanan informasi.

Kehidupan manusia saat ini sangat bergantung pada teknologi informasi dan komunikasi (TIK). Hal ini membuat individu, organisasi dan negara sangat rentan akan serangan terhadap sistem informasi, seperti *hacking, cyberterrorism, cybercrime*, dan lain-lain. Tidak banyak individu dan organisasi yang siap menghadapi serangan-serangan tersebut. Pemerintah memiliki peranan penting untuk memastikan keamanan informasi dengan mengembangkan infrastruktur informasi-komunikasi dan membangun sistem untuk memberikan perlindungan terhadap ancaman-ancaman keamanan informasi.

1.1 Konsep Dasar Keamanan Informasi

Apakah yang dimaksud dengan 'informasi'?

Secara umum, informasi didefinisikan sebagai hasil dari aktivitas mental; merupakan produk abstrak yang ditransmisikan melalui medium. Dalam bidang TIK, informasi adalah hasil dari pemrosesan, manipulasi dan pengaturan data, yaitu sekumpulan fakta.

Dalam bidang Keamanan Informasi, informasi diartikan sebagai sebuah 'aset'; merupakan sesuatu yang memiliki nilai dan karenanya harus dilindungi. Definisi informasi dan keamanan informasi mengikuti ISO/IEC 27001 ini akan digunakan di keseluruhan modul ini.

Nilai yang diberikan kepada informasi saat ini merefleksikan pergeseran dari masyarakat pertanian ke masyarakat industri dan akhirnya ke masyarakat informasi. Dalam masyarakat pertanian, tanah adalah aset paling penting dan negara dengan produksi tani terbesar memiliki kekuatan bersaing. Dalam masyarakat industri, kekuatan modal, seperti memiliki cadangan minyak, menjadi faktor utama dalam persaingan. Dalam masyarakat berbasis informasi dan pengetahuan, informasi adalah aset paling berharga dan kemampuan untuk mendapatkan, menganalisis dan menggunakan informasi memberikan keunggulan bersaing bagi negara manapun.

Karena perspektif telah bergeser dari nilai aset bersih (NAB) ke nilai aset informasi, semakin disepakati perlunya perlindungan terhadap infomasi. Informasi itu sendiri bernilai lebih dari medium yang memegang informasi. Tabel 1 memperlihatkan perbandingan antara aset informasi dengan aset nyata.

Tabel 1. Perbandingan Aset Informasi dan Aset Nyata

Karakteristik	Aset informasi	Aset nyata
Bentuk-pemeliharaan	Tidak memiliki bentuk fisik dan bersifat fleksibel	Memiliki bentuk fisik
Variabel nilai	Bernilai lebih tinggi ketika digabung dan diproses	Total nilai adalah jumlah dari tiap nilai
Berbagi	Reproduksi yang tak terbatas, dan orang-orang dapat berbagi nilainya	Reproduksi tidak mungkin; dengan reproduksi, nilai aset berkurang
Ketergantungan-medium	Perlu disampaikan melalui medium	Dapat disampaikan secara independen (karena bentuk fisiknya)

Seperti yang terlihat pada Tabel 1, aset informasi benar-benar berbeda dengan aset nyata. Karenanya, aset informasi rentan terhadap jenis risiko yang berbeda.

Risiko terhadap aset informasi

Seiring dengan meningkatnya nilai aset informasi, keinginan orang untuk mendapatkan akses ke informasi dan mengendalikannya juga meningkat. Dibentuk kelompok-kelompok untuk menggunakan aset informasi demi berbagai tujuan dan beberapa mengerahkan segala tenaga untuk mendapatkan aset informasi dengan berbagai cara. Yang terakhir termasuk *hacking,* pembajakan, penghancuran sistem informasi melalui virus komputer, dan sebagainya. Risiko-risiko yang menyertai informatisasi ini didiskusikan pada Bagian 2 modul ini.

Aspek-aspek negatif dari lingkungan berorientasi informasi termasuk antara lain:

Peningkatan perilaku tidak etis yang timbul dari anonimitas - TIK dapat digunakan untuk memelihara anonimitas, yang mempermudah seseorang untuk melakukan tindakan tidak etis dan kriminal, termasuk perolehan informasi secara ilegal.

Konflik kepemilikan dan kontrol informasi – Permasalahan yang disebabkan oleh kepemilikan dan kontrol informasi meningkat dengan adanya pengembangan informatisasi. Sebagai contoh, karena pemerintah mencoba membangun sebuah basisdata informasi pribadi di bawah payung '*e-government*', beberapa sektor menyatakan kekhawatiran akan kemungkinan gangguan privasi dari penyingkapan informasi pribadi ke pihak lain.

Kesenjangan informasi dan kesejahteraan diantara kelas dan negara - Ukuran pemegang aset informasi dapat menjadi barometer kesejahteraan di masyarakat berbasis pengetahuan/informasi. Negara maju memiliki kemampuan untuk menghasilkan lebih banyak informasi dan mendapatkan keuntungan dari penjualan informasi sebagai produk. Di sisi lain, negara miskin informasi memerlukan investasi yang besar hanya untuk dapat mengakses informasi.

Pertumbuhan keterbukaan informasi disebabkan oleh majunya jaringan – Masyarakat berbasis pengetahuan/informasi adalah masyarakat jaringan. Seluruh dunia terhubung layaknya sebuah jaringan tunggal, yang berarti bahwa kelemahan satu bagian jaringan dapat berakibat buruk pada bagian lain.

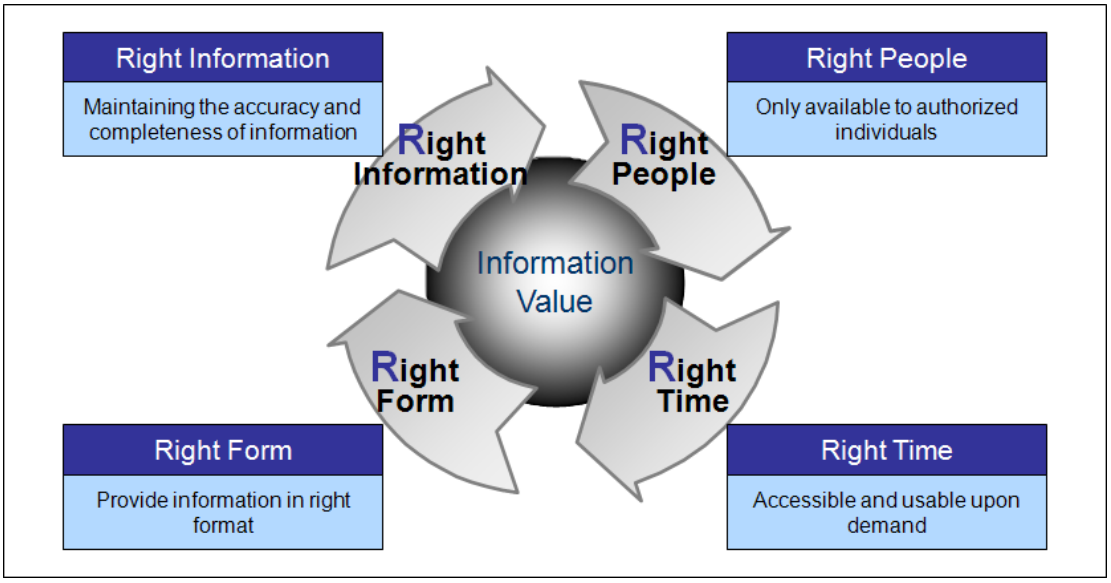
Apakah yang dimaksud dengan keamanan informasi?

Dalam menghadapi usaha perolehan informasi secara ilegal, orang-orang berusaha mencegah tindak kriminal terkait informasi atau berusaha meminimalisasi kerusakan akibat tindak kriminal tersebut. Inilah yang disebut dengan keamanan informasi.

Sederhananya, keamanan informasi menghargai nilai informasi dan melindunginya.

4R keamanan informasi

4R keamanan informasi adalah *Right Information* (Informasi yang benar), *Right People* (Orang yang tepat), *Right Time* (Waktu yang tepat) dan *Right Form* (Bentuk yang tepat). Pengaturan 4R adalah cara paling efisien untuk memelihara dan mengontrol nilai informasi.



Gambar 1. 4R Keamanan Informasi

'*Right Information*' mengacu pada ketepatan dan kelengkapan informasi, yang menjamin integritas informasi.

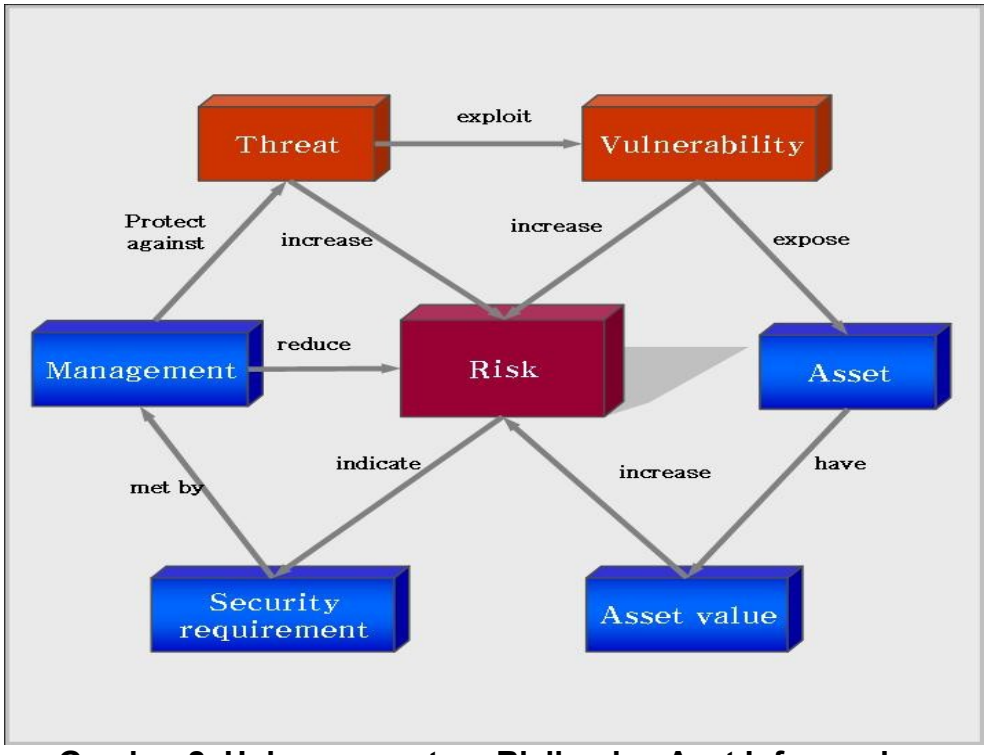
'*Right People*' berarti informasi tersedia hanya bagi individu yang berhak, yang menjamin kerahasiaan.

'*Right Time*' mengacu pada aksesibilitas informasi dan penggunaannya atas permintaan entitas yang berhak. Ini menjamin ketersediaan.

'*Right Form*' mengacu pada penyediaan informasi dalam format yang tepat.

Untuk menjaga keamanan informasi, 4R harus digunakan dengan tepat. Ini berarti bahwa kerahasiaan, integritas dan ketersediaan haruslah ditinjau ketika menangani informasi.

Keamanan informasi juga membutuhkan pemahaman yang jelas akan nilai aset informasi, serta kerentanannya terhadap berbagai ancaman. Ini disebut dengan manajemen risiko. Gambar 2 menunjukkan hubungan aset informasi dan risiko.



Gambar 2. Hubungan antara Risiko dan Aset Informasi

Risiko ditentukan oleh nilai aset, ancaman dan kerentanan. Rumusnya adalah sebagai berikut:

Risiko = ∫(Nilai Aset, Ancaman, Kerentanan)

Risiko berbanding lurus dengan nilai aset, ancaman dan kerentanan. Jadi, risiko dapat meningkat atau berkurang dengan memanipulasi besar dari nilai aset, ancaman dan kerentanan. Ini dapat dilakukan dengan manajemen risiko.

Metode-metode manajemen risiko adalah sebagai berikut:

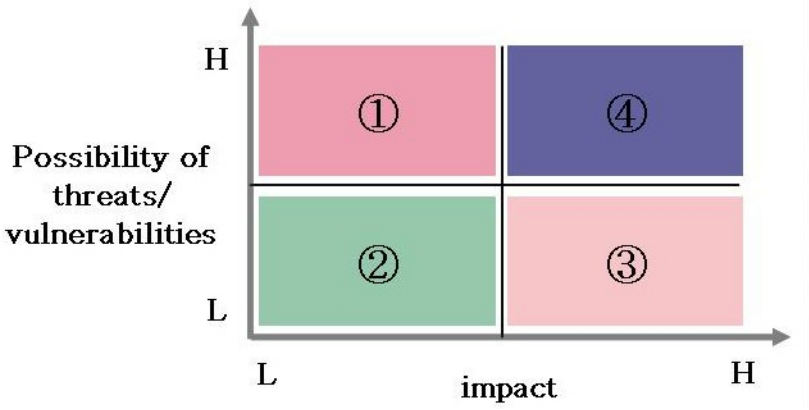
Pengurangan Risiko (Peringanan Risiko) - Ini dilakukan ketika kemungkinan ancaman/kerentanan tinggi tetapi dampaknya rendah. Diperlukan pemahaman akan ancaman dan kerentanan yang ada, mengubah atau menguranginya, dan membangun pertahanan. Akan tetapi, pengurangan risiko tidak mengurangi nilai risiko menjadi ‘0’.

Penerimaan Risiko - Ini dilakukan ketika kemungkinan ancaman/kerentanan rendah dan dampaknya kecil atau dapat diterima.

Pemindahan Risiko - Jika risiko sangat tinggi atau organisasi tidak mampu mempersiapkan kendali yang diperlukan, risiko dapat dipindahkan keluar dari organisasi. Contohnya adalah dengan mengambil polis asuransi.

Penghindaran Risiko - Jika ancaman dan kerentanan sangat mungkin terjadi dan dampaknya juga sangat tinggi, lebih baik menghindari risiko dengan misalnya melakukan alih daya perangkat pemrosesan data dan juga staf.

Gambar 3 adalah representasi grafis dari keempat metode manajemen risiko. Dalam gambar ini, kuadran '1' adalah pengurangan risiko, '2' adalah penerimaan risiko, '3' adalah pemindahan risiko, dan '4' adalah penghindaran risiko.



Gambar 3. Metode-metode Manajemen Risiko

Pertimbangan utama dalam memilih metode manajemen risiko yang tepat adalah efektivitas biaya. Analisis efektivitas biaya harus dilakukan sebelum rencana pengurangan, penerimaan, pemindahan, atau penghindaran risiko dilakukan.

1.2 Standar Kegiatan Keamanan Informasi

Kegiatan keamanan informasi tidak dapat dilakukan secara efektif tanpa mobilisasi rencana administrasi, fisik dan teknis yang menyatu.

Banyak organisasi telah merekomendasikan standar keamanan informasi. Contohnya antara lain persyaratan keamanan informasi dari *International Organization for Standardization and International Electrotechnical Commission* (ISO / IEC) dan daftar evaluasi dari *Certified Information Systems Auditor* (CISA), dan *Certified Information Systems Security Professional* (CISSP) dari *Information Systems Audit and Control Association* (ISACA). Standar ini merekomendasikan kegiatan keamanan informasi yang menyatu, seperti perumusan kebijakan keamanan informasi, penyusunan dan operasi organisasi keamanan informasi, manajemen sumber daya manusia, manajemen keamanan fisik, manajemen keamanan teknis, manajemen audit keamanan dan keberlanjutan bisnis.

Tabel 2 berisi daftar standar terkait domain keamanan informasi.

Tabel 2. Domain Keamanan Informasi dan Standar Terkait

***Domain* keamanan**	**ISO/IEC 27001**	**CISA**	**CISSP**
Administratif	▪ Kebijakan Keamanan	▪ Tata Kelola TI	▪ Penerapan Manajemen Keamanan ▪ Model dan Arsitektur Keamanan
	▪ Organisasi Keamanan Informasi	▪ Tata Kelola TI	
	▪ Manajemen Aset	▪ Perlindungan Aset Informasi	▪ Penerapan Manajemen Keamanan
	▪ Keamanan Sumber Daya Manusia		
	▪ Manajemen Insiden Keamanan Informasi	▪ Keberlanjutan Bisnis dan Pemulihan Bencana	▪ Perencanaan Keberlanjutan Bisnis dan Pemulihan Bencana
	▪ Manajemen Keberlanjutan Bisnis	▪ Keberlanjutan Bisnis dan Pemulihan Bencana	▪ Perencanaan Keberlanjutan Bisnis dan Pemulihan Bencana
	▪ Kepatuhan	▪ Proses Audit SI	▪ Hukum, Investigasi dan Etika
Fisik	▪ Keamanan Fisik dan Lingkungan		▪ Keamanan Fisik
Teknis	▪ Manajemen Komunikasi dan Operasi	▪ Manajemen Daur Hidup Sistem dan Infrastruktur	▪ Kriptografi ▪ Keamanan Teleko-munikasi dan Jaringan ▪ Keamanan Operasi
	▪ Pengaturan Akses		
	▪ Akuisisi, Pengembangan, dan Pemeliharaan SI	▪ Dukungan dan Penyampaian Pelayanan TI	

ISO/IEC27001[1] fokus kepada keamanan administratif. ISO/IEC27001 secara khusus menekankan audit dokumentasi dan operasi sebagai perilaku administratif dan ketaatan kepada kebijakan/pedoman dan hukum. Diperlukan konfirmasi yang terus menerus dan pertahanan oleh administrator. Jadi, ISO/IEC27001 mencoba mengatasi titik-titik lemah dari sistem keamanan, peralatan, dan lainnya dengan cara administratif.

Sebaliknya, tidak disebutkan keamanan sumber daya manusia ataupun fisik dalam CISA,[2] yang fokus pada kegiatan audit dan pengendalian sistem informasi. Karenanya, peranan auditor dan kinerja proses audit sangat penting.

CISSP[3] fokus utamanya pada keamanan teknis. CISSP menekankan pada pengaturan dan pengendalian peralatan seperti *server* atau komputer.

Latihan

1. Kajilah tingkat kesadaran keamanan informasi dari anggota organisasi Anda.

2. Apa saja langkah keamanan informasi yang dilaksanakan organisasi Anda? Klasifikasikan langkah-langkah dalam empat metode keamanan informasi.

3. Sebutkan contoh langkah keamanan informasi dalam domain administratif, fisik dan teknis di organisasi Anda atau organisasi lain di negara atau wilayah Anda.

Peserta pelatihan dapat melakukan latihan ini dalam kelompok kecil. Jika peserta berasal dari negara berbeda, pembagian kelompok dapat berdasarkan negara.

[1] ISO, "ISO/IEC27001:2005," http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.
[2] Lihat ISACA, "Standards for Information Systems Auditing," http://www.isaca.org/Template.cfm?Section=CISA_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=19566
[3] Lihat http://www.isc2.org/cissp

Ujian

1. Apakah perbedaan informasi dengan aset-aset lainnya?
2. Mengapa keamanan informasi berhubungan dengan kebijakan?
3. Apa cara-cara memastikan keamanan informasi? Sebutkan perbedaan berbagai metode dalam menangani keamanan informasi
4. Sebutkan perbedaan ketiga domain keamanan informasi (administratif, fisik dan teknis).

2. TREN DAN ARAH KEAMANAN INFORMASI

Bagian ini bertujuan untuk:
- Menggambarkan ancaman terhadap keamanan informasi; dan
- Menjelaskan tindakan untuk menghadapi ancaman tersebut.

2.1 Jenis-jenis Serangan Keamanan Informasi

Hacking

Hacking adalah tindakan memperoleh akses ke komputer atau jaringan komputer untuk mendapatkan atau mengubah informasi tanpa otorisasi yang sah.

Hacking dapat dikelompokkan dalam *hacking* 'iseng', kriminal atau politis, bergantung pada tujuan serangan. *Hacking* hiburan adalah modifikasi program dan data tanpa izin hanya untuk memenuhi rasa penasaran *hacker*. *Hacking* kriminal dilakukan untuk penipuan atau pengintaian. *Hacking* politis adalah merusak situs *web* untuk menyebarkan pesan-pesan politis tanpa izin.[4]

Baru-baru ini, *hacking* makin terlibat dalam *cyberterror* dan *cyberwarfare*, mengakibatkan ancaman serius terhadap keamanan nasional.

Perang Jaringan Orang Cina dan Orang Amerika

Sebuah kelompok *hacker* AS yang disebut PoizonBox dituduh merusak lebih dari 350 situs *web* Cina dalam satu bulan. Kelompok ini juga diduga menyerang 24 situs *web* Cina, termasuk situs *web* delapan organisasi pemerintah Cina, dalam satu hari pada 30 April 2001. *Hacker-hacker* Cina kemudian mengumumkan *Sixth Network War of National Defense* dan menyerang situs-situs *web* AS, termasuk situs *web* organisasi pemerintah AS, selama satu minggu dari 30 April hingga 1 Mei 2001. Serangan tersebut membuat Pentagon meningkatkan status keamanan sistem komputernya dari INFO-CON NORMAL menjadi INFO-CON ALPHA. Pada 1 Mei 2001, *Federal Bureau of Investigation's National*

[4] Suresh Ramasubramanian, Salman Ansari and Fuatai Purcell, "Governing Internet Use: Spam, Cybercrime and e-Commerce," dalam Danny Butt (ed.), *Internet Governance: Asia-Pacific Perspectives* (Bangkok: UNDP-APDIP, 2005), 95, http://www.apdip.net/projects/igov/ICT4DSeries-iGov-Ch5.pdf.

Infrastructure Protection Center mengeluarkan peringatan bahwa *hacker-hacker* Cina menyerang situs *web* pemerintah dan perusahaan AS.

Sesudah perang jaringan, AS menyadari bahwa ancaman elektronik (seperti *hacking*) dapat menyebabkan banyak kerusakan pada organisasi pemerintah AS dan kemudian meningkatkan pertahanan terhadap *cyberthreats* dengan menambah anggaran keamanan informasi dan memperbaiki kebijakan informasi didalam organisasi pemerintah.

Sumber:
Attrition.org, "Cyberwar with China: Self-fulfilling Prophecy" (2001), http://attrition.org/security/commentary/cn-us-war.html.

Denial-of-Service

Serangan *Denial-of-service* (DoS) mencegah pengguna yang sah dari penggunaan layanan ketika pelaku mendapatkan akses tanpa izin ke mesin atau data. Ini terjadi karena pelaku 'membanjiri' jaringan dengan volume data yang besar atau sengaja menghabiskan sumber daya yang langka atau terbatas, seperti *process control blocks* atau koneksi jaringan yang tertunda. Atau mereka mengganggu komponen fisik jaringan atau memanipulasi data yang sedang dikirimkan, termasuk data terenkripsi.[5]

Teror *Cyber* terhadap Estonia

Pada tanggal 4 Mei 2007 di ibukota Estonia, pemindahan monumen kejayaan USSR dari pusat kota ke pemakaman militer membangkitkan serangan teror *cyber* selama tiga minggu terhadap Estonia yang terdiri dari serangan DoS pada jutaan komputer. Jaringan komputer dan situs *web* istana presiden, parlemen Estonia, berbagai departemen pemerintah, partai yang berkuasa, pers, dan bank hancur. Bahkan jaringan nirkabel juga diserang.

Estonia kemudian menemukan bahwa lokasi penyerang berada di organisasi pemerintah Rusia. Pemerintah Rusia menolak tuduhan tersebut.

Ketika serangan teror *cyber* terjadi, Estonia tidak dapat segera merespon karena kurangnya tim yang menanggapi kecelakaan dan kebijakan keamanan informasi.

[5] ESCAP, "Module 3: Cyber Crime and Security," http://www.unescap.org/icstd/POLICY/publications/internet-use-for-business-development/module3-sources.asp.

Sumber:
Beatrix Toth, “Estonia under cyber attack” (Hun-CERT, 2007),
http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

Malicious code (Kode Berbahaya)

Malicious code adalah program yang menyebabkan kerusakan sistem ketika dijalankan. Virus, *worm* dan *Trojan horse* merupakan jenis-jenis *malicious code*.

Virus komputer adalah sebuah program komputer atau kode program yang merusak sistem komputer dan data dengan mereplikasi dirinya sendiri melalui peng-*copy*-an ke program lain, *boot sector* komputer atau dokumen.

Worm adalah virus yang mereplikasi dirinya sendiri yang tidak mengubah *file*, tetapi ada di *memory* aktif, menggunakan bagian dari sistem operasi yang otomatis dan biasanya tidak terlihat bagi pengguna. Replikasi mereka yang tidak terkontrol memakan sumber daya sistem, melambatkan atau menghentikan proses lain. Biasanya hanya jika ini terjadi keberadaan *worm* diketahui.

Trojan horse adalah program yang sepertinya bermanfaat dan/atau tidak berbahaya tetapi sesungguhnya memiliki fungsi merusak seperti *unloading hidden program* atau *command scripts* yang membuat sistem rentan gangguan.

Krisis Internet 1.25 Republik Korea

Pada 25 Januari 2003, sebuah virus komputer yang disebut ‘*Slammer worm*’ menyebabkan putusnya koneksi Internet di seluruh negara di Republik Korea. Putusnya koneksi Internet ini, selama lebih dari sembilan jam, disebabkan oleh gangguan terhadap layanan *domain name server* (DNS) oleh *worm* tersebut.

Sebagai hasil dari putusnya koneksi tersebut, *online shopping malls* mengalami kerugian sekitar US$ 200.000-500.000 dan kerugian hingga US$ 22,5 miliar dalam *online trading*. Dilaporkan bahwa kerusakan yang disebabkan oleh *Slammer worm* lebih parah daripada kerusakan yang disebabkan oleh Codred dan Nimda karena pelakunya merupakan pengguna umum.

Krisis Internet ini memotivasi pemerintah Korea untuk melakukan manajemen yang komprehensif terhadap Penyedia Jasa Internet dan Perusahaan Keamanan Informasi. Sistem untuk perlindungan infrastruktur informasi dan penilaian keamanan informasi dibangun, dan organisasi atau komite keamanan informasi dibentuk di tiap organisasi.

Social engineering

'*Social engineering*' adalah sekumpulan teknik untuk memanipulasi orang sehingga orang tersebut membocorkan informasi rahasia. Meskipun hal ini mirip dengan permainan kepercayaan atau penipuan sederhana, istilah ini mengacu kepada penipuan untuk mendapatkan informasi atau akses sistem komputer. Di banyak kasus pelaku tidak pernah bertemu secara langsung dengan korban.

Phishing, tindakan mencuri informasi personal melalui Internet dengan tujuan penipuan finansial, merupakan contoh dari *social engineering*. *Phishing* telah menjadi aktivitas kriminal yang banyak dilakukan di Internet.

Bank Swedia Diserang Perampokan *Online* Terbesar

Pada tanggal 19 Januari 2007, Bank Swedia Nordea diserang *phishing online*. Serangan dimulai oleh sebuah Trojan yang dikirim atas nama bank ke beberapa nasabahnya. Pengirim meminta nasabah untuk mengunduh aplikasi '*spam fighting*'. Pengguna yang mengunduh berkas yang dilampirkan, dinamai 'raking.zip' atau 'raking.exe', terinfeksi oleh Trojan yang juga dikenal sebagai 'haxdoor.ki' oleh beberapa perusahaan keamanan.

Haxdoor biasanya memasang *keyloggers* untuk merekam *keystrokes* dan menyembunyikan dirinya menggunakan *rootkit*. Muatan varian .ki dari Trojan diaktifkan ketika nasabah berusaha *log-in* ke situs *online banking* Nordea. Pengguna diarahkan ke situs palsu, dimana mereka memasukkan informasi *log-in* penting, termasuk angka-angka untuk *log-in*. Setelah pengguna memasukkan informasi, pesan kesalahan muncul, menyatakan bahwa situs sedang mengalami gangguan teknis. Pelaku kemudian menggunakan data nasabah yang terkumpul untuk mengambil uang dari rekening nasabah pada situs *web* Nordea yang asli.

Nasabah Nordea menjadi sasaran *e-mail* yang berisi Trojan tersebut selama lebih dari 15 bulan. Dua ratus lima puluh nasabah bank menjadi korban, dengan total kerugian antara tujuh dan delapan juta Krona Swedia (US$ 7.300-8.300). Kasus ini menunjukkan bahwa *cyberattacks* bahkan dapat menyerang institusi keuangan yang proteksi keamanannya tinggi.

Sumber:
Tom Espiner, "Swedish bank hit by 'biggest ever' online heist," *ZDNet.co.uk* (19 January 2007), http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm.

2.2 Tren Ancaman Keamanan Informasi[6]

Salah satu kegiatan penting dalam menjaga keamanan informasi adalah analisis tren ancaman keamanan, yaitu pencarian pola ancaman keamanan sepanjang waktu untuk mengenal cara-cara pola berubah dan berkembang, berbelok, atau bergeser. Proses iteratif untuk mengumpulkan dan menyambungkan informasi serta meningkatkan profil insiden ini dilakukan untuk dapat mengantisipasi kemungkinan ancaman dan mempersiapkan penanganannya.

Organisasi yang melakukan analisis tren ancaman keamanan informasi dan berbagi laporan tren ancaman keamanan antara lain:

- CERT (http://www.cert.org/cert/)
- Symantec (http://www.symantec.com/business/theme.jsp?themeid=threatreport)
- IBM (http://xforce.iss.net/)

Tren ancaman keamanan informasi yang telah dilaporkan dijelaskan di bawah ini.

Otomasi alat penyerangan[7]

Saat ini, penyusup menggunakan alat otomatis yang memungkinkan untuk mengumpulkan informasi dari ribuan *host* Internet dengan cepat dan mudah. Jaringan dapat 'di-*scan*' dari lokasi *remote*, dan *host* dengan kelemahan tertentu dapat diidentifikasi menggunakan alat otomatis ini. Penyusup mengumpulkan informasi untuk digunakan di lain waktu, dibagi, ditukar dengan penyusup lain, atau diserang seketika. Beberapa alat (seperti cain&abel) mengotomasi serangkaian serangan kecil untuk tujuan tertentu. Sebagai contoh, penyusup dapat menggunakan paket penjejak untuk mendapatkan *password router* atau *firewall*, *log-in* ke dalam *firewall* untuk mematikan *filter*, dan kemudian menggunakan *network file service* untuk membaca data di *server*.

Alat penyerangan yang sulit dideteksi

Beberapa alat penyerangan menggunakan pola penyerangan baru yang tak terdeteksi oleh alat deteksi saat ini. Sebagai contoh, teknik anti-forensik digunakan untuk menyembunyikan sifat dari alat penyerangan. Alat polimorfik berubah bentuk setiap saat digunakan. Beberapa alat ini menggunakan protokol umum seperti *hypertext transfer protocol* (HTTP), sehingga sulit membedakan

[6] Bagian ini diambil dari Tim Shimeall dan Phil Williams, *Models of Information Security Trend Analysis* (Pittsburgh: CERT Analysis Center, 2002), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.

[7] Bagian ini diambil dari CERT, "Security of the Internet," Carnegie Mellon University, http://www.cert.org/encyc_article/tocencyc.html.

mereka dari lalu-lintas jaringan normal.[8] Salah satu contohnya adalah *worm* MSN Messenger. Sebuah *worm* dalam klien MSN Messenger Instant-Messaging (IM) mengirimkan berkas ke kontak yang ada di buku alamat pengguna yang telah terserang. Berkas yang dikirimkan dirancang untuk menyerang sistem setelah mengirimkan peringatan bahwa mereka akan menerima sebuah berkas. Perilaku pengguna IM ditiru, membuat hal ini mengkhawatirkan.[9]

Penemuan kerentanan yang lebih cepat

Kerentanan yang ditemukan di dalam produk piranti lunak dan dilaporkan ke *Computer Emergency Response Team Coordination Center* (CERT/CC) selalu lebih dari dua kali lipat setiap tahunnya, sehingga mempersulit administrator untuk selalu *up to date* dengan *patch*. Penyusup mengetahui hal ini dan memanfaatkannya.[10] Beberapa penyusup meluncurkan serangan *zero-day* (atau *zero-hour*), yaitu ancaman komputer yang memanfaatkan kerentanan aplikasi komputer yang belum memiliki *patch* atau perlindungan karena belum diketahui oleh administrator.[11]

Peningkatan ancaman asimetrik dan konvergensi metode serangan

Ancaman asimetrik adalah kondisi dimana penyerang memiliki keunggulan terhadap yang bertahan. Jumlah ancaman asimetrik meningkat dengan penggunaan otomasi ancaman dan kecanggihan alat serang.

Konvergensi metode serangan adalah konsolidasi berbagai metode serangan oleh penyerang untuk menciptakan jaringan global yang mendukung aktivitas pengrusakan terkoordinasi. Contohnya adalah MPack, *Trojan* yang terpasang di komputer pengguna melalui kontak ke *server* MPack. Penyerang membuat lalu lintas ke *server* ini dengan menyerang situs *web* yang sah dan membuat pengunjung situs tersebut mengarah ke *server web* berbahaya, atau dengan mengirimkan *link* ke *server web* berbahaya tersebut melalui *spam*. *Server* berbahaya ini lalu mengarahkan *browser* pengguna ke *server* MPack.[12]

---

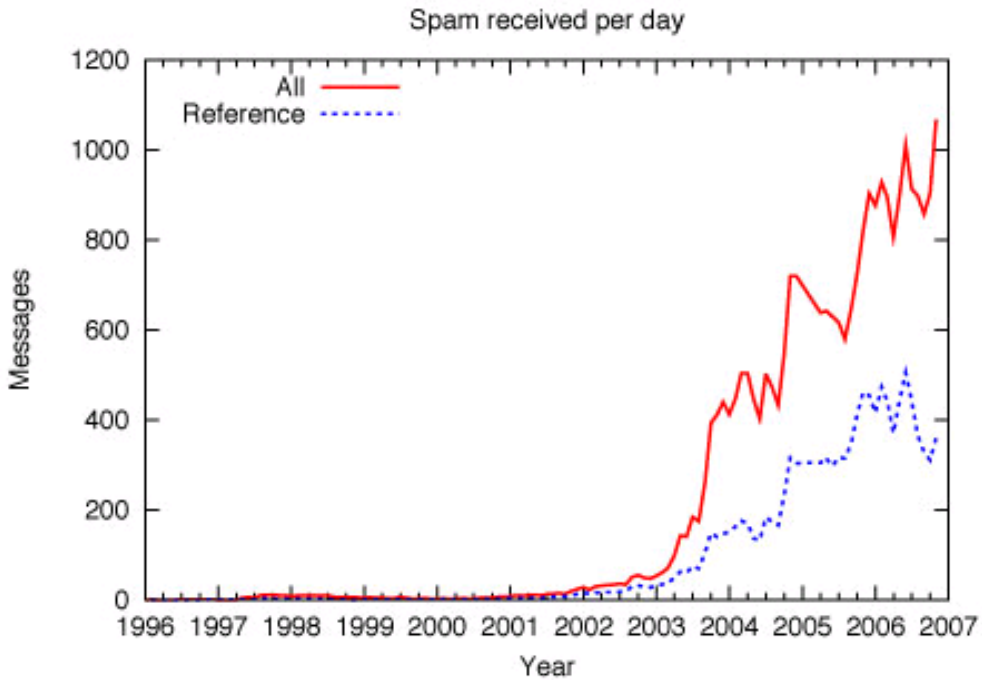
[8] Suresh Ramasubrahmanian et. al., op. cit., 94.
[9] Munir Kotadia, "Email worm graduates to IM," *ZDNet.co.uk* (4 April 2005), http://news.zdnet.co.uk/security/0,1000000189,39193674,00.htm.
[10] Suresh Ramasubrahmanian et. al., op. cit.
[11] Wikipedia, "Zero day attack," Wikimedia Foundation Inc., http://en.wikipedia.org/wiki/Zero_day_attack.
[12] Symantec, *Symantec Internet Security Threat Report: Trends for January–June 07,* Volume XII (September 2007), 13, http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_exec_summary_09_2007.en-us.pdf.

Meningkatnya ancaman dari serangan infrastruktur

Serangan infrastruktur adalah serangan yang pada umumnya mempengaruhi komponen penting dari Internet. Serangan tersebut ditakuti karena banyaknya organisasi dan pengguna Internet serta makin tergantungnya mereka pada Internet untuk menjalankan bisnis sehari-hari. Hasil dari serangan infrastruktur antara lain adalah DoS, membahayakan informasi sensitif, penyebaran informasi yang salah, dan pengalihan signifikan sumber daya dari proses lainnya.

Botnet adalah contoh dari serangan infrastruktur. Istilah 'botnet' mengacu pada sekumpulan komputer terinfeksi yang dikendalikan dari jauh oleh sebuah '*command control server*'. Komputer terinfeksi tersebut menyebarkan *worm* dan *Trojan* melalui sistem jaringan.

Spam meningkat dengan cepat karena penggunaan botnet. *Spam* mengacu pada pesan tidak diinginkan yang berjumlah banyak, yang dikirimkan melalui *e-mail*, pesan instan (*instant messages*), mesin pencari, *blog* dan bahkan telepon bergerak. Gambar 4 menunjukkan tren volume *spam*.



Gambar 4. Statistik *Spam*
(Sumber: spamnation.info, "Spam Statistics," http://spamnation.info/stats/)

Mengatasi Botnet

Untuk mengurangi kerusakan akibat *botnet*, *International Telecommunication Union* (ITU) menyarankan kombinasi metodologi sosial, teknis, dan kebijakan.

Kebijakan: Hukum dan peraturan *cybercrime* dan *antispam* yang efektif
- Peningkatan kapasitas diantara para *stakeholder* terkait
- Kerangka kerja komprehensif untuk kerjasama internasional
- Konsistensi antara hukum *cybercrime* dan privasi
- Kerangka kerja penerapan mitigasi *botnet* dan *cybercrime* secara lokal.

Teknis: Alat dan teknik untuk mengidentifikasi dan mengumpulkan informasi tentang *botnet* aktif
- Praktik terbaik ISP untuk mitigasi aktivitas *botnet*
- Praktik terbaik *registrar* dan *registry* untuk mitigasi aktivitas *botnet*
- Peningkatan kapasitas untuk penyedia transaksi *online* dan *e-commerce.*

Sosial: Pendidikan secara luas tentang pengamanan dan keamanan Internet
- Fasilitasi akses TIK yang aman bagi para pengguna.

Toolkit PTF ITU SPAM merupakan paket komprehensif untuk membantu perencana kebijakan, regulator dan perusahaan dalam menyesuaikan kebijakan dan meraih keyakinan kembali dalam *e-mail*. *Toolkit* ini juga menyarankan untuk berbagi informasi antar negara dalam mencegah masalah internasional.

Perubahan tujuan penyerangan

Dulu, serangan komputer dan jaringan dilakukan atas dasar rasa penasaran atau kepuasan diri. Sekarang, tujuannya biasanya uang, fitnah dan penghancuran. Terlebih, serangan jenis ini mewakili hanya sebagian kecil dari spektrum *cybercrime* yang luas.

Cybercrime adalah perusakan, gangguan atau penyimpangan aliran data dan informasi dijital secara sengaja untuk alasan politik, ekonomi, agama atau ideologi. Kejahatan yang paling umum diantaranya adalah *hacking*, DoS, *malicious code* dan *social engineering*. Baru-baru ini, *cybercrime* menjadi bagian dari *cyberterror* dan *cyber-warfare*, yang efeknya merugikan keamanan nasional.

Tabel 3 di bawah ini menunjukkan apa yang pelaku *cybercrime* dapatkan.

Tabel 3. Hasil dari *Cybercrime* di Tahun 2007

Aset	Tarif berlaku (dalam USD)
Pembayaran tiap instalasi *adware* yang berbeda	30 sen di AS, 20 sen di Canada, 10 sen di Inggris, 2 sen di lainnya
Paket *malware*, versi dasar	USD 1.000 - 2.000
Paket *malware* dengan layanan tambahan	Bervariasi, mulai dari USD 20
Sewa *exploit kit* – 1 jam	USD 0,99 hingga USD 1
Sewa *exploit kit* – 2,5 jam	USD 1,60 hingga USD 2
Sewa *exploit kit* – 5 jam	USD 4, bisa bervariasi
Salinan tak terdeteksi dari Trojan untuk pencurian informasi	USD 80, bisa bervariasi
Serangan DoS terdistribusi	USD 100 per hari
10.000 PC yang terancam	USD 1.000
Pencurian informasi rekening bank	Bervariasi, mulai dari USD 50
1 juta *e-mail* baru (belum diverifikasi)	USD 8 keatas, bergantung pada kualitas

Sumber: Trend Micro, *2007 Threat Report and Forecast* (2007), 41, http://trendmicro.mediaroom.com/file.php/66/2007+Trend+Micro+Report_FINAL.pdf.

2.3 Peningkatan Keamanan

Melihat tren ancaman keamanan dan teknologi serangan, pertahanan yang kuat memerlukan strategi yang fleksibel agar bisa beradaptasi dengan perubahan lingkungan, kebijakan dan prosedur yang baik, penggunaan teknologi keamanan yang tepat, dan kewaspadaan yang terus menerus.

Program peningkatan keamanan perlu dimulai dengan melihat kondisi keamanan saat ini. Menjadi satu bagian dengan program keamanan adalah kebijakan dan prosedur yang terdokumentasi, serta teknologi yang mendukung implementasi.

Pengamanan Administratif

Pengamanan administratif terdiri dari strategi, kebijakan, dan pedoman keamanan informasi.

Strategi keamanan informasi menentukan arah semua kegiatan keamanan informasi.

Kebijakan keamanan informasi adalah dokumen rencana tingkat tinggi dari keamanan informasi seluruh organisasi. Kebijakan berisi kerangka kerja untuk membuat keputusan spesifik, seperti rencana keamanan fisik dan administratif.

Karena kebijakan keamanan informasi harus memiliki sudut pandang jangka panjang, hindari konten yang bersifat spesifik ke teknologi, dan perlu mencakup pengembangan *business continuity planning* (BCP) yang efektif.

Pedoman keamanan informasi harus ditetapkan sesuai dengan strategi dan kebijakan keamanan informasi. Pedoman menspesifikasikan regulasi untuk setiap area yang terkait dengan keamanan informasi. Dan karena pedoman harus komprehensif dan berlingkup nasional, mereka harus dikembangkan dan disampaikan oleh pemerintah untuk ditaati oleh organisasi.

Standar keamanan informasi harus khusus dan spesifik sehingga mereka dapat diterapkan ke semua bidang keamanan informasi. Setiap negara perlu mengembangkan standar sesudah menganalisis standar keamanan administratif, fisik dan teknis yang banyak digunakan di dunia. Standar haruslah sesuai dengan lingkungan TIK yang umum.

Strategi, kebijakan dan pedoman keamanan informasi suatu negara harus sesuai dengan hukum yang terkait. Lingkupnya harus berada dalam batas hukum nasional dan internasional.

Proses dan operasi keamanan informasi

Ketika strategi, kebijakan dan pedoman keamanan informasi telah ditetapkan, berikutnya proses dan prosedur operasi keamanan informasi perlu disusun. Karena yang melakukan serangan terhadap informasi atau yang membocorkan informasi internal adalah manusia, maka manajemen sumber daya manusia adalah faktor paling penting dalam operasi keamanan informasi. Karena itu, dibutuhkan hal-hal berikut:

1. Program pendidikan dan pelatihan keamanan informasi - Terdapat banyak metode untuk meningkatkan tingkat keamanan informasi organisasi tetapi pendidikan dan pelatihan adalah kegiatan dasar. Anggota organisasi harus menghargai kebutuhan akan keamanan informasi dan mendapatkan keahlian terkait melalui pendidikan dan pelatihan. Namun demikian, penting untuk mengembangkan program yang bervariasi untuk memaksimalkan keterlibatan karena program pendidikan dan pelatihan keamanan informasi yang baku dapat menjadi tidak efektif.

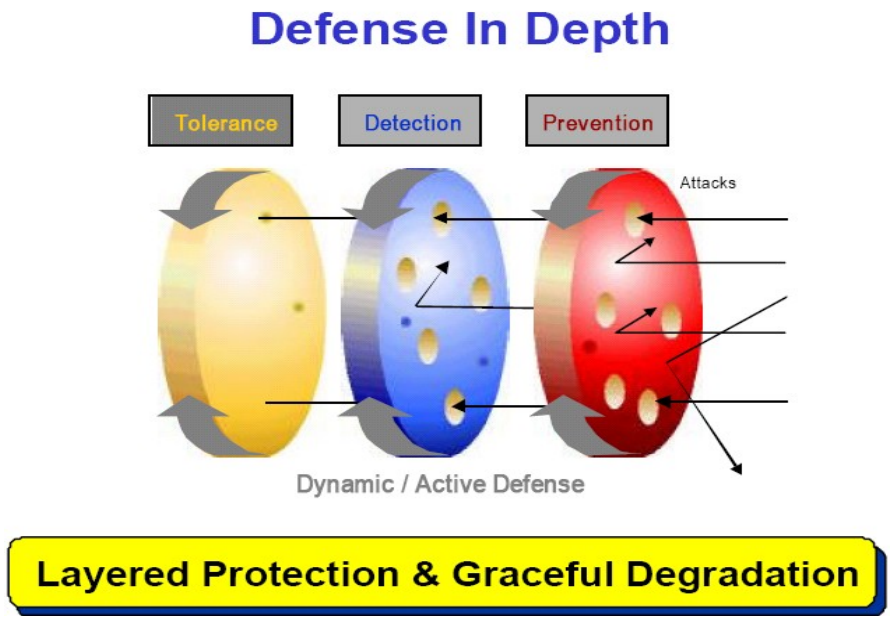
2. Penguatan promosi melalui berbagai kegiatan - Partisipasi pegawai adalah penting untuk suksesnya implementasi strategi, kebijakan, dan pedoman keamanan informasi. Keamanan informasi perlu dipromosikan ke para pegawai melalui berbagai kegiatan harian.

3. Pengamanan dukungan – Meskipun tingkat kesadaran akan keamanan informasi diantara pegawai adalah tinggi dan mereka memiliki keinginan kuat untuk memelihara keamanan informasi, sulit untuk memastikan keamanan informasi tanpa dukungan dari pimpinan puncak organisasi. Dukungan dari *Chief Executive Officer* dan *Chief Information Officer* harus didapatkan.

Pengamanan dengan Teknologi

Berbagai teknologi telah dikembangkan untuk membantu organisasi mengamankan sistem informasinya terhadap penyusup. Teknologi ini membantu melindungi sistem dan informasi dari serangan, untuk mendeteksi kegiatan tidak biasa atau mencurigakan, dan untuk merespon akan kejadian yang mempengaruhi keamanan.

Sistem keamanan saat ini telah dirancang dan dikembangkan berdasarkan model *Defense-In-Depth* (DID) yang mengarah pada penyatuan manajemen dari teknologi yang digunakan. Model ini berbeda dengan garis pertahanan, mempunyai hanya satu lapis pertahanan untuk menghadapi semua ancaman. Model DID terdiri dari pencegahan, deteksi dan toleransi, dimana ancaman terus berkurang di setiap fase (Gambar 5).



Gambar 5. *Defense in Depth*
(Sumber: *Defense Science Board, Protecting the Homeland: Defensive Information Operations 2000 Summer Study Volume II. Washington, DC: Defense Science Board*, 2001, 5, http://www.acq.osd.mil/dsb/reports/dio.pdf)

Teknologi pencegah

Teknologi pencegah melindungi dari penyusup dan ancaman pada tingkat sistem atau *storage*. Teknologi ini termasuk antara lain:

1. Kriptografi - Juga mengacu pada enkripsi, kriptografi adalah proses pengkodean informasi dari bentuk aslinya (disebut *plaintext*) menjadi sandi, bentuk yang tidak dapat dipahami (disebut *ciphertext*). Deskripsi mengacu

pada proses penerjemahan kembali dari *ciphertext* menjadi *plaintext*. Kriptografi digunakan untuk melindungi berbagai aplikasi. Informasi lebih lanjut mengenai kriptografi dan teknologi terkait (IPSec, SSH, SSL, VPN, OTP, dll.) tersedia di halaman *web* berikut ini:

- IETF RFC (http://www.ietf.org/rfc.html)
- *RSA Laboratories' Frequently Asked Questions About Today's Cryptography* (http://www.rsa.com/rsalabs/node.asp?id=2152)

2. *One-time passwords* (OTP) - Sesuai dengan namanya, *password* sekali pakai hanya dapat digunakan sekali. *Password* statis lebih mudah disalahgunakan oleh *password loss*, *password sniffing*, dan *brute-force password cracks*, dan sejenisnya. Risiko ini dapat dikurangi dengan terus menerus mengubah *password*, yaitu dengan OTP. Untuk alasan ini, OTP digunakan untuk mengamankan transaksi keuangan elektronik seperti *online banking*.

3. *Firewall* - *Firewall* mengatur beberapa aliran lalu lintas antara jaringan komputer dari *trust level* yang berbeda seperti antara Internet, yang termasuk zona tanpa kepercayaan, dan jaringan internal, yang merupakan zona dengan tingkat kepercayaan yang lebih tinggi. Zona dengan tingkat kepercayaan menengah, terletak antara Internet dan jaringan internal, sering disebut sebagai 'perimeter network' atau *demilitarized zone*.

4. Alat penganalisis kerentanan - Karena jumlah metode serangan serta kerentanan yang ada di aplikasi yang umum digunakan semakin meningkat, perlu untuk mengkaji kerentanan sistem secara teratur. Dalam keamanan komputer, kerentanan adalah kelemahan yang membuat penyerang dapat mengganggu sistem. Kerentanan dapat dihasilkan dari *password* yang lemah, *bug* pada piranti lunak, virus komputer, injeksi kode, injeksi SQL atau *malware*. Alat penganalisis kerentanan mendeteksi semua kerentanan tersebut. Alat tersebut mudah didapatkan secara *online* dan terdapat juga perusahaan yang menyediakan layanan analisis. Akan tetapi, yang tersedia secara gratis untuk komunitas Internet bisa jadi disalahgunakan oleh penyusup. Untuk informasi lebih lanjut, lihat:
   - *INSECURE Security Tool* (http://sectools.org)
   - *FrSIRT Vulnerability Archive* (http://www.frsirt.com/english)
   - *Secunia Vulnerability Archive* (http://secunia.com)
   - *SecurityFocus Vulnerability Archive* (http://www.securityfocus.com/bid)

   Alat penganalisis kerentanan jaringan menganalisis kerentanan sumber daya jaringan seperti *router*, *firewall* dan *server*.

   Alat penganalisis kerentanan *server* menganalisis hal-hal seperti *password* yang lemah, konfigurasi yang lemah dan kesalahan otorisasi pada berkas di sistem internal. Alat penganalisis kerentanan *server* relatif memberikan hasil yang lebih akurat dibanding alat penganalisis kerentanan jaringan karena alat ini menganalisis lebih banyak kerentanan di dalam sistem internal.

Alat penganalisis kerentanan *web* menganalisis kerentanan aplikasi *web* seperti XSS dan injeksi SQL pada *web*. Untuk informasi lebih lanjut, lihat *Open Web Application Security Project* di http://www.owasp.org/index.php/Top_10_2007.

Teknologi deteksi

Teknologi deteksi digunakan untuk mendeteksi dan melacak kondisi abnormal dan gangguan dalam jaringan atau sistem penting. Teknologi deteksi antara lain:

1. Antivirus – Peranti lunak antivirus merupakan program komputer untuk mengidentifikasi, menetralisir atau mengeliminasi kode berbahaya, seperti *worm*, serangan *phishing*, *rootkits*, *Trojan horse* dan *malware* lainnya.[13]

2. *Intrusion detection system* (IDS) - IDS mengumpulkan dan menganalisis informasi dari berbagai area dalam sebuah komputer atau jaringan untuk mengidentifikasi kemungkinan penerobosan keamanan. Fungsi deteksi gangguan termasuk analisis pola kegiatan abnormal dan kemampuan untuk mengenali pola penyerangan.

3. *Intrusion prevention system* (IPS) – IPS mengidentifikasi potensi ancaman dan bereaksi sebelum mereka digunakan untuk menyerang. IPS memonitor lalu lintas jaringan dan mengambil tindakan segera menghadapi potensi ancaman berdasarkan pada aturan-aturan yang telah ditetapkan oleh administrator jaringan. Sebagai contoh, IPS dapat memblok lalu lintas jaringan dari alamat IP yang mencurigakan.[14]

Teknologi terintegrasi

Teknologi terintegrasi mengintegrasikan fungsi-fungsi penting untuk keamanan informasi aset-aset inti, seperti prediksi, deteksi dan pelacakan gangguan. Teknologi terintegrasi diantaranya:

1. *Enterprise security management* (ESM) - Sistem ESM mengatur, mengontrol dan mengoperasikan solusi keamanan informasi seperti IDS dan IPS mengikuti kebijakan yang ditetapkan. ESM digunakan sebagai strategi untuk mengatasi kelemahan solusi lain dengan memanfaatkan kelebihan dari masing-masing solusi keamanan informasi dan memaksimalkan efisiensi keamanan informasi dibawah kebijakan yang ditetapkan.

[13] Wikipedia, “Antivirus software,” Wikimedia Foundation, Inc., http://en.wikipedia.org/wiki/Antivirus_software.
[14] SearchSecurity.com, “Intrusion prevention,” TechTarget, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1032147,00.html.

ESM yang dapat mengatur teknologi keamanan yang ada muncul karena keterbatasan sumber daya manusia yang mengoperasikan teknologi keamanan, peningkatan serangan seperti konvergensi metode serangan, dan munculnya alat penyerangan yang sulit untuk dideteksi. Dengan ESM, efisiensi manajemen meningkat dan terbentuk langkah aktif untuk mengatasi.

2. *Enterprise risk management* (ERM) - ERM adalah sistem yang membantu memprediksi seluruh risiko yang terkait dengan organisasi, termasuk area di luar keamanan informasi, dan mengatur langkah mengatasinya secara otomatis. Penggunaan ERM untuk melindungi informasi membutuhkan bahwa tujuan tepat dari manajemen risiko dan rancangan pengembangan sistem telah dinyatakan. Banyak organisasi membangun dan mengoptimalkan ERM mereka sendiri melalui lembaga konsultasi keamanan informasi profesional ketimbang mereka sendiri yang melakukannya.

Pertanyaan

1. Ancaman keamanan informasi apa yang mudah menyerang organisasi Anda? Mengapa?

2. Solusi teknologi keamanan informasi mana yang tersedia di organisasi Anda?

3. Apakah organisasi Anda memiliki kebijakan, strategi dan pedoman keamanan informasi? Jika ya, seberapa cukupkah hal-hal tersebut terhadap ancaman yang mudah menyerang organisasi Anda? Jika tidak, apa yang akan Anda rekomendasikan untuk organisasi Anda terkait kebijakan, strategi dan pedoman keamanan informasi?

Ujian

1. Mengapa penting melakukan analisis tren ancaman keamanan informasi?

2. Mengapa manajemen sumber daya manusia adalah faktor paling penting dalam operasi keamanan informasi? Apakah kegiatan utama dalam manajemen sumber daya manusia untuk keamanan informasi?

3. Jelaskan model teknologi keamanan *Defense-in-Depth*. Bagaimana model tersebut bekerja?

3. AKTIVITAS KEAMANAN INFORMASI

Bagian ini bertujuan untuk:
- Memberikan contoh aktivitas keamanan informasi di berbagai negara sebagai penuntun dalam penyusunan kebijakan keamanan informasi; dan
- Melihat kerjasama internasional dalam implementasi kebijakan keamanan informasi.

3.1 Aktivitas Keamanan Informasi Nasional

Strategi keamanan informasi Amerika Serikat (AS)

Setelah serangan teroris pada 11 September 2001 (9/11), AS mendirikan *Department of Homeland Security* untuk memperkuat keamanan nasional tidak hanya terhadap ancaman fisik tetapi juga terhadap *cyberthreats*. AS menerapkan aktivitas keamanan informasi yang efektif dan komprehensif melalui sistem *Information Security Officer*. Strategi keamanan informasi ini meliputi *National Strategy for Homeland Security, National Strategy for the Physical Security of Critical Infrastructures and Key Assets,* dan *National Strategy to Secure Cyberspace.*

National Strategy to Secure Cyberspace[15] menetapkan visi *cybersecurity* dan perlindungan terhadap infrastruktur dan aset penting. Strategi tersebut juga mendefinisikan tujuan dan aktivitas spesifik untuk mencegah *cyberattacks* terhadap infrastruktur dan aset penting. Lima prioritas nasional yang ditetapkan dalam *National Strategy to Secure Cyberspace* adalah:

- *National Cyberspace Security Response System*
- *National Cyberspace Security Threat and Vulnerability Reduction Program*
- *National Cyberspace Security Awareness and Training Program*
- *Securing Governments' Cyberspace*
- *National Security and International Cyberspace Security Cooperation.*

Memperketat Hukum Keamanan Informasi

Cyber Security Enhancement Act of 2002[16] (CSEA) mencakup bab dua dari *Homeland Security Law*. Memberikan amandemen pedoman pidana terhadap

[15] The White House, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, 2003), http://www.whitehouse.gov/pcipb.
[16] Computer Crime and Intellectual Property Section, *SEC. 225. Cyber Security Enhancement Act of 2002* (Washington DC: Department of Justice, 2002), http://www.usdoj.gov/criminal/cybercrime/homeland_CSEA.htm.

beberapa kejahatan komputer seperti, pengecualian pengungkapan darurat, pengecualian kejujuran, larangan iklan Internet ilegal, dan perlindungan privasi.

Pengecualian Pengungkapan Darurat (*Emergency Disclosure Exception*): Sebelum 9/11, *Electronic Communications Privacy Act* (ECPA) melarang penyedia layanan komunikasi elektronik (seperti ISP) dari pengungkapan komunikasi pengguna (seperti pesan suara, *e-mail*, dan *attachment*). *Emergency Disclosure Exception* mengizinkan ISP untuk mengungkapkan isi *e-mail* atau komunikasi elektronik dengan lembaga penegak hukum tanpa surat perintah sesuai dengan *USA Patriot Act* yang disahkan setelah 11 September 2001. Peraturan pengecualian keterbukaan dalam kasus darurat telah dikuatkan dalam CSEA. Lembaga pemerintah yang menerima konten mencurigakan diharuskan melapor, dalam 90 hari setelah pengungkapan, kepada *Attorney General* (Kejaksaan Agung), tanggal pengungkapan, pihak yang terlibat, informasi yang diungkap dan jumlah pendaftar terkait, serta jumlah komunikasi.

Pengecualian Kejujuran: CSEA menetapkan pembebasan dari tuntutan pidana dan perdata dalam kasus mencuri dengar yang diminta oleh pemilik atau operator komputer.

Larangan iklan Internet untuk perangkat ilegal: ECPA melarang manufaktur, distribusi, kepemilikan dan iklan *online* dari perangkat untuk menangkap (*intercept*) komunikasi berbasis kabel, lisan, dan elektronik. Perangkat mencuri dengar elektronik dapat diiklankan. Namun, pengiklan harus mengetahui isi iklan.

Penguatan hukuman untuk serangan komputer: Dibawah *US Computer Fraud and Abuse Act*, sengaja mengakses komputer dan merusak tanpa izin adalah ilegal. Sebelum 9/11, setiap orang yang dinyatakan bersalah dalam tindak kriminal ini dihukum penjara tidak lebih dari lima tahun dalam kasus serangan pertama dan tidak lebih dari 10 tahun dalam kasus serangan kedua. Setelah 9/11, hukuman untuk tindakan tersebut direvisi untuk hukuman penjara tidak lebih dari 10 tahun untuk serangan pertama dan tidak lebih dari 20 tahun untuk serangan kedua. Klausa tambahan dalam CSEA menetapkan penyerang dapat dihukum penjara tidak lebih dari 20 tahun jika penyerang menyebabkan atau mencoba menyebabkan cedera jasmani serius; dia dapat diberikan hukuman seumur hidup jika menyebabkan atau mencoba menyebabkan kematian.

Pengecualian tanggung jawab membantu: ECPA mengecualikan dari tuntutan kriminal terhadap penyedia layanan komunikasi yang membantu menangkap (*intercept*) komunikasi atau yang memberikan informasi ke penegak hukum.

Federal Information Security Management Act (FISMA)[17] mencakup bab ketiga *e-Government Act of* 2002. Hukum ini melindungi infrastruktur jaringan nasional,

[17] Office of Management and Budget, *Federal Information Security Management Act: 2004 Report to Congress* (Washington, DC: Executive Office of the President of the United States, 2005), http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf.

dan menyerukan peningkatan usaha untuk melindungi keamanan informasi bagi seluruh masyarakat, lembaga keamanan nasional dan lembaga penegak hukum. Tujuan utama *Federal Information Security Management* adalah: (1) untuk memberikan kerangka kerja komprehensif untuk meningkatkan efisiensi kontrol keamanan informasi dari operasi dan aset; dan (2) untuk mengembangkan kontrol dan rencana pemeliharaan yang tepat untuk melindungi informasi/sistem informasi, dan menyediakan mekanisme untuk meningkatkan manajemen program keamanan informasi.

Strategi keamanan informasi Uni Eropa (UE)

Dalam *Communication* di bulan Mei 2006,[18] Komisi Eropa menjelaskan strategi keamanan informasi UE yang terdiri dari sejumlah langkah interdependen melibatkan banyak *stakeholder*. Langkah-langkah tersebut termasuk penyusunan *Regulatory Framework for Electronic Communication* di tahun 2002, artikulasi dari inisiatif i2010 untuk pembentukan *European Information Society*, dan pembentukan *European Network and Information Security Agency* (ENISA) pada tahun 2004. Berdasarkan *Communication*, langkah-langkah tersebut mencerminkan pendekatan trisula untuk isu keamanan di Masyarakat Informasi yang mencakup langkah keamanan informasi dan jaringan, kerangka kerja pengaturan komunikasi elektronik (termasuk isu privasi dan keamanan data), dan memerangi *cybercrime*.

Communication mencatat bahwa serangan pada sistem informasi, peningkatan penggunaan perangkat bergerak, munculnya '*ambient intelligence*', dan peningkatan tingkat kesadaran pengguna sebagai isu utama keamanan yang ingin diatasi oleh Komisi Eropa melalui dialog, kerjasama dan pemberdayaan. Strategi-strategi ini dijelaskan dalam *Communication* sebagai berikut:

Dialog

Komisi mengajukan serangkaian langkah yang dirancang untuk membangun dialog yang terbuka, inklusif dan *multi-stakeholder*:

- Pelatihan *benchmarking* untuk kebijakan nasional terkait keamanan informasi dan jaringan, untuk membantu mengidentifikasi praktik yang paling efektif untuk kemudian diterapkan dengan lebih luas di seluruh UE. Khususnya, pelatihan ini mengidentifikasi praktik terbaik untuk meningkatkan kesadaran UKM dan masyarakat mengenai risiko dan tantangan sehubungan dengan keamanan informasi dan jaringan; dan
- Debat *multi-stakeholder* yang terstruktur mengenai cara terbaik untuk

[18] Europa, "Strategy for a secure information society (2006 communication)," European Commission, http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

memanfaatkan instrumen peraturan yang ada. Debat ini akan dikelola dalam konteks konferensi dan seminar.

Kerjasama

Penyusunan kebijakan yang efektif membutuhkan pemahaman yang jelas mengenai sifat dasar tantangan yang akan ditangani, serta data ekonomi dan statistik yang *up-to-date* dan handal. Untuk itu, Komisi meminta ENISA untuk:

- Membangun kerjasama atas dasar kepercayaan dengan Negara-Negara Anggota dan *stakeholder* untuk mengembangkan kerangka kerja yang tepat dalam mengumpulkan data; dan
- Menguji kelayakan berbagi informasi dan sistem siaga Eropa untuk membantu respon yang efektif terhadap berbagai ancaman. Sistem ini juga mencakup portal Eropa dalam berbagai bahasa yang memberikan informasi akan ancaman, risiko, dan tanda bahaya.

Secara paralel, Komisi akan mengundang Negara Anggota, sektor swasta dan komunitas riset untuk membangun kerjasama dalam memastikan ketersediaan data tentang industri keamanan TIK.

Pemberdayaan

Pemberdayaan *stakeholder* merupakan prasyarat untuk menumbuhkan kesadaran mereka terhadap kebutuhan dan risiko keamanan. Untuk alasan ini, Negara Anggota diundang untuk:

- Secara proaktif berpartisipasi dalam pelatihan *benchmarking* bagi kebijakan nasional yang diusulkan;
- Bekerjasama dengan ENISA, melakukan kampanye kesadaran akan manfaat dari adopsi praktik, perilaku, dan teknologi keamanan yang efektif;
- Membantu peluncuran layanan *e-government* untuk memajukan praktik keamanan yang baik; dan
- Menstimulasi pengembangan program keamanan informasi dan jaringan sebagai bagian dari kurikulum pendidikan tinggi.

Stakeholder sektor swasta didorong berinisiatif untuk:

- Menetapkan tanggung jawab bagi produsen piranti lunak dan ISP sehubungan dengan penyediaan tingkat keamanan yang cukup dan teraudit;
- Memajukan keragaman, keterbukaan, interoperabilitas, penggunaan dan kompetisi sebagai pendorong utama keamanan, dan untuk menstimulasi penerapan produk dan layanan peningkatan keamanan untuk memberantas pencurian ID dan serangan laiinya yang mengganggu privasi;
- Menyebarkan praktik keamanan yang baik untuk operator jaringan, penyedia layanan dan UKM;
- Memajukan program pelatihan di sektor swasta untuk memberikan

pengetahuan dan keterampilan yang diperlukan pegawai dalam implementasi praktek keamanan;
- Bekerja menuju skema sertifikasi keamanan yang terjangkau untuk produk, proses dan layanan yang akan memenuhi kebutuhan spesifik UE; dan
- Melibatkan sektor asuransi dalam pengembangan alat dan metode manajemen risiko.

Sumber:
Disadur dari Europa, "Strategy for a secure information society (2006 communication)," European Commission, http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

Council of Europe Convention on Cybercrime (CECC)

Disamping itu, tahun 2001 UE mengumumkan dibentuknya *Council of Europe Convention on Cybercrime* (CECC) yang "meletakkan pedoman bagi semua pemerintah yang ingin mengembangkan legislasi menghadapi *cybercrime*" dan "menyediakan kerangka kerja bagi kerjasama di bidang ini." Sebanyak 39 negara Eropa menandatangani perjanjian ini, termasuk juga Kanada, Jepang, Afrika Selatan dan AS. Hal ini menjadikan CECC, yang mulai berlaku bulan Juli 2004, "satu-satunya perjanjian internasional mengikat yang berlaku sampai saat ini."[19]

Eurepean Network and Information Security Agency (ENISA)

ENISA didirikan oleh Parlemen Eropa dan Dewan Uni Eropa pada tanggal 10 Maret 2004 "untuk membantu meningkatkan keamanan informasi dan jaringan dalam Komunitas [Uni Eropa] dan mendorong bertumbuhnya budaya keamanan informasi dan jaringan untuk kepentingan masyarakat, konsumen, serta organisasi bisnis dan sektor publik."

Visi *Permanent Stakeholder Group* (PSG) untuk ENISA[20] dinyatakan pada bulan Mei 2006 yang melihat ENISA sebagai pusat unggulan dalam keamanan informasi dan jaringan, sebuah forum bagi *stakeholder* NIS, dan pendorong kesadaran keamanan informasi bagi semua warga negara Uni Eropa. Untuk tujuan ini, aksi jangka panjang untuk ENISA telah dinyatakan dalam Visi PSG (Gambar 6):

[19] Council of Europe, "Cybercrime: a threat to democracy, human rights and the rule of law," http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.
[20] Paul Dorey and Simon Perry, ed., *The PSG Vision for ENISA* (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

Gambar 6. Aksi Jangka Panjang ENISA
(Paul Dorey dan Simon Perry, ed., *The PSG Vision for ENISA*,
Permanent Stakeholders Group, 2006,
http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf)

1. **Kerjasama dan koordinasi otoritas keamanan informasi dan jaringan Negara Anggota**

Kerjasama antara badan-badan nasional sangat rendah pada saat ini. Banyak hal dapat dilakukan dengan meningkatkan komunikasi dan kerjasama antara lembaga-lembaga nasional, terutama dalam berbagi praktik terbaik dari lembaga yang lebih maju ke mereka yang baru saja mulai.

2. **Kerja sama dengan lembaga penelitian**

Tujuan ENISA harus langsung ke riset dasar dan mentargetkan pengembangan teknis agar fokus pada bidang yang bermanfaat paling besar dalam mengelola risiko keamanan sebenarnya dalam sistem dunia nyata. ENISA seharusnya tidak mendukung agenda penelitian dengan sendirinya, tetapi bekerja untuk penyelarasan proses yang ada dan penentuan prioritas program yang ada.

3. **Bekerja sama dengan vendor piranti lunak dan perangkat keras**

Vendor piranti lunak dan perangkat keras pada dasarnya adalah pesaing dan sulit bagi mereka untuk setuju secara terbuka pada praktik bersama. ENISA dapat menyediakan opini dan forum yang tidak memihak untuk diskusi sensitif, dengan tetap memelihara situasi yang sehat terhadap perilaku anti-kompetitif.

Visi jangka panjang ENISA harus lebih fokus pada pembuatan jaringan dan teknologi informasi yang handal, yang tahan terhadap *worm* dan masalah lainnya, bukan memperluas tren keamanan yang meningkat saat ini. Ini dapat dicapai dengan promosi teknik untuk mengembangkan piranti lunak dan arsitektur yang benar, aman, dan handal.

4. Berpartisipasi dalam lembaga yang menetapkan standar

Untuk identifikasi dan publikasi inisiatif dengan nilai terbesar, ENISA perlu melacak dan memantau topik seputar NIS di lembaga yang menetapkan standar, termasuk menindaklanjuti hasil pekerjaan dari berbagai lembaga akreditasi dan sertifikasi keamanan yang ada.

5. Berpartisipasi dalam proses legislatif melalui lobi dan opini

ENISA harus berusaha untuk mendapatkan posisi sebagai badan konsultan terpercaya untuk didengarkan di proses awal rancangan dan pengajuan arah serta perundang-undangan lainnya dalam isu terkait NIS.

6. Bekerja sama dengan organisasi pengguna

Seringkali organisasi pengguna tidak direpresentasikan dengan baik dalam lembaga legislatif dan lembaga yang menetapkan standar, seperti juga vendor. ENISA dapat memberikan wawasan kepada kelompok pengguna tentang pekerjaan standar dan kesempatan untuk mempengaruhi pekerjaan tersebut.

7. **Identifikasi dan promosi praktik terbaik dari Negara-negara Aanggota untuk industri pengguna**

ENISA seharusnya tidak hanya melindungi kepentingan bisnis, tetapi juga meningkatkan kepercayaan pengguna dalam menggunakan Internet dan media dijital.

8. Bekerja untuk solusi politik dan teknis untuk manajemen identitas

Kurangnya keyakinan dalam Internet adalah kendala utama untuk e-bisnis berorientasi konsumen dan berskala besar. Kemampuan untuk dapat secara akurat memeriksa identitas pemilik sebuah situs, alamat *e-mail*, atau layanan *online* merupakan langkah besar untuk memperbarui dan meningkatkan kepercayaan pengguna umum akan Internet. Solusi teknis di bidang ini harus dicari melalui proses yang dipimpin oleh industri, tetapi ENISA dapat bekerja untuk kebijakan yang berlaku di seluruh UE untuk otentikasi entitas yang *online*.

9. **Usaha yang seimbang untuk masalah keamanan “Informasi” dan “Jaringan”**

ENISA harus berkomunikasi dengan penyedia layanan Internet dan jaringan (ISP/NSP) terbesar untuk membantu mereka melihat praktik terbaik demi kepentingan bisnis dan konsumen di seluruh Eropa. Ini penting karena ISP/NSP berperanan penting dalam meningkatkan keamanan Internet secara luas. Kerjasama dan koordinasi aksi yang dilakukan ISP dirasakan kurang saat ini.

Sumber:
Disadur dari Paul Dorey dan Simon Perry, ed., *The PSG Vision for ENISA* (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

Strategi keamanan informasi Republik Korea

Meskipun Republik Korea adalah salah satu negara paling maju di dunia dalam hal teknologi Internet, mereka baru-baru saja menanggapi perlunya menjaga keamanan informasi. Di tahun 2004, pemerintah Korea melalui Ministry of Information and Communication (MIC) mengeluarkan *Information Security Roadmap* jangka menengah dan jangka panjang dengan tujuan untuk membangun platform keamanan informasi untuk memastikan lingkungan koneksi yang aman untuk *Broadband Convergence Network* dan untuk mengembangkan teknologi keamanan terhadap penyalinan ilegal *next-generation mobile equipment*. MIC juga berusaha mengenalkan *Privacy Impact Assessment* (PIA) dan membangun sarana untuk *adult certification* menggunakan nomor registrasi penduduk. Selain itu, Republik Korea telah menandatangani Perjanjian Seoul.Melbourne untuk membangun kolaborasi diantara negara-negara Asia Pasifik untuk mengataasi *spam* melalui penerapan sistem kontrol *spam*, respon secara teknologi, pelatihan dan peningkatan kesadaran pengguna, peningkatan kerjasama publik dan swasta dengan berbagi informasi antara negara serta pertukaran sumber daya manusia.

Tujuan khusus *Information Security Roadmap* adalah untuk: (1) menjamin keamanan infrastruktur jaringan; (2) memastikan kehandalan layanan dan perangkat TI baru; dan (3) mempromosikan dasar keamanan informasi di Republik Korea. Implementasi *roadmap* ini memerlukan alokasi anggaran empat tahun sebesar USD 247,89 miliar (USD 43 miliar pada 2005, USD 55,5 miliar pada 2006, dan USD 80,1 miliar pada 2008).

Memastikan keamanan infrastruktur jaringan: Menurut *Roadmap*, keamanan infrastruktur jaringan dilakukan dengan mengembangkan struktur platform keamanan informasi untuk integrasi dan *interlocking* dari berbagai jaringan komputer yang heterogen; membangun manajemen keamanan DNS generasi selanjutnya, dan pengembangan mekanisme pemisahan jaringan untuk mencegah kerusakan di lingkungan *Broadband Convergence Network* menyebar ke jaringan swasta dan sebaliknya.

Memastikan kehandalan layanan dan perangkat TI yang baru: Model penilaian dampak keamanan informasi yang dapat menilai ancaman dan kerentanan administratif, teknis dan fisik akan dikembangkan untuk dapat secara efektif mencegah penembusan keamanan informasi dalam layanan TI yang baru.

Prosedur sertifikasi untuk evaluasi tingkat keamanan informasi akan ditetapkan. Untuk layanan TI generasi selanjutnya, sistem sertifikasi akan ditingkatkan untuk menyertakan sertifikasi orang, otoritas, catatan transaksi, dan lain-lain.

Selain itu, sebuah rencana untuk pengembangan teknologi keamanan informasi telah disusun yang meliputi teknologi otorisasi yang sesuai untuk jaringan rumah, teknologi identifikasi terminal untuk mencegah akses ilegal, teknologi keamanan untuk robot layanan generasi selanjutnya, dan teknologi keamanan untuk konten generasi selanjutnya.

Penyusunan dasar keamanan informasi: *Korean Information Security Roadmap* berisi ketentuan untuk memperbaiki peraturan dalam rangka memenuhi kebutuhan dari lingkungan komunikasi informasi yang berubah dan untuk siap menghadapi ancaman di masa depan. Yang pertama, *Internet Incident Response Service Centre* harus ditingkatkan untuk mampu mengatasi insiden penyusupan Internet yang bentuknya makin canggih. Sistem kerjasama keamanan informasi domestik dan luar negeri harus diperkuat, dan diberikan dukungan bagi mereka yang keamanan informasinya lemah. Kedua, hukum perlindungan privasi dan teknologi terkait harus dikembangkan dan *Spam Response Service Centre* harus dioperasikan. Ketiga, hukum tentang keamanan informasi yang ada harus ditingkatkan untuk memenuhi kebutuhan lingkungan *ubiquitous*. Demikian juga, kesadaran keamanan informasi harus dipromosikan melalui kampanye keamanan informasi dan program pelatihan ahli.

Strategi keamanan informasi Jepang[21]

Dalam mencapai tujuannya menjadi 'negara maju dalam keamanan informasi',[22] Jepang menetapkan sekumpulan tujuan rinci, prinsip dasar dan proyek di bidang keamanan informasi. *Information Security Policy Council* and *National Information Security Center* (NISC) adalah organisasi inti yang mengawasi semua pekerjaan terkait keamanan informasi di Jepang. Di bidang penelitian *cyberthreats*, dibentuk *Cyber Clean Center* untuk menganalisis karakteristik *bots* dan menyusun metode penanganan yang efektif dan aman.

Strategi keamanan informasi Jepang terdiri dari dua bagian: (1) *First National Strategy on Information Security*, yang diterapkan secara umum; dan (2) *Secure*

[21] Bagian ini diambil dari NISC, *Japanese Government's Efforts to Address Information Security Issue* (November 2007), http://www.nisc.go.jp/eng/.
[22] Information Security Policy Council, *The First National Strategy on Information Security* (2 Februari 2006), 5. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

Japan YYYY. ***First National Strategy on Information Security*** mengakui kebutuhan semua 'entitas' dalam masyarakat TI "untuk berpartisipasi dalam penciptaan sebuah lingkungan yang aman untuk penggunaan TI." Strategi ini mengakui entitas "yang benar-benar mengadopsi dan melaksanakan langkah sebagai komponen dari masyarakat TI."[23] Entitas yang dimaksud dibagi menjadi empat: pemerintah pusat dan lokal, infrastruktur penting, bisnis dan individu. Masing-masing perlu menetapkan peranan dan rencananya sendiri dan mengoperasikannya (Tabel 4).

Tabel 4. Peran dan Rencana Masing-masing Kategori Berdasarkan *First National Strategy on Information Security*

Kategori	Peran	Rencana
Pemerintah pusat dan lokal	Memberikan 'Praktik Terbaik' untuk metode keamanan informasi	Standar untuk Langkah
Infrastruktur penting	Memastikan penyediaan yang stabil dari layanan mereka sebagai basis kehidupan sosial masyarakat dan aktivitas ekonomi	Rencana Aksi Infrastruktur Utama
Bisnis	Melaksanakan metode keamanan informasi sehingga dapat dipandang tinggi oleh pasar	Metode dikenalkan oleh Menteri dan Lembaga
Individu	Meningkatkan kesadaran sebagai pemain utama kehidupan TI	Metode dikenalkan oleh Menteri dan Lembaga

Sumber: NISC, *Japanese Government's Efforts to Address Information Security Issues* (November 2007), http://www.nisc.go.jp/eng/.

Kebijakan praktis dari *First National Strategy on Information Security* adalah sebagai berikut:

- Memajukan teknologi keamanan informasi - Pengembangan teknologi khusus untuk pemerintah dan mendorong pengembangan teknologi menuju '*Grand Challenge*' inovasi teknologi dasar dengan perspektif jangka panjang;
- Memajukan kerjasama dan kolaborasi internasional - Berkontribusi untuk penetapan basis internasional untuk keamanan dan penjaminan ulang informasi dan membuat kontribusi internasional yang dipimpin Jepang;
- Pengembangan sumber daya manusia - Pengembangan sumber daya manusia dengan keterampilan praktis, bakat, serta kemampuan luas, dan mengatus sistem kualifikasi untuk keamanan informasi; dan
- Pengawasan kejahatan dan langkah perlindungan/perbaikan untuk hak dan kepentingan - Menguatkan kontrol *cybercrime* dan pengembangan dasar hukum yang relevan, serta pengembangan teknologi untuk peningkatan keamanan *cyberspace*.

[23] Ibid., 11.

Secure Japan YYYY adalah rencana tahunan keamanan informasi. *Secure Japan* 2007 berisi 159 langkah implementasi keamanan informasi dan arah rencana untuk 24 prioritas pada 2007. Ringkasnya:

- Peningkatan metode keamanan informasi bagi lembaga pemerintah pusat;
- Metode penyebaran bagi badan yang tertinggal dalam mengambil metode untuk memastikan keamanan informasi, serta untuk publik umum; dan
- Usaha intensif untuk menguatkan platform keamanan informasi.

Pertanyaan

1. Apakah persamaan atau perbedaan aktivitas keamanan informasi di negara Anda dengan yang dijelaskan di atas?

2. Apakah ada aktivitas keamanan informasi yang sedang dilaksanakan di negara-negara yang disebutkan di bagian ini yang tidak dapat diterapkan atau relevan dengan negara Anda? Jika iya, yang manakah dan mengapa mereka tidak dapat diterapkan atau tidak relevan?

3.2 Aktivitas Keamanan Informasi Internasional

Aktivitas keamanan informasi PBB

Di **World Summit on the Information Society (WSIS)**[24] yang disponsori oleh PBB, disusun deklarasi prinsip dan rencana aksi untuk pertumbuhan masyarakat informasi yang efektif serta pengurangan 'kesenjangan informasi'. Rencana aksi menyatakan aksi-aksi berikut:

- Peran pemerintah dan semua *stakeholder* dalam mendukung TIK untuk pembangunan
- Infrastruktur informasi dan komunikasi sebagai pondasi penting untuk masyarakat informasi yang inklusif
- Akses informasi dan pengetahuan
- Pembangunan kapasitas
- Membangun kepercayaan dan keamanan dalam penggunaan TIK
- [Menciptakan] lingkungan yang mendukung
- Aplikasi TIK dalam semua aspek kehidupan
- Keragaman budaya, bahasa dan konten lokal
- Media

[24] World Summit on the Information Society, "Basic Information: About WSIS," http://www.itu.int/wsis/basic/about.html.

- Sisi etika dalam Masyarakat Informasi
- Kerjasama regional dan internasional.[25]

Internet Governance Forum (IGF)[26] adalah organisasi pendukung PBB untuk menangani Tata Kelola Internet. Dibentuk sesudah fase kedua WSIS di Tunisia untuk mendefinisikan dan mengatasi isu tata kelola Internet. Forum IGF kedua, yang diadakan di Rio de Janeiro pada tanggal 12-15 November 2007, berfokus pada isu keamanan informasi seperti *cyberterrorism*, *cybercrime*, dan keamanan anak-anak di Internet.

Aktivitas keamanan informasi OECD[27]

Organisation for Economic Co-operation and Development (OECD) adalah sebuah forum dimana pemerintah dari 30 negara bekerja sama dengan dunia bisnis dan masyarakat sipil dalam menghadapi tantangan ekonomi, sosial, lingkungan dan tata kelola di era globalisasi ekonomi dunia. Didalam OECD, *Working Party on Information Security and Privacy* (WPISP) bekerja dibawah bantuan *Committee for Information, Computer and Communications Policy* untuk memberikan analisis dampak TIK terkait keamanan informasi dan privasi, dan mengembangkan rekomendasi kebijakan hasil konsensus untuk mempertahankan kepercayaan dalam ekonomi Internet.

Hasil kerja WPISP dalam hal keamanan informasi: Di tahun 2002, OECD mengeluarkan "*Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*"[28] untuk meningkatkan "keamanan dalam pengembangan sistem informasi dan jaringan serta penerapan cara baru dalam berpikir dan berperilaku ketika menggunakan dan berinteraksi dengan sistem informasi dan jaringan".[29]

Untuk berbagi pengalaman dan praktik terbaik dalam keamanan informasi, diselenggarakan *Global Forum on Information Systems and Network Security* di tahun 2003 dan *OECD-APEC Workshop on Security of Information Systems and Networks* di tahun 2005.

Hasil kerja WPISP terkait privasi: "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*" yang dikeluarkan pada tahun 1980 mewakili konsensus internasional dalam mengelola informasi personal di sektor publik dan swasta. "*Privacy Online: OECD Guidance on Policy and Practice*" yang dikeluarkan pada tahun 2002 berfokus pada teknologi peningkatan privasi,

[25] World Summit on the Information Society, *Plan of Action* (12 December 2003), http://www.itu.int/wsis/docs/geneva/official/poa.html.
[26] Internet Governance Forum, http://www.intgovforum.org/.
[27] Bagian ini diambil dari WPISP, "Working Party on Information Security and Privacy" (May 2007).
[28] OECD, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (Paris: OECD, 2002), http://www.oecd.org/dataoecd/16/22/15582260.pdf.
[29] Ibid., 8.

kebijakan privasi *online*, pelaksanaan dan perbaikan, dan lain-lain yang terkait dengan *e-commerce*. Saat ini, WPISP sedang mengerjakan *Privacy Law Enforcement Cooperation*.

Hasil kerja lainnya: Pada tahun 1998, OECD mengeluarkan "*Guidelines on Cryptography Policy*" dan mengadakan *Ottawa Ministerial Declaration on Authentication for Electronic Commerce*. Pada tahun 2002 hingga 2003 dilakukan "*Survey of Legal and Policy Frameworks for E-Authentication Services and e-Signatures in OECD Member Countries*". Pada tahun 2005, dikeluarkan "*The Use of Authentication across Borders in OECD Countries*".

Di tahun 2004, telah ditulis "*Biometric-Based Technologies*", dan pada tahun 2005 dibentuk kelompok kerja terkait *spam*. Kegiatan lain yang sedang dikerjakan adalah manajemen identitas dijital, *malware*, *radio frequency identification* (RFID) yang bersifat pervasif, sensor dan jaringan, dan kerangka kerja umum untuk implementasi keamanan informasi dan privasi.

Aktivitas keamanan informasi APEC[30]

Asia-Pacific Economic Cooperation (APEC) melakukan kegiatan keamanan informasi di kawasan Asia Pasifik melalui *Telecommunication and Information Working Group* (TEL), yang terdiri dari tiga kelompok pengarah: kelompok pengarah liberalisasi, kelompok pengarah pengembangan TIK, dan kelompok pengarah Keamanan dan Kemakmuran.

Semenjak pertemuan tingkat menteri APEC bidang industri telekomunikasi dan informasi keenam di Lima, Peru di bulan Juni 2005, kelompok pengarah bidang Kemanan dan Kemakmuran telah melakukan pembicaraan tentang *cybersecurity* dan *cybercrime*. Strategi *Cyber-Security* APEC dimana termasuk didalamnya penguatan kepercayaan konsumen dalam menggunakan *e-commerce*, menjadi pemersatu usaha di berbagai ekonomi. Usaha–usaha tersebut termasuk pengesahan dan pelaksanaan hukum *cybersecurity* yang konsisten dengan *UN General Assembly Resolution 55/63*[31] dan Konvensi *Cybercrime*.[32] Proyek pengembangan kapasitas TEL *Cyber-crime Legislation Initiative and Enforcement* akan mendukung institusi dalam pelaksanaan hukum baru.

Anggota APEC juga bekerja bersama-sama membentuk *Computer Emergency Response Teams* (CERTs) sebagai sistem pertahanan peringatan dini terhadap

[30] Bagian ini diambil dari APEC, "Telecommunications and Information Working Group," http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[31] 'Memerangi penyalahgunaan informasi ' menyoroti bahwa salah satu dampak perkembangan teknologi adalah peningkatan aktivitas kriminal di dunia maya..

[32] Perjanjian yang dilakukan di Budapest dalam rangka menegakkan integritas sistem komputer dengan menyatakan bahwa segala aksi yang melanggar integritas adalah tindakan kriminal. Lihat http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

serangan *cyber*. Republik Korea memberikan pelatihan kepada anggota negara berkembang, dan memberikan pedoman dalam membentuk dan mengoperasikan CERT.

Perlindungan terhadap UKM dan pengguna di rumah dari serangan *cyber* dan virus merupakan prioritas dan sejumlah perangkat telah dikembangkan untuk tujuan tersebut. Informasi tentang penggunaan Internet yang aman, permasalahan keamanan terkait teknologi nirkabel, dan pertukaran *e-mail* yang aman juga selalu diberikan.

Usaha mengurangi penyalahgunaan informasi melalui berbagi informasi, pengembangan prosedur dan hukum, serta langkah-langkah lain untuk melindungi bisnis dan masyarakat akan terus menjadi prioritas bagi APECTEL. Sebagai bagian dari agenda untuk isu keamanan, APECTEL menyetujui "*Guide on Policy and Technical Approach against Botnet*" dan *Workshop on Cyber Security and Critical Information Infrastructure* pada tahun 2007.

Aktivitas keamanan informasi ITU[33]

ITU adalah lembaga PBB untuk TIK. Bermarkas di Jenewa, Swiss, ITU memiliki 191 Negara Anggota dan lebih dari 700 Anggota Sektor dan Asosiasi.

Peranan ITU dalam membantu komunikasi dunia terbagi menjadi tiga sektor utama. Sektor komunikasi radio (ITU-R) berfokus pada pengelolaan spektrum frekuensi radio internasional dan sumber daya orbit satelit. Sektor standarisasi (ITU-T) fokus pada standarisasi jaringan dan layanan komunikasi-informasi. Sektor Pembangunan (ITU-D) membantu menyebarkan akses ke TIK yang adil, berkesinambungan, dan terjangkau sebagai cara merangsang pertumbuhan sosial dan ekonomi yang lebih luas. ITU juga mengelola kegiatan TELECOM dan salah satu lembaga yang berperan penting dalam pelaksanaan WSIS.

Di bidang *cybersecurity*, inisiatif utama ITU termasuk *WSIS Action Line C.5*, *ITU Global Cybersecurity Agenda*, dan *ITU Cybersecurity Gateway*.

Fokus utama *WSIS Action Line C.5* adalah:

- Perlindungan terhadap infrastruktur informasi utama (CIIP-*Critical Information Infrastructure Protection*);
- Promosi budaya global *cybersecurity*;
- Harmonisasi pendekatan hukum nasional, koordinasi dan penegakan hukum internasional;
- Mengatasi *spam*;
- Pengembangan kemampuan dalam pengamatan, peringatan dan penanganan insiden;

[33] Bagian ini diambil dari ITU, "About ITU," http://www.itu.int/net/about/index.aspx.

- Berbagi informasi tentang pendekatan nasional, praktik terbaik, serta pedoman;dan
- Perlindungan privasi, data dan konsumen.

ITU Global Cybersecurity Agenda (GCA) ialah kerangka kerja ITU untuk kerja sama internasional yang bertujuan memberikan solusi untuk meningkatkan kepercayaan dan keamanan di masyarakat informasi. GCA memiliki lima pilar strategi: kerangka kerja hukum, tindakan teknis, struktur organisasi, pengembangan kapasitas dan kerja sama internasional. Strategi tersebut diuraikan dalam tujuan-tujuan berikut:

- Mengembangkan model hukum *cybercrime* yang dapat diterapkan secara global serta cocok dengan sistem hukum nasional/regional yang ada;
- Membuat struktur organisasi dan kebijakan nasional dan regional terkait *cybercrime*;
- Menetapkan kriteria keamanan minimum dan skema terakreditasi untuk aplikasi dan sistem piranti lunak, yang dapat diterima secara global;
- Menyusun kerangka kerja global untuk pengawasan, peringatan dan penanganan insiden untuk memastikan koordinasi inisiatif yang lintas batas;
- Membuat dan mendukung sistem identitas dijital yang umum dan universal serta struktur organisasi yang diperlukan untuk memastikan pengakuan informasi dijital seseorang yang lintas batas geografis;
- Mengermbangkan strategi global untuk membantu pembangunan kapasitas manusia dan institusi dalm rangka meningkatkan pengetahuan yang lintas sektor dan dalam semua bidang yang disebutkan di atas; dan
- Memberikan saran pada kerangka kerja potensial untuk strategi *multi stakeholder* global untuk kerja sama, dialog dan koordinasi internasional di semua bidang yang telah disebutkan di atas.

ITU Cybersecurity Gateway bertujuan untuk menyediakan sumber daya informasi yang mudah digunakan akan inisiatif yang terkait dengan *cybersecurity* nasional dan internasional. Ini tersedia untuk masyarakat, pemerintah, bisnis dan organisasi internasional. Layanan yang disediakan *Gateway* mencakup berbagi informasi, pengawasan dan pemberian peringatan, hukum dan perundang-undangan, privasi dan perlindungan, serta solusi dan standar industri.

ITU-D juga mengawasi program kerja *Cybersecurity* ITU yang disusun untuk membantu negara mengembangkan teknologi untuk keamanan *cyberspace* tingkat tinggi. Program tersebut membantu hal-hal yang terkait pada:

- Penyusunan strategi dan kemampuan nasional untuk *cybersecurity* dan CIIP
- Pembentukan mekanisme hukum *cybercrime* dan penegakannya yang tepat
- Pembangunan kemampuan pengawasan, pemberian peringatan dan penanganan insiden
- Mengatasi *spam* dan ancaman terkait

- Menjembatani kesenjangan standarisasi keamanan antara negara maju dan negara berkembang
- Membangun sebuah *ITU Cybersecurity/CIIP Directory*, basisdata kontak dan publikasi *Who's Who*
- Menentukan indikator *cybersecurity*
- Menumbuhkan aktivitas kerjasama regional
- Berbagi informasi dan mendukung *ITU Cybersecurity Gateway*
- Promosi aktivitas terkait.

Kegiatan ITU-D lainnya yang terkait *cybersecurity* adalah kegiatan gabungan dalam StopSpamAlliance.org, kegiatan pembangunan kapasitas regional terhadap hukum *cybercrime* dan penegakannya, pengembangan dan distribusi perangkat *botnet mitigation*,[34] publikasi *cybersecurity/cybercrime*,[35] perangkat model hukum *cybercrime* bagi negara berkembang, dan perangkat evaluasi diri *cybersecurity* nasional.[36]

Aktivitas keamanan informasi ISO/IEC

Information Security Management System (ISMS) adalah, sesuai dengan namanya, sebuah sistem untuk mengelola keamanan informasi. ISMS terdiri dari proses dan sistem untuk memastikan kerahasiaan, integritas dan ketersediaan aset informasi dalam meminimalisasi risiko keamanan. Sertifikasi ISMS semakin dikenal di seluruh dunia, dimana tahun 2005 menjadi saat yang menentukan dalam sejarah standarisasi internasional ISMS dengan dirilisnya dua dokumen: IS 27001 yang berisi kebutuhan untuk membangun ISMS, dan IS 17799: 2000, dipublikasikan sebagai IS 17799:2005, menetapkan kontrol-kontrol dasar dalam implementasi ISMS.

Standar de facto ISMS adalah BS 7799, yang dikembangkan oleh *British Standards Institution* (BSI) di tahun 1995 sebagai standar manajemen keamanan informasi. Pada tahun 1998, ketika spesifikasi kebutuhan telah dikembangkan berlandaskan standar ini, 'standar manajemen keamanan informasi' diubah menjadi Bagian 1 dan spesifikasi kebutuhan menjadi Bagian 2. Bagian 1 berisi kontrol-kontrol untuk manajemen keamanan informasi, sedangkan Bagian 2 menyatakan kebutuhan untuk membentuk ISMS, dan menjelaskan proses keamanan informasi (Siklus *Plan-Do-Check-Act*) untuk peningkatan berkelanjutan landasan manajemen risiko.

---

[34] Suresh Ramasubramanian dan Robert Shaw, "ITU Botnet Mitigation Project: Background and Approach" (Presentasi ITU, September 2007), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf.

[35] ITU-D Applications and Cybersecurity Division, "Publications," ITU, http://www.itu.int/ITU-D/cyb/publications/.

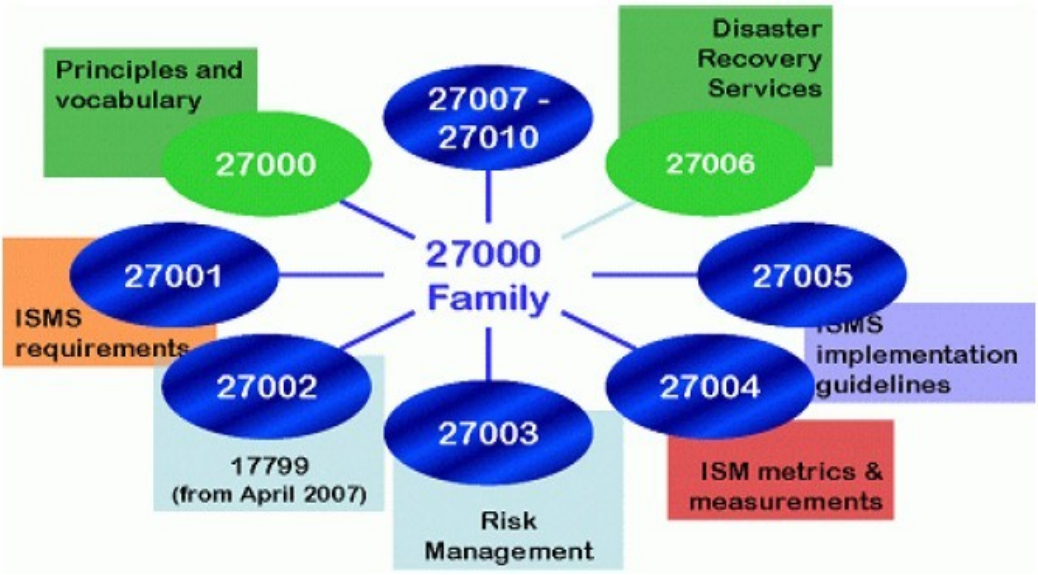
[36] ITU-D Applications and Cybersecurity Division, "ITU National Cybersecurity / CIIP Self-Assessment Tool," ITU, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Bagian 1 ditetapkan sebagai IS 17799 oleh ISO/IEC JTC 1/SC27 WG1 di tahun 2000. Sejak itu, IS 17799 terus ditinjau (dengan lebih dari 2000 komentar) dan direvisi, dan versi final didaftarkan ke standar internasional pada November 2005. IS 17799: 2000 berisi 126 daftar kontrol dengan 10 bidang manajemen kontrol. IS 17799 direvisi pada tahun 2005 yang berisi 11 domain kontrol administratif dan 133 kontrol.

Bagian 2 dari BS 7799 yang ditetapkan pada tahun 1999 telah digunakan sebagai standar untuk sertifikasi ISMS. Bagian 2 direvisi pada September 2002 agar selaras dengan ISO 9001 dan ISO 14001. ISO mengadopsi Bagian 2 BS7799: 2002 melalui metode jalur cepat untuk memenuhi permintaan standar internasional ISMS dan mendaftarkannya sebagai standar internasional ISO27001 dengan sedikit revisi dalam waktu yang singkat. Perubahan yang dilakukan diantaranya adalah penambahan konten tentang efektifitas dan perubahan pada lampiran.

Karena dua dokumen penting yang terkait pada ISMS telah distandarisasi internasional, keluarga standar keamanan internasional muncul dibawah skema nomor seri 27000, yang sama dengan sistem manajemen lain (Kualitas: seri 9000, Manajemen lingkungan: seri 14000). IS 27001, versi revisi dari IS 17799:2005 memasukkan kebutuhan untuk membentuk ISMS dan IS17799:2005 dimana didalamnya berisi kontrol dasar dalam implementasi ISMS. IS27001 berubah menjadi IS27002 pada tahun 2007. Pedoman untuk implementasi ISMS, sebuah standar manajemen risiko keamanan informasi, serta pengukuran manajemen sistem keamanan informasi yang dikembangkan oleh JTC1 SC27 ada di dalam seri 27000.

Gambar 7 menunjukkan keluarga standar terkait ISMS. Aktivitas sertifikasi ISMS memperoleh momentum dan diharapkan bahwa standar ISMS atau pedoman yang cocok dengan industri tertentu dikembangkan berdasarkan pada ISMS untuk sistem umum. Contohnya adalah usaha untuk mengembangkan pedoman ISMS yang merefleksikan karakteristik industri komunikasi.



Gambar 7. Keluarga ISO/IEC 27001
(ANSIL, Roadmap ISO/IEC 2700x, ISMS, Forum Eurosec 2007, http://www.ansil.eu/files/pres-eurosec2007-23052007.pdf)

Pertanyaan

Dari beberapa kegiatan keamanan informasi yang dilakukan oleh organisasi internasional di Bagian ini, manakah yang telah di adopsi di negara Anda? Bagaimana mereka diimplementasikan?

Ujian

1. Apa kemiripan diantara kegiatan keamanan informasi yang dilaksanakan oleh negara-negara yang dijelaskan dalam Bagian ini? Apa perbedaannya?

2. Apakah prioritas keamanan informasi dari organisasi internasional yang dijelaskan dalam Bagian ini?

4. METODOLOGI KEAMANAN INFORMASI

Bagian ini bertujuan untuk menjelaskan metodologi keamanan informasi secara teknis, fisik, dan administratif yang digunakan secara internasional.

4.1 Metodologi Keamanan Informasi

Metodologi keamanan informasi bertujuan untuk meminimalisasi kerusakan dan memelihara keberlangsungan bisnis dengan memerhatikan semua kemungkinan kelemahan dan ancaman terhadap aset informasi. Untuk menjamin keberlangsungan bisnis, metodologi keamanan informasi berusaha memastikan kerahasiaan, integritas dan ketersediaan aset informasi internal. Hal ini termasuk penerapan metode dan kontrol manajemen risiko. Pada dasarnya, yang dibutuhkan adalah rencana yang bagus dan meliputi aspek administratif, fisik, serta teknis dari keamanan informasi.

Aspek administratif

Terdapat banyak ISMS yang fokus pada aspek administratif. Salah satu yang paling umum digunakan adalah ISO/IEC27001.

ISO/IEC27001, standar ISMS internasional, berdasarkan pada BS7799, yang disusun oleh BSI. BS7799 berisi kebutuhan untuk implementasi dan pengelolaan ISMS dan standar-standar umum yang digunakan untuk standar keamanan berbagai organisasi serta manajemen keamanan yang efektif. Bagian 1 dari BS7799 menjelaskan kegiatan keamanan yang diperlukan berdasarkan praktik keamanan terbaik dalam organisasi. Bagian 2, yang menjadi ISO/IEC27001 saat ini, berisi persyaratan minimum yang dibutuhkan untuk operasi ISMS dan penilaian aktivitas keamanan.

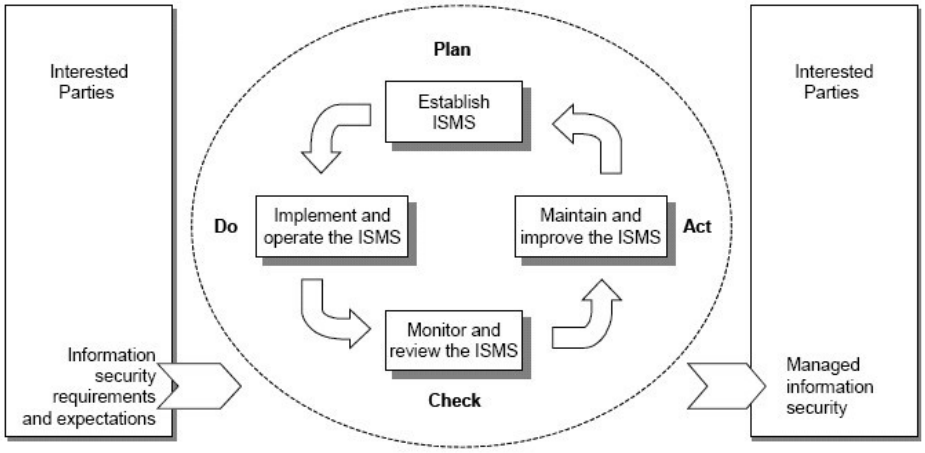
Kegiatan keamanan dalam ISO/IEC27001 terdiri dari 133 kontrol dan 11 domain (Tabel 5).

Tabel 5. Kontrol di ISO/IEC27001

Domain	*Item*
A5.	Kebijakan keamanan
A6.	Organisasi keamanan informasi
A7.	Manajemen aset
A8.	Keamanan sumber daya manusia
A9.	Keamanan fisik dan lingkungan
A10.	Manajemen komunikasi dan operasi

Domain	*Item*
A11.	Kontrol akses
A12.	Pengadaan, pengembangan dan pemeliharaan sistem informasi
A13.	Manajemen insiden keamanan informasi
A14.	Manajemen keberlangsungan bisnis
A15.	Kepatuhan (*compliance*)

ISO/IEC27001 mengadopsi model proses *Plan-Do-Check-Act*, yang digunakan untuk mengatur struktur seluruh proses ISMS. Dalam ISO/IEC27001, semua bukti hasil penilaian ISMS harus didokumentasikan; sertifikasinya harus diaudit secara eksternal setiap enam bulan; dan seluruh proses diulangi sesudah tiga tahun untuk terus mengatur ISMS.



Gambar 8. Model Proses *Plan-Do-Check-Act* yang Diterapkan ke Proses *ISMS*
(Sumber: ISO/IEC JTC 1/SC 27)

Kontrol keamanan harus direncanakan dengan memperhatikan kebutuhan keamanan. Semua sumber daya manusia, termasuk penyedia, kontraktor, konsumen dan spesialis dari luar, harus berpartisipasi dalam kegiatan ini. Penetapan kebutuhan keamanan berlandaskan pada tiga faktor berikut:

- Kajian risiko
- Kebutuhan hukum dan klausa kontrak
- Pemrosesan informasi untuk operasi organisasi

Analisis kesenjangan adalah proses pengukuran tingkat keamanan informasi saat ini dan menetapkan arah masa depan keamanan informasi. Hasil analisis kesenjangan diturunkan dari jawaban pemilik aset akan 133 kontrol dan 11 domain. Sesudah area yang lemah teridentifikasi melalui analisis kesenjangan, kontrol yang sesuai per area dapat ditetapkan.

Kajian risiko terdiri dari dua bagian: kajian nilai aset dan kajian ancaman dan kerentanan. Kajian nilai aset adalah penilaian kuantitatif aset informasi. Kajian ancaman meliputi penilaian ancaman terhadap kerahasiaan, integritas dan ketersediaan informasi. Di bawah ini adalah contoh perhitungan penilaian risiko.

Nama aset	Nilai aset	Ancaman			Kerentanan			Risiko		
		C	I	A	C	I	A	C	I	A
Nama aset #1	2	3	3	1	3	1	1	8	6	5

- Nilai Aset + Ancaman + Kerentanan = Risiko
- Kerahasiaan: Nilai Aset(2) + Ancaman(3) + Kerentanan(3) = Risiko(8)
- Integritas: Nilai Aset(2) + Ancaman(3) + Kerentanan(1) = Risiko(6)
- Ketersediaan: Nilai Aset(2) + Ancaman(1) + Kerentanan(1) = Risiko(5).

Penerapan kontrol: Setiap nilai risiko akan berbeda sesuai dengan hasil kajian risiko. Diperlukan keputusan untuk menerapkan kontrol yang sesuai untuk masing-masing nilai aset yang berbeda. Risiko perlu dibagi ke dalam risiko yang dapat diterima dan risiko yang tidak dapat diterima mengikuti kriteria 'Tingkatan Jaminan'. Kontrol perlu diterapkan ke aset informasi dengan risiko yang tidak dapat diterima. Kontrol diterapkan berdasarkan kontrol ISO/IEC, tetapi akan lebih efektif jika penerapan kontrol disesuaikan dengan kondisi organisasi.

Setiap negara memiliki badan sertifikasi ISO/IEC27001. Tabel 6 menunjukkan jumlah sertifikasi tiap negara.

Tabel 6. Jumlah Sertifikasi Tiap Negara

Jepang	2863*	Belanda	11	Bulgaria	2
India	433	Singapura	11	Kanada	2
Inggris	368	Filipina	10	Gibraltar	2
Taiwan	202	Arab Saudi	10	Isle of Man	2
Cina	174	Pakistan	10	Maroko	2
Jerman	108	Federasi Rusia	10	Oman	2
Amerika Serikat	82	Perancis	9	Qatar	2
Hungaria	74	Kolombia	7	Yaman	2
Republik Korea	71	Slovenia	7	Armenia	1
Republik Ceko	66	Swedia	7	Bangladesh	1
Itali	54	Slovakia	6	Belgia	1
Hong Kong	38	Kroasia	5	Mesir	1
Polandia	36	Yunani	5	Iran	1
Australia	28	Afrika Selatan	5	Kazakhstan	1

Austria	26	Bahrain	4	Kyrgyzstan	1
Irlandia	26	Indonesia	4	Libanon	1
Malaysia	26	Kuwait	4	Lithuania	1
Spanyol	26	Norwegia	4	Luxembourg	1
Brazil	20	Sri Lanka	4	Macedonia	1
Mexico	20	Swiss	4	Moldova	1
Thailand	17	Chili	3	Selandia Baru	1
Romania	16	Macau	3	Ukraina	1
Turki	15	Peru	3	Uruguay	1
Uni Emirat Arab	14	Portugal	3	Total Relatif	4997
Islandia	11	Viet Nam	3	**Total Absolut**	**4987**

Catatan: Jumlah sertifikasi yang diperlihatkan diambil pada 21 Desember 2008.
Sumber: *International Register of ISMS Certificates*, "Number of Certificates per Country," ISMS International User Group Ltd., http://www.iso27001certificates.com.

Aspek Fisik

Saat ini belum ada sistem manajemen keamanan informasi fisik yang berlaku secara internasional. Namun demikian, akan dijelaskan *Federal Emergency Management Agency* (FEMA) 426,[37] yang merupakan standar ISMS fisik di Amerika Serikat dan digunakan di banyak negara sebagai metodologi.

FEMA 426 memberi panduan untuk melindungi gedung terhadap serangan teroris. FEMA 426 ditujukan pada "komunitas ilmu bangunan yang terdiri dari para arsitek dan insinyur, untuk mengurangi kerusakan fisik gedung, infrastruktur terkait, dan manusia yang disebabkan oleh serangan teroris."[38] Seri pedoman terkait adalah FEMA 427 ("*A Primer for the Design of Commercial Buildings to Mitigate Terrorist Attacks*"), FEMA 428 ("*A Primer to Design Safe School Projects in Case of Terrorist Attacks*"), FEMA 429 ("*Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings*"), FEMA 430 (arsitek), and FEMA 438 (*course*).

FEMA 426 tidak langsung terkait dengan keamanan informasi, tetapi mampu mencegah kebocoran, kehilangan atau penghancuran informasi akibat serangan fisik terhadap bangunan. Secara khusus, FEMA 426 sangat terkait dengan rencana keberlangsungan bisnis yang merupakan komponen dari keamanan administratif. Dengan menerapkan FEMA 426, aspek fisik dari rencana keberlangsungan bisnis dapat dilindungi.

[37] FEMA, "FEMA 426- Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings," http://www.fema.gov/plan/prevent/rms/rmsp426.
[38] Ibid.

Aspek teknis

Belum ada ISMS untuk aspek teknis. Namun, standar evaluasi umum internasional seperti sertifikasi *Common Criteria* (CC) mungkin dapat digunakan.

Sertifikasi Common Criteria[39]

Sertifikasi CC memiliki akar komersial. CC disusun untuk mengatasi kekhawatiran akan perbedaan tingkat keamanan produk TI dari berbagai negara. Standar internasional ini untuk evaluasi produk TI ini disusun oleh Kanada, Perancis, Jerman, Inggris dan AS.

Secara khusus, CC berisi kebutuhan keamanan TI dari produk atau sistem dalam kategori yang terpisah yaitu kebutuhan fungsional dan penjaminan. Kebutuhan fungsional CC menyatakan perilaku keamanan yang diinginkan. Kebutuhan penjaminan digunakan untuk memastikan bahwa tindakan pengamanan yang dilakukan telah efektif dan diimplementasikan dengan benar. Fungsi keamanan CC terdiri dari 136 komponen dari 11 kelas yang membentuk 57 keluarga. Kebutuhan penjaminan terdiri dari 86 komponen dari sembilan kelas yang membentuk 40 keluarga.

Kebutuhan Fungsional Keamanan (*Security Functional Requirement* (SFR)): SFR menentukan semua fungsi keamanan untuk *Target of Evaluation* (TOE). Tabel 7 berisi daftar kelas fungsi keamanan yang termasuk dalam SFR.

Tabel 7. Komposisi Kelas dalam SFR

Kelas		Rincian
FAU	Audit keamanan	Fungsi-fungsi seperti proteksi data audit, format *record* dan seleksi peristiwa, serta perangkat analisis, alarm pelanggaran dan analisis *real-time*
FCO	Komunikasi	Menggambarkan kebutuhan secara spesifik bagi TOE yang digunakan untuk pengiriman informasi
FCS	Dukungan kriptografi	Menetapkan penggunaan manajemen kunci kriptografi dan operasi kriptografi
FDP	Proteksi data pengguna	Menetapkan kebutuhan terkait dengan perlindungan data pengguna
FIA	Identifikasi dan otentikasi	Menanggapi kebutuhan fungsi untuk menetapkan dan memverifikasi identitas pengguna yang diklaim
FMT	Manajemen keamanan	Menentukan manajemen dari berbagai aspek *TOE Security Functions* (TSF): atribut keamanan, data dan fungsi TSF
FPR	Privasi	Berisi kebutuhan yang dapat ditarik untuk memenuhi kebutuhan privasi pengguna, sekaligus tetap menjaga

[39] Common Criteria, http://www.commoncriteriaportal.org.

Kelas		Rincian
		sistem sefleksibel mungkin untuk memelihara kontrol yang cukup bagi operasional sistem
FPT	Proteksi TSF	Berisi kebutuhan fungsional yang terkait dengan integritas dan manajemen mekanisme dari TSF dan integritas data TSF
FRU	Utilisasi sumber daya	Berisi ketersediaan sumber daya yang dibutuhkan seperti pemrosesan kapabilitas dan/atau kapasitas penyimpanan
FTA	Akses TOE	Menentukan kebutuhan fungsional untuk pengontrolan sesi-sesi pengguna
FTP	Jalur/saluran yang dipercaya	Memberikan kebutuhan untuk jalur komunikasi yang dipercaya antara pengguna dan TSF

(Sumber: Common Criteria, Common Methodology for Information Technology Security Evaluation, September 2007, CCMB-2007-09-004)

Komponen jaminan keamanan (*Security assurance components* (SACs)): Filosofi CC membutuhkan artikulasi ancaman keamanan dan komitmen terhadap kebijakan keamanan organisasional melalui tindakan keamanan yang tepat dan cukup. Langkah yang diadopsi harus membantu identifikasi kerentanan, mengurangi kemungkinan dari dieksploitasi, dan mengurangi kerusakan ketika kerentanan dimanfaatkan.[40] Tabel 8 memperlihatkan daftar kelas yang termasuk dalam SAC.

Tabel 8. Komposisi Kelas dalam SAC

Kelas		Rincian
APE	Evaluasi *Protection Profile* (PP)	Ini dibutuhkan untuk menunjukkan bahwa PP sudah baik dan konsisten dan, jika PP berdasar pada satu atau lebih PP atau paket lainnya, bahwa PP merupakan perwujudan yang benar dari PP dan paket yang digunakan.
ASE	Evaluasi *Security Target* (ST)	Ini dibutuhkan untuk menunjukkan bahwa ST sudah baik dan konsisten dan, jika ST berdasar pada satu atau lebih PP lainnya atau pada paket, bahwa ST merupakan perwujudan yang benar dari PP dan paket yang digunakan.
ADV	Pengembangan	Ini memberikan informasi tentang TOE. Pengetahuan yang didapat digunakan sebagai dasar untuk melakukan analisis kerentanan dan pengujian terhadap TOE, seperti dijelaskan dalam kelas ATE dan AVA.
AGD	Dokumen pedoman	Untuk persiapan dan operasi TOE yang aman, perlu digambarkan semua aspek yang relevan untuk penanganan TOE yang aman. Kelas tersebut juga menanggapi kemungkinan salah konfigurasi atau penanganan TOE yang tidak diharapkan.

[40] Common Criteria, *Common Criteria for Information Technology Security Evaluation – Part 3 : Security assurance requirements* (August 1999, Vesion 2.1), http://www.scribd.com/doc/2091714/NSA-Common-Critira-Part3.

Kelas		Rincian
ALC	Dukungan daur-hidup	Dalam daur-hidup produk, termasuk didalamnya kemampuan manajemen konfigurasi (CM), ruang lingkup CM, penyampaian, kemanan pengembangan, perbaikan kerusakan, definisi, perangkat dan teknik daur-hidup, membedakan apakan TOE dibawah tanggung jawab pengembang atau pengguna.
ATE	Tes	Penekanan di kelas ini adalah pada konfirmasi bahwa TSF beroperasi sesuai dengan deskripsi desainnya. Kelas ini tidak berurusan dengan penetrasi pengujian.
AVA	Kajian kerentanan	Kajian kerentanan mencakup berbagai kerentanan dalam pengembangan dan operasi TOE.
ACO	Komposisi	Menetapkan kebutuhan penjaminan untuk memastikan bahwa TOE yang disusun akan beroperasi secara aman ketika mengandalkan fungsionalitas keamanan yang disediakan oleh komponen peranti lunak, *firmware* atau perangkat keras yang dievaluasi sebelumnya.

(Sumber: Common Criteria, Common Methodology for Information Technology Security Evaluation, September 2007, CCMB-2007-09-004)

Metode evaluasi CC

1. **Evaluasi PP**: PP mendeskrispsikan sekumpulan kebutuhan keamanan yang bebas-dari-implementasi untuk kategori TOE dan berisi pernyataan masalah keamanan dimana produk yang *compliant* berusaha selesaikan. PP berisi kebutuhan penjaminan dan fungsional, dan memberi alasan pemilihan komponen fungsional dan penjaminan. Biasanya dibuat oleh konsumen atau komunitas konsumen untuk kebutuhan keamanan TI.

2. **Evaluasi ST**: ST merupakan dasar persetujuan antara pengembang TOE, konsumen, pengevaluasi dan otoritas evaluasi atas apa yang ditawarkan TOE, dan ruang lingkup evaluasi. Yang terlibat oleh ST juga dapat meliputi yang mengelola, memasarkan, mengadakan, memasang, mengkonfigurasi, mengoperasikan, dan menggunakan TOE. ST berisi beberapa informasi spesifik-implementasi yang menunjukkan bagaimana produk memenuhi kebutuhan keamanan. Evaluasi ini dapat mengacu pada satu atau lebih PP. Dalam kasus ini, ST harus memenuhi kebutuhan keamanan umum yang ada di setiap PP dan bisa jadi menetapkan kebutuhan lanjut.

Common Criteria Recognition Arrangement

Common Criteria Recognition Arrangement (CCRA) berfungsi untuk memberikan persetujuan sertifikasi CC di berbagai negara. CCRA bertujuan untuk memastikan bahwa evaluasi CC dilakukan terhadap standar yang konsisten, menghilangkan atau mengurangi duplikasi evaluasi produk TI atau profil proteksi, dan meningkatkan kesempatan di pasar global untuk industri TI dengan memberikan sertifikasi diantara negara anggota.

CCRA terdiri dari 24 negara anggota. Terbagi menjadi dua, 12 merupakan *Certificate Authorizing Participants* (CAP) dan 12 lainnya adalah *Certificate Consuming Participants* (CCP). CAP adalah *produsen* sertifikat evaluasi. Mereka adalah sponsor dari badan sertifikasi yang beroperasi di negara mereka sendiri dan mereka mengesahkan sertifikat yang dikeluarkan. Sebuah negara harus menjadi anggota CCRA dan bertindak sebagai CCP minimal selama dua tahun sebelum negara tersebut dapat mendaftar untuk menjadi CAP. CCP adalah *konsumen* dari sertifikat evaluasi. Meskipun mereka mungkin tidak memelihara kemampuan evaluasi keamanan TI, mereka telah menunjukkan keinginan untuk menggunakan produk tersertifikasi/tervalidasi dan profil proteksi. Untuk menjadi anggota CCRA, sebuah negara harus menyampaikan permohonan tertulis ke Komite Manajemen.

Gambar 9. CAP dan CCP

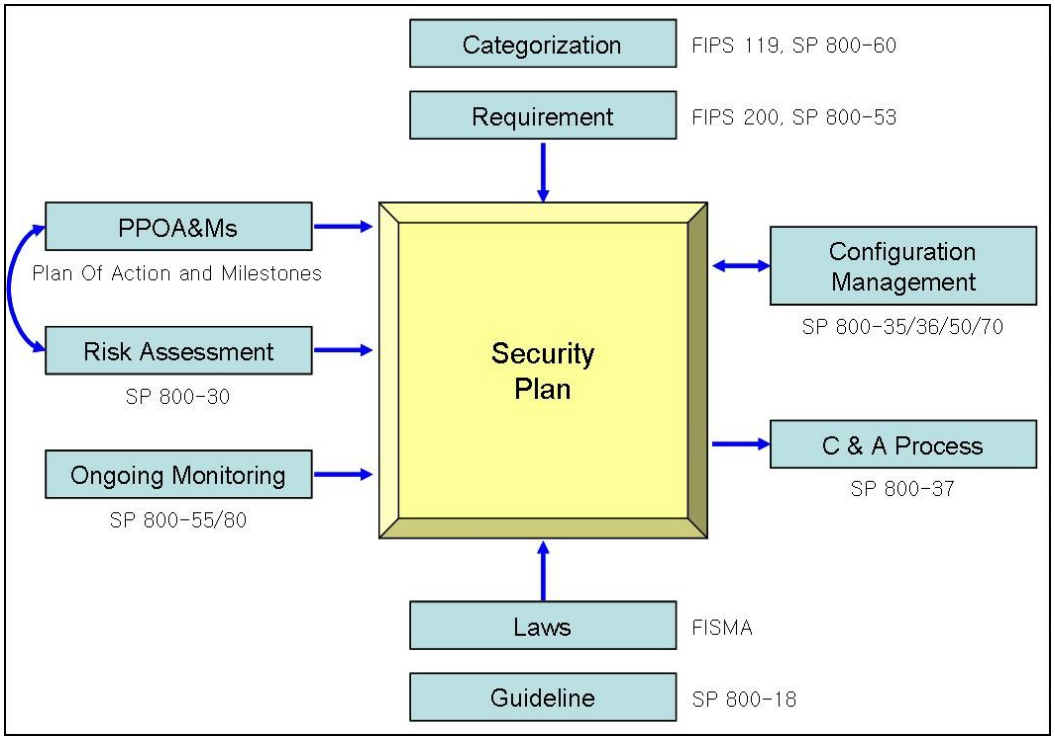
4.2 Contoh Metodologi Keamanan Informasi

US National Institute of Standards and Technology

Berdasarkan FISMA, *US National Institute of Standards and Technology* (NIST) telah mengembangkan pedoman dan standar untuk memperkuat keamanan informasi dan sistem informasi yang dapat digunakan oleh institusi Federal. Pedoman dan standar bertujuan untuk:

- Memberikan spesifikasi untuk persyaratan keamanan minimum dengan mengembangkan standar yang dapat digunakan untuk kategorisasi dari informasi dan sistem informasi Federal;
- Melakukan kategorisasi keamanan informasi dan sistem informasi;
- Memilih dan menentukan kontrol keamanan sistem informasi yang mendukung lembaga eksekutif pemerintah Federal; dan
- Verifikasi efisiensi dan efektivitas kontrol keamanan terhadap kerentanan.

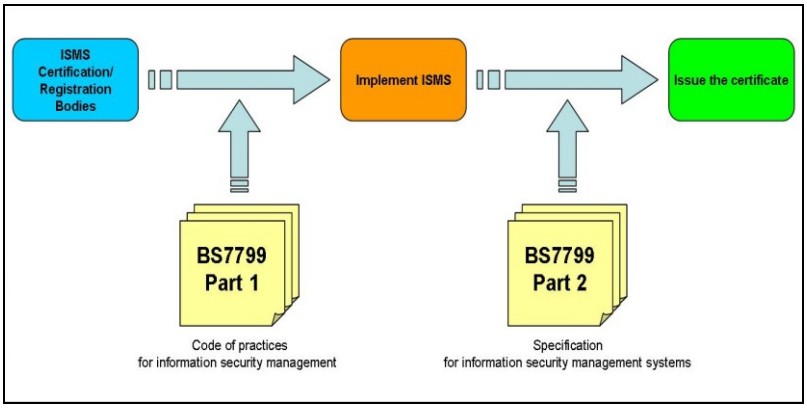
Pedoman terkait FISMA dipublikasikan dalam bentuk publikasi khusus dan juga publikasi *Federal Information Processing Standards*. Ada dua seri publikasi khusus: seri 500 untuk teknologi informasi dan seri 800 untuk keamanan komputer. Gambar 10 menunjukkan proses yang dilakukan lembaga pemerintah AS dalam menyusun rencana keamanan mereka berdasarkan standar ini.



Gambar 10. Masukan/Keluaran Proses Perencanaan Keamanan

Inggris (BS7799)

Seperti yang dijelaskan sebelumnya, BSI menganalisis aktivitas keamanan organisasi di Inggris dan memberikan sertifikasi BS7799, yang sekarang telah dikembangkan menjadi ISO27001 (BS7799 bagian 2) dan ISO27002 (BS7799 bagian 1). Gambar 11 menunjukkan prosedurnya.



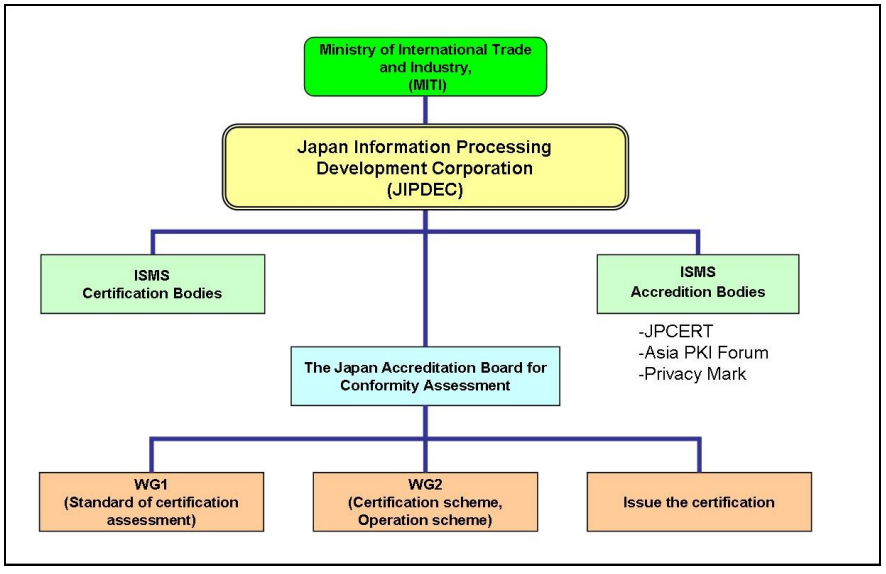
Gambar 11. Proses Sertifikasi BS7799

Jepang (dari ISMS Ver2.0 ke BS7799 Bagian 2: 2002)

ISMS Ver2.0 dari *Japan Information Processing Development Corporation* telah beroperasi di Jepang sejak April 2002. Belakangan ini telah diganti dengan BS7799 Part 2: 2002.

Tingkat permohonan sertifikasi telah meningkat sejak pemerintah pusat memromosikan perencanaan keamanan informasi. Pemerintah daerah juga telah menyediakan uang hibah bagi lembaga yang ingin mendapatkan sertifikasi ISMS. Namun, ISMS Ver2.0 hanya menekankan aspek administratif dan tidak mencakup aspek teknis keamanan informasi. Selain itu, sebagian besar organisasi hanya tertarik untuk mendapatkan sertifikasi, bukan untuk meningkatkan kegiatan keamanan informasi mereka.

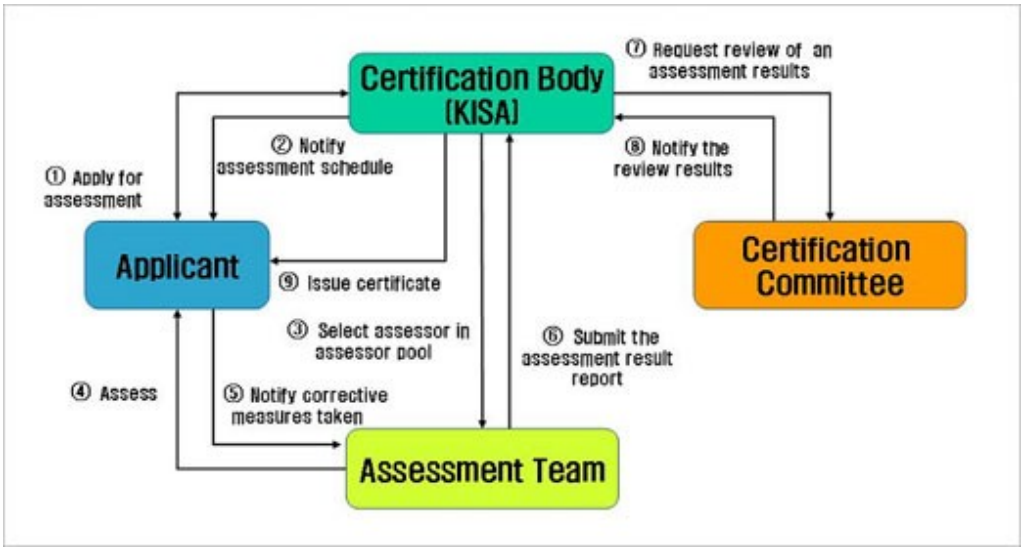
Gambar 12 menunjukkan sistem sertifikasi ISMS di Jepang



Gambar 12. Sertifikasi ISMS di Jepang

Republik Korea (ISO/IEC27001 dan/atau KISA ISMS)

Sertifikasi ISMS oleh *Korea Information Security Agency* (KISA), dikembangkan terutama oleh MIC, digunakan ketika ISO/IEC 27001 sedang disebarluaskan oleh BSI-Korea. ISMS KISA adalah sistem manajemen sintetis yang mencakup rencana keamanan teknis/fisik. Jadi, sistem sertifikasi ISMS KISA menguatkan area keamanan informasi teknis yang dirasakan kurang di ISO/IEC27001. Secara khusus, adopsi '*Safety Procedure*' sebagai syarat sertifikasi menguatkan pengujian teknis. Gambar 13 menunjukkan proses sertifikasi ISMS KISA.



Gambar 13. Sertifikasi ISMS KISA
(Sumber: KISA, 2005, "Procedure of Application for ISMS Certification," http://www.kisa.or.kr/index.jsp)

Jerman (*IT Baseline Protection Qualification*)

BSI Jerman (*Bundesamt fűr Sicherheit in der Informationstechnik*) adalah lembaga nasional untuk keamanan informasi. Lembaga tersebut menyediakan layanan keamanan TI untuk pemerintah Jerman, kota, organisasi dan individu di Jerman.

BSI telah menyusun *IT Baseline Protection Qualification* berdasarkan standar internasional, *ISO Guide 25[GUI25]* dan standar Eropa, EN45001, yang diterima oleh Komite Eropa untuk Pengujian dan Sertifikasi TI. Jenis-jenis sertifikasi meliputi *IT Baseline Protection Certificate*, *Self-declared* (*IT Baseline Protection higher level*) dan Self-declared (*IT Baseline Protection entry level*).

Lebih lanjut, telah disusun *Baseline protection manual* (BPM) dan *sub-manual BSI Standard Series:100-X*. Hal ini termasuk: *BSI Standard 100-1 ISMS, BSI Standard 100-2 Metodologi BPM* dan *BSI Standard 100-3 Analisis risiko*.[41]

Lainnya

Tabel 9 berisi daftar sertifikasi ISMS lainnya.

Tabel 9. Sertifikasi ISMS Negara Lain

	Lembaga sertifikasi	Standar
Kanada	*Communications Security Establishment*	MG-4 Pedoman Sertifikasi dan Akreditasi untuk Sistem Teknologi Informasi
Taiwan	*Bureau of Standards, Meteorology and Inspection*	CNS 17799 & CNS 17800
Singapura	*Information Technology Standards Committee*	SS493 : Bagian 1 (Kerangka Kerja Standar Keamanan TI) & SS493 : Bagian 2 (Layanan Keamanan) sedang disusun

[41] Antonius Sommer, "Trends of Security Strategy in Germany as well as Europe" (presentation made at the 2006 Cyber Security Summit, Seoul, Republic of Korea, 10 April 2006), http://www.secure.trusted-site.de/download/newsletter/vortraege/KISA.pdf.

5. PERLINDUNGAN PRIVASI

Bagian ini bertujuan untuk:
- Menelusuri perubahan konsep privasi;
- Menjelaskan tren internasional dalam perlindungan privasi; dan
- Memberikan gambaran dan contoh Kajian Dampak Privasi (*Privacy Impact Assessment*).

5.1 Konsep Privasi

Informasi pribadi adalah informasi yang berkaitan dengan individu yang dapat diidentifikasi[42] atau orang yang teridentifikasi[43]. Termasuk di dalamnya informasi seperti nama, nomor telepon, alamat, *e-mail*, nomor lisensi mobil, karakteristik fisik (dimensi wajah, sidik jari, tulisan tangan, dan lain-lain), nomor kartu kredit, dan hubungan keluarga.

Akses, pengumpulan, analisis, dan penggunaan informasi pribadi yang tidak pantas berdampak pada perilaku pihak lain terhadap pribadi yang bersangkutan dan pada akhirnya berdampak negatif terhadap kehidupan sosial, harta benda, dan keselamatan-nya. Oleh karena itu, informasi pribadi harus dilindungi dari akses, pengumpulan, penyimpanan, analisis dan penggunaan yang salah. Dalam hal ini, informasi pribadi adalah subyek perlindungan.

Ketika subyek perlindungan adalah hak terhadap informasi pribadi daripada informasi pribadi itu sendiri, inilah yang disebut konsep **privasi**. Ada lima cara untuk menjelaskan **hak untuk privasi**:

- Hak untuk bebas dari akses yang tidak diinginkan (misalnya akses fisik, akses melalui SMS)
- Hak untuk tidak membolehkan informasi pribadi digunakan dengan cara yang tidak diinginkan (misalnya penjualan informasi, pembocoran informasi, pencocokan)
- Hak untuk tidak membolehkan informasi pribadi dikumpulkan oleh pihak lain tanpa sepengetahuan atau seizin seseorang (misalnya melalui penggunaan CCTV dan *cookies*)

[42] Cabinet Office, *Privacy and Data-sharing: The way forward for public services* (April 2002), http://www.epractice.eu/resource/626.
[43] EurLex, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=Directive&an_doc=1995&nu_doc=46.

- Hak untuk memiliki informasi pribadi yang dinyatakan secara akurat dan benar (integritas)
- Hak untuk mendapatkan imbalan atas nilai informasi itu sendiri.

Konsep pasif privasi mencakup hak untuk dibiarkan sendiri (tidak diusik) dan hak alami terkait dengan martabat manusia. Hal ini terkait dengan undang-undang yang melarang masuk tanpa izin.

Konsep aktif privasi mencakup kontrol mandiri terhadap informasi pribadi atau hak untuk mengelola/mengendalikan informasi pribadi secara positif, termasuk hak untuk melakukan koreksi terhadap efek yang dihasilkan dari informasi pribadi yang tidak benar.

5.2 Tren dalam Kebijakan Privasi

Pedoman OECD dalam hal perlindungan privasi

Pada tahun 1980, OECD mengadopsi "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*," yang juga dikenal sebagai "*OECD Fair Information Practices*." Pada tahun 2002 "*Privacy Online: OECD Guidance on Policy and Practice*" diumumkan. [44] Pedoman tersebut diterapkan pada data pribadi (baik di sektor publik atau swasta) yang menimbulkan bahaya terhadap privasi dan kebebasan individu sebagai akibat dari cara informasi tersebut diproses, atau akibat dari sifat atau konteks dimana informasi tersebut digunakan. Prinsip-prinsip OECD yang dinyatakan dalam Pedoman tersebut menyatakan hak dan kewajiban individu dalam konteks otomasi proses data pribadi, serta hak dan kewajiban mereka yang terlibat dalam proses tersebut. Selain itu, prinsip-prinsip dasar yang digariskan dalam Pedoman tersebut juga dapat digunakan baik di tingkat nasional maupun internasional.

Delapan prinsip dalam pedoman OECD terkait perlindungan privasi adalah:[45]

1) Prinsip pembatasan pengumpulan

Perlu ada pembatasan dalam hal pengumpulan data pribadi. Data harus diperoleh dengan cara yang adil dan sah menurut hukum serta, jika diperlukan, sepengetahuan atau seizin subyek data.

---

[44] OECD, "Privacy Online: OECD Guidance on Policy and Practice," http://www.oecd.org/document/49/0,3343,en_2649_34255_19216241_1_1_1_1,00.html.
[45] Untuk membaca keseluruhan dokumen yang berisi prinsip-prinsip di atas, lihat "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

2) **Prinsip Kualitas data**

Data pribadi harus relevan dengan tujuan penggunaannya. Sesuai dengan penggunaan tersebut, data harus akurat, lengkap dan *up-to-date*.

3) **Prinsip pernyataan tujuan**

Tujuan pengumpulan data pribadi harus dinyatakan selambat-lambatnya pada saat pengumpulan data, dan penggunaan data sesudah itu hanya akan terbatas pada pemenuhan tujuan atau penggunaan lain yang tetap sesuai dengan tujuan, serta sebagaimana dinyatakan setiap terjadi perubahan tujuan.

4) **Prinsip penggunaan terbatas**

Data pribadi tidak boleh diungkapkan, dibuat menjadi tersedia atau digunakan untuk tujuan selain dari yang ditentukan sesuai dengan prinsip pernyataan tujuan kecuali dengan persetujuan dari subyek data atau otoritas hukum.

5) **Prinsip penjagaan keamanan**

Data pribadi harus dilindungi dengan penjagaan keamanan yang wajar terhadap risiko seperti kehilangan atau akses tanpa izin, perusakan, penggunaan, modifikasi atau penyingkapan data.

6) **Prinsip keterbukaan**

Harus ada kebijakan umum tentang keterbukaan pengembangan, praktik dan kebijakan terkait dengan data pribadi. Alat harus siap sedia untuk menentukan keberadaan dan sifat data pribadi, tujuan utama penggunaannya, serta identitas dan alamat dari pengendali data.

7) **Prinsip partisipasi individu**

Individu seharusnya memiliki hak untuk:
(a) Mendapatkan konfirmasi dari pengendali data apakah mereka memiliki data yang berkaitan dengan dia;
(b) Menerima komunikasi tentang data yang berhubungan dengan dia dalam waktu yang wajar, dengan biaya, jika ada, yang tidak berlebihan, dalam cara yang wajar, dan dalam bentuk yang mudah dimengerti oleh dia;
(c) Diberikan alasan jika permintaan yang dibuat berdasarkan sub-paragraf (a) dan (b) ditolak, dan untuk dapat mengajukan keberatan atas penolakan, dan
(d) Untuk mengajukan keberatan terhadap data yang berkaitan dengannya dan, jika keberatan tersebut berhasil, untuk meminta data dihapus, dikoreksi, dilengkapi atau diubah.

8) Prinsip akuntabilitas

Pengendali data harus bertanggung jawab untuk mematuhi langkah-langkah yang memberikan efek pada prinsip-prinsip yang dinyatakan di atas.

Pedoman PBB yang berkaitan dengan perlindungan privasi

Sejak akhir tahun 1960-an, dunia telah memberi perhatian akan efek terhadap privasi atas pemrosesan informasi secara otomatis. UNESCO khususnya telah menunjukkan perhatian akan privasi dan perlindungan privasi sejak "*UN Guidelines for the Regulation of Computerized Personal Data File*" diadopsi oleh Majelis Umum pada tahun 1990.

Pedoman PBB diterapkan ke dokumen (kertas) serta *file* data komputerisasi di sektor publik atau swasta. Panduan tersebut menyatakan serangkaian prinsip terkait jaminan minimum yang harus disediakan untuk perundang-undangan nasional atau hukum internal organisasi internasional, sebagai berikut:[46]

1) Prinsip sah dan keadilan

Informasi tentang seseorang harus tidak diperoleh atau diproses dalam cara yang tidak adil atau tidak sah, juga tidak digunakan untuk tujuan dan prinsip yang menyimpang dari *Charter of the United Nations*.

2) Prinsip akurasi

Pihak yang bertanggung jawab untuk kompilasi berkas atau bertanggung jawab untuk menyimpannya memiliki kewajiban untuk melakukan pemeriksaan rutin atas akurasi dan relevansi data yang direkam dan untuk memastikan bahwa data disimpan selengkap mungkin untuk mencegah kesalahan akibat kelalaian, dan bahwa data tersebut tetap diperbaharui secara rutin atau ketika informasi yang terkandung digunakan, sepanjang data itu diproses.

3) Prinsip pernyataan tujuan

Tujuan yang harus dipenuhi oleh *file* dan pemanfaatannya terkait dengan tujuan harus disampaikan, sah dan, ketika ditetapkan, diberitahukan atau dibawa ke perhatian orang yang terlibat, dan untuk itu perlu dipastikan bahwa:

(a) Semua data pribadi yang dikumpulkan dan direkam tetap relevan dan mencukupi tujuan yang ditetapkan;
(b) Tidak ada data pribadi yang digunakan atau diungkap untuk dimanfaatkan yang tidak sesuai dengan tujuannya, kecuali atas izin orang yang dimaksud;

[46] Prinsip-prinsip diambil dari *Office of the High Commissioner for Human Rights*, "Guidelines for the Regulation of Computerized Personal Data Files," http://www.unhchr.ch/html/menu3/b/71.htm.

(c) Periode dimana data pribadi disimpan tidak melebihi periode yang diperlukan untuk mencapai tujuan yang dinyatakan.

4) Prinsip akses orang yang berkepentingan

Setiap orang dengan bukti identitas memiliki hak untuk mengetahui apakah informasi yang menyangkut dia diproses dan untuk mendapatkannya dalam bentuk yang dapat dimengerti, tanpa penundaan atau biaya, dan untuk mendapatkan perbaikan yang tepat atau dihapuskan dalam kasus entri yang tidak sah, tidak perlu, atau tidak tepat dan, ketika dikomunikasikan, untuk diinformasikan alamatnya.

5) Prinsip non-diskriminasi

Bergantung pada pengecualian kasus terbatas yang dipertimbangkan di bawah prinsip 6, data yang dapat menimbulkan diskriminasi yang sewenang-wenang atau tidak sah, seperti informasi ras atau etnis, warna kulit, kehidupan seks, opini politik, agama, filosofi dan kepercayaan lain serta keanggotaan dalam asosiasi atau serikat tertentu, harus tidak diolah.

6) Kekuatan untuk membuat pengecualian

Pengecualian dari prinsip 1 hingga 4 dapat diizinkan hanya jika mereka diperlukan untuk melindungi keamanan nasional, tata tertib publik, kesehatan atau moralitas publik, termasuk juga, hak dan kebebasan pihak lain, terutama orang yang sedang dianiaya (klausa perikemanusiaan), selama bahwa pengecualian yang dilakukan jelas dinyatakan dalam hukum atau peraturan yang setara yang diumumkan sesuai dengan sistem hukum internal yang dinyatakan dengan jelas batasannya dan mengatur usaha penjagaan yang tepat.

Pengecualian pada prinsip 5 berkaitan pada pelarangan diskriminasi, dan untuk menjadi subjek penjagaan yang sama seperti dijelaskan pada pengecualian terhadap prinsip 1 hingga 4, dapat diizinkan dalam batas yang ditentukan oleh *International Bill of Human Rights* dan instrumen lainnya yang relevan dalam bidang perlindungan hak asasi manusia dan pencegahan diskriminasi.

7) Prinsip keamanan

Langkah yang tepat perlu diambil untuk melindungi berkas-berkas terhadap baik bahaya alami, seperti kehilangan atau kerusakan, dan bahaya manusia, seperti akses tanpa izin, penyalahgunaan data atau kontaminasi oleh virus komputer.

8) Pengawasan dan sanksi

Hukum di tiap negara harus menunjuk otoritas yang, sesuai dengan sistem hukum domestiknya, bertanggung jawab untuk mengawasi ketaatan terhadap

prinsip yang dinyatakan di atas. Otoritas ini harus menawarkan jaminan keadilan, independen terhadap seseorang atau lembaga yang bertanggung jawab dalam pemrosesan dan pembentukan data, serta kompetensi teknis. Dalam hal terjadi pelanggaran terhadap ketetapan hukum nasional yang merupakan implementasi dari prinsip yang disebutkan sebelumnya, sanksi kriminal atau sanksi lainnya harus dipertimbangkan bersamaan dengan perbaikan seseorang yang tepat.

9) Aliran data antar-batas

Ketika hukum di dua atau lebih negara mengenai aliran data antarbatas menawarkan penjagaan yang setara untuk perlindungan privasi, informasi harus bisa diedarkan sebebas mungkin di masing-masing teritori. Jika tidak ada penjagaan yang bersifat timbal balik, pembatasan sirkulasi tidak boleh terlalu dipaksakan dan hanya sejauh yang dibutuhkan untuk perlindungan privasi.

10) Bidang penerapan

Prinsip-prinsip yang ada harus dapat diterapkan ke semua berkas komputerisasi publik maupun swasta dan, dapat diperluas serta bergantung pada pengaturan yang tepat, ke berkas manual. Ketetapan khusus, juga opsional, dapat dibuat untuk memperluas seluruh atau sebagian prinsip untuk berkas yang sah dari seseorang khususnya ketika memuat beberapa informasi individu.

EU Data Protection Directive

EU's Council of Ministers mengadopsi *European Directive on the Protection of Individuals with Regard to Processing of Personal Data dan Free Movement of Such Data (EU Directive)* pada tanggal 24 Oktober 1995 yang menyediakan kerangka kerja pengaturan untuk menjamin keamanan dan pergerakan bebas data pribadi lintas batas nasional negara-negara anggota Uni Eropa (UE), dan juga untuk menetapkan dasar keamanan seputar informasi pribadi dimanapun data itu disimpan, dikirim atau diproses.

EU Data Protection Directive disusun sebagai usaha untuk menyatukan dan menyelaraskan dengan hukum masing-masing negara terkait perlindungan privasi. Artikel 1 dari *EU Directive* menyatakan bahwa “Negara Anggota harus melindungi hak-hak dasar dan kebebasan alami seseorang, dan khususnya hak mereka atas privasi, terkait dengan pemrosesan data pribadi.”

EU Directive melarang pengiriman informasi pribadi ke negara yang tidak memiliki tingkat perlindungan yang cukup, akibatnya terjadi antagonisme antara UE dengan pemerintah AS.[47]

[47] Domingo R. Tan, Comment, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union, 21 LOY. L.A. INT’L & COMP. L.J. 661, 666 (1999).

Setiap negara anggota UE telah merevisi hukum yang ada atau menetapkan hukum perlindungan privasi baru untuk melaksanakan *EU Directive*.

Contoh lain hukum UE mengenai perlindungan privasi adalah Artikel 8 *European Convention on Human Rights*, *Directive* 95/46/EC (*Data Protection Directive*), *Directive* 2002/58/EC (*the E-Privacy Directive*) dan *Directive* 2006/24/EC Article 5 (*The Data Retention Directive*).[48]

Perlindungan privasi di Republik Korea

Republik Korea memiliki pelanggan jaringan *broadband* terbanyak di dunia. Pada pertengahan tahun 2005, 25 persen populasi dan 75 persen rumah tangga telah berlangganan jaringan *broadband*.[49] Jaringan komunikasi nirkabel dan jaringan *broadband* Republik Korea saat ini diakui sebagai salah satu yang terbaik di dunia. Karenanya, frekuensi kebocoran informasi pribadi di dalam negeri telah meningkat secara signifikan, sehingga membutuhkan kebijakan dan solusi teknologi.

Sayangnya, pemerintah Korea tidak bergerak cukup cepat terhadap hal ini. UU Perlindungan Privasi masih ditunda dalam *National Assembly* dan tidak ada hukum independen untuk proteksi informasi pribadi.

Namun demikian, pemerintah Korea telah menetapkan "*Mid- and Long-term Information Security Roadmap for Realizing u-SafeKorea*" dan empat proyek prioritas utama sejak 2005 adalah: (1) menjamin keamanan infrastruktur utama; (2) menciptakan kepercayaan terhadap layanan baru TI; (3) menguatkan fungsi perlindungan informasi untuk mesin pertumbuhan yang baru; dan (4) membangun basis keamanan informasi di lingkungan baru *cyber*. Prioritas keempat juga mencakup sub proyek yang disebut 'Penguatan Sistem Perlindungan Privasi'.

Lebih lanjut, terdapat beberapa hukum yang terkait dengan perlindungan privasi seperti "*Personal Information Protection Law in Public*" dan "*Law on Telecom Networks and Information Protection*".

Personal Information Protection Law in Public: Hukum ini terdiri dari ketentuan penanganan dan pengelolaan informasi pribadi yang diproses di komputer institusi publik untuk perlindungan privasi, termasuk ketentuan yang terkait dengan kinerja bisnis publik yang wajar, dan perlindungan hak dan kepentingan masyarakat.

---

[48] Justice and Home Affairs, "Data Protection," European Commission, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.
[49] Internet World Stats, "Korea," Miniwatts Marketing Group, http://www.internetworldstats.com/asia/kr.htm.

Undang-undang Peningkatan Pemanfaatan Jaringan Informasi dan Komunikasi dan Perlindungan Informasi: Tujuan UU ini adalah untuk meningkatkan sistem perlindungan privasi di sektor swasta, yang sesuai dengan perluasan jaringan komunikasi informasi dan generalisasi pengumpulan dan penyebaran informasi pribadi. UU ini mengikuti proses perlindungan privasi berdasarkan pada daur hidup informasi pribadi, seperti pengumpulan, penggunaan, pengelolaan dan penghapusan. UU ini juga mencakup ketentuan yang terkait dengan hak pengguna akan informasi pribadi dan pembentukan dan operasi komite mediasi privasi.

Undang-undang Perlindungan Rahasia Komunikasi: UU ini membatasi lingkup target privasi dan kebebasan komunikasi untuk melindungi privasi komunikasi dan untuk menjamin kebebasan berkomunikasi. Hukum ini melarang penyadapan percakapan rahasia seperti melalui perekaman atau mencuri dengar, dan hukum ini melindungi privasi dalam komunikasi.

Undang-undang Perlindungan Informasi Lokasi: UU ini mengatur pengumpulan dan penggunaan informasi berbasis lokasi; untuk melindungi kebocoran, penyalahgunaan informasi; dan untuk meningkatkan penggunaan informasi dalam lingkungan yang aman. Hukum ini menyoroti kemampuan teknologi komunikasi saat ini untuk menentukan lokasi seseorang (sebagai contoh melalui ponsel), dan fakta bahwa kebocoran informasi lokasi dapat menyebabkan pelanggaran privasi yang serius. Jadi, hukum ini membuat peraturan untuk tidak pernah menyingkap informasi lokasi kecuali dalam kasus dimana hukum memerlukannya.

Perlindungan privasi di Amerika Serikat (AS)

AS telah mempercayakan kegiatan perlindungan privasi ke pasar mengingat terlalu banyak pembatasan oleh pemerintah telah menghambat aktivitas *e-commerce*. Sebagai hasilnya, muncul segel privasi seperti Trust-e atau *Better Business Bureau Online*, dan hukum perlindungan privasi tidak terintegrasi. *Privacy Act* tahun 1974 memberikan perlindungan privasi informasi di sektor publik sementara hukum yang berbeda mengatur privasi di sektor swasta. Tidak ada organisasi yang menangani masalah perlindungan privasi di sektor swasta. Di sektor publik, *Office of Management and Budget* (OMB) berperanan dalam menetapkan kebijakan privasi pemerintah federal mengikuti *Privacy Act*. Di sektor swasta, *Federal Trade Commission* diberi wewenang mengeksekusi hukum yang melindungi privasi *online* anak-anak, informasi kredit konsumen, dan praktik perdagangan yang wajar.

Hukum AS yang terkait dengan perlindungan privasi adalah sebagai berikut:

- *The Privacy Act*, 1974
- *Consumer Credit Protection Act*, 1984
- *Electric Communications Privacy Act*, 1986

- *Gramm-Leach-Bliley Act*, 1999
- *Health Insurance Portability and Accountability Act*, 1996
- *Sarbanes-Oxley Act*, 2002
- *Children's Online Privacy Protection Act*, 1998.

Langkah perlindungan privasi di Jepang

Pada tahun 1982, Jepang menetapkan langkah perlindungan privasi berdasarkan delapan prinsip dasar OECD. Di tahun 1988, hukum perlindungan privasi di sektor publik diumumkan dan memperlihatkan efek. Di sektor swasta, *Guideline for the Protection of Privacy* dikeluarkan oleh Departemen Industri dan Perdagangan Internasional di tahun 1997. Untuk meningkatkan kesesuaian hukum perlindungan privasi nasional dengan pedoman internasional, *Advanced Information and Telecommunications Society Promotion Headquarters* telah mendorong legislasi hukum perlindungan informasi pribadi.

Sebagai tambahan, *Data Protection Authority* telah ditunjuk sebagai lembaga independen yang akan memastikan ketaatan terhadap perlindungan privasi dan membantu individu dalam kasus pelanggaran privasi. *Data Protection Authority* diberi mandat untuk meningkatkan transparansi pemrosesan informasi, menjamin hak dan keuntungan subyek data, dan memastikan bahwa baik lembaga pemroses informasi maupun pengguna informasi melakukan kewajiban mereka. *Authority* tersebut juga diharapkan berperanan dalam melindungi kepentingan nasional terutama dalam kasus yang melibatkan perpindahan informasi yang melewati batas nasional.

Hukum Jepang yang terkait dengan perlindungan privasi adalah sebagai berikut:

- *Act for the Protection of Computer Processed Personal Data Held by Administrative Organs*, 1988
- *Regulations of Local Governments* (dikeluarkan pada tahun 1999 untuk 1.529 pemerintah lokal)
- *Act for the Protection of Personal Information*, 2003
- *Act on the Protection of Personal Information Held by Administrative Organs*, 2003
- *Act for the Protection of Personal Information Retained by Independent Administrative Institutions*, 2003
- *Board of Audit Law*, 2003
- *Guidelines for Privacy Protection with regard to RFID Tags*, 2004.

Pertanyaan

1. Kebijakan dan hukum apa yang diterapkan di negara Anda untuk melindungi privasi informasi?

2. Apa masalah atau akibat yang timbul dari pengesahan dan/atau pelaksanaan kebijakan dan hukum tersebut?

3. Prinsip apa (lihat Pedoman OECD dan Pedoman PBB) yang Anda pikir dapat mendukung kebijakan dan hukum perlindungan privasi di negara Anda?

5.3 *Privacy Impact Assessment* – Kajian Dampak Privasi

Apakah PIA?

PIA adalah proses sistematis dari investigasi, analisis dan evaluasi efek privasi konsumen atau nasional dari penggunaan sistem informasi baru atau modifikasi sistem informasi yang ada. PIA berdasar pada 'prinsip pencegahan awal' – yaitu mencegah lebih baik daripada mengobati. PIA bukan hanya evaluasi terhadap sistem tetapi mempertimbangkan efek serius privasi dari pengenalan atau perubahan sistem baru. Jadi, hal ini berbeda dari audit perlindungan privasi yang memastikan ketaatan kebijakan internal dan kebutuhan external untuk privasi.

Karena PIA dilakukan untuk menganalisis faktor gangguan privasi ketika sistem baru dibangun, PIA perlu dilakukan di fase awal pengembangan, ketika penyesuaian terhadap spesifikasi pengembangan masih memungkinkan. Akan tetapi, ketika risiko gangguan serius muncul dalam pengumpulan, penggunaan dan pengelolaan informasi pribadi selama pengoperasian layanan yang ada, sangat diperlukan untuk melakukan PIA dan kemudian memodifikasi sistem.

Proses PIA[50]

PIA secara umum terdiri dari tiga langkah (Tabel 10).

[50] Bagian ini diambil dari *Information and Privacy Office*, *Privacy Impact Assessment: A User's Guide* (Ontario: Management Board Secretariat, 2001), http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Tabel 10. Proses PIA

Analisis Konseptual	Analisis Aliran Data	Analisis Tindakan
Menyiapkan deskripsi dengan bahasa sederhana akan lingkup dan dasar pemikiran bisnis dari usulan kegiatan. Identifikasi awal dan potensi masalah privasi dan risikonya, serta *stakeholder* utamanya. Menyediakan deskripsi rinci aspek penting dari usulan, termasuk analisis kebijakan terhadap permasalahan utama Dokumentasikan aliran utama informasi pribadi. Lakukan observasi masalah lingkungan untuk meninjau bagaimana yurisdiksi lain menangani kegiatan serupa. Identifikasi masalah dan perhatian *stakeholder*. Nilai reaksi publik.	Analisis aliran data melalui diagram proses bisnis dan identifikasi elemen data individu tertentu atau kelompok data. Kaji kepatuhan usulan dengan *freedom of information* (FOI) dan hukum privasi, dan program yang relevan. Nilai kecocokan usulan dengan prinsip-prinsip umum privasi. Analisis risiko berbasis analisis privasi dari usulan dan identifikasi solusi yang mungkin. Tinjau opsi desain dan identifikasi masalah /perhatian privasi yang belum terselesaikan dan belum ditangani. Menyiapkan penanganan terhadap permasalahan privasi yang belum terpecahkan.	Tinjau dan lakukan analisis perangkat keras fisik dan desain sistem dari usulan kegiatan untuk memastikan pemenuhan kebutuhan desain privasi. Memberikan tinjauan final terhadap usulan kegiatan. Melakukan analisis privasi dan risiko terhadap setiap perubahan baru dari usulan kegiatan terkait dengan desain perangkat keras dan piranti lunak untuk memastikan kepatuhan dengan FOI dan hukum privasi, program yang relevan, dan prinsip-prinsip umum privasi. Menyiapkan rencana komunikasi.

Sumber: Information and Privacy Office, *Privacy Impact Assessment: A User's Guide* (Ontario: Management Board Secretariat, 2001), 5, http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Lingkup penilaian PIA

PIA dilakukan ketika:

1. Membangun sistem informasi baru yang akan memegang dan mengelola informasi pribadi dalam jumlah besar;
2. Menggunakan teknologi baru dimana privasi dapat terganggu;
3. Memodifikasi sistem informasi yang ada yang memegang dan mengelola informasi pribadi; dan
4. Mengumpulkan, menggunakan, menyimpan dan/atau menghancurkan informasi pribadi dimana risiko gangguan privasi dapat timbul.

Tetapi tidak diperlukan untuk melakukan PIA terhadap semua sistem informasi. PIA tidak harus dilakukan ketika hanya dilakukan perubahan kecil terhadap program dan sistem yang ada.

Contoh-contoh PIA

Tabel 11 berisi sistem PIA di tiga negara.

Tabel 11. Contoh PIA Nasional

	Amerika Serikat	Kanada	Australia/Selandia Baru
Dasar Hukum	*Section 208* dari *e-Government Act* tahun 2002 OMB memberikan persyaratan PIA dalam OMB-M-03-22	Mengenalkan kebijakan dan pedoman PIA pada bulan Mei 2002 Mewajibkan eksekusi PIA pada basis hukum umum pada privasi	Dengan sukarela melaksanakan PIA (tanpa dasar hukum) *PIA Handbook* untuk mendukung PIA (2004, Selandia Baru), pedoman PIA (2004, Australia)
Subyek	Semua cabang eksekutif departemen dan lembaga serta kontraktor yang menggunakan TI atau yang mengoperasikan situs *web* untuk tujuan interaksi dengan publik; kegiatan lintas-lembaga yang relevan, termasuk *e-government*	Semua program dan layanan yang disediakan lembaga pemerintah	Tanpa kewajiban atau batasan
Aktor	Lembaga yang melakukan proyek *e-government* yang menangani informasi pribadi	Lembaga pemerintah yang mengembangkan atau mengoperasikan program dan layanan	Lembaga terkait atau dengan permintaan lembaga konsultan eksternal
Publikasi	Membuat PIA tersedia secara publik melalui situs *web* lembaga, publikasi di *Federal Register*, atau cara lainnya, yang mungkin dimodifikasi atau dilepaskan untuk alasan keamanan, atau untuk melindungi informasi yang rahasia, sensitif atau privat yang ada dalam penilaian Lembaga akan memberikan salinan PIA untuk tiap sistem dimana pembiayaan diminta, kepada *Director of OMB*	Membuat rangkuman PIA tersedia secara publik Menyediakan salinan akhir PIA dan sebelumnya melapor ke *Office of the Privacy Commissioner* untuk mendapatkan saran atau petunjuk yang tepat terkait strategi perlindungan	Hasil PIA biasanya tidak tidak dibuat tersedia untuk publik (tidak ada kewajiban untuk melaporkan dan mempublikasikan)

Ujian

1. Bagaimana informasi pribadi berbeda dengan jenis informasi lainnya?

2. Mengapa informasi pribadi harus dilindungi?

3. Apakah signifikansi prinsip-prinsip OECD dan PBB pada perlindungan privasi?

4. Mengapa penilaian dampak privasi perlu dilakukan?

6. PEMBENTUKAN DAN OPERASI CSIRT

Bagian ini bertujuan untuk:
- Menjelaskan bagaimana membentuk dan mengoperasikan *Computer Security Incident Response Team* (CSIRT) nasional; dan
- Memberikan model CSIRT dari berbagai negara.

Cybercrime dan berbagai ancaman terhadap keamanan informasi perlu diperhatikan secara serius karena efek ekonominya sangat besar. Sebagai contoh, *Japan Network Security Association* mengestimasi kerugian ekonomi dari keluarnya informasi swasta sebesar 446 juta USD – atau 347 USD per orang – pada tahun 2006. *Ferris Research* mengestimasi kerusakan dari *spam* di AS sekitar 8,9 miliar USD di tahun 2002, 20 miliar USD di tahun 2004 dan 50 miliar USD di tahun 2005.

Pembentukan CSIRT merupakan cara efektif untuk mengurangi dan meminimalisasi kerusakan dari serangan terhadap sistem informasi dan penerobosan keamanan informasi.

6.1 Pengembangan dan Operasi CSIRT

CSIRT merupakan sebuah organisasi, seperti organisasi formal atau adhoc lainnya, yang bertanggung jawab atas penerimaan, pemantauan dan penanganan laporan dan aktivitas insiden keamanan komputer. Tujuan dasar CSIRT adalah untuk memberikan layanan penanganan insiden keamanan komputer untuk meminimalisasi kerusakan dan memungkinkan pemulihan yang efisien dari insiden keamanan komputer.[51]

Pada tahun 1988, penyebaran *worm* pertama bernama Morris terjadi dan menyebar dengan sangat cepat ke seluruh dunia. Sesudah itu, *Defence Advanced Research Projects Agency* membentuk *Software Engineering Institute* dan kemudian membentuk CERT/CC di *Carnegie Mellon University* di bawah kontrak pemerintah AS. Sejak itu, setiap negara di Eropa membentuk organisasi sejenis. Karena tidak ada satupun CSIRT yang mampu mengatasi insiden kerentanan yang luas, *Forum of Incident Response and Security Teams* (FIRST) dibentuk pada tahun 1990. Melalui FIRST, banyak lembaga keamanan informasi dan CSIRT dapat bertukar pendapat dan berbagi informasi.

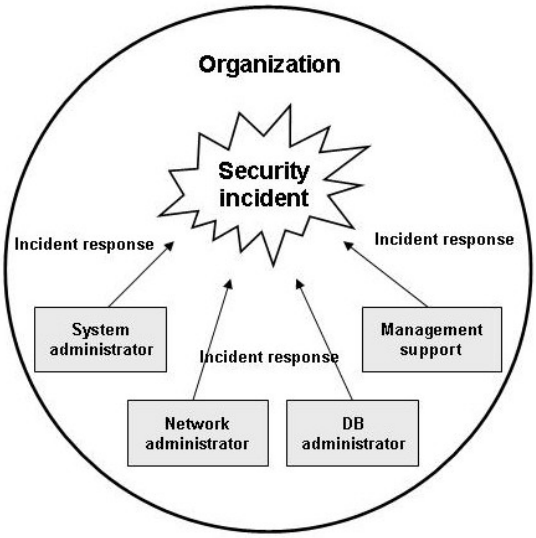
[51] CERT, "CSIRT FAQ," Carnegie Mellon University, http://www.cert.org/csirts/csirt_faq.html.

Memilih Model CSIRT yang tepat[52]

Terdapat lima model organisasi CSIRT yang umum. Model yang paling tepat untuk sebuah organisasi – yaitu yang mempertimbangkan berbagai kondisi seperti lingkungan, status keuangan dan sumber daya manusia – perlu diadopsi.

1) Model Tim Keamanan (menggunakan staf TI yang ada)

Model tim keamanan bukan model CSIRT yang umum. Faktanya, justru berlawanan dengan CSIRT yang umum. Dalam model ini, tidak ada organisasi sentral yang bertanggung jawab untuk menangani insiden keamanan komputer. Sebagai pengganti, tugas penanganan insiden dilakukan oleh administrator sistem dan jaringan, atau oleh spesialis sistem keamanan lainnya.



Gambar 14. Model Tim Keamanan

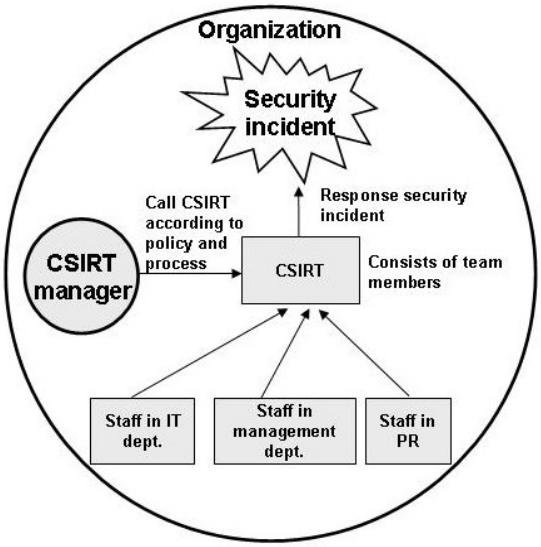
2) Model CSIRT Terdistribusi Internal

Model ini juga dikenal sebagai 'CSIRT terdistribusi'. Tim dalam model ini terdiri dari administrator CSIRT yang bertanggung jawab untuk pelaporan dan manajemen keseluruhan, dan staf dari divisi-divisi lain dari lembaga/perusahaan. CSIRT model ini merupakan organisasi yang diakui secara resmi dengan tanggung jawab untuk melakukan semua aktivitas penanganan insiden. Karena tim dibentuk dalam sebuah perusahaan atau lembaga, tim ini dianggap 'internal'.

[52] Bagian ini diambil dari Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle dan Mark Zajicek, *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

Model CSIRT terdistribusi internal berbeda dengan model Tim Keamanan dalam hal berikut:

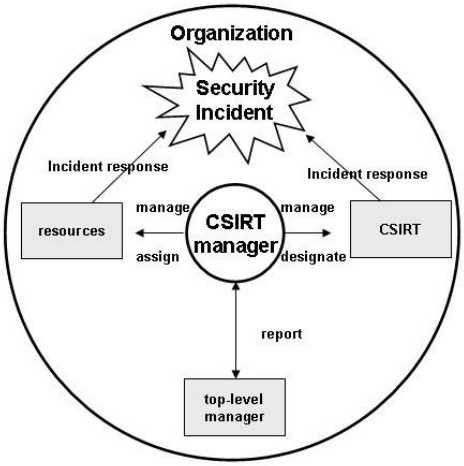
- Keberadaan kebijakan, prosedur, dan proses yang lebih formal untuk menangani insiden;
- Ditetapkannya metode komunikasi dengan keseluruhan perusahaan terkait ancaman keamanan dan strategi penanganan; dan
- Manajer dan anggota tim CSIRT yang ditunjuk dan ditugaskan secara khusus untuk penanganan insiden.



Gambar 15. Model CSIRT Terdistribusi Internal

3) Model CSIRT Terpusat Internal

Dalam model CSIRT Terpusat Internal, tim yang lokasinya terpusat mengendalikan dan mendukung organisasi. CSIRT memiliki tanggung jawab menyeluruh terhadap pelaporan, analisis dan penanganan insiden. Jadi, anggota tim tidak dapat menangani pekerjaan lain dan menghabiskan seluruh waktu mereka untuk bekerja dalam tim dan menangani seluruh insiden. Selain itu, manajer CSIRT melapor pada manajemen tingkat tinggi seperti *Chief Information Officer*, *Chief Security Officer* atau *Chief Risk Officer*.

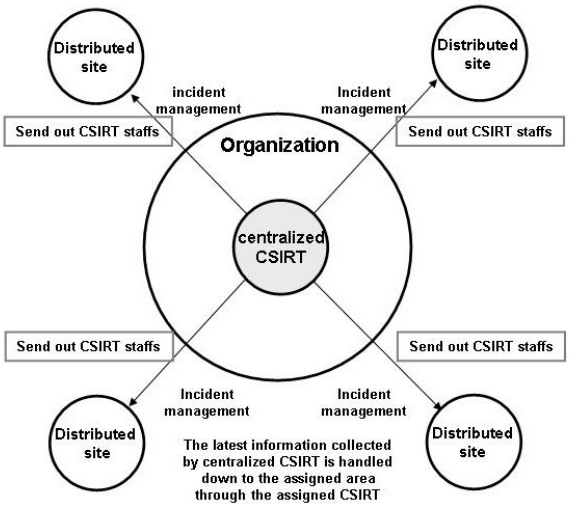


Gambar 16. Model CSIRT Terpusat Internal

4) Model CSIRT Gabungan Terdistribusi dan Terpusat

Juga dikenal sebagai 'CSIRT gabungan'. Dimana CSIRT terpusat tidak dapat mengendalikan dan mendukung keseluruhan organisasi, beberapa anggota tim didistribusikan ke lokasi/cabang/divisi organisasi untuk menyediakan tingkat pelayanan yang sama dalam area tanggung jawab mereka seperti yang disediakan pada CSIRT terpusat.

Tim terpusat menyediakan analisis data, metode pemulihan dan strategi mitigasi. Tim ini juga melengkapi anggota tim terdistribusi dengan dukungan penanganan insiden, kerentanan dan artefak. Anggota tim terdistribusi di setiap lokasi melaksanakan strategi tersebut dan memberikan keahlian dalam bidangnya.



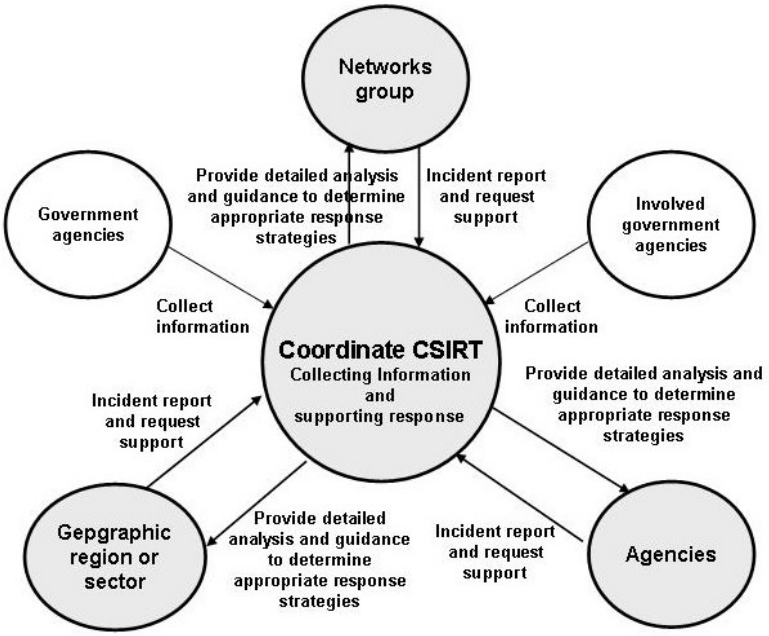
Gambar 17. CSIRT Gabungan

5) Model CSIRT Terkoordinasi

CSIRT terkoordinasi menguatkan fungsi dari tim terdistribusi dalam CSIRT kombinasi. Dalam model CSIRT terkoordinasi, anggota tim dalam CSIRT kombinasi dikelompokkan kedalam CSIRT independen berdasarkan pada beberapa karakteristik seperti konektivitas jaringan, batas geografis, dan lain-lain. Mereka dikendalikan oleh CSIRT terpusat.

Model CSIRT terkoordinasi tepat untuk sistem CSIRT nasional. Model ini dapat diterapkan untuk aktivitas internal dalam organisasi dan untuk mendukung dan berkoordinasi erat dengan lembaga eksternal.

Aktivitas koordinasi dan fasilitasi meliputi berbagi informasi, penyediaan strategi mitigasi, penanganan insiden, metode pemulihan, penelitian/analisis tren dan pola aktivitas insiden, basisdata kerentanan, *clearinghouse* perangkat keamanan, serta layanan pemberian nasihat dan siap siaga.



Gambar 18. CSIRT Terkoordinasi

Pembentukan CSIRT: Langkah-langkah membentuk CSIRT nasional[53]

Terdapat lima tahapan dalam membentuk CSIRT. Tujuan, visi atau peranan CSIRT harus menjadi pedoman kemajuan melalui tingkatan-tingkatan yang ada.

[53] Bagian ini diambil dari Georgia Killcrece, *Steps for Creating National CSIRTs* (Pittsburgh: Carnegie Mellon University, 2004), http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

Tahap 1 – Mendidik *stakeholder* tentang pengembangan tim nasional

Tahap 1 adalah tingkat kesadaran, dimana *stakeholder* mengembangkan pemahaman atas apa yang perlu dilakukan dalam membentuk CSIRT. Melalui berbagai metode pembelajaran, mereka belajar mengenai:

- Pendorong dan motivator dibalik perlunya CSIRT nasional;
- Kebutuhan untuk mengembangkan kemampuan penanganan insiden oleh CSIRT nasional;
- Mengidentifikasi orang-orang yang akan terlibat dalam diskusi pembentukan tim nasional;
- Sumber daya dan infrastruktur penting yang ada di dalam negara;
- Jenis-jenis saluran komunikasi yang perlu ditentukan untuk berkomunikasi dengan para konstituen CSIRT;
- Hukum, peraturan dan kebijakan tertentu lainnya yang akan memengaruhi pengembangan CSIRT nasional;
- Strategi pembiayaan untuk mengembangkan, merencanakan, melaksanakan dan mengoperasikan kemampuan penanganan;
- Teknologi dan infrastruktur informasi jaringan yang akan diperlukan untuk mendukung operasi tim nasional;
- Rencana dan interdependensi penanganan dasar yang akan digunakan di berbagai sektor;
- Sekumpulan layanan utama yang berpotensi untuk diberikan oleh CSIRT ke konstituen-nya; dan
- Praktik dan pedoman terbaik.

Tahap 2 – Perencanaan CSIRT: Pembangunan pengetahuan dan informasi yang didapat selama Tahap 1

Tahap 2 berisi perencanaan CSIRT berdasarkan pada pengetahuan dan informasi yang didapat selama Tahap 1. Permasalahan yang dibahas di Tahap 1 ditinjau dan dibahas lebih lanjut, untuk kemudian dibuat rinciannya dan diterapkan ke rencana implementasi. Rencana tersebut ditetapkan dengan mempertimbangkan aktivitas berikut:

a) Identifikasi persyaratan dan kebutuhan CSIRT nasional —
   - Hukum dan peraturan yang akan memengaruhi operasi tim nasional
   - Sumber daya penting yang perlu diidentifikasi dan dilindungi
   - Insiden dan tren saat ini yang dilaporkan atau seharusnya dilaporkan
   - Kemampuan penanganan insiden dan keahlian keamanan komputer
b) Mendefinisikan visi CSIRT nasional
c) Mendefinisikan misi tim nasional
d) Menentukan konstituen yang akan dilayani oleh CSIRT
e) Mengidentifikasi cara berkomunikasi antara konstituen dan tim nasional
f) Mengidentifikasi jenis-jenis persetujuan, kepemimpinan dan dukungan (pemerintah) nasional

g) Mengidentifikasi jenis-jenis keahlian dan pengetahuan staf yang diperlukan untuk mengoperasikan tim
h) Mendefinisikan jenis-jenis peran dan tanggung jawab CSIRT nasional
i) Menyusun proses manajemen insiden CSIRT serta menentukan hubungannya dengan proses sejenis di organisasi konstituen eksternal
j) Mengembangkan sekumpulan kriteria standar dan terminologi yang konsisten untuk pengelompokan dan pendefinisian aktivitas dan kejadian insiden
k) Mendefinisikan bagaimana CSIRT nasional akan berinteraksi dengan konstituen, CSIRT di negara lain, dan juga rekan eksternal.
l) Menentukan proses yang dibutuhkan untuk integrasi dengan rencana pemulihan bencana, rencana penanganan insiden, rencana keberlangsungan bisnis, manajemen krisis, dan rencana manajemen darurat lainnya.
m) Menyusun jadwal proyek
n) Menyusun rencana CSIRT nasional berdasarkan hasil dari kegiatan perencanaan, visi dan kerangka kerja terkait.

Tahap 3 – Implementasi CSIRT

Di Tahap 3, tim proyek menggunakan informasi dan rencana dari Tahap 1 dan 2 untuk mengimplementasikan CSIRT. Proses implementasinya sebagai berikut:

a) Mendapatkan dana dari sumber yang diidentifikasi selama tahap perencanaan
b) Mengumumkan secara luas bahwa CSIRT nasional sedang dibentuk dan memberitahukan dimana informasi tambahan dapat diperoleh (tentang kemajuan pengembangan, pelaporan kebutuhan, dll.)
c) Penyusunan mekanisme koordinasi dan komunikasi dengan *stakeholder* dan kontak lainnya
d) Implementasi sistem informasi dan infrastruktur jaringan yang aman untuk mengoperasikan CSIRT nasional (misalnya *server*, aplikasi, perangkat telekomunikasi yang aman dan sumber daya pendukung infrastruktur lain)
e) Mengembangkan operasi dan proses untuk staf CSIRT, termasuk standar yang disepakati di tahap perencanaan dan pelaporan pedoman
f) Pengembangan kebijakan dan prosedur internal untuk mengakses dan mengoperasikan perangkat CSIRT dan perangkat pribadi, selain juga kebijakan penggunaan yang dapat diterima
g) Implementasi proses interaksi CSIRT nasional dengan konstituennya
h) Mengidentifikasi dan merekrut (atau menugaskan ulang) personel, mendapatkan pendidikan dan pelatihan yang tepat untuk staf CSIRT, serta menentukan peluang usaha lainnya untuk mendidik dan melatih konstituen.

Tahap 4 – Pengoperasian CSIRT

Di tahap operasional, layanan dasar yang harus disediakan oleh CSIRT nasional didefinisikan dan efisiensi operasional untuk memanfaatkan kemampuan manajemen insiden dievaluasi. Dari hasil tersebut, rincian operasional disusun dan ditingkatkan. Kegiatan pada tahap ini adalah:

a) Aktif melaksanakan berbagai layanan yang disediakan CSIRT nasional
b) Mengembangkan dan melaksanakan mekanisme evaluasi efektivitas operasi CSIRT nasional
c) Meningkatkan CSIRT nasional berdasarkan hasil evaluasi
d) Memperluas misi, layanan dan staf yang tepat dan dapat bertahan untuk meningkatkan layanan pada konstituen
e) Melanjutkan pengembangan dan peningkatan kebijakan dan prosedur CSIRT.

Tahap 5 – Kolaborasi

CSIRT nasional dapat menjalin hubungan yang terpercaya dengan *stakeholder* melalui operasi yang efisien (Tahap 4). Namun, CSIRT nasional juga perlu bertukar informasi dan pengalaman dalam menangani insiden melalui kerjasama jangka panjang dengan CSIRT domestik, CSIRT internasional, atau institusi lain. Kegiatan pada tahap ini termasuk:

a) Berpartisipasi dalam kegiatan berbagi data dan informasi serta mendukung pengembangan standar berbagi data dan informasi diantara konstituen, CSIRT lain, ahli keamanan komputer, dan rekan lainnya
b) Berpartisipasi secara global dalam fungsi sebagai '*watch dan warning*' untuk mendukung komunitas CSIRT
c) Meningkatkan kualitas kegiatan CSIRT dengan menyediakan pelatihan, *workshop* dan konferensi yang membahas tren serangan dan strategi penanganan
d) Kolaborasi dengan pihak lainnya dalam komunitas untuk mengembangkan dokumen dan pedoman praktik terbaik
e) Meninjau dan merevisi proses untuk manajemen insiden sebagai bagian dari proses peningkatan yang terus berjalan.

Layanan CSIRT[54]

Layanan yang diberikan CSIRT dapat dikelompokkan ke dalam layanan reaktif, layanan proaktif dan layanan manajemen kualitas layanan.

Layanan reaktif merupakan layanan inti CSIRT. Termasuk diantaranya:

1) **Siaga dan peringatan** - Layanan ini termasuk memberikan informasi dan metode penanganan untuk menangani masalah-masalah seperti kerentanan keamanan, penyusupan, virus komputer atau *hoax*.

2) **Penanganan insiden** - Termasuk penerimaan, *triaging*, menjawab permintaan dan laporan, serta menganalisis dan menentukan prioritas insiden dan peristiwa. Kegiatan penanganan spesifik termasuk diantaranya:

[54] Bagian ini diambil dari Carnegie Mellon University, *CSIRT Services* (2002), http://www.cert.org/archive/pdf/CSIRT-services-list.pdf.

- **Analisis insiden** - Pengujian terhadap semua informasi dan bukti atau artefak pendukung yang terkait dengan insiden. Tujuan analisis ini untuk mengidentifikasi lingkup insiden, tingkat kerusakan yang disebabkan oleh insiden tersebut, sifat insiden serta strategi penanganan yang ada.

- **Pengumpulan bukti forensik** - Pengumpulan, pemeliharaan, dokumentasi dan analisis bukti dari sistem komputer yang terserang untuk menentukan perubahan pada sistem dan untuk membantu rekonstruksi peristiwa yang mengarah pada serangan.

- **Penjejakan atau penelusuran** - Termasuk penjejakan atau penelusuran bagaimana penyusup bisa memasuki sistem dan jaringan. Aktivitas ini termasuk penelusuran asal penyusup atau identifikasi sistem yang telah diakses oleh si penyusup.

3) **Penanganan insiden di lokasi** - CSIRT memberikan pengarahan, bantuan langsung di lokasi untuk membantu konstituen pulih dari insiden.

4) **Bantuan penanganan insiden** - Membantu dan memandu korban serangan untuk pulih dari insiden melalui telepon, *e-mail*, fax atau dokumentasi.

5) **Koordinasi penanganan insiden** - Usaha penanganan diantara pihak yang terlibat dengan insiden dikoordinasikan. Biasanya mencakup korban serangan, lokasi lain yang terlibat, dan lokasi manapun yang membutuhkan bantuan dalam analisis serangan ini. Juga mungkin termasuk pihak yang menyediakan dukungan TI kepada korban, seperti ISP dan CSIRT lainnya.

6) **Penanganan kerentanan** – Mencakup penerimaan informasi dan laporan mengenai kerentanan perangkat keras dan piranti lunak, analisis efek kerentanan, dan pengembangan strategi penanganan untuk mendeteksi dan memperbaiki kerentanan.

   - **Analisis kerentanan** - Mengacu pada analisis teknis dan pengujian kerentanan perangkat keras atau piranti lunak. Analisis ini mencakup peninjauan kode sumber, penggunaan *debugger* untuk menentukan dimana kerentanan muncul, atau mencoba mereproduksi masalah pada sistem uji.

   - **Penanganan kerentanan** - Termasuk menentukan penanganan yang tepat untuk mitigasi atau perbaikan kerentanan. Layanan ini termasuk juga langkah penanganan dengan memasang *patch*, perbaikan atau *workaround*. Termasuk didalamnya memberitahukan kepada yang lainnya tentang strategi mitigasi, memberikan nasihat dan peringatan bahaya.

   - **Koordinasi penanganan kerentanan** - CSIRT memberitahukan kepada konstituen tentang kerentanan dan berbagi informasi tentang cara memperbaiki atau melakukan mitigasi. CSIRT juga mengelompokkan strategi-strategi penanganan kerentanan yang berhasil. Kegiatan ini termasuk analisis kerentanan atau laporan kerentanan serta menyatukan

analisis teknis yang dilakukan oleh berbagai pihak. Layanan ini juga mencakup pemeliharaan *knowledge base* atau arsip publik dan swasta tentang informasi kerentanan dan strategi penanganan yang sesuai.

7) **Penanganan artefak** – Mencakup analisis, penanganan, kerjasama dan penanganan artefak yang meliputi virus komputer, *Trojan horse*, *worm*, *exploit scripts* dan perangkatnya.

   - **Analisis artefak** - CSIRT melakukan analisis dan uji teknis terhadap berbagai artefak yang ditemukan di dalam sistem.

   - **Penanganan artefak** - Menentukan aksi yang tepat untuk mendeteksi dan menghapus artefak dari sistem.

   - **Koordinasi penanganan artefak** - Termasuk penyatuan dan berbagi hasil analisis dan strategi penanganan terkait artefak, dengan peneliti, CSIRT, vendor dan ahli keamanan lainnya.

Layanan proaktif adalah untuk meningkatkan proses keamanan dan infrastruktur dari lembaga konstituen sebelum insiden terjadi atau terdeteksi. Layanan yang diberikan adalah sebagai berikut:

1) **Pemberitahuan** - Hal ini termasuk peringatan penyusupan, peringatan kerentanan, pemberian nasihat keamanan, dan lain-lain. Pemberitahuan semacam di atas memberikan informasi kepada konstituen tentang perkembangan baru dengan dampak jangka menengah hingga jangka panjang, seperti kerentanan atau alat penyusupan yang baru ditemukan. Adanya pemberitahuan memungkinkan konstituen untuk melindungi sistem dan jaringan mereka terhadap masalah yang baru saja ditemukan sebelum mereka tereksploitasi.

2) **Pengawasan teknologi** – Mencakup pengawasan dan peninjauan perkembangan teknis terbaru, aktivitas penyusupan dan tren terkait untuk membantu mengidentifikasi ancaman di masa mendatang. Hasil dari layanan ini dapat berupa pedoman, atau rekomendasi yang fokus pada isu keamanan jangka menengah hingga jangka panjang.

3) **Audit atau penilaian keamanan** - Layanan ini memberikan analisis dan tinjauan rinci infrastruktur keamanan organisasi, mengikuti persyaratan yang ditetapkan oleh organisasi atau oleh standar industri lain yang digunakan.

4) **Konfigurasi dan pemeliharaan perangkat, aplikasi, infrastruktur, dan layanan keamanan** - Layanan ini memberikan pedoman untuk konfigurasi dan pemeliharaan perangkat, aplikasi dan infrastruktur komputasi umum.

5) **Pengembangan perangkat keamanan** - Layanan ini termasuk pengembangan baru piranti lunak, *plug-in*, *patch,* perangkat spesifik ke konstituen, yang dibuat dan disebarkan untuk keamanan.

6) **Layanan deteksi penyusupan** - CSIRT yang melakukan layanan ini meninjau log IDS yang ada, menganalisisnya, dan memulai penanganan kejadian-kejadian yang melewati batas yang sudah ditetapkan.

7) **Penyebaran informasi terkait keamanan** – Layanan ini memberikan konstituen sekumpulan informasi komprehensif yang berguna dan mudah - ditemukan untuk membantu meningkatkan keamanan.

Layanan manajemen kualitas keamanan dirancang untuk memberikan pengetahuan yang didapat dari penanganan insiden, kerentanan dan serangan dalam satu kesatuan. Layanan ini mencakup:

1) **Analisis risiko** - Mencakup peningkatan kemampuan CSIRT untuk menilai ancaman, memberikan kajian risiko aset informasi secara kualitatif dan kuantitatif serta realistis, dan mengevaluasi strategi perlindungan dan penanganan.

2) **Perencanaan keberlangsungan bisnis dan pemulihan bencana** – Keberlangsungan bisnis dan pemulihan bencana yang disebabkan serangan keamanan komputer dipastikan melalui perencanaan yang cukup.

3) **Konsultasi keamanan** - CSIRT juga dapat memberikan saran praktis dan petunjuk untuk operasi bisnis.

4) **Peningkatan kesadaran** - CSIRT mampu untuk meningkatkan kesadaran keamanan dengan mengidentifikasi dan memberikan informasi dan pedoman tentang praktik dan kebijakan keamanan yang dibutuhkan konstituen.

5) **Pendidikan/Pelatihan** - Layanan ini mencakup pendidikan dan pelatihan dengan topik seperti pedoman pelaporan insiden, metode penanganan yang tepat, perangkat penanganan insiden, metode pencegahan insiden, dan informasi penting lainnya untuk melindungi, mendeteksi, melaporkan dan menangani insiden keamanan komputer. Bentuk pelatihan bisa berupa seminar, *workshop*, kursus dan tutorial.

6) **Evaluasi atau sertifikasi produk** - CSIRT dapat melaksanakan evaluasi produk terhadap perangkat, aplikasi atau layanan lain untuk memastikan keamanan dan kepatuhan produk terhadap praktek keamanan yang dapat diterima oleh CSIRT atau organisasi.

Tabel 12 menunjukkan tingkatan masing-masing layanan CSIRT – yaitu inti, tambahan atau layanan tidak biasanya – dalam tiap model CSIRT.

Tabel 12. Layanan CSIRT

Kategori Layanan	Layanan		Tim Keamanan	Terdistribusi	Terpusat	Gabungan	Terkoordinasi
Reaktif	Siaga dan Peringatan		Tambahan	Inti	Inti	Inti	Inti
	Pena-nganan Insiden	Analisis Insiden	Inti	Inti	Inti	Inti	Inti
		Penanganan Insiden di Lokasi	Inti	Tambahan	Tambahan	Tambahan	Tidak biasa
		Bantuan Penanganan Insiden	Tidak biasa	Inti	Inti	Inti	Inti
		Koordinasi Penanganan Insiden	Inti	Inti	Inti	Inti	Inti
	Pena-nganan Artefak	Analisis Kerentanan	Tambahan	Tambahan	Tambahan	Tambahan	Tambahan
		Penanganan Kerentanan	Inti	Tambahan	Tidak biasa	Tambahan	Tambahan
		Koordinasi Penanganan Kerentanan	Tambahan	Inti	Inti	Inti	Inti
		Analisis Artefak	Tambahan	Tambahan	Tambahan	Tambahan	Tambahan
		Penanganan Artefak	Inti	Tambahan	Tambahan	Tambahan	Tambahan
		Koordinasi Penanganan Artefak	Tambahan	Tambahan	Inti	Inti	Inti
Proaktif	Pemberitahuan		Tidak biasa	Inti	Inti	Inti	Inti
	Pengawasan Teknologi		Tidak biasa	Tambahan	Inti	Inti	Inti
	Audit atau Penilaian Keamanan		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Konfigurtasi dan pemeliharaan perangkat, aplikasi, infrastruktur, dan layanan keamanan		Inti	Tambahan	Tambahan	Tambahan	Tidak biasa
	Pengembangan Perangkat Keamanan		Tambahan	Tambahan	Tambahan	Tambahan	Tambahan
	Layanan Deteksi Penyusupan		Inti	Tambahan	Tambahan	Tambahan	Tidak biasa
	Penyebaran Informasi Terkait Keamanan		Tidak biasa	Tambahan	Inti	Inti	Inti
Manajemen Kualitas Keamanan	Analisis Risiko		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Perencanaan Keberlangsungan Bisnis dan Pemulihan Bencana		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Konsultasi Keamanan		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan
	Peningkatan Kesadaran		Tidak biasa	Tambahan	Tambahan	Tambahan	Inti
	Pendidikan/Pelatihan		Tidak biasa	Tambahan	Tambahan	Tambahan	Inti
	Evaluasi atau Sertifikasi Produk		Tidak biasa	Tambahan	Tambahan	Tambahan	Tambahan

Sumber: Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle dan Mark Zajicek, *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

6.2 CSIRT Internasional

Saat ini, terdapat sejumlah CSIRT internasional yang khusus dibentuk untuk menangani insiden keamanan komputer di seluruh dunia. Ketika CSIRT nasional dapat menangani serangan dan melaksanakan fungsi lainnya, serangan internasional membutuhkan perhatian CSIRT internasional.

Forum of Incident Response Security Teams (FIRST)[55]

FIRST terdiri dari CERT, lembaga pemerintah dan perusahaan keamanan dari 41 negara. Keanggotaannya mencakup 191 organisasi, termasuk CERT/CC dan US-CERT. FIRST adalah lembaga untuk berbagi informasi dan kerjasama diantara tim penanganan insiden. Tujuannya adalah untuk mengaktifkan kegiatan penanganan insiden dan perlindungan, serta memotivasi kerjasama antar anggota dengan memberikan mereka teknologi, pengetahuan dan perangkat untuk menangani insiden. Aktivitas FIRST adalah sebagai berikut:

- Pengembangan dan berbagi praktik terbaik, prosedur, perangkat, informasi teknis dan metodologi penanganan insiden dan perlindungan;
- Memotivasi pengembangan kebijakan, layanan dan produk keamanan berkualitas baik;
- Mendukung dan mengembangkan pedoman keamanan komputer yang tepat;
- Membantu pemerintah, pengusaha dan lembaga pendidikan untuk membangun sebuah tim penanganan insiden dan memperluasnya; dan
- Memfasilitasi dalam berbagi teknologi, pengalaman dan pengetahuan diantara anggota untuk lingkungan elektronik yang lebih aman.

CERT Asia Pasifik[56]

Asia-Pacific Computer Emergency Response Team (APCERT) dibentuk pada bulan Februari 2003 untuk berfungsi sebagai jaringan para ahli keamanan, memperkuat penanganan insiden, dan meningkatkan kesadaran keamanan di kawasan Asia Pasifik. Konferensi pertama CSIRT Asia Pasifik diselenggarakan di Jepang pada tahun 2002. APCERT dibentuk setahun kemudian pada konferensi di Taipei yang dihadiri oleh 14 CSIRT Asia Pasifik. Di bulan Agustus 2007, APCERT telah memiliki 14 anggota tetap dan enam anggota asosiasi.

Anggota APCERT sepakat bahwa insiden keamanan komputer saat ini sangat banyak, kompleks dan sulit untuk dikontrol oleh satu organisasi atau negara manapun, dan bahwa penanganan yang lebih efektif dapat dilakukan dengan kerjasama antar anggota APCERT. Seperti di FIRST, konsep terpenting dalam APCERT adalah hubungan saling percaya antara anggota untuk bertukar informasi dan saling bekerjasama. Jadi, kegiatan APCERT dirancang untuk:

[55] FIRST, "About FIRST," FIRST.org, Inc., http://www.first.org/about/.
[56] APCERT, "Background," http://www.apcert.org/about/background/index.html.

- Meningkatkan kerjasama regional dan internasional Asia-Pasifik;
- Membangun langkah bersama untuk menangani insiden keamanan jaringan regional atau skala besar;
- Meningkatkan berbagi informasi dan pertukaran teknologi keamanan, termasuk informasi tentang virus komputer, *exploit scripts*, dan lain-lain;
- Meningkatkan kerjasama penelitian terhadap masalah umum;
- Membantu CERT lainnya di kawasan untuk menangani insiden keamanan komputer secara efektif; dan
- Memberikan saran dan solusi masalah hukum terkait dengan keamanan informasi dan penanganan insiden regional.

European Government CERT[57]

European Government CERT (EGC) adalah komite non-resmi yang berhubungan dengan CSIRT di negara-negara Eropa. Anggotanya adalah Finlandia, Perancis, Jerman, Hungaria, Belanda, Norwegia, Swedia, Swiss dan Inggris. Peran dan tanggung jawabnya adalah:

- Membangun langkah bersama untuk menangani insiden keamanan jaringan regional atau skala besar;
- Meningkatkan berbagi informasi dan pertukaran teknologi terkait insiden keamanan dan ancaman kode berbahaya serta kerentanan;
- Mengidentifikasi area-area pengetahuan dan keahlian yang dapat dibagi di dalam kelompok;
- Mengidentifikasi area-area untuk kerjasama penelitian dan pengembangan untuk subyek yang menjadi perhatian para anggota; dan
- Mendorong formasi CSIRT pemerintah di negara-negara Eropa.

European Network and Information Security Agency (ENISA)[58]

Tujuan ENISA adalah untuk meningkatkan keamanan jaringan dan keamanan informasi di Uni Eropa (UE) dengan membangun budaya NIS. Dibentuk pada bulan Januari 2004 oleh *Council of Minsters and the European Parliament* untuk menghadapi tindak kejahatan berteknologi tinggi. Peranan ENISA adalah:

- Memberikan dukungan untuk memastikan NIS bagi anggota ENISA atau UE;
- Membantu menstabilkan pertukaran informasi antara *stakeholder*; dan
- Meningkatkan koordinasi fungsi yang terkait dengan NIS.

ENISA diharapkan dapat berkontribusi terhadap usaha internasional untuk mitigasi virus dan *hacking* serta pengawasan *online* terhadap ancaman.

[57] EGC, http://www.egc-group.org.
[58] ENISA, “About ENISA,” http://www.enisa.europa.eu/pages/About_ENISA.htm.

6.3 CSIRT Nasional

Beberapa negara telah membentuk CSIRT nasional. Tabel 13 menunjukkan negara dan CSIRT mereka serta *situs web*-nya.

Tabel 13. Daftar CSIRT Nasional[59]

Negara	Nama Resmi	Situs *web*
Argentina	Computer Emergency Response Team of the Argentine Public Administration	http://www.arcert.gov.ar
Australia	Australia Computer Emergency Response Team	http://www.aucert.org.au
Brazil	Computer Emergency Response Team Brazil	http://www.cert.br
Brunei Darussalam	Brunei Computer Emergency Response Team	http://www.brucert.org.bu
Kanada	Public Safety Emergency Preparedness Canada	http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp
Chile	Chilean Computer Emergency Response Team	http://www.clcert.cl
Cina	National Computer Network Emergency Response Technical Ream - Coordination Center of China	http://www.cert.org.cn
Denmark	Danish Computer Emergency Response Team	http://www.cert.dk
El Salvador	Response Team for Computer Security Incidents	
Finlandia	Finnish Communication Regulatory Authority	http://www.cert.fi
Perancis	CERT-Administration	http://www.certa.ssi.gouv.fr
Jerman	CERT-Bund	http://www.bsi.bund.de/certbund
Hong Kong	Hong Kong Computer Response Coordination Centre	http://www.hkcert.org
Hungaria	CERT-Hungary	http://www.cert-hungary.hu
India	CERT-In	http://www.cert-in.org.in
Indonesia	Indonesia Computer Emergency Response Team	http://www.cert.or.id
Jepang	JP CERT Coondination Center	http://www.jpcert.or.jp
Lithuania	LITNET CERT	http://cert.litnet.lt
Malaysia	Malaysian Computer Emergency Response Team	http://www.mycert.org.my
Meksiko	Universidad Nacional Autonoma de Mexico	http://www.cert.org.mx
Belanda	GOVCERT.NL	http://www.govcert.nl
Selandia Baru	Centre for Critical Infrastructure Protection	http://www.ccip.govt.nz
Norwegia	Norweigian National Security Authority	http://www.cert.no
Filipina	Philippines Computer Emergency	http://www.phcert.org

[59] CERT, "National Computer Security Incident Response Teams," Carnegie Mellon University, http://www.cert.org/csirts/national/contact.html.

Negara	Nama Resmi	Situs *web*
	Response Team	
Polandia	Computer Emergency Response Team Polska	http://www.cert.pl
Qatar	Qatar Computer Emergency Response Team	http://www.qcert.org
Saudi Arabia	Computer Emergency Response Team - Saudi Arabia	http://www.cert.gov.sa
Singapura	Singapore Computer Emergency Response Team	http://www.singcert.org.sg
Slovenia	Slovenia Computer Emergency Response Team	http://www.arnes.si/english/si-cert
Republik Korea	CERT Coordination Center Korea	http://www.krcert.or.kr
Spanyol	IRIS-CERT	http://www.rediris.es/cert
Swedia	Swedish IT Incident Centre	http://www.sitic.se
Thailand	Thai Computer Emergency Response Team	http://www.thaicert.nectec.or.th
Tunisia	Computer Emergency Response Team - Tunisian Coondination Center	http://www.ansi.tn/en/about_cert-tcc.htm
Turki	TP-CERT	http://www.uekae.tubitak.gov.tr
Inggris	GovCertUK	http://www.govcertuk.gov.uk
Amerika Serikat	United States -Computer Emergency Response Team	http://www.us-cert.gov
Viet Nam	Viet Nam Computer Emergency Response Team	http://www.vncert.gov.vn

Latihan

Apakah ada CSIRT nasional di negara Anda?

1. Jika ya, jelaskan model apakah yang digunakan dan bagaimana mereka bekerja. Nilai seberapa efektif mereka dalam melaksanakan fungsinya.
2. Jika tidak, tentukan model CSIRT mana yang tepat untuk negara Anda dan jelaskan apa yang diperlukan untuk membentuk CSIRT nasional di negara Anda.

Ujian

1. Apa fungsi utama CSIRT?
2. Apakah perbedaan CSIRT internasional dengan CSIRT nasional?
3. Apa saja yang diperlukan untuk membentuk CSIRT?

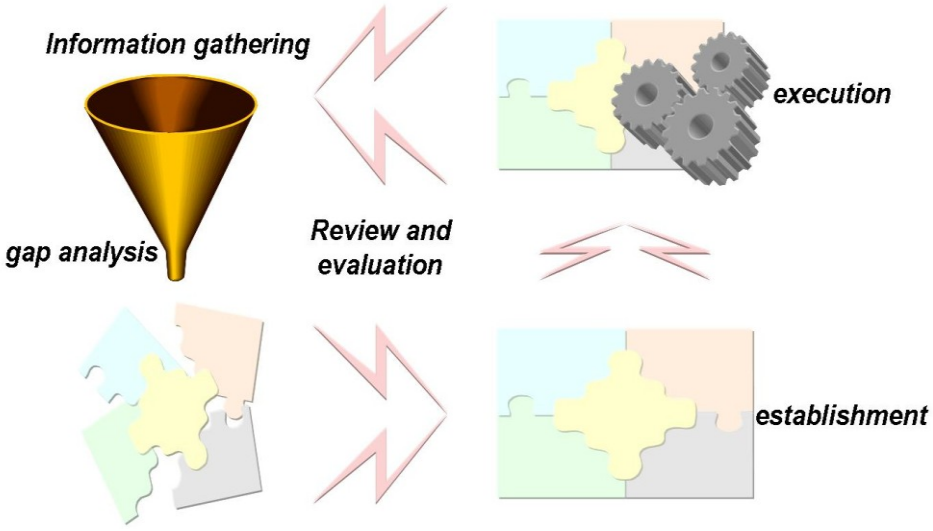
7. DAUR HIDUP KEBIJAKAN KEAMANAN INFORMASI

Bagian ini bertujuan untuk:
- Memberikan gambaran umum tentang proses pembuatan kebijakan keamanan informasi; dan
- Menjelaskan permasalahan yang harus diperhatikan oleh pembuat kebijkan dalam menyusun kebijakan keamanan informasi.

Penyusun kebijakan perlu memperhatikan beberapa hal, seperti dasar pemikiran kebijakan, sumber daya yang tersedia, arah kebijakan, kebutuhan hukum dan anggaran, serta hasil yang diharapkan. Di bab ini, pertimbangan-pertimbangan ini dibahas dalam konteks tahapan penyusunan kebijakan keamanan informasi.

Perlu dicatat bahwa masing-masing negara memiliki pertimbangan kebijakan dan konteks yang tidak persis sama. Proses penyusunan kebijakan yang dijelaskan di bagian ini adalah yang bersifat umum dan didasarkan pada asumsi dimana belum ada kebijakan keamanan informasi nasional.

Seperti pada kebijakan lainnya, daur hidup kebijakan keamanan informasi dapat dibagi dalam empat fase: (1) pengumpulan informasi dan analisis kesenjangan; (2) penetapan kebijakan; (3) implementasi kebijakan; dan (4) pengendalian dan umpan balik (Gambar 19). Sebagai tambahan, kebijakan keamanan informasi nasional harus mencakup strategi keamanan informasi, hubungan resmi, organisasi keamanan informasi, teknologi keamanan informasi, dan hubungan antar mereka.



Gambar 19. Daur Hidup Kebijakan Keamanan Informasi

7.1 Pengumpulan Informasi dan Analisis Kesenjangan

Fase pertama dalam merumuskan kebijakan keamanan informasi adalah pengumpulan informasi dan analisis kesenjangan.

Dalam pengumpulan informasi, tinjauan terhadap contoh keamanan informasi dan kebijakan terkait di negara lain akan sangat berguna, termasuk juga kebijakan terkait yang ada di dalam negara itu sendiri.

Dalam analisis kesenjangan, penting untuk memahami infrastruktur yang ada terkait dengan keamanan informasi, seperti hukum dan sistem yang ada, serta area atau kesenjangan yang perlu diisi. Ini merupakan langkah penting karena ini menentukan arah atau prioritas kebijakan keamanan informasi yang dibentuk.

Pengumpulan informasi

Pengumpulan kasus dari luar negeri: dalam menemukan kasus yang relevan dari negara lain, penyusun kebijakan perlu memperhatikan kesamaan dalam —

- Tingkat keamanan informasi nasional
- Arah pembentukan kebijakan
- Infrastruktur jaringan dan sistem.

Berdasarkan kesamaan ini, materi berikut dapat dikumpulkan —

- Informasi pada pembentukan dan operasi organisasi yang ikut serta dalam keamanan informasi (lihat Bagian 3 dan 6 modul ini)
- Kebijakan, hukum dan peraturan keamanan informasi (lihat Bagian 3)
- Metodologi keamanan informasi yang digunakan secara internasional dan contoh dari negara-negara berbeda (lihat Bagian 4)
- Tren ancaman dan metode penanganan atau pengendalian yang bergantung pada jenis serangan (lihat Bagian 2 dan 6)
- Metode penanganan untuk perlindungan privasi (lihat Bagian 5).

Pengumpulan materi dalam negeri: Meskipun banyak penyusun kebijakan bukan ahli dalam keamanan informasi, mereka melaksanakan aktivitas yang terkait dengan keamanan informasi. Khususnya, mereka merancang hukum, peraturan dan kebijakan dalam area yang terkait dengan keamanan informasi. Akan tetapi, karena hukum, peraturan dan kebijakan cenderung fokus pada area tertentu, korelasi antara mereka mungkin tidak langsung terlihat jelas oleh penyusun kebijakan. Karena itu, terdapat kebutuhan untuk mengumpulkan dan menganilisis serta mengevaluasi semua hukum, peraturan dan kebijakan yang terkait dengan keamanan informasi.

Analisis kesenjangan

The Art of War Sun Tzu mengatakan, “Ketahui musuhmu.” Ini berarti kita harus mengetahui keterbatasan kita serta keterbatasan musuh. Dalam kasus penyusunan kebijakan keamanan informasi, hal ini berarti mengetahui apa yang perlu untuk dilindungi melalui kebijakan keamanan informasi serta kerentanan dan ancaman keamanan informasi.

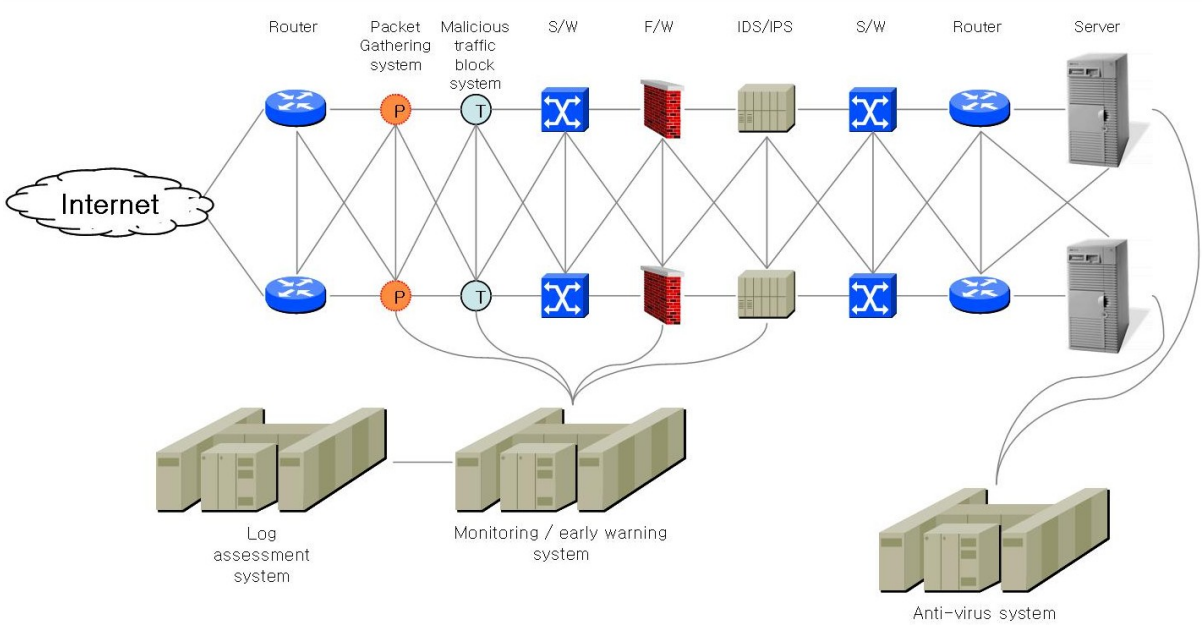
Analisis kesenjangan dapat dibagi menjadi dua fase:

1. Memahami kemampuan dan kapasitas negara – yaitu sumber daya manusia dan organisasi, serta infrastruktur informasi dan komunikasi – dalam bidang umum keamanan informasi; dan
2. Mengidentifikasi ancaman eksternal pada keamanan informasi.

Penyusun kebijakan perlu **akrab dengan sumber daya manusia dan organisasi keamanan informasi** – yaitu institusi publik dan swasta dalam bidang yang terkait dengan keamanan informasi. Mereka perlu mengetahui organisasi yang terlibat dalam bidang keamanan informasi dan memahami lingkup kerja, peran dan tanggung jawab mereka. Hal ini penting agar tidak terjadi duplikasi struktur dalam keamanan informasi.

Di tahap ini juga perlu dilakukan identifikasi para ahli keamanan informasi dari latar belakang hukum, kebijakan, teknologi, pendidikan dan bidang terkait.

Infrastruktur informasi-komunikasi adalah struktur TI yang mengumpulkan, memroses, menyimpan, mencari, mengirim dan menerima informasi dan sistem manajemen elektronik. Singkatnya, ini adalah sistem informasi dan jaringan. **Memahami status infrastruktur informasi-komunikasi saat ini** sangat penting terutama ditinjau dari sisi ekonomi. Karena diperlukan investasi yang besar untuk menghubungkan seluruh negara, dan fasilitas informasi-komunikasi yang telah ada perlu dimanfaatkan semaksimal mungkin. Gambar 20 menunjukkan contoh infrastruktur informasi-komunikasi untuk keamanan informasi. Ini tidak termasuk semua item yang diperlukan dan yang diberikan di sini hanya untuk ilustrasi. Perhatikan hubungan antara berbagai komponen jaringan.



Gambar 20. Contoh Struktur Sistem dan Jaringan

Penyusun kebijakan perlu memahami bagaimana jaringan dan sistem untuk keamanan informasi disusun.

Langkah kedua dalam analisis kesenjangan adalah **identifikasi ancaman keamanan informasi eksternal**. Seperti dijelaskan di Bagian 2, ancaman informasi tidak hanya meningkat tetapi juga semakin canggih. Penyusun kebijakan perlu memahami ancaman ini untuk dapat memutuskan metode penanganan yang diperlukan. Khususnya, penyusun kebijakan perlu memahami:

- Tingkat penetrasi ancaman pada keamanan informasi
- Jenis serangan terbaru dan yang paling umum
- Jenis-jenis ancaman dan tingkat kekuatan mereka di masa mendatang.

Setelah menganalisis organisasi nasional, sumber daya manusia, dan infrastruktur informasi-komunikasi, serta memahami komponen ancaman di bidang keamanan informasi, penting untuk menentukan komponen yang rentan. Hal ini menentukan sejauh mana negara dapat menolak komponen ancaman eksternal. Penentuan ini dapat dilakukan dengan pemeriksaan berikut ini:

- Status CERT saat ini dan kemampuannya untuk bereaksi
- Status ahli keamanan informasi saat ini
- Tingkatan dan intensitas konstruksi sistem keamanan informasi
- Perlindungan hukum terhadap pelanggaran aset informasi
- Lingkungan fisik untuk melindungi aset informasi.

Tujuan analisis kesenjangan adalah untuk mengidentifikasi langkah penanganan praktis yang perlu diambil. Perlu ditekankan bahwa ini adalah langkah yang paling dasar dalam penyusunan kebijakan keamanan informasi.

7.2 Merumuskan Kebijakan Keamanan Informasi

Merumuskan kebijakan keamanan informasi nasional mencakup: (i) menentukan arah kebijakan; (ii) membentuk organisasi keamanan informasi beserta peran dan tanggung jawabnya; (iii) menyatakan kerangka kerja kebijakan keamanan informasi; (iv) menyusun dan/atau merevisi hukum supaya konsisten dengan kebijakan; dan (v) mengalokasikan anggaran implementasi kebijakan informasi.

(i) Menentukan arah kebijakan dan mendorongnya

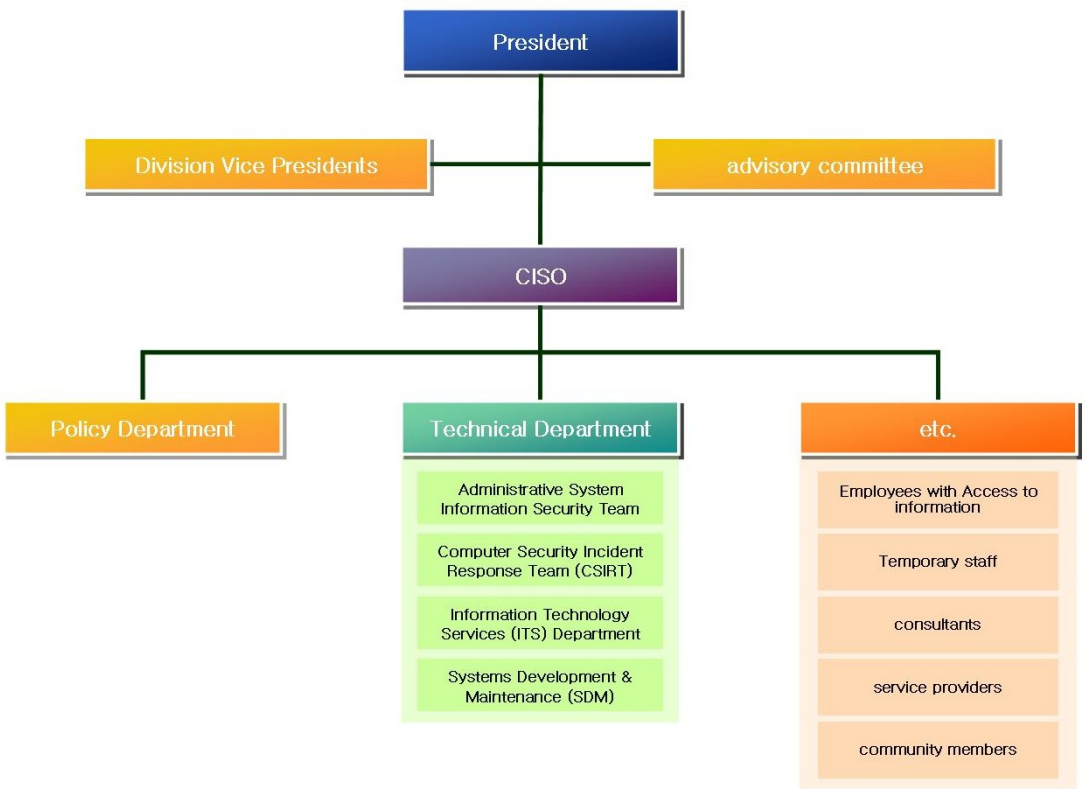
Di banyak kasus, penyusunan kebijakan keamanan informasi harus dipelopori oleh pemerintah ketimbang menyerahkannya ke sektor swasta. Khususnya, pemerintah perlu menetapkan kebijakan, berperanan penting dalam menyediakan infrastruktur yang diperlukan, dan memberikan dukungan jangka panjang. Sektor swasta bergabung ke proyek ini kemudian, terutama untuk mengambil bagian dalam penelitian dan pengembangan, serta konstruksi sistem.

Partisipasi sektor swasta yang direncanakan meliputi kegiatan peningkatan kesadaran bersamaan dengan pembangunan dan penguatan infrastruktur informasi-komunikasi. Jika pemerintah bertujuan mendorong sektor swasta untuk menerima strategi keamanan informasi, maka pemerintah perlu berperan sebagai pendukung daripada sebagai pengatur. Hal ini termasuk penyebaran pedoman keamanan informasi.

(ii) Konstitusi organisasi keamanan informasi, dan penentuan peran dan tanggung jawab[60]

Ketika arah kebijakan keamanan informasi telah ditetapkan, organisasi pelaksana harus diangkat. Gambar 21 menunjukkan struktur organisasi keamanan informasi nasional yang umum.

[60] Bagian ini diambil dari Sinclair Community College, “Information Security Organization - Roles and Responsibilities,” http://www.sinclair.edu/about/information/usepolicy/pub/infscply/Information_Security_Organization_-_Roles_and_Responsibilities.htm.



Gambar 21. Contoh Organisasi Keamanan Informasi Nasional

Organisasi keamanan informasi nasional sedikit berbeda di tiap negara, bergantung pada karakteristik dan budaya masing-masing. Namun, prinsip dasarnya adalah untuk memastikan bahwa peran dan tanggung jawab tergambar dengan jelas.

Organisasi Administratif

Division Vice-President memiliki tanggung jawab utama terhadap informasi yang dikumpulkan, dipelihara dan/atau diidentifikasi serta dimanfaatkan atau 'dimiliki' oleh divisinya masing-masing. Mereka dapat menunjuk seorang *Information Security Officer* (ISO) dan individu lainnya untuk membantu ISO dalam melaksanakan kebijakan keamanan informasi. Staf yang ditunjuk harus memastikan bahwa aset informasi yang berada dalam kendali mereka telah ditunjuk pemiliknya, bahwa penilaian risiko telah dilaksanakan, dan proses mitigasi berdasarkan pada risiko-risiko tersebut telah diimplementasikan.

Pengawas (Direktur, Ketua, Manajer, dan lain-lain) mengatur pegawai yang memiliki akses ke informasi dan sistem informasi dan menentukan, melaksanakan dan menegakkan kontrol keamanan informasi yang digunakan di bidangnya masing-masing. Mereka harus memastikan bahwa semua pegawai mengerti

tanggung jawab masing-masing terkait dengan keamanan informasi, dan bahwa pegawai memiliki akses yang diperlukan untuk melakukan pekerjaannya. Pengawas perlu meninjau secara rutin semua tingkatan akses pengguna untuk memastikan bahwa mereka sudah tepat, dan mengambil tindakan yang diperlukan untuk mengoreksi inkosistensi atau kekurangan.

***Chief Information Security Officer* (CISO)** bertanggung jawab untuk koordinasi dan pengawasan kebijakan keamanan informasi. Bekerja bersama dengan berbagai divisi, CISO dapat memberi saran kepada pengawas divisi tertentu untuk memilih wakil mereka dalam pengawasan dan koordinasi elemen kebijakan tertentu. CISO juga membantu pemilik informasi dengan praktik terbaik keamanan informasi dalam:

- Menetapkan dan menyebarkan peraturan yang dapat dilaksanakan terkait akses dan penggunaan sumber daya informasi yang dapat diterima;
- Melaksanakan/Koordinasi penilaian dan analisis risiko keamanan informasi;
- Membuat pedoman dan langkah keamanan yang layak untuk melindungi data dan sistem;
- Membantu pemantaian dan pengelolaan kerentanan keamanan sistem;
- Melaksanakan/Koordinasi audit keamanan informasi; dan
- Membantu investigasi/penyelesaian masalah dan/atau dugaan pelanggaran kebijakan keamanan informasi nasional.

Organisasi Teknis

Administrative System Information Security Team mengembangkan dan melaksanakan langkah untuk memastikan bahwa kontrol administratif keamanan aplikasi memberikan *stakeholder* akses yang tepat ke informasi sekaligus memenuhi persyaratan etis dan hukum nasional dalam melindungi informasi rahasia, sensitif dan penting.Tim mengembangkan proses dan standar untuk memberikan ketersediaan, integritas, dan kerahasiaan yang optimal dari informasi sistem administratif, termasuk proses bagi pengguna untuk meminta akses awal dan perubahan akses, dokumentasi akses pengguna yang diizinkan; serta hak dan kewajiban pengguna/pengawas; dan penyelesaian konflik dan permasalahan yang terkait dengan keamanan.

Tim ini termasuk juga *Division Information Security Officers* dan CISO. Penasihat dari Tim ini adalah *Department Information Security Officers and Administrative Systems Administrators*.

CSIRT memberikan informasi dan membantu *stakeholder* dalam pelaksanaan langkah proaktif untuk mengurangi risiko insiden keamanan komputer, dan dalam investigasi, penanganan dan meminimalkan kerusakan akibat dari insiden. CSIRT juga menentukan dan merekomendasikan langkah-langkah lebih lanjut. Dua lapisan dalam CSIRT terdiri dari tim operasional yang bertugas untuk identifikasi awal, penanganan, *triage* dan penentuan kebutuhan eskalasi, dan tim manajemen

yang bertugas untuk memelopori penanganan nasional terhadap insiden penting. CISO dan staf TI yang didelegasikan dari *Information Technology Services* dan *Systems Development and Maintenance* adalah bagian dari operasional CSIRT. Tim manajemen CSIRT terdiri dari *Chief Information Officer*, *Chief of Police*, *Director of Public Information*, *Director of Information Technology Services*, *Director of Systems Development and Maintenance*, CISO, manajer sistem dan jaringan, penasihat hukum, penasihat sumber daya manusia, dan delegasi dengan keahlian teknis tertentu yang ditunjuk oleh *Vice President*.

Departemen Layanan Teknologi Informasi mencakup administrator sistem dan jaringan beserta jajarannya, dan penyedia layanan teknis seperti *IT Help Desk*, teknisi pendukung pengguna dan administrator komunikasi suara. Mereka bertanggung jawab terhadap integrasi perangkat, kontrol, dan praktik keamanan informasi teknis dalam lingkungan jaringan. Mereka menerima laporan kegagalan keamanan informasi atau insiden yang dicurigai dari pengguna.

Pengembangan dan Pemeliharaan Sistem mencakup pengembang dan administrator basisdata. Mereka mengembangkan, mempraktikkan, mengintegrasikan dan melaksanakan praktik terbaik keamanan untuk aplikasi nasional, dan melatih pengembang aplikasi *web* dalam penggunaan prinsip keamanan aplikasi.

Lainnya

Pegawai dengan akses ke informasi dan sistem informasi harus patuh pada kebijakan dan prosedur nasional yang ada, serta praktik atau prosedur tambahan yang ditetapkan oleh atasan atau direktur mereka. Hal ini termasuk melindungi akun *password* mereka dan melaporkan penyalahgunaan informasi atau insiden keamanan informasi yang dicurigai ke pihak yang berwenang (biasanya pengawas mereka).

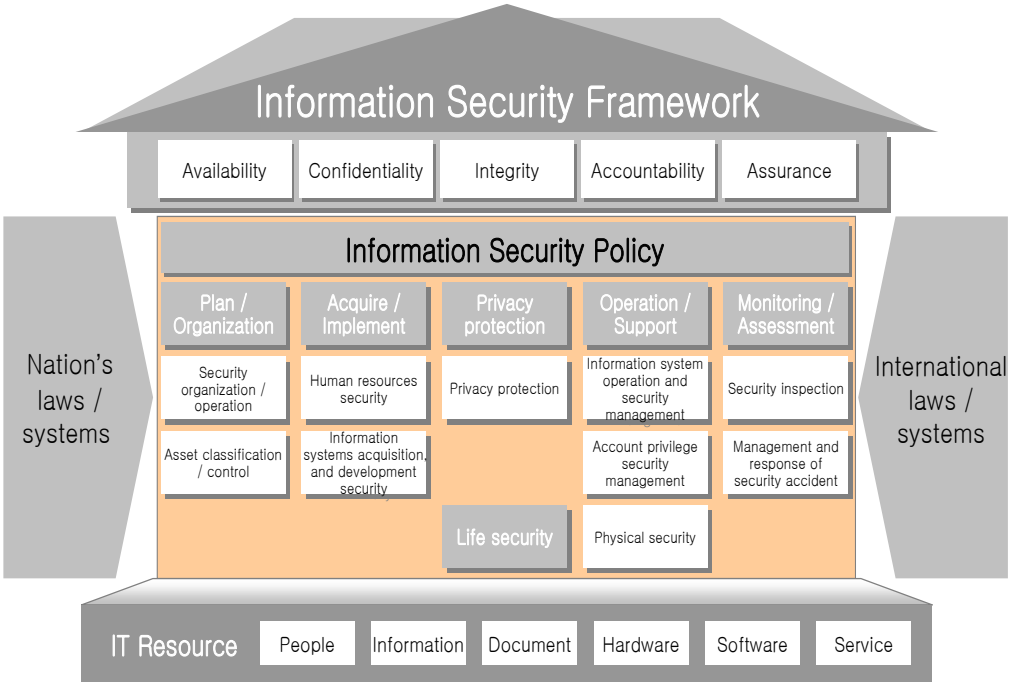
Pegawai tidak tetap dianggap sebagai pegawai dan memiliki tanggung jawab yang sama seperti pegawai penuh- atau paruh-waktu yang memiliki akses ke informasi dan sistem informasi.

Konsultan, penyedia layanan dan pihak ketiga yang dikontrak lainnya diberikan akses ke informasi pada basis ‘perlu mengetahui’ (*need to know*). Akun jaringan yang dibutuhkan oleh pihak ketiga harus dimintakan oleh ‘sponsor’ dalam organisasi yang akan memastikan bahwa pihak ketiga mengerti tanggung jawab terkait dengan akun jaringan tersebut, dan disetujui oleh *vice-president* atau direktur yang berwenang. Pengguna ini harus menjaga *password*-nya tetap aman dan bertanggung jawab pada semua kegiatan yang dihasilkan dari penggunaan *user ID*-nya dalam lingkup kendalinya.

(iii) Penetapan kerangka kerja kebijakan keamanan informasi

Kerangka kerja keamanan informasi

Kerangka kerja keamanan informasi menentukan parameter untuk kebijakan keamanan informasi dan memastikan bahwa kebijakan tersebut mempertimbangkan sumber daya TI (masyarakat, dokumen informasi, perangkat keras, piranti lunak, layanan); mencerminkan hukum dan peraturan internasional; dan memenuhi prinsip ketersediaan, kerahasiaan, integritas, akuntabilitas dan jaminan informasi. Gambar 22 menunjukkan kerangka kerja keamanan informasi.



Gambar 22. Kerangka kerja keamanan informasi

Kebijakan keamanan informasi adalah bagian paling penting dari kerangka kerja keamanan informasi. Kebijakan ini mencakup lima area, yang disebutkan di bawah ini.

a) **Rencana dan Organisasi**: Area ini meliputi organisasi dan operasi keamanan, serta klasifikasi dan kontrol aset.

Organisasi dan operasi keamanan mencakup –
- Organisasi dan sistem dari organisasi keamanan informasi nasional
- Prosedur masing-masing organisasi keamanan informasi
- Konstitusi dan manajemen keamanan informasi nasional
- Kerjasama dengan lembaga internasional terkait
- Kerjasama dengan kelompok ahli.

Klasifikasi dan kontrol aset mencakup—
- Pemberian kepemilikan dan standar klasifikasi untuk aset informasi penting
- Instruksi pendaftaran dan penilaian risiko aset informasi penting
- Manajemen hak akses terhadap aset informasi penting
- Publikasi dan pengeluaran aset informasi penting
- Penilaian ulang dan pengakhiran aset informasi penting
- Manajemen keamanan dokumen.

b) **Pengadaan dan Implementasi**: Area ini termasuk keamanan sumber daya manusia, dan keamanan pengadaan dan pengembangan sistem informasi.

Keamanan sumber daya manusia menetapkan metode manajemen untuk penerimaan pegawai baru yang mencakup —
- Langkah keamanan sumber daya manusia dan pelatihan keamanan
- Pemrosesan pelanggaran hukum dan peraturan keamanan
- Manajemen keamanan akses pihak ketiga
- Manajemen keamanan akses personel alih daya
- Manajemen pekerjaan pihak ketiga dan *outsourcing* pegawai
- Manajemen keamanan ruangan dan perlengkapan komputer
- Akses ke fasilitas dan bangunan utama.
- Pemrosesan insiden keamanan.

Keamanan pengadaan dan pengembangan sistem informasi mencakup —
- Pemeriksaan keamanan ketika sistem informasi diadakan
- Manajemen keamanan program aplikasi *in-house* maupun alih daya
- Sistem enkripsi nasional (program dan kunci enkripsi, dan sebagainya)
- Pengujian setelah pengembangan program
- Persyaratan keamanan ketika pengembangan di-alih daya-kan
- Verifikasi keamanan dalam pengadaan dan pengembangan.

c) **Perlindungan Privasi**: Dimasukkannya perlindungan privasi dalam kebijakan keamanan informasi bersifat tidak wajib. Namun, akan lebih baik untuk menyertakannya mengingat perlindungan privasi adalah isu internasional. Ketentuan perlindungan privasi harus mencakup hal berikut —
  - Pengumpulan dan penggunaan informasi pribadi
  - Permintaan izin sebelumnya ketika memanfaatkan privasi seseorang
  - PIA.

d) **Operasi dan Dukungan**: Area ini terkait dengan keamanan fisik dan teknis. Penggunaan jaringan dan sistem diatur secara rinci, dan keamanan fisik dari infrastruktur informasi dan komunikasi ditetapkan.

Manajemen keamanan dan operasi sistem informasi menyangkut penetapan hal-hal berikut —
- Manajemen keamanan dan operasi *server*, jaringan, aplikasi dan basisdata

- Pengembangan sistem keamanan informasi
- Catatan dan *back-up* dari aksi-aksi yang sah
- Manajemen penyimpanan informasi
- Komputasi *mobile*
- Standar untuk penjagaan dan pengamanan data komputer
- Layanan *e-commerce.*

Manajemen keamanan hak akun - Kontrol akses dan manajemen akun harus dibuat untuk menjamin kerahasiaan penggunaan tempat penyimpanan informasi nasional. Hal ini termasuk —

- Pendaftaran, penghapusan, manajemen hak pengguna sistem informasi nasional
- Manajemen akun dan hak dalam jaringan ter-enkripsi.

Keamanan fisik - Keamanan fisik mengacu pada perlindungan fasilitas informasi dan komunikasi yang menyimpan informasi penting. Termasuk —

- Konfigurasi dan pengelolaan metode area keamanan
- Kontrol akses dan pengiriman untuk pusat komputer
- Pencegahan kerusakan dari bencana alam dan lainnya.

e) **Pemantauan dan Penilaian**: Area kebijakan keamanan informasi membutuhkan formulasi standar dan proses untuk pencegahan insiden keamanan serta pengelolaan dan penanganan insiden keamanan.

Inspeksi keamanan termasuk —

- Pembentukan rencana inspeksi keamanan
- Pelaksanaan inspeksi keamanan secara rutin
- Pengorganisasian/penyusunan bentuk laporan
- Pengidentifikasian subyek dari target inspeksi dan laporan keamanan.

Manajemen dan penanganan insiden keamanan mencakup —

- Tugas dan peran tiap organisasi dalam pemrosesan insiden keamanan
- Prosedur untuk memantau dan mengenali gejala insiden keamanan
- Prosedur pemrosesan insiden keamanan dan metode penanganan
- Langkah yang perlu dilakukan sesudah pemrosesan insiden keamanan.

(iv) Penyusunan dan/atau pengubahan hukum agar konsisten dengan kebijakan keamanan informasi

Hukum harus konsisten dengan kebijakan keamanan informasi. Perlu ada hukum yang mengatur organisasi pemerintah dan perusahaan swasta. Tabel 14-16 memperlihatkan hukum yang berkaitan dengan keamanan informasi di Jepang, UE dan AS. Di Jepang, hukum TI yang mewakili adalah *Basic Act on the Formation of an Advanced Information and Telecommunications Network Society*.

Hukum ini adalah standar dasar untuk keamanan informasi di Jepang dan hukum lain yang berkaitan harus sesuai dengannya.

Tabel 14. Hukum Terkait Keamanan Informasi di Jepang

Undang-undang	Target Industri	Target Peraturan	Hukuman
Unauthorized Computer Access Law	Semua industri	Tindakan yang membantu akses tidak sah dan memberikan informasi ID orang lain tanpa pemberitahuan	
Act on the Protection of Personal Information	Usaha swasta yang menggunakan informasi pribadi untuk tujuan bisnis	Manajemen informasi privasi (alamat, nomor telepon, *e-mail*, dll)	Hukum pidana, denda
Act on Electronic Signatures and Certification		Fasilitasi *e-commerce* yang mengambil manfaat dari Internet dan aktivitas ekonomi melalui jaringan	

Tabel 15. Hukum Terkait Keamanan Informasi di UE

Undang-undang	Rincian
A Common Regulatory Framework (Directive 2002/21/EC)	• Memberikan kerangka kerja pengaturan jaringan dan layanan telekomunikasi • Bertujuan untuk melindungi privasi melalui jaringan komunikasi yang aman
EU Directive on Data Protection (Directive 1995/46/EC)	• Pedoman pemrosesan dan penghapusan informasi pribadi • Hukum dasar yang menetapkan tanggung jawab negara anggota dan pengakuan kewenangan penuh individu atas informasi pribadi • Lebih ketat daripada standar AS
EU Directive on Electronic Signatures (Directive 1999/93/EC) *EU Directive on Electronic Commerce (Directive 2000/31/EC)*	• Mengatur penggunaan tanda tangan elektronik • Mengatur pelaksanaan *e-commerce*
Cybercrime Treaty	• Perjanjian internasional paling komprehensif mengenai *cybercrime*; mendefinisikan secara rinci semua aksi kriminal menggunakan Internet beserta dendanya
Data Preservation Guideline on Communication and Networks	• Mensyaratkan penyedia layanan komunikasi untuk mempertahankan data panggilan dari enam bulan sampai 24 bulan (diumumkan sesudah serangan teroris di Madrid tahun 2004 dan London tahun 2005)

Tabel 16. Hukum Terkait Keamanan Informasi di AS

Undang-undang	Target Industri	Target Peraturan	Hukuman
Federal Information Security Management Act of 2002	Lembaga administratif federal	Informasi lembaga administratif, sistem TI, program keamanan informasi	-
Health Insurance Privacy and Accountability Act of 1996	Lembaga kesehatan dan penyedia layanan kesehatan	Data elektronik berisi informasi kesehatan seseorang	Hukum pidana, denda
Gramm-Leach-Bliley Act of 1999	Lembaga keuangan	Privasi informasi konsumen	Hukum pidana, denda
Sarbanes-Oxley Act of 2002	Perusahaan terdaftar pada *Stock Exchange of USA*	Kontrol internal dan catatan keuangan publik	Hukum pidana, denda
California Database Security Breach Information Act of 2003	Lembaga administratif dan perusahaan swasta di California	Informasi privasi terenkripsi	Denda dan pemberitahuan pada korban

(v) Pengalokasian anggaran untuk pelaksanaan kebijakan informasi

Pelaksanaan kebijakan membutuhkan biaya. Tabel 17 menunjukkan anggaran keamanan informasi di Jepang dan AS di tahun-tahun belakangan ini.

Tabel 17. Anggaran Perlindungan Informasi di Jepang dan AS

Jepang	2004	2005
Total anggaran tahunan	JPY 848.967.000.000.000	JPY 855.195.000.000.000
Anggaran keamanan informasi	JPY 267.000.000.000	JPY 288.000.000.000
Persentase dari total anggaran	0,03%	0,03%
AS	2006	2007
Total anggaran tahunan	USD 2.709.000.000.000	USD 2.770.000.000.000
Anggaran keamanan informasi	USD 5.512.000.000	USD 5.759.000.000
Persentase dari total anggaran	0,203%	0,208%

Latihan

Jika negara Anda memiliki kebijakan keamanan informasi, lacak perkembangan-nya dari sisi lima aspek formulasi kebijakan keamanan informasi yang dijelaskan di atas. Artinya, jelaskan:

1. Arah kebijakan
2. Organisasi keamanan informasi
3. Kerangka kerja kebijakan
4. Hukum yang mendukung kebijakan keamanan informasi
5. Alokasi biaya untuk keamanan informasi

Jika negara Anda belum memiliki kebijakan keamanan informasi, uraikan kemungkinan dari masing-masing lima aspek di atas dalam menyusun kebijakan. Gunakan pertanyaan-pertanyaan berikut sebagai panduan:

1. Apa yang seharusnya menjadi arah kebijakan keamanan informasi di negara Anda?
2. Bagaimana pengaturan organisasi yang harus ditempatkan? Organisasi mana yang perlu dilibatkan dalam pengembangan kebijakan keamanan informasi dan implementasinya di negara Anda?
3. Apa permasalahan khusus yang harus diatasi oleh kerangka kerja kebijakan?
4. Hukum apa yang harus ditetapkan dan/atau dicabut untuk mendukung kebijakan informasi?
5. Apa pertimbangan anggaran yang harus diperhatikan? Dari mana sebaiknya dana didapatkan?

Peserta pelatihan dari negara yang sama dapat melakukan kegiatan ini bersama-sama.

7.3 Implementasi/Pelaksanaan Kebijakan

Implementasi kebijakan keamanan informasi yang lancar membutuhkan kerjasama antara pemerintah, swasta dan agen internasional. Gambar 23 menunjukkan area spesifik implementasi kebijakan informasi dimana kerjasama sangat penting.

Gambar 23. Area Kerjasama dalam Implementasi Kebijakan Keamanan Informasi

Pengembangan kebijakan keamanan informasi

Tabel 18 memperlihatkan bagaimana pemerintah, sektor swasta dan organisasi internasional dapat berkontribusi pada pengembangan kebijakan keamanan informasi nasional.

Tabel 18.
Contoh Kerjasama dalam Pengembangan Kebijakan Keamanan Informasi

Sektor	Kontribusi pada Pengembangan Kebijakan
Pemerintah	• Organisasi perencanaan dan strategi nasional: memastikan kecocokan kebijakan informasi dengan rencana nasional • Organisasi TIK: memastikan kerjasama pembentukan standar teknologi keamanan informasi nasional • Organisasi analisis tren keamanan informasi: menggambarkan analisis dan tren keamanan domestik dan internasional dalam kebijakan • Organisasi analisis hukum: memeriksa kecocokan antara kebijakan keamanan informasi dan hukum yang ada • Organisasi informasi nasional: kerjasama dalam penentuan arah dan penetapan strategi • Lembaga investigasi: kerjasama dalam pemrosesan insiden keamanan

Sektor swasta	• Perusahaan konsultasi keamanan informasi: menggunakan agen profesional dalam penyusunan kebijakan keamanan informasi • Laboratorium teknologi keamanan informasi swasta: membentuk standar teknologi yang terkait dengan keamanan informasi • Departemen keamanan informasi di perguruan tinggi: memberikan keahlian dalam formulasi kebijakan
Organisasi internasional	• Memastikan pemenuhan standar kebijakan nasional • Kerjasama penanganan ancaman dan insiden internasional

Manajemen dan perlindungan infrastruktur informasi dan komunikasi

Penggunaan informasi yang efektif (pengumpulan, pemeliharaan, dll) membutuhkan administrasi dan perlindungan infrastruktur TI yang tepat. Sebuah kebijakan keamanan informasi yang baik tidak akan bermanfaat jika tidak didukung infrastruktur TI yang baik.

Manajemen dan perlindungan infrastruktur informasi dan komunikasi yang efektif membutuhkan kerjasama antara jaringan, sistem dan manajer bidang TI. Kerjasama institusi publik dan swasta juga memberikan manfaat (Tabel 19).

Tabel 19. Contoh Kerjasama dalam Administrasi dan Perlindungan Infrastruktur Informasi dan Komunikasi

Sektor	Kontribusi pada Administrasi dan Perlindungan Infrastruktur Informasi dan Komunikasi
Sektor pemerintah	• Organisasi yang terkait dengan jaringan informasi dan komunikasi: menentukan komposisi dan tingkat keamanan jaringan informasi dan komunikasi nasional • Laboratorium teknologi informasi dan komunikasi: menyebarkan standar publik dan mengadopsi teknologi yang berguna
Sektor swasta	• Penyedia ISP: kerjasama dalam komposisi jaringan informasi dan komunikasi nasional • Laboratorium teknologi informasi dan komunikasi: memberikan layanan pengembangan teknis dan bekerjasama dalam operasi teknologi keamanan dan infrastruktur informasi dan komunikasi yang stabil
Organisasi internasional	• Kerjasama dengan organisasi standar teknologi internasional untuk informasi dan komunikasi internasional, dan pengamanan teknologi informasi baru

Pencegahan dan penanganan terhadap ancaman dan insiden

Penanganan secara efektif terhadap ancaman dan gangguan keamanan informasi membutuhkan kerjasama diantara organisasi informasi nasional,

lembaga investigasi dan institusi hukum, serta organisasi yang melakukan inspeksi insiden keamanan dan mengestimasi kerusakan. Juga perlu untuk bekerjasama dengan organisasi yang mampu menganalisis kerentanan secara teknis dan memberikan langkah penanganan teknis.

Tabel 20.
Contoh Kerjasama dalam Menangani Insiden Keamanan Informasi

Sektor	Kontribusi
Organisasi pemerintah	• Organisasi penanganan insiden keamanan: memberikan analisis situasi, menangani insiden *hacking*, dan teknologi untuk menangani pelanggaran dan insiden • Organisasi informasi nasional: menganalisis dan menginspeksi keamanan informasi yang terkait dengan pelanggaran dan insiden • Lembaga investigasi: bekerjasama dengan organisasi yang terlibat dalam penahanan dan penuntutan pelanggar • Organisasi yang memberikan evaluasi keamanan: menguji keamanan dan kehandalan produksi jaringan informasi dan keamanan informasi • Organisasi pendidikan keamanan informasi: menganalisis penyebab insiden keamanan informasi dan mendidik masyarakat untuk mencegah terulangnya insiden
Kelompok swasta	• Organisasi penanganan insiden swasta: memberikan dukungan penanganan dan teknis • Lembaga investigasi swasta: bekerjasama dengan lembaga investigasi pemerintah
Organisasi internasional	• Dalam kasus insiden dan ancaman internasional, melapor dan bekerja sama dengan Interpol, CERT/CC

Pencegahan insiden keamanan informasi

Pencegahan pelanggaran dan kecelakaan keamanan informasi mencakup pengawasan, pendidikan dan manajemen perubahan. CSIRT nasional merupakan organisasi pengawas utama. Hal yang penting adalah menyesuaikan kebijakan informasi dan pengawasan data sesungguhnya. Jadi, penting untuk membicarakan lingkup pengawasan kebijakan informasi. Lebih lanjut, penting untuk mendidik pegawai pemerintah dan sektor swasta, serta masyarakat umum, mengenai kebijakan keamanan informasi. Mungkin diperlukan untuk mengubah beberapa sikap terhadap informasi dan perilaku yang berdampak pada keamanan informasi. Pendidikan dan manajemen perubahan keamanan informasi ditentukan dalam US SP 800-16 (*Information Technology Security Training Requirements*).

Tabel 21. Contoh Kerjasama dalam Pencegahan Pelanggaran dan Insiden Keamanan Informasi

Sektor	Koordinasi
Organisasi pemerintah	• Agen pengawasan: pengawasan jaringan berkelanjutan dan deteksi ancaman keamanan yang lebih canggih • Agen pengumpulan: berbagi informasi dengan organisasi internasional dan situs-situs keamanan • Institusi pelatihan: pelatihan simulasi secara rutin untuk mengembangkan kemampuan untuk menangani pelanggaran dan kecelakaan keamanan informasi dengan cepat
Organisasi swasta	• Penyedia ISP, kontrol keamanan dan perusahaan anti-virus: menyediakan statistik lalu lintas, informasi jenis serangan dan profil *worm*/virus
Organisasi internasional	• Memberikan informasi jenis serangan, profil *worm*/virus, dan lain-lain

Keamanan privasi

Dibutuhkan kerjasama untuk membangun langkah perlindungan privasi Internet, pencegahan insiden informasi lokasi pribadi, perlindungan informasi biologis pribadi, dan pelaporan pelanggaran privasi.

Tabel 22. Contoh Koordinasi dalam Perlindungan Privasi

Sektor	Koordinasi
Lembaga pemerintah	• Organisasi analisis sistem: melakukan bisnis berkaitan dengan informasi lokasi pribadi, dan analisis tren dalam perlindungan informasi pribadi internal dan eksternal • Organisasi perencanaan: meningkatkan hukum/sistem, langkah teknis/administratif dan manajemen standar • Dukungan teknis: koordinasi sertifikasi pengguna *cyber* untuk bisnis • Organisasi pelayanan: kerjasama dukungan untuk penanganan pelanggaran privasi dan *spam*
Organisasi swasta	• Organisasi keamanan informasi pribadi: pendaftaran persyaratan dan mengatur asosiasi kerjasama untuk keamanan informasi pribadi • Konsultasi keamanan informasi pribadi
Organisasi Internasional	• Bekerja sama untuk menerapkan standar keamanan informasi pribadi internasional

Kerjasama internasional

Keamanan informasi tidak dapat dicapai melalui usaha satu negara saja karena pelanggaran keamanan informasi cenderung berlingkup internasional. Jadi, kerjasama internasionl dalam perlindungan keamanan informasi, baik di sektor pemerintahan maupun swasta, harus dilakukan.

Untuk sektor swasta, organisasi internasional yang relevan untuk promosi dan perlindungan keamanan informasi adalah CERT/CC. Untuk pemerintah, ENISA (untuk UE) dan ITU bertujuan untuk menumbuhkan kerjasama keamanan informasi diantara banyak negara.

Di setiap negara harus terdapat institusi pemerintah yang berperan untuk membantu kerjasama organisasi pemerintah dan swasta dengan lembaga dan institusi internasional.

Latihan

1. Identifikasi lembaga pemerintah dan organisasi swasta di negara Anda yang perlu bekerjasama dalam implementasi kebijakan keamanan informasi nasional. Identifikasi juga organisasi internasional yang perlu diajak bekerjasama.

2. Untuk setiap bidang kerjasama dalam implementasi kebijakan informasi seperti terlihat pada Gambar 23, tentukan aksi atau aktivitas spesifik yang lembaga dan organisasi ini dapat lakukan.

Peserta pelatihan dari negara yang sama dapat melakukan kegiatan ini bersama.

7.4 Peninjauan dan Evaluasi Kebijakan Keamanan Informasi

Langkah terakhir dalam penyusunan kebijakan keamanan informasi adalah mengevaluasi kebijakan dan melengkapi bidang yang kurang dikembangkan. Revisi kebijakan adalah penting sesudah efisiensi kebijakan keamanan informasi telah ditentukan.

Metode evaluasi kebijakan domestik dapat diterapkan untuk menentukan efisiensi kebijakan keamanan informasi nasional. Aspek-aspek metode ini dibahas di bawah ini.

Penggunaan organisasi audit

Terdapat organisasi yang berperan melakukan penilaian dan evaluasi kebijakan. Organisasi tersebut harus melakukan audit rutin terhadap kebijakan keamanan infomasi nasional. Lebih lanjut, organisasi ini harus independen dari organisasi penyusun kebijakan keamanan informasi dan organsasi yang menerapkannya.

Revisi kebijakan keamanan informasi

Area permasalahan biasanya teridentifikasi selama audit kebijakan. Perlu ada proses merevisi kebijakan untuk mengatasi area masalah tersebut.

Perubahan dalam lingkungan

Penting untuk bereaksi secara sensitif terhadap perubahan dalam lingkungan kebijakan. Perubahan yang timbul dari ancaman (serangan) internasional dan kerentanan, perubahan infrastruktur TI, perubahan tingkatan informasi penting, dan perubahan penting lainnya harus segera tercermin dalam kebijakan keamanan informasi nasional.

Ujian

1. Bagaimana tahapan yang berbeda dari daur hidup kebijakan keamanan informasi mempengaruhi satu sama lain? Dapatkah Anda melewati tahapan? Jelaskan!

2. Mengapa kerjasama antar berbagai sektor penting dalam pengembangan dan implementasi kebijakan keamanan informasi?

BACAAN TAMBAHAN

Butt, Danny, ed. 2005. *Internet Governance: Asia-Pacific Perspectives.* Bangkok: UNDP-APDIP. http://www.apdip.net/publications/ict4d/igovperspectives.pdf.

CERT. CSIRT FAQ. Carnegie Mellon University. http://www.cert.org/csirts/csirt_faq.html.

CERT. Security of the Internet. Carnegie Mellon University. http://www.cert.org/encyc_article/tocencyc.html.

Dorey, Paul dan Simon Perry, ed. 2006. *The PSG Vision for ENISA*. Permanent Stakeholders Group. http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

ESCAP. Module 3: Cyber Crime and Security. http://www.unescap.org/icstd/POLICY/publications/internet-use-for-business-development/module3-sources.asp.

Europa. Strategy for a secure information society (2006 communication). European Commission. http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

Information and Privacy Office. 2001. Privacy Impact Assessment: A User's Guide. Ontario: Management Board Secretariat. http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

Information Security Policy Council. *The First National Strategy on Information Security*. 2 Februari 2006. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf.

ISO. ISO/IEC27001:2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.

ITU dan UNCTAD. 2007. Challenges to building a safe and secure Information Society. In *World Information Society Report 2007*, 82-101. Geneva: ITU. http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/report.html.

ITU-D Applications and Cybersecurity Division. ITU National Cybersecurity / CIIP Self-Assessment Tool. ITU. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

Killcrece, Georgia. 2004. *Steps for Creating National CSIRTs*. Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle dan Mark Zajicek. 2003. *Organizational Models for Computer Security Incident Response Teams (CSIRTs).* Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive/pdf/03hb001.pdf.

OECD. 2002. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. Paris: OECD. http://www.oecd.org/dataoecd/16/22/15582260.pdf.

OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

Shimeall, Tim dan Phil Williams. 2002. *Models of Information Security Trend Analysis*. Pittsburgh: CERT Analysis Center. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.11.8034.

The White House. 2003. *The National Strategy to Secure Cyberspace*. Washington, DC: The White House. http://www.whitehouse.gov/pcipb.

CATATAN UNTUK INSTRUKTUR

Seperti tertulis di bagian 'Tentang Seri Modul', modul ini dan modul lainnya dalam seri ini dirancang untuk tetap bernilai bagi pembaca yang beragam dengan latar belakang kondisi negara yang bermacam-macam. Modul ini dirancang untuk dipresentasikan, seluruhnya atau sebagian, dalam berbagai cara, baik *online* maupun *offline*. Modul ini dapat dipelajari oleh seseorang atau kelompok di lembaga pelatihan maupun kantor pemerintah. Latar belakang peserta dan durasi dari sesi pelatihan akan menentukan tingkat kedalaman dari isi presentasi.

'Catatan' ini menawarkan pada instruktur beberapa ide dan saran untuk penyajian isi modul dengan lebih efektif.

Pengaturan Sesi

Sesi 90 menit

Berikan gambaran umum mengenai konsep dasar dan standar atau prinsip internasional dari keamanan informasi dan perlindungan privasi (Bagian 1 dan 5 modul ini). Tekankan kebutuhan kebijakan keamanan informasi dan perlindungan privasi yang efektif dan tepat.

Sesi tiga jam

Bagi sesi menjadi dua bagian. Di bagian pertama, fokus pada konsep dasar dan tren dalam keamanan informasi, termasuk deskripsi analisis tren ancaman keamanan informasi (Bagian 2). Di bagian kedua, fokus pada konsep dasar dan prinsip perlindungan privasi, lakukan diskusi isu-isu yang berdampak terhadap perlindungan privasi, dan jelaskan secara ringkas penilaian dampak privasi.

Sesi satu hari penuh (enam jam)

Setelah menjelaskan konsep dan prinsip keamanan informasi dan perlindungan privasi, fokus pada pengembangan kebijakan keamanan informasi dan implementasinya (Bagian 7). Anda dapat memulainya dengan bertanya kepada peserta tentang implikasi kebijakan dari prinsip-prinsip keamanan informasi dan perlindungan privasi. Lalu sajikan secara singkat daur hidup kebijakan keamanan informasi sebelum fokus pada proses perumusan kebijakan. Peserta dari negara yang memiliki kebijakan keamanan informasi dapat diminta untuk menilai kebijakannya terkait prinsip dan proses yang telah dibahas, sementara mereka yang dari negara tanpa kebijakan keamanan informasi mungkin diminta untuk menuliskan beberapa aspek kebijakan tersebut (lihat aktivitas belajar pada akhir Bagian 7.2).

Sesi dua hari

Hari pertama dapat diisi seperti penjelasan di atas, sementara hari kedua dapat berfokus pada aktivitas dan metodologi keamanan informasi (Bagian 3 dan 4), khususnya pada pembentukan CSIRT (Bagian 6). Contoh-contoh dari negara lain dapat dipotong, dan peserta perlu didorong untuk menentukan model CSIRT yang paling tepat dan mendesain mekanisme intervensi keamanan sesuai dengan konteks nasional mereka.

Interaktivitas

Penting untuk mendapatkan interaksi dari peserta dan melakukan latihan praktik. Modul ini memberikan banyak informasi berguna tetapi peserta pelatihan perlu mampu unutk menganalisis secara kritis informasi yang diberikan dan menerapkannya ketika informasi tersebut berguna. Beberapa studi kasus diberikan di modul ini dan, jika memungkinkan, perlu dibahas dalam hal konsep dan prinsip keamanan informasi. Akan tetapi, para peserta juga perlu didorong untuk menggali isu-isu dan masalah otentik dalam keamanan informasi dan perlindungan privasi sesuai dengan konteks mereka.

TENTANG KISA

Korea Information Security Agency **(KISA)** dibentuk pada tahun 1996 oleh pemerintah sebagai lembaga yang bertanggung jawab untuk promosi penyusunan kebijakan yang efisien untuk peningkatan keamanan informasi di seluruh negara. Fungsinya mencakup pencegahan dan penanganan pelanggaran Internet, penanganan *spam*, perlindungan privasi, verifikasi tanda tangan elektronik, perlindungan infrastruktur penting, evaluasi keamanan untuk produk keamanan informasi dan dukungan industri, pengembangan kebijakan dan teknologi yang mendalam, dan peningkatan kesadaran untuk membentuk masyarakat informasi yang aman dan terpercaya.

UN-APCICT

The United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT) adalah bagian dari *the United Nations Economic and Social Commission for Asia and the Pacific* (ESCAP). UN-APCICT bertujuan untuk memperkuat upaya negara-negara anggotanya untuk menggunakan TIK dalam pengembangan sosio-ekonomi melalui peningkatan kapasitas individu dan institusi. UN-APCICT berfokus pada tiga pilar, yaitu:

1. Pelatihan. Untuk meningkatkan pengetahuan TIK dan keahlian dari penyusun kebijakan dan profesional TIK, dan memperkuat kapasitas instruktur TIK dan institusi pelatihan TIK;
2. Penelitian. Untuk melakukan studi analisis terkait dengan pengembangan sumber daya manusia TIK; dan
3. *Advisory*. Untuk memberikan layanan pemberian pertimbangan terkait program-program pengembangan sumber daya manusia untuk anggota ESCAP.

UN-APCICT berlokasi di Incheon, Republik Korea.

http://www.unapcict.org

ESCAP

ESCAP adalah bagian dari PBB untuk pengembangan kawasan. ESCAP berperan sebagai pusat pengembangan sosial dan ekonomi PBB di kawasan Asia dan Pasifik. Tugasnya adalah menggalang kerjasama diantara 53 anggota dan 9 *associate members*. ESCAP menyediakan hubungan strategis antara program di level negara maupun global dengan isu-isu yang berkembang. ESCAP mendukung pemerintah negara-negara di kawasan dalam konsolidasi posisi kawasan dan memberikan saran dalam mengatasi tantangan sosio-ekonomi di era globalisasi. Kantor ESCAP berlokasi di Bangkok, Thailand.

http://www.unescap.org

Seri Modul Akademi Esensi TIK untuk Pimpinan Pemerintahan

Penyunting: Shahid Akhtar dan Patricia Arinto

Modul 1 – Kaitan antara Penerapan TIK dan Pembangunan yang Bermakna

Modul 2 – Kebijakan, Proses, dan Tata Kelola TIK untuk Pembangunan

Modul 3 – Penerapan *e-Government*

Modul 4 – Tren TIK untuk Pimpinan Pemerintahan

Modul 5 – Tata Kelola Internet

Modul 6 - Keamanan Jaringan dan Keamanan Informasi dan Privasi

Modul 7 - Teori dan Penerapan Manajemen Proyek TIK

Modul 8 – Alternatif Pendanaan Proyek-proyek TIK untuk Pembangunan

http://www.unapcict.org/academy