Kontra Intelijen dan Keamanan Intelijen dalam Bisnis dan Pemerintahan

Pengungkapan informasi yang bersifat selektif tentang informasi itu sendiri merupakan sebuah sumber daya krusial yang dimiliki sebuah perusahaan dalam mengambil tindak-langkah kompetitif. Pengungkapan sebuah informasi hanya boleh dilakukan sebagai bagian integral dari strategi kompetitif.

PERISAI EMAS DAN PERISAI PENGGENTAR

Berbeda dengan serangan ke Pelabuhan Dieppe yang membawa sial pada 1941, lokasi pendaratan di Normandia adalah sebuah rahasia yang terjaga dengan rapi. Konsensus mengenai opini para ahli adalah bahwa Sekutu dan Inggris secara khusus telah melakukan pekerjaan yang luar biasa dalam mengalihkan perhatian arah serangan ke Calais dan bukan ke Normandia. Tanpa adanya informasi maju pada masa itu mengenai lingkup dan lokasi yang tepat dari serangan, Jerman gagal menggerakkan arsernal tempurnya ke Normandia guna melancarkan serangan balasan terhadap pendaratan tersebut serta mencegah Sekutu memperoleh tempat berpijak di benua Eropa.

Definisi

Kontra intelijen adalah sebuah perisai protektif berlapis-majemuk yang menyembunyikan kelemahan Anda, yang berkat pengetahuan terhadap kelemahan tersebut, dapat memanfaatkannya dengan biaya dari pihak Anda. Ia juga

dapat digunakan untuk membatasi pengungkapan kekuatan Anda bagi mereka yang perlu mengetahuinya. Ia adalah proses defensif yang terus berlangsung, yang dengannya sebuah organisasi "melakukan pengamatan ke dalam melalui lensa-lensa musuh" guna menghambat pengungkapan kegiatan mata-mata ekonomi, cyber, dan industrial, pengungkapan terhadap pelarian bakat, penyuapan, terorisme, gangguan, kelalaian, pemaparan yang berlebih-lebihan, akuisisi gelap terhadap hak-milik di bidang informasi serta terhadap risiko-risiko keamanan lainnya.

Sayang sekali, sering terjadi, baru setelah timbul kesalahan, kontra intelijen mendapat perhatian dan sesudah itu, hanya karena kontra intelijen praktis terabaikan, maka timbul kesalahan dalam hal-hal di atas. Guna memayunginya dari para mata-mata, tamu-tak-diundang, *hakckers*, dan pencuri, organisasi-organisasi membelanjakan $78 miliar setahun untuk bidang keamanan, dan dari jumlah tersebut $7 miliar untuk perlengkapan dan piranti keras komputer. Namun kebanyakan kebocoran intelijen serta pelanggaran keamanan dapat dilacak pada sebab-sebab manusiawi di dalam organisasi.

Dalam tulisan ini diketengahkan dua sasaran komplementer. Pertama, kita akan menggunakan contoh-contoh untuk mengingatkan risiko aktual yang bahkan mempengaruhi perusahaan yang dijalankan secara paling baik. Kedua, kita akan memberikan sebuah peta jalan mengenai tindakan-tindakan spesifik yang dapat diambil guna memayungi sebuah organisasi dari kemungkinan terkena risiko-risiko semacam itu. Uraian selanjutnya akan menguji isu-isu implementasi yang dikaitkan dengan usaha memelihara para sekutu yang kuat serta mengemudikan organisasi untuk menjauh dari keputusan yang terdorong oleh peristiwa-peristiwa kejutan.

BAGAIMANA ORGANISASI YANG BAIK KEHILANGAN INTELIJEN

Slogan dalam Perang Dunia II "bibir terbuka, kapal tenggelam" mencerminkan perintah pertama dari kontra intelijen ini. Pemeriksaan terbaik serta perintah dari intelijen kompetitif menjadi tak berguna jika organisasi Anda atau para pemasoknya membocorkan intelijen serta kemampuan yang dicapai dengan susah payah kepada para pesaing. Ini adalah sebuah pelajaran yang dipelajari oleh Microsoft, IBM, dan

Gillette dalam bertarung melawan Oracle, Fujitsu, dan Bic. Mari kita amati para predator, sumber-sumber kebocoran, dan beberapa kasus dalam kehidupan nyata.

Predator

Beberapa perusahaan menggunakan mata-mata yang menyamar sebagai para pembeli guna mengumpulkan informasi mengenai para pesaing. Yang lainnya bergerak lebih jauh dengan mendirikan perusahaan pembersih-kantor bersertifikat-ISO serta asosiasi nirlaba guna mendapatkan akses ke dalam laboratorium dari para pesaingnya. Perusahaan-perusahaan telepon milik pemerintah di seluruh dunia secara rutin mengintersepsi panggilan-telepon, pengiriman faks, informasi tentang tukar-menukar data elektronik, (data tentang pajak, penawaran, kontrak, dan harga-harga). Para diplomat, pegawai negeri sipil, dan eksekutif bisnis memanfaatkan hubungan yang dipeliharan dengan cermat serta transaksi bisnis resmi sebagai tindak penyamaran terhadap pertemuan intelijen klandestin.

Sumber-sumber dan Garis Penyebaran Kebocoran

Pergantian para staf serta kegiatan keseharian sebuah bisnis dapat menjadi penyebab kebocoran informasi konfidensial. "Ketika dilakukan dengan bebas, pengungkapan yang terkontrol terkadang dapat melayani kepentingan korporat. Namun ketika pengungkapan itu dilakukan tanpa sadar dalam arus bisnis yang biasa, maka sebuah perusahaan akan kehilangan kemampuan kompetitifnya. Kebanyakan rahasia perusahaan diperoleh secara resmi. Membuka bagian atas dari sumber-sumber dapat berupa pengungkapan yang eksesif terhadap pemerintah (file korporat), para staf (*internal newsletter*), media (*press release*, briefing mendadak), penerbit urusan perdagangan, bank, perwakilan kredit (*Standar & Poor's, Dun & Bradstreet*), serta pihak-pihak ketiga lainnya yang menyebarkan kebocoran intelijen ini. Pelaku kejahatan dalam proses ini dapat berupa orang yang tidak tahu, yang lalai, orang yang tidak terpisahkan, buruh yang tidak puas atau ragu-ragu, para klien, vendor, mitra kerja, dan mantan pegawai.

Kasus mengenai anggota Angkatan Darat yang tidak puas, Aaron R. Eden, sudah umum diketahui. Dengan menggunakan sebuah alat berupa *remote control* Back Orifice 2000 di rumahnya,

Eden berhasil mencuri kata-sandi (*password*) beserta piranti lunak komputer, dan mengubah ribuan catatan mengenai anggota militer di dalam komputer yang terdapat di *Enlisted Records and Evaluation Center* dari Angkatan Darat AS di Indianapolis. "Dalam menyiapkan kasusnya melawan Eden, unit kejahatan komputer memperlihatkan bahwa pihak swasta tertentu telah menghidupkan sistem jaringan, seakan-akan ia adalah si pengatur sistem, dengan menghapus file-file personal ketika si pengatur sistem tersebut tidak berada di dalam gedung. Teknologi yang digunakan untuk mengumpulkan bukti ini meliputi penerapan undang-undang EnCase, yang memungkinkan para agen rahasia men-*scan hard* drives. Pada hakikatnya, unit kejahatan teknologi informasi (IT) melancarkan serangan terkontrol atas jaringan wilayah lokal (*local area network* – LAN), guna melihat bagaimana insiden itu terjadi. Sebagai tambahan, para agen investigatif sama prihatinnya terhadap serangan yang dilancarkan dari dalam seperti halnya serangan yang dilancarkan para *hackers* dari luar."

"Kini, tidak ada suatu perwakilan manapun yang bisa kebal terhadap serangan *hacker*, seperti Eden, yang sabar, berdedikasi dan penuh keahlian secara teknologis. Dan, di tangan korporasi yang bersifat terlarang, di tangan para sindikat kriminal, atau negara-negara yang menjadi musuh, teknik-teknik seperti yang telah digunakan Eden dapat membawa seluruh departemen, bahkan seluruh kota dan negara untuk bertekuk lutut.

Menyelam dengan Membawa Barang Kotor: Bagaimana Pihak Lawan secara Nyaman Memetakan Bisnis Anda Berdasarkan Segumpal Kecil Emas di dalam Keranjang Sampah Anda

Setiap orang yang memiliki satu jalur bebas-biaya untuk mendapatkan laporan bulanan terinci mengenai nomor telepon dari pembicaraan yang masuk ditambah ringkasan dan rincian pembayaran. Kebanyakan organisasi hanya memperhatikan lembaran ringkasan dengan catatan yang harus dibayar. Daftar rincian dapat melebihi 500 halaman dan umumnya dibuang ke keranjang sampah dengan pengandaian ongkos setiap panggilan telepon itu teramat murah. Namun daftar itu menjadi sangat informatif bagi pesaing Anda, yang tidak akan perlu bersusah payah untuk mendapatkannya.

Sebagai tambahan terhadap pemberian nomor telepon kepada para pelanggan Anda, maka daftar ini adalah sebuah potret dari pola bisnis Anda. Bahkan jika kertas sampah tersebut memang dimaksud untuk dirobek-robek, staf Anda, petugas kebersihan kantor, staf angkutan jarak-jauh terkadang bisa menawarkan ribuan dolar hanya untuk meng-kopi daftar tersebut sebelum dibuang ke keranjang sampah.

Oracle pernah menyamarkan para agen untuk mengumpulkan kertas sampah Mircrosoft dari tempat pembuangan sampah. Ketika kejadian ini terungkap, Oracle tidak mengingkarinya. Dalam kasus lainnya, seorang diplomat Eropa tertangkap-tangan membawa berkantong-kantong sampah dari seorang eksekutif teknologi-tinggi yang berkediaman di Houston.

Bahkan secara teknis, mungkinlah untuk mengumpulkan sampel DNA dari kertas tisu yang sudah digunakan di dalam keranjang sampah – dan dari segi hukum tidak ada apa pun yang bisa mencegahnya.

Ilustrasi berikut ini memperlihatkan hingga sejauh mana seseorang perlu waspada baik di tempat kerja maupun di rumah.

Perangkap yang Bisa Dicegah namun Mahal Harganya bila Diabaikan

Kontra intelijen juga berarti memasang mata pada sekutu-sekutu strategis serta membentuk tindak pengamatan mendasar guna menguragi risiko. Coba perhatikan keadaan menyedihkan dari Xillix, British Columbia, yang gagal melakukannya.

"Xillix, sebuah perusahaan BC di bidang peralatan medis, menjalin persekutuan strategis dengan Olympus Optical dari Jepang pada awal 1990-an dan mengungkapkan semua rahasia dagang mereka. Tanpa diketahui pihak manajemen Xillix, Olympus mendaftar sejumlah hak-paten Jepang berdasarkan teknologi yang menjadi milik Xillix. Baru pada 1998, Xillix menemukan hal ini ketika sebuah hak paten Olympus di AS diterbitkan. Sekalipun Xillix memenangkan gugatan hukum berikutnya, perusahaan tersebut nyaris bangkrut. Sebuah usaha intelijen-kompetitif yang sederhana tentu saja sudah bisa memberikan peringatan dini, karena aplikasi hak paten Jepang ini sudah diterbitkan bertahun-tahun sebelumnya."

Hotel dan Tempat-tempat Pertemuan: Ranjang Hangat untuk

Kebocoran

Sementara petugas kebersihan hotel tengah mempersiapkan kamar Anda, para agen yang menyamar, dengan berpura-pura sebagai tamu, dapat mengakses tempat ini bahkan mengecek isi tas Anda. FBI menasihati para eksekutif untuk bepergian dengan bagasi ultra-ringan dan selalu menjaga agar dokumen berharga itu senantiasa berada dalam pengawasan dan bisa dijangkau. Mereka sebaiknya tidak menerima fax, atau menyebutkan nama perusahaan mereka, terutama di hotel-hotel di luar negeri. Lokasi sensitif lainnya termasuk meja-meja restoran bahkan kursi pesawat terbang yang bisa tersadap.

Sebagai ilustrasi, Hewlett-Packard secara kebetulan menemukan adanya peluncuran sebuah produk baru yang kompetitif dari seorang pegawai hotel yang mem-booking sebuah konferensi yang disiarkan secara nasional dari pesaingnya. Contoh ini menegaskan bahwa sebaiknya menggunakan kode untuk nama atau menggunakan pihak ketiga dalam merencanakan fungsi-fungsi dan pertemuan strategis.

Pengunjung yang Ramah dengan

Agenda Terselubung

"Perusahaan juga harus membatasi akses ke tempat-tempat di mana rahasia perdagangan disimpan, dan di mana pemrosesan konfidensial dijalankan. Salah satu perusahaan yang mengakui kebocoran dalam rencana keamanan korporatnya adalah W.K.Kellogg Co. dari Battle Creek, MI. Perusahaan ini bermaksud menghentikan praktik yang berlangsung 18 tahun, yakni melakukan kegiatan tour publik ke pabrik-pabriknya, ternyata konsultan keamanan menemukan mata-mata dari produsen sereal Eropa ikut dalam tour ke pabrik tersebut. Kellogg merasa pasti bahwa mereka tengah mengamati metode-metode manufaktur."

Peter Schweitzer menggambarkan beberapa kasus mata-mata ekonomi yang dilancarkan sekutu AS dengan targetnya pada korporasi AS. Dari antaranya, kunjungan seorang ahli kimia, dengan misi intelijen tersamar ke perusahaan DuPont. Orang ini "dengan kurang hati-hati" mencelupkan "ujung dasinya ke dalam lemak komponen kimia. Terlepas dari protesnya atas nilai sentimental dasi tersebut, pegawai DuPont menuntut bahwa sang tamu tersebut harus menyerahkan dasinya kepada perusahaan."

Memasang Iklan untuk Jabatan yang Tidak Ada

Majalah *Fortune* mengungkapkan praktik yang dilakukan Hotel Marriott dengan memasang iklan untuk jabatan yang tidak ada dan mewawancarai para manajer dari jaringan-jaringan hotel pesaing untuk mendapat intelijen mengenai penghasilan dan bonus, latihan, serta praktik-praktik manajemen lainnya. Dalam usaha mereka untuk mendapatkan orang berbakat, beberapa manajer bahkan bergerak lebih jauh seperti yang dianjurkan Leonard Condezio:

"Anda membaca sebuah kisah sukses dalam jurnal dagang dan Anda terkesan. Bukannya menunggu hingga orang yang diinginkan itu melamar pekerjaan, tetapi menelpon, dan mengatakan, 'Hei, ngomong-ngomong, saya baru saja membaca tentang Anda; Anda melakukan pekerjaan yang baik. Apakah Anda ingin berbicara dengan kami mengenai suatu kemungkinan di masa depan?' Ketika mendengar tentang sebuah perubahan keorganisasian, maka coba pertimbangkan untuk mengontak seorang anggota staf ... coba tanyakan apakah mereka senang dengan perubahan ... 'Saya telah menemui Anda beberapa waktu lalu dan saya merasa terkesan. Saya sadar bahwa sudah terjadi sebuah perubahan, dan jika hal itu tidak berjalan baik sebagaimana yang Anda harapkan, silakan telepon saya jika Anda merasa tertarik untuk datang bergabung dengan kami.' Anda menyadari bahwa seseorang baru saja mempunyai seorang bayi, membeli sebuah rumah baru, mobil baru, dan sedang membayar uang sekolah anak-anaknya di perguruan tinggi. Mungkin Anda merasa dapat menawarkan kualitas hidup yang lebih baik, atau paket bonus yang lebih baik, kompensasi yang lebih baik, dan bahwa Anda mempunyai sebuah pekerjaan yang masih terbuka. Silakan telepon orang-orang yang pernah bekerja, mungkin Anda dapat menawarkan sesuatu yang lebih memikat, dan mereka akan datang kepada Anda dengan enthusiasme yang besar. Apa pun kasusnya: merger, pembelian seluruh saham, atau sebuah manajemen baru yang diambil alih perusahaan. Tindakan-tindakan ini mendatangkan perubahan, yang berarti pula sebuah peluang bagi Anda. Ini sekadar cara lain untuk mencari orang (tenaga kerja)."

Ancaman yang Semakin Meningkat: Lap Top dan PDA Anda

Pada Juli 2001, FBI melaporkan kehi-

langan 184 laptopnya termasuk 13 yang dicuri. "Sekurang-kurang satu dari laptop tersebut, dan mungkin sekali empat dari antaranya mengandung informasi yang terklasifikasi. Setelah dua tahun, Departemen Energi dan Departemen Dalam Negeri melakukan pengungkapan yang sama."

Di London, sebuah tabloid ditawari dokumen rahasia tingkat tinggi mengenai pesawat tempur *stealth* yang terdapat dalam sebuah laptop yang tertinggal di stasiun keretaa api Inggris. Kementerian Pertahanan Inggris melaporkan bahwa rata-rata 50 buah laptop lenyap setiap tahun, umumnya terjadi di dalam angkutan umum. Hingga pada 2002, laptop milik Kementerian Pertahanan Inggris dengan informasi yang terklasifikasi dibawa dalam tas kantor yang dilengkapi piranti yang dapat menghapus naskah pada hard disk ketika pengunciannya dipaksakan atau ketika laptop itu dibuka tanpa kata sandi yang benar.

Sebagai tambahan, "perusahaan-perusahaan telah melaporkan penggangsiran rumah, di mana komputer-komputer laptop atau disket-disket dicuri, bahkan disket-disket itu bisa diperoleh dengan mudah, termasuk bahan-bahan yang jauh lebih berharga dalam lingkup yang sama. Contoh-contoh ini tidak selalu dilaporkan atau melulu dilaporkan sebagai kejahatan mengganggsir rumah, tanpa mempertimbangkan kemungkinan bahwa targetnya lebih kepada informasi daripada alat perlengkapan." Seorang konsultan GE *Power Systems* ditahan karena mencuri satu bilah turbin gas serta informasi rahasia yang termasuk dalam "kumpulan besar dari disket komputer, buku panduan, *notebook* dan artikel-artikel ilmiah."

Di Amerika Utara, lebih dari 200 *palm top* dan 60 laptop lenyap setiap hari di restoran, bandara, hotel, taksi, dan stasiun kereta api. Dalam 95% dari kasus tersebut, informasi yang terkandung di dalam *hard drive* dapat dibaca dalam tempo bebeberapa detik hanya dengan menggunakan *Actives routine* yang dapat mengabaikan pemakaian kata sandi. Namun terdapat sejumlah besar produk murah dan peralatan preventif yang dapat mencegah pengungkapannya oleh pihak yang tidak resmi. Ini mencakup penguncian fisik (*Microsaver, Kryptonite*), detektor gerak (*Spy, sonicLock*), dan sirene tersembunyi seperti *BlackIce, Defender, LapTrak, CyberAnger*, dan *Computrace* yang dapat menghubungkan mesin yang hilang tersebut dengan si pemiliknya, si produsen alat atau *provider* piranti lu-

nak yang dapat menyiagakan polisi atau pihak militer. Banyak mesin yang disesuaikan dengan produk ini telah ditemukan kembali dari para pencuri.

DI MANA MENEMUKAN KEAHLIAN YANG ANDAL

Pemerintah

Contoh-contoh di atas tidak berdiri sendiri. Setiap orang tahu mengenai kebocoran atau penggarongan yang mempengaruhi bisnis dan pemerintah. Para ahli kontra intelijen dan *American Society of Information Security* (ASIS) menunjukkan bahwa penyerobotan di bidang keamanan yang tidak diketahui pihak perusahaan jauh melampaui kasus-kasus yang dilaporkan dengan rasio 15 berbanding 1 pada perusahaan-perusahaan yang lalai, dan keadaan ini pun tidak lebih baik dengan rasio 3 berbanding 1 pada perusahaan-perusahaan yang dijalankan dengan teramat baik.

Untunglah, pasar dan beberapa lembaga perwakilan pemerintah menawarkan bantuan tak ternilai yang dapat menurunkan rasio tersebut, dalam bebebera kasus, atas dasar pemulihan biaya (terutama di bidang-bidang yang sangat sensitif seperti IT).

Di Kanada, *Communications Security Establishment* (CSE) menawarkan semacam seni keahlian di bidang keamanan IT secara komersial. Di R & D dan keamanan nasional, CSE bekerja sama dengan Perwakilan Keamanan Nasional (*National Security Agency* – NSA) dan Kelompok Keamanan Komunikasi Elektronik (*Communication-Electronics Security Group* – CESG), rekannya dari Inggris. Ketiganya adalah pemimpin dunia di bidang konektivitas keamanan – kriptografi (mengamankan telekomunikasi, mengamankan aplikasi Web, e-mail dan komputer) serta keamanan radiasi (Tempest). Sekalipun misi utama IT difokuskan kepada pemerintah dan keamanan di bidang pertahanan, CSE memberikan jasa konsultasi, latihan, perkiraan mengenai mudahnya terjadi kebocoran serta bantuan teknik di bidang perlindungan informasi dan keamanan IT terhadap produsen perlengkapan, pengembang piranti-lunak, bank, dan perusahaan lainnya.

Eksekutif Kontra Intelijen Nasional (*National Counterintelligence Executive* – NCIX) memberikan laporan mengenai metode yang digunakan para agen asing guna mendapatkan hak-milik intelektual korporat AS secara gelap. Lem-

baga ini juga merumuskan langkah-langkah defensif yang diterapkan oleh perwakilan pemerintah untuk melawan kegiatan-kegiatan semacam itu. FBI secara rutin memberikan e-mail melalui ANSIR, sebuah komponen dari Sistem Peringatan Terhadap Ancaman Nasional (*the National Threat Warning System* – NTWS). Lembaga ini memberikan latihan mengenai kesadaran akan ancaman serta langkah-langkah yang digunakan untuk melindungi kekayaan intelektual dari akuisisi gelap. Pusat Perlindungan Infrastruktur Nasionalnya membantu perusahaan-perusahaan AS untuk melacak dan dan menghukum para pencurinya di seluruh dunia.

Kantor Intelijen dan Analisis Ancaman (*Intelligence and Threat Analysis* – ITA) dari Departemen Luar Negeri Amerika Serikat menjaga sebuah portal perubahan elektronik yang tidak terklasifikasi untuk menggambarkan lebih dari 50.000 kasus ancaman dari luar negeri dan informasi lainnya yang berkaitan dengan keamanan. CIA dan DOD melakukan perkiraan risiko dan dan memberikan sesi briefing mengenai perjalanan yang bersifat defensif, praktik-praktik pengumpulan intelijen, dan mengenai piranti keras serta piranti lunak yang digunakan oleh berbagai negara serta para pengunjung yang memasang target mereka pada pengetahuan dan teknologi Amerika Serikat. DOD menjalankan program untuk langkah-langkah kontra keamanan dan menerbitkan *Security Awareness Bulletin* serta video *Counting Espionage*.

Dinas Intelijen Keamanan Kanada (*the Canadian Security Intelligence Service*– CSIS) memberikan contoh-contoh serta daftar yang berguna mengenai indikator yang mencurigakan dari kegiatan mata-mata ekonomi.

MITRE adalah sebuah organisasi kelas dunia nirlaba yang melayani bidang pertahanan, pemerintahan, dan organisasi nirlaba AS. Lembaga ini memberikan solusi berskala luas mengenai kebutuhan akan keamanan informasi. Contoh-contohnya mencakup kebijakan keamanan, latihan, analisis risiko, database yang aman, autentifikasi jaringan, serta keamanan Internet. MITRE telah menciptakan Felt, sebuah bahasa untuk mempelajari tingkah laku dan para penjaga keamanan. Lembaga ini juga mengoperasikan pusat-pusat R & D untuk Departemen Pertahanan, Administrasi Penerbangan Federal, dan Jawatan Pajak (*Internal Revenue Service*). Teknologi "pemetaan yang cepat" dari MITRE telah digunakan sehari-hari di

Ground Zero untuk "memungkinkan orang menyelamatkan para kru dalam melokalisasi api, kaleng-kaleng kimia, serta bahan berbahaya lainnya termasuk reruntuhan gedung" untuk memfasilitasi keamanan dan pemulihan yang cepat.

Solusi Konsultasi DuPont memberikan akses eksklusif kepada kepemimpinan global E.I. du Pont de Nemours dan pengalaman unik di dalam perlindungan hak milik intelektual dan fisik. Misinya adalah untuk berbagi pengetahuan dengan para klien yang terakreditasi yang jadi sumber pengetahuan perusahaan induk, dengan praktik-praktik terbaik dan keselamatan dalam keamanan intelijen.

Solusi Keamanan Global IBM memberikan keamanan yang bersifat maju, serta menghasilkan piranti lunak keamanan dan jasa konsultasi. Sebagai tambahan terhadap jaringan dunia yang luas dari 3.000 ahli keamanan dan insinyur, IBM memiliki lebih dari 100 tenaga ahli riset dalam bidang teknologi yang berkaitan dengan keamanan yang bekerja di lab-lab keamanan dan pusat-pusat keahlian yang berkaitan dengan keamanan. IBM juga menjadi mitra Kroll, sebuah provider global yang menonjol dalam kaitan dengan manajemen risiko dan jasa kontra intelijen, untuk menilai keamanan infrastruktur IT, kegiatan mata-mata, intrusi-cyber, risiko gangguan bisnis, dan kemampuan pemulihan matapetaka.

Solusi Keamanan Terintegrasi merupakan sebuah pemimpin di bidang pengembangan dan dan pengiriman sistem keamanan akses fisik yang terintegrasi. Pemasangannya dilakukan di bandara, kedutaan, lembaga pertahanan, perusahaan *high-tech*, New York *Stock Exchange* dan beberapa institusi keuangan.

Keamanan RSA (*RSA Security*) memberikan solusi *e-security* termasuk autentifikasi, otorisasi, penulisan kode rahasia, serta sistem manajemen kunci publik. Kofenrensi RSA-nya merupakan kriptografi yang menonjol serta peristiwa yang berkaitan dengan keamanan data di muka bumi.

Para penjahit dari Kelompok Konsultasi Phoenix mengintegrasikan intelijen bisnis yang kompetitif dengan program kontra intelijen berdasarkan kebutuhan-kebutuhan khusus dari setiap klien yang menggunakan metode yang efektif, legal, dan etis.

ThunderStore memusatkan perhatian-

nya pada ancaman dari para pemakai yang terpercaya, entah mereka itu pegawai yang lalai, kurang cermat, yang tidak puas, atau para sekutu. Lembaga ini memberikan solusi untuk menghadapi ancaman dari dalam melalui penanganan akses secara elektronik serta memonitor penggunakan sumber daya digital (file, aplikasi, protokol komunikasi), serta proses bisnis, melakukan dokumentasi atas tingkah laku si pemakai, serta memastikan penyelesaiannya dengan kebijakan keamanan-intelijen. Pendekatan terhadap keamanan intelijen merupakan hal yang berlapis-majemuk. Sebagai tambahan terhadap tindakan penggunakan komputer secara tidak sah, terhadap penyalinan dan manipulasi file serta dokumen, *ThunderStore* juga memungkinkan penulisan dokumen secara rahasia, dan ini termasuk salah satu dari berbagai opsi.

Rpost adalah sebuah e-mail baru serta pelayanan registrasi dokumen elektronik yang menggunakan proses yang tidak terlihat baik oleh si pengirim maupun si penerima. Sebagai suatu badan penengah yang independen, Rpost menawarkan sistem keamanan pengiriman pesan "yang bisa dilacak, yang transparan dan kebal terhadap suap" guna melindungi si pengirim.

Pada waktunya yang tepat, intelijen tentang aktivitas kriminal dan keselamatan publik dapat menyelamatkan kehidupan manusia. Kode 9-1-1 yang diperkuat adalah sebuah sistem yang dikenal untuk meningkatkan efektivitas polisi serta pelayanan darurat lainnya secara otomatis dan cepat dengan mendapatkan si penelepon secepat mungkin begitu telepon berdering, bahkan jika si penelepon menggantungkan telepon sebelum melakukan kontak apa pun dengan *call center*. Kode 9-1-1 yang berlawanan adalah sistem jiplakan yang lebih baru, yang meningkatkan arus intelijen dari polisi dan perwakilan keselamatan-publik lainnya untuk kembali kepada komunitas. Kode ini memberikan data intelijen melalui e-mail, voice mail atau fax kepada tetangga dan para pelanggan dengan kebutuhan tertentu. Kode 9-1-1 yang berlawanan tersebut haruslah menjadi bagian integral dari sistem pencegahan risiko, dari setiap lembaga penerapan undang-undang, dari setiap pemakaian, agen pengirim, fasilitas Puskesmas dan setiap perusahaan yang menangani produk potensial yang bersifat merusak (makanan, narkoba, bahan kimia) atau lokasi-lokasi yang berisiko tinggi.

Pelayanan Darurat CML adalah sebuah pemimpin dunia dalam memberikan

sistem telekomunikasi dan pengiriman radio kepada *call center* 9-1-1 dan kepada Titik-titik Jawaban Keselamatan Publik lainnya. Perlengkapannya menangani *call centers* 9-1-1 di seluruh dunia. Dengan lebih dari 900 lokasi yang terdapat hanya di AS, CML memiliki intelijen yang luas untuk membantu lembaga penerapan hukum serta organisasi-organisasi dengan kepentingan terkait dalam tindak pengamanan keselamatan publik dan dalam kesiapannya secara tepat untuk menangani insiden-insiden yang bersifat darurat.

Mendapatkan Intelijen Murah

Sebuah badan independen, Federasi Para Ilmuwan Amerika, memberikan tips dan jaringan kepada perwakilan intelijen pemerintah di seluruh dunia.

Beberapa situs memberikan sebuah forum bebas kepada konsumen dan para pembeli korporat untuk menerbitkan dan memberikan pandangan tentang keberatan mereka mengenai produk dan pelayanan. Sebagian membayar *royalty* berdasarkan tingkat keseringan akses terhadap keberatan yang diterbitkan.

Seperti yang dipakai dalam komunitas kontra intelijen, *Cyberalert*, *Spyonit*, dan *Ad Facts* merupakan jasa pelayanan riset elektronik gratis.

Akhirnya, Leonard Fuld menawarkan sebuah kepustakaan yang luas dan "webliografi" mengenai untelijen kompetitif maupun jasa kontra intelijen.

PETA JALAN KONTRA INTELIJEN

Risiko-risiko Target

Pengamatan kontra intelijen haruslah mencakup jumlah para pemilih dan elemen-elemen yang gampang terkena risiko yang tersebar di seluruh rantai nilai Anda. Jumlah para pemilih ini meliputi pelanggan sekarang dan terdahulu, para pemasok, staf, mitra bisnis, dan para musuh yang mencakup para pesaing yang bertarung menurut aturan permainan, hingga kelompok fanatik bawah-tanah yang tidak melakukannya.

20 Langkah Praktis untuk Membentuk Kontra Intelijen di Sepanjang Rantai Nilai Anda

Idealnya, kontra intelijen ditanamkan di seluruh rantai nilai Anda. Ini berarti bahwa ada penjagaan konstan terha-

dap front-front berikut ini:

1. Belajarlah tentang senjata dan praktik-praktik kontra intelijen. Berkonsultasilah dengan *web sites* yang direkomendasikan, termasuk Dinas Rahasia AS: *web page* berjudul *The Best Praktices for Seizing Electronic Evidence.*

2. Berkonsultasilah dengan *provider* demikian pula dengan para pemimpin intelijen dalam pimpinan perusahaan yang sejalan dengan cara berusaha dan rekam-jejak (*track record*) yang bersifat etis, dan dalam beroperasi di tengah medan persaingan yang tidak kompetitif dan tidak saling berhubungan.

3. Definisikan properti yang bernilai (entah itu bersifat fisik, intelektual, atau maya). Tinjau kembali kebijakan untuk pengungkapan informasi dan asset yang bersifat visibel. Pastikan bahwa semua asset korporat, termasuk informasi yang bersifat-terbuka, disesuaikan dengan kebijakan terbaru. Dokumentasikan secara sistematis pengetahuan rahasia dan hal yang berkaitan dengannya untuk mendapat peraturan perlindungan kekayaan intelektual.

4. Identifikasikan target-target kontra intelijen, yakni, setiap orang yang kepentingan terkaitnya adalah memperoleh keuntungan dari kemudahan mendapatkan akses yang tidak sah ke kekayaan intelektual dan kekayaan fisik, atau merusak kedudukan Anda terhadap para klien, mitra, staf, dan jumlah konstituen lainnya. Seberapa banyak mereka telah tahu tentang Anda dan bagaimana mereka telah mendapatkannya? Identifikasikan sasaran-sasaran terbaru serta sasaran pengumpulan intelijen yang masuk akal berkaitan dengan target-target di atas. Berapa banyaknya nilai dolar dari sikap-membisu Anda serta asset-asset intelijen eksplisit yang berharga bagi musuh?

5. Definisikan hal-hal yang gampang terkena bencana secara struktural: Bagaimana lingkungan hidup Anda (yakni lokasi, industri, keadaan tetangga, iklim kerja) menghasilkan satu risiko yang ditargetkan dan/atau risiko jaminan. Kemudahan terkena bencana timbul bersamaan dengan ketidakpuasan karyawan, komunikasi yang tidak memadai serta kepemimpinan yang buruk. Tanpa mencari tahu akar permasalahan dari ketidakpuasan serta tanpa menjaga

iklim kerja yang positif, maka kegiatan kontra intelijen paling banter hanya akan memberikan hasil marginal. Bahkan lebih buruk lagi, hasil-hasil itu bisa menimbulkan gejolak, terutama jika tidak terdapat transparansi, atau tidak terdapatnya kepercayaan para staf. Perhatikan bahwa standar yang tinggi dari *privacy* atau perlindungan data personal termasuk di antara prasyarat untuk membangun kredibilitas dan kepercayaan.

6. Identifikasikan hal-hal yang gampang menimbulkan bencana pada sumber daya manusia, yakni orang yang gampang terkena risiko di halaman belakang Anda dan motivasi potensial mereka (keserakahan, kecanduan narkoba atau berhutang, keadaan di masa lampau, dan tingkah laku yang aneh). Identifikasikan titik-titik yang paling lemah dalam rantai pasokan Anda dalam hubungan dengan para pelanggan Anda. Amati agen intelijen yang terlatih baik yang dapat melamar pekerjaan di perusahaan Anda dan/atau orang berkedok sebagai klien, pemasok, atau wakil media yang resmi. Para calon ini tidak memperlihatkan ciri pembawaan para staf yang gampang terkena risiko. Mereka akan bekerja keras untuk memadukannya dengan komunitas, mendapatkan kepercayaan dari sang majikan atau mendapatkan kontak bisnis dan mengumpulkan intelijen yang bersifat eksplisit atau rahasia. Organisasi-organisai yang memimpin industri mereka terkadang dengan tidak diketahui justru menjadi mangsa dari para agen ini yang beroperasi secara rahasia demi persaingan atau demi musuh-musuh yang lain.

7. Lacaklah jalur-jalur yang bisa terpantau dari staf Anda, yang mungkin mencakup pekerjaan, rumah pribadi, tempat-tempat pribadi, hotel dan sebagainya. Ingat bahwa intelijen yang berharga bisa ditemukan kembali oleh Oracle dari tempat sampah di rumah-rumah pribadi dari staf Microsoft. Juga lakukan perjalanan dengan beban yang ringan dan selalu jaga agar dokumen dan data berharga selalu ada dalam pandangan atau jangkauan.

8. Pelihara dan monitor buku harian mengenai interaksi terpadu antara organisasi Anda dan semua stakeholder, termasuk para pengunjung di dalam web site Anda. Beginilah caranya bagaimana Microsoft mampu untuk merekonstruksi inkubasi se-

rangan atas "pengingkaran pelayanan" yang mematilemaskan portalnya pada 25 Januari, 2001.

9. Gunakan sistem operasi yang diperkuat dari segi keamanan, seperti SE Linux, yang "memberikan sebuah mekanisme untuk memaksakan pemisahan informasi berdasarkan tuntutan akan kerahasiaan dan integritas. Ini memungkinkan kita untuk bisa mendapatkan ancaman merusak dan mem-*bypass* aplikasi mekanisme keamanan serta memungkinkan persempitan bahaya yang bisa disebabkan oleh aplikasi yang jahat atau cacat.

10. Ambil tindak langkah perlawanan untuk mendeteksi dan mencegah kegiatan mata-mata elektronik seperti halnya modifikasi yang tidak sah, desktruksi dan substitusi dari komponen jaringan dan informasi Anda. Perhatikan bahwa pesaing Anda, para agen asing dan para calo intelijen bisa menemukan cara halus untuk masuk ke dalam dasar pemikiran Anda dan menyembunyikan perlengkapan mata-mata elektronik yang kuat dalam ruang konferensi atau bahkan di kamar mandi. Mereka juga secara legal dapat memperoleh gambaran satelit yang akurat dengan tingkat resolusi yang kurang dari satu meter untuk mengamati instalasi Anda, tempat parkir, tempat pemuatan barang, dan armada truk ke tempat tujuan. Gambar dari satelit komersial IKONOS dan stelit DK Rusia kini dijual untuk perusahaan-perusahaan kecil dan koperasi pertanian.

11. Ambil langkah pamungkas untuk mencegah perusakan asset-asset dan rahasia bisnis (misalnya piranti lunak intelijen yang kompetitif, data, daftar, rencana, peralatan, pengetahuan teknik, sistem, jaringan telekomunikasi, *web sites*, praktik-praktik dan teknologi). Tempatkan para penjaga atau pembawa asset jauh dari pelayanan intelijen yang bersifat bermusuhan serta agen-agen risiko-keamanan (misalnya orang, penyakit komputer, virus, kuda Troya, mata-mata elektronik, steganografi). Untuk para anggota staf yang bisa diminta memberikan *password* di bawah paksaan, berikanlah *password* alternatif yang dapat membunyikan alarm.

12. Semai dan sebarkanlah asset-asset yang berbasiskan pengetahuan (misalnya intelijen perdagangan, kode-kode sumber, kertas bekas, metodo-

logi proses) di sejumlah lokasi dan tim yang aman untuk mengurangi risiko dari akses total, kontaminasi atau kerugian. Latihan penyemaian harus disesuaikan dengan tututan hukum terhadap sebuah perintah pengadilan untuk "menghentikannya" seandaikan ini diperlukan.

13. Coba pertimbangkan hambatan hukum dan etnis, para pelacak dan sarana untuk mengatasi manuver, untuk melakukan diskolasi, untuk mengamati dan melakukan kerusakan sebagai tindakan kompensatif terhadap para pengganggu. Lakukanlah hal itu terutama terhadap para pesaing besar yang ingin menyelinap ke dalam, merampok kekayaan perusahaan atau berkolusi dengan orang-dalam. Sistem ini harus dapat beroperasi secara rahasia guna mengintersepsi serangan para predator selagi masih dalam taraf inkubasi.

Jika Anda mencurigai sebuah akses yang tidak resmi di dalam data Anda, kertas bekas, transmisi fax, atau sistem e-mail, maka sebarkanlah kertas-kertas yang tidak terpakai, komunikasi faks, dan e-mail dengan jebakan informasi untuk memprovokasi tindakan pelacakan. Inilah caranya bagaimana sebuah bank Swiss menemukan dan menggagalkan skema perdagangan orang-dalam. Para staf dari sebuah biro Eropa dari *Los Angeles Times* melakukan hal yang sama ketika *log system* mengungkapkan akses ke e-mail mereka pada saat mereka sendiri tidak ada di tempat. Si pelaku kejahatan, yakni seorang korespoden senior asing, membaca sebuah e-mail palsu yang dikirimkan kepada rekannya di kantor yang lain. Lantaran tidak sadar akan operasi rahasia, ia mengangkat isu-isu palsu tersebut yang berakibat pada pemecatannya.

14. Coba hindari untuk melakukan transaksi dan komunikasi sensitif dengan menggunakan laptop, hp, atau alat-alat yang bisa diletakkan di tangan, kecuali jika alat-alat tersebut bersertifikat dan kebal terhadap pencangkokan. Guna memastikan agar informasi rahasia tetap tidak bisa ditembus oleh pihak yang tidak sah, gunakan protokol penulisan rahasia yang andal untuk mendukung transaksi antara media penyimpanan, tempat penyembunyian, *motherboard*, serta komunikasi yang menggunakan kabel atau tanpa kabel. Pertimbangkan juga kartu ketaatan-Fortezza untuk mengamankan sis-

tem penyampaian pesan.

15. Gunakan skenario perencanaan, simulasi, *brainstorming*, untuk memerankan sang pengacara jahat dengan menuliskan serial langkah-langkah potensial dari para pesaing serta para pemain yang menjadi lawan, mantan karyawan yang menggerutu, dan mantan mitra kerja. Dalam kasus-kasus besar yang menjadi taruhan ini, sering berharga untuk bertanya kepada eksekutif yang telah pensiun dari para pesaing atau ahli strategi perang, ahli hukum yang berpengalaman, serta para pembuat film untuk terus membayangi musuh yang tengah bermunculan. Dalam praktik konsultasi kami, kami telah melakukan kontes penulisan naskah di kalangan anggota tim dari pelbagai klien untuk mendapatkan pengamatan ke dalam pikiran dari masing-masing pesaing tersebut, entah secara langsung ataupun tidak langsung.

Pada era 1980-an, Alcan cukup intens untuk memenangkan pasar Ontario bernilai $70 juta untuk *pop can*. Pihak eksekutif Alcan menekankan pada simulasi tidak hanya menyangkut strategi para pesaing langsung seperti Alcoa, Pechiney, dan Kaiser, tetapi juga para pesaing tidak langsung seperti para produsen gelas, plastik, dan baja (Selco dan Dofaco), dan bahkan "musuh di tingkat akar rumput" seperti Pollution Probe.

Diciptakan pada 1999 dengan hibah selama 5 tahun dari Angkatan Darat AS, *Institute for Creative Technology* (ICT) di Universitas *South California* (USC) merupakan pusat riset simulasi yang paling maju "dalam memadukan manusia virtual di dalam peran kunci sebagai pelaku, seraya memainkan peran sebagai kekuatan yang bersahabat atau yang bermusuhan. Setelah serangan pada 11 September, "spesialis intelijen pemerintah secara rahasia telah mengumpulkan skenario para teroris dari pembuat dan penulis skenario film top dari Hollywood.

16. Latihlah para staf dan sekutu terdekat untuk memanfaatkan sistem sosial yang dimaksudkan untuk membangun dan memelihara pusat intelijen. Peringatkan setiap orang tentang peluang-peluang yang memungkinkan perusahaan yang tak etis melakukan kegiatan mata-mata industri, termasuk memasang iklan karier palsu hanya demi mempero-

leh intelijen kompetitif dari para pelamar yang tak berdosa.

17. Siapkan rencana pemulihan malapetaka dan rencana-rencana pengganti terbaru.

18. Bendunglah risiko-risiko yang masih tersisa.

19. Pastikan bahwa CEO sering menekankan jaringan vital antara keunggulan mutu, keamanan intelijen, dan kontra intelijen. Bahkan Departemen Energi, tempat terdapatnya keamanan tertinggi, "telah menekankan keunggulan itu secara memadai dalam kualitas kerja ilmiah dan kerja teknisnya, namun baru belakangan ini saja menekankan keamanan, dan baru dalam beberapa waktu terakhir mengartikulasikan pentingnya kontra intelijen.

20. Pastikan bahwa kontra intelijen merupakan sebuah investasi berharga yakni bahwa ia menjadi subjek perbaikan konstan. Lakukan audit reguler dan perkiraan mengenai kemudahan terkena serangan guna memastikan bahwa langkah ini melekat pada garis besar pedoman di atas. Persempitlah wawasan dan portofolio pemberian tugas melalui pemangkasan yang terus menerus guna memusatkan perhatian pada sasaran yang memberikan hasil besar. Bandingkan selalu harga dari kontra intelijen dengan kerusakan yang bisa dicegahnya.

RINGKASAN

Organisasi-organisasi harus mulai dengan membentuk kebijakan kontra intelijen, membangun kesadaran dan menyewa orang terpercaya yang mempraktikkan pencegahan di tempat kerja dan di tempat lain. Mempraktikkan keamanan intelijen berarti menggunakan teknologi Web-yang-aman, menyebarkan file-file, direktori cetakan, serta dokumen-dokumen konfidensial. Buatlah video-recording menyangkut semua yang keluar masuk secara konstan di tempat kerja. Perkokoh langkah-langkah balasan. Bayangi terus aktivitas musuh. Tentukan batas tanggung jawab. Pasanglah jejak langkah virtual dan *auto-dialing chip* pada perlengkapan industri yang mahal dan piranti keras komputer. Juga penting untuk mengkomunikasikan strategi yang dapat berlaku sebagai penggentar pada agen-agen risiko potensial.

KESIMPULAN

Seperti halnya intelijen kompetitif, kontra intelijen adalah misi penting bagi setiap organisasi. Dua-duanya harus menjadi bagian integral dari budaya dan strukturnya. Namun dalam kebanyakan organisasi, hanya sedikit pegawai memiliki keahlian dalam intelijen kompetitif, dan jauh lebih kurang lagi yang memiliki keahlian dalam kontra intelijen. Banyak pihak yang hanya bertindak untuk merespons peristiwa-peristiwa mengejutkan, lantas melakukannya dengan tergesa-gesa. Namun pengetahuan praktis mengenai disiplin dapat menjadi signifikan dan bernilai tinggi dalam mencegah atau menangani risiko sebagaimana ilustrasi yang dianjurkan dalam buku ini.

Sejumlah klien di sektor keuangan dan teknologi tinggi telah menemukan bahwa hanya dengan bersandar pada perkerjaan para ahli merupakan halnya merugikan dan tidak praktis. Mereka menemukan logika "mengajarkan orang untuk memancing ikan" dalam kontra intelijen sebagai langkah yang paling efektif menuju keuntungan mekanis pemanfaatan waktu dan usaha dari beberapa ahli dengan kemampuan inti di bidang ini.❑

(Diindonesiakan oleh Frans Kl.)