

Recognized Security Organization :
**Menanti Kepastian
 Pemerintah**

MEMBANGUN SISTEM keamanan di pelabuhan tidaklah semudah yang diduga. Pelabuhan-pelabuhan Indonesia lahir dan berkembang dari pola kehidupan masyarakat tradisional, di mana pelabuhan merupakan tempat untuk mencari penghidupan. Oleh karenanya, ketika sebuah pelabuhan menerapkan keamanan ketat pada tempat-tempat khusus, warga masyarakat yang selama ini mencari penghidupan di pelabuhan harus menyingkir.

Desain keamanan di pelabuhan kini tidak lagi menjadi monopoli kerja pemerintah atau operator pelabuhan semata. Berdasarkan regulasi yang ditetapkan oleh *International Maritime Organization*, pelabuhan berskala internasional dan kapal-kapal dengan bobot di atas 500 gros ton harus memiliki

sertifikat ISPS Code sebagai standar keamanan yang diakui bersama. Pelabuhan dan kapal-kapal berukuran besar ini dapat memperoleh sertifikat ISPS Code apabila lolos dalam proses verifikasi yang dilakukan oleh Dirjen Perhubungan Laut sebagai wakil pemerintah.

Sebelum proses verifikasi dilakukan maka pihak operator pelabuhan dan kapal akan mengundang perusahaan-perusahaan konsultan keamanan untuk mendesain keamanan pelabuhan dan kapal. Konsultan-konsultan inilah yang dikenal dengan nama *Recognized Security Organization (RSO)*. Sejauh ini di Indonesia ada sekitar 28 perusahaan yang memiliki izin sebagai RSO dalam tiga gelombang penerbitan izin. Izin perusahaan sebagai RSO hanya berlaku untuk dua tahun saja. Setelah dua tahun

pemerintah akan mempertimbangkan apakah perlu atau tidak untuk memperpanjang izin RSO perusahaan.

Walpon Silitonga, *Marine and Insurance Manager* PT. Superintending Company of Indonesia (Sucofindo), menjelaskan bahwa, jumlah RSO yang memegang kontrak sebagai konsultan keamanan hanya sedikit. Ada RSO yang memiliki proyek konsultasi keamanan sama sekali, sementara ada RSO proyeknya banyak. Oleh karena itu, ketika izin mayoritas RSO habis tahun 2006, ia memperoleh informasi bahwa hanya ada empat RSO mengajukan permohonan perpanjangan izin sebagai RSO. "ISPS Code memerlukan audit satu kali dalam lima tahun. Jika RSO tidak ada proyek, pasti

bangkrut. Karena dia harus tunggu lima tahun lagi," tambahnya.

Max Kasengkang, Director RSO PROTECOM, menilai bahwa pemerintah dalam hal ini Dirjen Perhubungan Laut perlu menilai ulang dari hasil evaluasi pemberian izin selama dua tahun tersebut. Perusahaannya memperoleh izin sebagai RSO sewaktu Dirjen Perhubungan Laut membuka gelombang ketiga bagi perusahaan-perusahaan yang ingin mengajukan izin sebagai RSO. PROTECOM sendiri, lebih dikenal sebagai perusahaan jasa keamanan di Indonesia.

Keinginan perusahaan-perusahaan jasa keamanan untuk terjun menjadi RSO menjadi fenomena menarik. Max Kasengkang mengungkapkan setidaknya ada tiga perusahaan jasa keamanan yang terjun sebagai RSO selain PROTECOM. Ia menilai, kemampuan dan pengalaman perusahaan-perusahaan jasa keamanan dalam kegiatan pengamanan fisik merupakan nilai tambah bagi perusahaan jasa keamanan untuk ikut berkecimpung

menjadi RSO. Walpon Silitonga juga menilai perusahaan jasa keamanan memiliki kelebihan dalam hal *intelligence* dan *security design*. "Tetapi fokusnya tetap pada *inspection, supervision, testing, dan assessment* di pelabuhan. Apakah mereka sanggup mengerjakan tugas-tugas tersebut?" tambahnya.

Sucofindo sendiri telah menjadi konsultan keamanan di sejumlah pelabuhan khusus, pelabuhan umum, dan kapal dagang internasional. Ketika ditanyakan mengenai dominasi RSO BUMN dalam proyek-proyek konsultan keamanan di pelabuhan, Max Kasengkang hanya mengangkat bahu sambil berkata bahwa, kemungkinan dominasi RSO BUMN dalam proyek-proyek konsultan keamanan cukup tinggi. Akan tetapi Walpon Silitonga membantah adanya kemungkinan tersebut. "Klien kami mayoritas swasta yang mengelola pelabuhan khusus. Kami harus ikuti proses tendernya. Tidak pernah kami menerima perlakuan istimewa. Semua harus *fight!*" ungkapnya.

Potensi bisnis bagi RSO di Indonesia sebenarnya cukup besar. Indonesia sebagai negara maritim tentunya memerlukan pelabuhan-pelabuhan dagang yang disinggahi oleh kapal-kapal dagang internasional. Akan tetapi besarnya potensi ini baru dapat dirasakan jika audit eksternal dilaksanakan setahunnya. ISPS Code mengatur kewajiban audit eksternal sebanyak satu kali dalam lima tahun. Akan tetapi pemerintah Indonesia kini tengah mempersiapkan regulasi yang mewajibkan adanya audit eksternal setiap 2,5 tahun. Perkembangan ancaman keamanan aksi terorisme yang terus berubah setahunnya tentu memerlukan pembaharuan atau variasi sistem keamanan agar pelabuhan tidak dengan mudah ditembus oleh pelaku kejahatan atau teroris. Tentunya memiliki kewajiban moral untuk mengikuti perkembangan situasi ancaman di lokasi klien-klien mereka (SJ)

Security Journal

FORMULIR BERLANGGANAN

Kepada

PT Indosearch Media Pratama

Fortune Building lantai 1

Jl. Mampang Prapatan 96

Jakarta Selatan

Telp/Fax: (021) 7948718

Kami bermaksud berlangganan Security Journal

Nama Lengkap :

Perusahaan :

Alamat Perusahaan :

Telp. :

Faksimili :

email :

Paket Berlangganan :

3 bulan Rp. 75.000 6 bulan Rp. 150.000

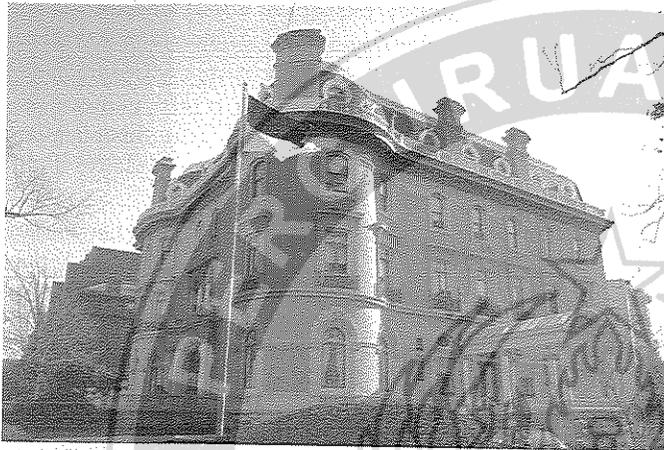
12 bulan Rp. 300.000 24 bulan Rp. 600.000

Versi : Indonesia

Inggris

Gratis pengiriman dalam wilayah Jabodetabek
 Ongkos Kirim : Jawa - Bali Rp. 5.000
 Luar Jawa Rp. 12.000

Pengamanan Kantor Pemerintah



PERISTIWA KEMALINGAN tidak saja terjadi di Istana Presiden beberapa waktu lalu, tapi juga merembet ke berbagai kantor pemerintahan lain. Sebagai contoh beberapa minggu sebelum ini pembobolan berlangsung di lantai 2 dan 6 Departemen Luar Negeri. Selain itu, pencurian juga menimpa gedung Mahkamah Agung (MA) ditandai dengan raibnya berkas dokumen perkara korupsi seberat ± 15 kg yang dikirim dari Pengadilan Negeri Limboto Gorontalo. Tak luput pula, pencurian di pelataran parkir Gedung Dewan Perwakilan Rakyat Daerah (DPRD) DKI Jakarta, di mana seorang staf Komisi Pemilihan Umum DKI Jakarta kehilangan *laptop* yang berisi berkas pemilihan kepala daerah di Jakarta dan sejumlah barang lainnya di dalam mobil yang diparkir di situ. Di samping itu masih banyak kasus sejenis yang terjadi di berbagai kantor pemerintah dengan tingkat kerugian berskala kecil yang sejauh ini tidak dilaporkan pada pihak berwajib.

Berbagai kejadian ini menimbulkan pertanyaan bagaimana bentuk pengamanan yang dilakukan pada kantor-kantor pemerintah? Berbagai jawaban muncul, salah satunya dari aparat keamanan setempat, seperti dituturkan

salah satu kepala keamanan internal Mahkamah Agung (MA) bahwa tenaga pengamanan yang ada di MA jauh dari ideal, sulit memenuhi penjagaan selama 24 jam jika tenaga pengamanan sangat terbatas. Tidak hanya persoalan tenaga pengamanan, jawaban lain

diberikan staf kantor Departemen Luar Negeri, terkait dengan ketidakakuratan penggunaan teknologi pengamanan, seperti CCTV yang dipasang di lantai 2 gedung Departemen Luar Negeri, sebagaimana diberitakan tidak mampu mendeteksi pelaku pembobolan karena alasan gelapnya ruangan. Hal menarik di sini adalah cara pemasangan teknologi CCTV yang tidak tepat sasaran dan kurang mempunyai spesifikasi baik, sangat mempengaruhi upaya pengungkapan pelaku tindak kejahatan dan perbuatan menyimpang dalam lokasi yang dimaksud.

Dugaan pro-kontra bermunculan terhadap lemahnya pengamanan di beberapa kantor pemerintah, antara lain lainnya petugas pengamanan, bentuk pengamanan fisik yang terkesan seadanya, keterbatasan dana dan sumber daya manusia, dan seterusnya. Lepas dari berbagai dugaan ini, yang pasti kehilangan dan kerugian akibat kasus-kasus ini adalah hilangnya sejumlah informasi dan dokumen penting yang disimpan dalam berbagai media penyimpan apakah itu *laptop*, *flashdisk*, disket maupun bundelan kertas tersegel. Pengamanan terhadap berbagai informasi dan dokumen

merupakan bagian integral dari pengamanan. Data-data pemeseharusnya memperoleh perlindungan karena menyangkut kepentingan pemerintah dan masyarakat

Ragam peristiwa ini menunjukkan bahwa kantor pemerintah merupakan obyek vital yang tak luput dari sasaran pembobolan dan rentan terhadap ancaman serta tindakan kriminal. Opini yang berkembang mengungkapkan bahwa terdapat beberapa ciri pencurian pada kantor pemerintah pelakunya bukan orang biasa tapi yang profesional dan mengarah keterlibatan orang dalam. Ini dikarenakan begitu mudahnya pelaku menargetkan petugas pengamanan setempat samping tentunya kepentingan politik atau ekonomi yang mendalangi aksi pelaku.

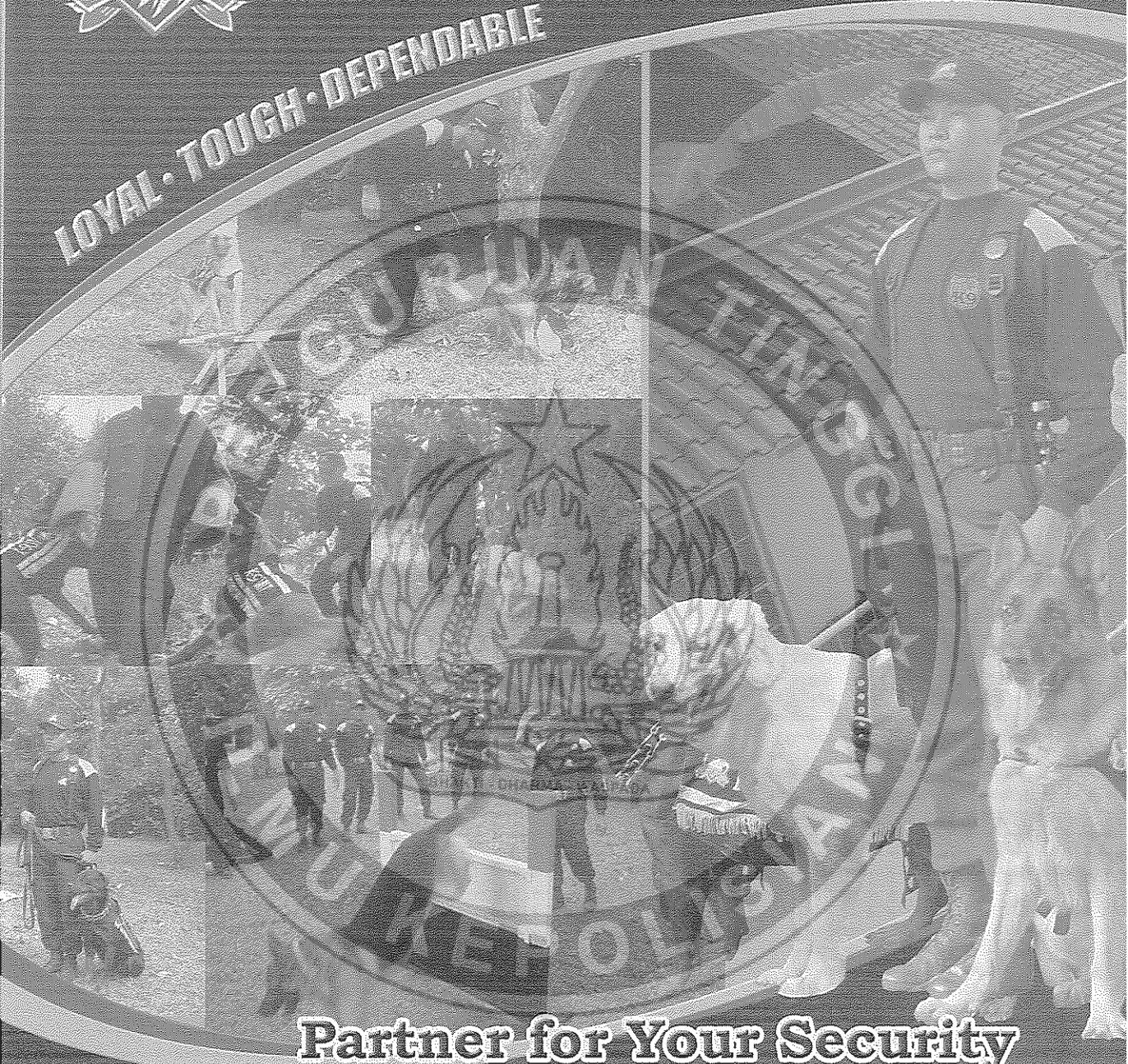
Orang dalam yang dimaksud mencakup pejabat setempat, karyawan, petugas kebersihan, pihak luar yang diijinkan hilir mudik dalam ruang kantor, bahkan petugas pengamanan sendiri. Perlakuan sikap terhadap orang dalam yang dicurigai, secara garis besar seharusnya telah tertuang dalam standar pengamanan khususnya perlindungan personil dan perlindungan prosedur

Dengan demikian manajemen pengamanan kantor pemerintah harus mencakup prosedur yang terintegrasi pengamanan personil dan perlindungan informasi yang baik. Informasi yang baik adalah aset berharga di dalam batas tertentu tidak untuk konsumsi publik. Ancaman terhadap informasi dan aturan prosedural sangat beragam, mulai dari yang sederhana sampai rumit. Karena itu pengamanan terhadapnya tidak semata menekankan aspek fisik, tapi penguasaan teknologi informasi dan pengujian prosedur merupakan persyaratan mutlak. Pengamanan kantor pemerintah harus menampilkann pengamanan secara terpadu yang berkesinambungan, beban pengamanan tidak semata diemban petugas pengamanan tapi harus disadari dan diwaspadai seluruh karyawan dan pihak terkait di dalam kantor tersebut. (



PT Putratama Bhakti
Plaza Fortune 2nd—3
Jl. Mampang Prapatan 96 South
Phone (021) 7998711 (

LOYAL · TOUGH · DEPENDABLE



Partner for Your Security

K9 PROTECOM

**GUARD, PATROL, EXPLOSIVE DETECTION
NARCO DETECTION, RIOT CONTROL
MONITORING SYSTEM**

www.protecom99.com

e-mail: k9unit@protecom99.com