Niko Malian
Country Security Manager
PT British American Tobacco (BAT) Indonesia

"Pemeriksaan dilakukan di *grey area*"

Permasalahan akses ke dalam perusahaan selalu berkaitan dengan dua hal, perilaku kelompok eksternal terhadap keberadaan perusahaan yang mengganggu kelancaran akses dan aksi kriminal yang dilakukan oleh internal perusahaan. Keduanya menjadi permasalahan kompleks ketika di awal berdirinya sebuah perusahaan, kurangnya perencanaan yang baik pada faktor-faktor yang menyangkut masalah keamanan. "Banyak perusahaan yang kurang memperhatikan pentingnya masalah *"security assessment,"* ungkap Niko Malian, membuka percakapan dengan *Security Journal* di ruang kerjanya. Pria yang mengawali kariernya sebagai security, enam belas tahun silam di berbagai komplek bisnis ini membagi pengalaman dan strateginya dalam mengelola akses kontrol dan menangani tuntutan kelompok masyarakat di sekitar lokasi usaha. Berikut petikannya.

Apa strategi Anda menghadapi kelompok yang kerap meminta sumbangan atau lapangan kerja?

Kalau ada organisasi kepemudaan minta pekerjaan sebagai sekuriti, saya hadapi mereka dan jelaskan bahwa kami menggunakan tenaga keamanan *outsourcing* yang profesional. Kalau Anda minta pekerjaan sebagai sekuriti, silakan berhubungan langsung ke *outsourcing* kami. Jangan Anda membayangkan akan langsung dapat bekerja, karena *outsourcing* juga punya kualifikasi tersendiri. Sebab bila kita mempekerjakan orang yang tidak berkualitas sebagai tenaga *security* itu sama saja dengan menunda sebuah permasalahan internal terutama bagi *security* departemen itu sendiri.

Seberapa besar sebenarnya gangguan sosial di kawasan industri?

Kalau saya berkaca di beberapa kawasan industri, ada misalnya truk yang baru datang di pintu gerbang sudah dibuntuti motor banyak sekali. Bahkan ada perusahaan-perusahaan yang cenderung berpikiran, "Ah gampang nanti tinggal bayar saja kok". Padahal, dalam perhitungan anggaran perusahaan tidak ada anggaran untuk membayar retribusi untuk hal-hal seperti itu atau bila adapun sifatnya akan dipaksakan. Semuanya diserahkan ke seberapa besar perusahaan itu menilai resiko yang ada di kawasan industri.

Apakah benar harus ada spesifikasi akses untuk masuk ke pabrik?

Itu betul. Pengalaman membuktikan bahwa, dengan menyatukan akses karyawan dengan kegiatan/operasional pabrik, truk misalnya, pasti tidak nyaman. Belum lagi soal keamanan. Sudah jelas kontrol *security* pasti lemah karena bila kedatangan atau keluarnya truk bersamaan dengan jam karyawan pulang/datang, sekuriti pasti kesulitan bertugas karena prosedur keamanan tidak maximal dilakukan. Saya melakukan

pembagian rute/jalur bagi kendaraan hingga ke pejalan kaki di lokasi kami. Pejalan kaki, motor, dan mobil, diatur jalurnya sehingga kontrolnya mudah dan diarahkan ke pos keamanan untuk pendaftaran atau registrasi. Kalau tamu mendaftar langsung ke kantor *security*, sedangkan karyawan melapor ke sekuriti untuk diabsenkan di mesin absensi. Karena ditempat kami karyawan tidak boleh melakukan absen sendiri.

Kenapa absen karyawan dilakukan oleh security?
Umumnya karyawan terkadang selalu ingin cari yang mudah dan enak. Semua orang mencari cara efisien dan efektif tanpa memikirkan tingkat produktivitas. Misalnya ada 20 pegawai di seksi A yang lembur, sedangkan yang absen hanya 14 orang. Sisa enam orang ini pasti ditanyakan ke petugas keamanan oleh supervisornya. Hal lain misalnya, ada karyawan yang terdata lembur, tetapi ada suatu masalah yang terjadi di luar pabrik (misalnya: kecelakaan). Jadi jaring pengamanan terakhir adalah sekuriti. Oleh sebab itu saya menyarankan ke manajemen, biarlah pengontrolan juga dilakukan oleh *security* sebagai pintu terakhir demi tercapainya target yang diinginkan perusahaan.

Berkaitan dengan truk barang, desain seperti apa yang cocok bagi akses truk?
Kita meniru konsep kedutaan yang mempergunakan *grey area*, di mana pemeriksaan dilakukan sebelum truk masuk dan keluar lokasi dilakukan di *grey area*. Kalau saya melihat konsep ini di kedutaan, sangat bagus dan dapat dipertanggung jawabkan. Setelah selesai semua proses pemeriksaan standard keamanan surat dan muatan di periksa, baru diperkenankan untuk keluar/masuk areal lokasi.

Bukankah akan terjadi kemacetan di jalan akibat grey area?
Itulah proses *security* harus diikuti. Kalau kita mengikuti prosedur *security*, pasti memerlukan waktu. Saya tentunya harus memberikan pengertian, misalnya ke bagian logistik dalam kesempatan rapat manajemen, supaya mereka juga ikut *concern* terhadap permasalahan keamanan (*security awareness*). Oleh karena itu, bila Anda ingin melihat seberapa besar kepedulian suatu perusahaan terhadap masalah keamanan, lihatlah kepada siapa *security manager* melaporkan langsung hasil kerjanya. Kalau di tempat saya saat ini atasan langsung saya adalah President Direktur (CEO) dan ini menjadi prinsip saya selama bekerja dalam bidang ini: keamanan adalah melindungi dan menggerakan roda bisnis.

Bagaimana kemudian Anda mendeteksi kehilangan-kehilangan benda bernilai kecil yang tiba-tiba ada di mobil karyawan tanpa kejelasan data pengiriman barang?
Perlu diingat bahwa pekerjaan *security* adalah bersifat *preventive action*. Artinya kita harus melakukan pencegahan dalam rangka memperkecil tingkat kejahatan atau pelanggaran ketertiban. Bila ada penemuan barang tidak bertuan, saya menilai itu sebagai sebuah uji coba untuk melakukan pencurian. Pengalaman saya, barang itu saya ambil dan beri tekanan ke pihak yang kehilangan barang, "Hei... Hati-hati barangmu sudah ada yang mau coba-coba curi". Tindakan ini juga menjadi penekanan bagi pelaku. Jangan langsung permisif dengan menarik kesimpulan 'yang penting barang kita tidak hilang'.

Internal theft *juga kerap melibatkan karyawan administatif dan manajemen yang tidak bersentuhan langsung dengan proses produksi. Bagaimana sebaiknya menangani hal ini?*
Nah untuk masalah tersebut saya melakukan *security counseling* atau *security briefing* setiap 1 bulan sekali dengan departemen-departemen yang ada. Saya tekankan bahwa filosofi *security* adalah *preventive*. Anak buah saya hanya 200-300 orang sementara jumlah karyawan melebihi jumlah sekuriti. Saya harus menekankan mereka untuk menjadikan wilayah kerja mereka aman. Kalau mereka tidak *aware* dengan *cubical* mereka, akan semakin sulit bagi *security* untuk menciptakan rasa aman

Berdasarkan pengalaman Anda, bagian apa dalam sebuah pabrik yang rawan tindak pelanggaran oleh pihak internal?
Semua bagian mengandung resiko, dan sekuriti adalah pintu terakhir. Makanya *body check* dan pelaksanaan prosedur *security* secara maximal harus dilakukan dari level bawah sampai level atas. Mobil-mobil para *senior manager* terkadang menjadi alat potensial untuk menyembunyikan barang karena terkadang sekuriti sungkan memeriksa mobil *boss*, karena apa yang kita lakukan dilihat oleh para karyawan level bawahnya.

Apa strategi Anda mengendalikan proses pengamanan di gudang atau pabrik yang ada di berbagai wilayah?
Wah, ini sudah strategi ya. Saya minimal melakukan dua kali *business travel* ke seluruh area terutama yang struktur pengamanannya masih harus ditingkatkan berdasarkan analisa wilayah yang ada. *Kedua*, saya senantiasa *online* dengan *site manager* di area tersebut. Saya selalu meminta mereka memberikan gambaran kondisi daerah. Misalnya di Lombok terjadi perang antar suku atau perkelahian antar kampung. Saya akan mendata aset perusahaan yang ada di sana dan menghubungi para petinggi di lokasi, apakah ada dampak kejadian ke lokasi kita, begitu seterusnya.

Kenapa tidak ada loss prevention department di perusahaan ini?
Saya tidak mau *security* dibedakan dengan *loss prevention*. *Loss prevention* adalah bagian dari kerja *security*. Kalau *loss prevention* hanya menangani masalah resiko kehilangan dan pencegahannya, maka *security* tidak hanya mengelola resiko kehilangan. *Loss prevention* hanya memperkecil *scope* sementara tanggung jawab *security* besar. Misalnya, saya harus kerja sama dengan IT karena potensi orang untuk berbuat jahat lagi tidak dengan fisik saja. *Hacker* misalnya, dapat menghancurkan data perusahaan setiap saat. Belum lagi hal lain yang menyangkut masalah BCP (*Bussiness Contigency Plan*), dll.

Apa yang kemudian dibutuhkan untuk mensinergikan security *dengan* loss prevention?
Threat Assessment. Setiap akhir tahun, seorang *security manager* yang profesional seharusnya melakukan *assessment*, sehingga ia tahu hal-hal potensial apa yang dapat mengancam perusahaan di masa depan. Setidaknya di tahun berikutnya. Security dinilai hanya sebagai alat pengamanan semata karena *threat assessment* tidak dilakukan. Manajemen dapat melihat tidak adanya perubahan yang signifikan terhadap strategi pengamanan yang di lakukan *security manager* bila hanya berdasar laporan bulanan. *Threat assessment* merupakan salah satu tolak ukur keberhasilan tugas dan profesi sebagai seorang *security manager* dalam memberikan kontribusi strategis kepada Perusahaan dalam bentuk analisa *security tahunan* sebagai acuan untuk strategi ditahun berikutnya yang tentu akan berpengaruh terhadap kelangsungan lancarnya operasional perusahaan (*Protecting and Enabling Bussiness*) (AP)