DETEKSI *RED FLAG* PADA AKSES INTERNAL

SJ4-07-001

Ada sesuatu yang tersembunyi dalam kalimat Kastino. "Dengan UMR hanya Rp. 824.000, kami harus pintar-pintar cari uang tambahan," ungkapnya sambil menghembuskan asap rokok dalam bentuk bulat-bulat. Pekerja sebuah perusahaan otomotif di Cikarang, Bekasi-Jawa Barat ini agak enggan ketika ditanya *Security Journal* berkaitan banyaknya kehilangan *spare parts* di perusahaan tempatnya bekerja.

Dalam dunia manufaktur, retail, grosir sampai dengan jasa, selalu akan ditemui ungkapan-ungkapan pekerja seperti Kastino tersebut. UMR yang tidak pernah memuaskan para pekerja, maupun bentuk ketidakpuasan lain akan dijadikan alasan bagi para pekerja untuk melakukan tindakan-tindakan kecurangan sampai dengan kriminal di lingkungan pekerjaannya. Faktanya 95 persen perusahaan di seluruh dunia pernah mengalami kerugian akibat tindak kriminal yang dilakukan oleh pekerjanya. Ironisnya, manajemen baru tersadar akan tingginya pencurian yang dilakukan internal, paska perusahaan menerima kerugian dalam jumlah besar. Padahal *item* yang seringkali diambil sangatlah penting, mulai dari *parts*, komponen, informasi bahkan sampai dengan daftar pelanggan.

Security Journal menemukan banyak sekali keluhan dari para manajemen perusahaan terhadap tingginya tindak kriminal yang dilakukan oleh karyawan internal. "Ada satu kejadian yang saya alami ketika baru diangkat sebagai *inventory manager*. Pada saat melakukan *stock opname*, kardus yang ada di gudang tertata rapi. *Labelling* pun lengkap. Saya sempat terkecoh dengan hanya membaca tulisan yang ada di *label*. Namun pada saat saya membuka salah satu kardus, ternyata isinya batu bata," ungkap Frans, manajer *inventory* sebuah perusahaan *spare parts* di Cikarang-Jawa Barat. Ungkapan Frans, salah satu dari sekian responden *Security Journal* memberikan contoh kompleksnya tindak kriminal yang dilakukan oleh orang dalam.

Management Misconception

John Case dalam sebuah bukunya, *Employee Theft – The Profit Killer* menyebutkan bahwa pada dasarnya kecurangan dan tindak kriminal lainnya selalu dimulai dari ketidakmampuan pihak manajemen dalam mengelola keamanan internal. Case bahkan menyebut bahwa pada banyak perusahaan, kriminalitas yang dilakukan karyawan internal lebih disebabkan terlalu percayanya para manajer terhadap bawahannya serta ketidakmampuan mengenali definisi kejahatan internal itu sendiri.

G. Jack Bologna, Robert J. Lindquist dan Joseph T. Wells mendefinisikan kecurangan dalam kalimat "*Fraud is criminal deception intended to financially benefit the deceiver*" atau kecurangan adalah tindak kriminal yang bermaksud untuk memberi manfaat keuangan kepada si pelaku. Kriminal di sini berarti setiap tindakan kesalahan serius yang dilakukan dengan maksud jahat. Dan dari tindakan jahat tersebut ia memperoleh manfaat dan merugikan secara finansial.

Biasanya tindak kriminal mencakup tiga hal yaitu pertama, tindakan. Kedua adalah penyembunyian dan ketiga konversi. Misalnya pencurian atas harta persediaan adalah tindakan, kemudian pelaku akan menyembunyikan kecurangan tersebut misalnya dengan membuat bukti transaksi pengeluaran fiktif. Selanjutnya setelah perbuatan pencurian dan penyembunyian dilakukan, pelaku akan melakukan konversi dengan cara memakai sendiri atau menjual persediaan tersebut.

Pada kasus yang lain, di sebuah perusahaan otomotif daerah Cikarang, *Security Journal* menemukan fakta bahwa para karyawan dan manajemen bekerja sama sedemikian rupa, termasuk melibatkan pihak luar (pengiriman) dalam mekanisme kejahatan internal secara sistematis. Pihak keamanan *outsourcing* yang bertugas di perusahaan tersebut menyebutkan bahwa pihaknya ditekan oleh pemilik perusahaan untuk menyelesaikan tingginya masalah pencurian *spare part* yang dilakukan oleh orang dalam (internal), namun pada sisi yang lain, secara prosedural pihaknya tidak diperbolehkan oleh manajemen untuk menjaga area-area khusus.

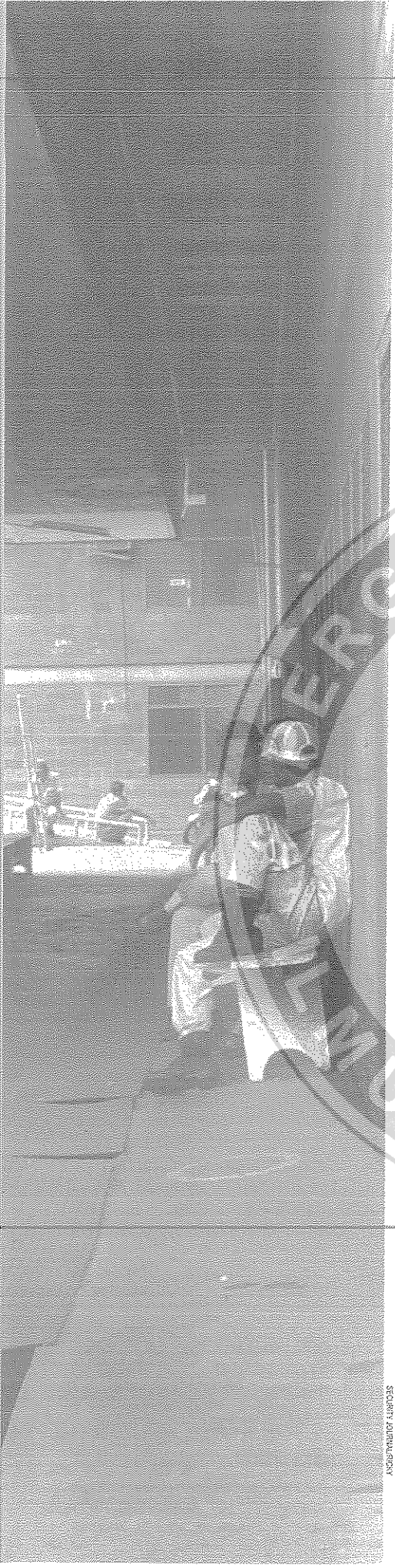
"Kami tidak diperbolehkan untuk menempatkan sekuriti di area pengepakan barang. Kami hanya diperbolehkan melakukan *plotting* (penempatan guard--red) di pos-pos yang disediakan. Kami menjadi serba salah, maju tidak bisa mundur juga sama saja," papar Hartoyo, *chief security* di perusahaan tersebut. Fenomena tersebut mempertegas bahwa *employee theft* tidak hanya dilakukan oleh satu atau dua kelompok, namun bisa dilakukan oleh banyak kelompok internal. "Bahkan kami juga tidak boleh melakukan *body check* terhadap karyawan perempuan, padahal kami sudah jelaskan bahwa yang akan melakukan *body check* adalah sekuriti perempuan juga," tambah Hartoyo pelan.

> Biasanya yakni pada saat awal, kejahatan/kecurangan akan tercermin dalam pola-pola tertentu, baik yang merupakan kondisi/keadaan lingkungan, maupun perilaku seseorang. Kondisi inilah yang sering disebut sebagai titik rawan kriminal atau *red flag*.

Pendeteksian Titik Rawan

Lalu, apa prosedur standar agar tindak kriminal mampu dikendalikan? Konsepsi *loss prevention* dan *asset protection management* merupakan sebagian dari sejumlah konsep yang dapat digunakan. Prinsip dasarnya

Pemeriksaan di gerbang utama: Proses deteksi dini agar sekuriti tidak menjadi "pemadam kebakaran"



adalah memahami kemungkinan terjadinya risiko-risiko di wilayah usaha. Kemampuan melakukan deteksi dini menjadi kunci pembuka. Namun, model pendeteksian tidak dapat digeneralisir terhadap semua tindak kriminal yang dilakukan karyawan internal. Masing-masing tindak kriminal yang dilakukan pihak internal memiliki karakteristik tersendiri, sehingga untuk dapat mendeteksi tindak kriminal oleh pihak internal perlu pemahaman yang baik terhadap jenis-jenis tindak kriminal yang timbul di dalam sebuah perusahaan.

Sebagian besar bukti-bukti kriminal sering berbentuk bukti yang sifatnya tidak langsung. Petunjuk adanya tindak kriminal biasanya ditunjukkan oleh munculnya gejala-gejala (*symptoms*) seperti adanya perubahan gaya hidup atau perilaku seseorang, dokumentasi yang tidak semestinya, keluhan dari pelanggan ataupun kecurigaan dari rekan sekerja. Biasanya kejahatan/kecurangan akan tercermin dalam pola-pola tertentu, baik yang merupakan kondisi/keadaan lingkungan maupun perilaku seseorang. Kondisi inilah yang sering disebut sebagai titik rawan kriminal atau *red flag*.

"Kami mencoba untuk mencurigai beberapa karyawan yang memiliki kendaraan pribadi yang mahal. Dengan UMR yang ada, sebenarnya sulit bagi karyawan memiliki kendaraan sebagus itu. Namun tetap saja sulit bagi kami untuk membuktikan apakah yang kami curigai benar-benar pelaku penyelundupan barang keluar." "*Body check* yang kami lakukan setiap hari tidak pernah menjumpai penyelundupan namun kehilangan tetaplah tinggi," jelas Hartoyo saat mencoba menjelaskan langkah deteksi yang diambil menyusul banyaknya kejadian kehilangan. Seperti halnya Hartoyo, akan sulit bagi pelaku keamanan manapun untuk menangkap perilaku jika hanya mendasarkan pada *red flag* tanpa melihat kembali pada prosedur keamanan yang ada. Beberapa ahli menyebut bahwa titik awal pendeteksian sangat beragam, mulai dari pemberian wewenang khusus kepada departemen sekuriti sampai dengan perumusan konsepsi keamanan perusahaan (*corporate security*). Hal ini tentu saja dimaksudkan tidak hanya meletakkan fungsi sekuriti pada *physical* saja tetapi juga menjangkau keamanan *non-physical*.

Tabel 1. Integrasi Elemen Keamanan Perusahaan

LINGKUNGAN PENGAMANAN	ACUAN KEAMANAN	PROSEDUR PENGAMANAN
Gaya, filosofi dan tujuan perusahaan	Validitas	Pembagian tugas keamanan (*physical security* dan *non physical security*)
Struktur Organisasi	Otorisasi/wewenang	Kejelasan wewenang melalui penetapan *person in charge*
Manajemen sistem Informasi	Klasifikasi dan waktu	Kelengkapan dokumen dan data
Fasilitas dan Aset	Kelengkapan	Kontrol fisik terhadap aset dan kejadian
Kebijakan terhadap karyawan dan prosedur kerja	Klasifikasi dan waktu	Penilaian Keamanan (*Security Review*)

Security Journal juga menemukan sebuah metode menarik yang dilakukan karyawan dalam melakukan aksi kriminal berupa penyelundupan barang keluar. Di sebuah pabrik garmen di area Jakarta Utara, metode penyelundupan barang keluar dilakukan pula secara berkelompok dengan sistem *parts*. Pada saat dilakukan pemeriksaan, petugas keamanan hanya menemukan beberapa karyawan membawa perca kain dalam ukuran kecil dan tidak berbentuk. Penyelundupan tersebut berjalan cukup lama. Setelah dilakukan penelusuran lebih jauh mulailah ditemukan modusnya, yaitu perca-perca kain tersebut digabungkan menjadi sebuah baju yang berharga mahal.

Dengan kasus tersebut, kembali lagi bahwa kontrol terhadap akses hanya mampu untuk mendeteksi *red flag* yang ada namun tidak akan mampu secara cepat

Aktivitas karyawan di setiap bagian perusahaan harus terawasi oleh personil keamanan

menuntaskan kejahatan yang terjadi. Masih dibutuhkan model lebih besar yang mampu menjangkau tidak hanya pada ranah *physical security*. Pengendalian keamanan intern tetap membutuhkan model *asset protection* yang komprehensif yang mampu menjamin keamanan harta perusahaan dan kegiatan operasinya terhadap kejahatan.

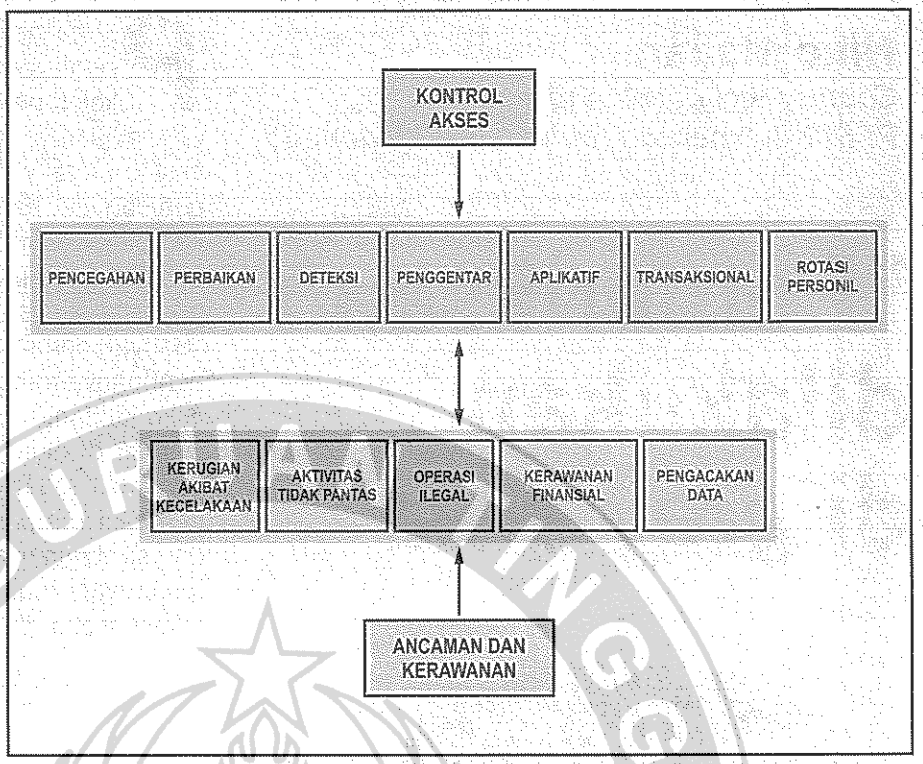
Pengamanan Internal Melalui *Security Review*

Setidaknya ada tiga elemen dalam struktur pengendalian keamanan intern yang perlu diperhatikan dengan baik, yaitu lingkungan pengamanan, acuan keamanan, dan prosedur pengendalian keamanan. Bagan relasi ketiga elemen berintegrasi ke dalam tugas *Corporate Security Department* diletakkan dalam manajemen induknya sebagaimana tertuang pada Tabel 1.

Jika struktur *internal control* sudah ditempatkan dan berjalan dengan baik, peluang adanya tindak kriminal yang tak terdeteksi akan banyak berkurang. Penyelidik tindak kriminal harus mengenal dan memahami dengan baik setiap elemen dalam struktur pengendalian keamanan intern agar dapat melakukan evaluasi dan mencari kelemahannya. *Security review* sendiri sebaiknya dilakukan secara periodik untuk mampu menangkal cara-cara baru tindak kriminal internal.

Security review pada dasarnya bukanlah sesuatu yang mudah untuk dilakukan. *Review* dapat mengidentifikasi hal-hal di mana kebijakan dan prosedur tidak diikuti secara memuaskan. Keterlibatan manajemen dalam melakukan koreksi dapat menjadi faktor yang signifikan dalam memperoleh standar keamanan internal yang *update* terhadap kejadian dan potensi. Melakukan evaluasi kinerja secara berkala merupakan satu elemen penting dalam merangsang kinerja kualitas. Di samping itu, evaluasi ini juga merupakan forum yang efektif untuk menegakkan dukungan manajemen dalam prinsip-prinsip keamanan.

Struktur operasi *security review* setidaknya terdiri atas dua komponen *review*, yaitu *control and protection*, dan penaksiran ancaman, serta kerawanan. Tujuan dari kontrol dan proteksi dalam *security review* adalah melihat terlaksananya *confidentiality*, *intergity*, dan *availbility*. Hal yang harus diperhatikan adalah *preventive control*, *corrective control*, *detective control*, *deterrent control*, *application control*, *transaction control* dan *rotation of duties* yang lebih menekankan kepada kerahasiaan dan keutuhan sistem operasi perusahaan. Semua hal di atas lebih memfokuskan juga pada prosedur pengawasan yang optimal dalam melakukan berbagai hal mulai dari pencegahan hingga rotasi tugas yang baik. Apabila tidak dilakukan dengan benar akan menjadi ancaman dan membuka lebar pintu keamanan.



Penaksiran ancaman dan kerawanan berisi pemantauan ulang tentang jenis ancaman dan kelemahan yang dapat mengancam operasional keamanan yang sudah dilakukan melalui kontrol akses yang ada. Untuk *threat* dan *vulnerability* beberapa hal yang akan dibahas adalah *accidental loss*, aktivitas tidak pantas, operasi ilegal, *account vulnerability* sampai dengan data *scavenging attacks*. Hal-hal ini tidak mencakup semua ancaman tetapi dapat mewakili berbagai macam kelemahan yang kurang menjadi perhatian dan sering menjadi ancaman tidak terduga dan mengganggu operasional keamanan yang dilakukan.

Ancaman dan kerawanan yang tidak terdeteksi terhadap segala akses terbuka dalam lingkungan internal selalu punya potensi memberikan gangguan di masa depan. Jika dibiarkan akan mengasilkan pembuatan kebijakan yang tidak benar (seperti pelarangan *security guard* berjaga di ruang pengiriman), gangguan terhadap fungsi bisnis, hilangnya kepercayaan publik, kehilangan finansial, sampai dengan penambahan biaya operasi. Secara umum, ketidakmampuan mendeteksi secara awal terhadap akses beserta ancaman dan kerawanannya selalu akan menimbulkan ketidakmampuan mencapai *confidentiality*, *integrity*, dan *availability*. Akibatnya jelas yakni *loss*. Ungkapan pekerja seperti Kastino yang menyebutnya sebagai pintar-pintar mencari "tambahan" adalah hasil akhir yang diterima perusahaan yakni kerugian yang berjalan terus menerus. Jika sudah demikian, efektivitas kerja dan efisiensi hanyalah angin kosong yang memenuhi seluruh ruang. Jika tidak ingin terjadi hal demikian, siagakanlah *watchdog* yang dimiliki. Tidak sekedar menakuti atau hanya menandai adanya penjagaan fisik namun mengembalikannya kedalam tugasnya yakni mengamankan. *Security is a process, not given.* (SJ)