

## 2011: Tahun Kesadaran Keamanan Informasi

Richardus Eko Indrajit (Guru Besar Institut Perbanas – Ketua IDSIRTII)

Apa persamaan antara kasus Prita, Ariel, Wikileaks, dan Blackberry? Secara sekilas memang masing-masing memiliki nuansa dan domain yang berbeda, namun secara esensial atau prinsip keempatnya memiliki kesamaan, yaitu berkaitan dengan masalah “keamanan informasi”.

Kasus Prita berada dalam wilayah individu (sosial) yang masuk ke ranah bisnis komersial karena keluhannya yang disampaikan melalui jejaring sosial dianggap merugikan nama baik RS Omni Internasional. Sementara itu Kasus Ariel berada dalam wilayah pribadi (privacy) yang masuk ke ranah publik pada saat rekamannya “bocor” di internet, yang berakibat dikecamnya perilaku sejumlah selebritis karena telah berperilaku jauh di luar nilai-nilai sosial budaya yang berlaku di masyarakat. Lain lagi Kasus Wikileaks yang mengguncangkan dunia karena dengan sengaja dibocorkannya sejumlah dokumen penting intelijen ke ranah publik internasional melalui dunia siber yang membuat marah bangsa besar seperti Amerika Serikat dan sekutu setianya selama ini. Dan yang terakhir adalah polemik mengenai Kasus Blackberry yang berkuat pada pendapat perlu-tidaknya para pelaku bisnis/ekonomi yang memiliki pelanggan di Indonesia untuk menghargai “kedaulatan data” pelanggannya dengan cara membangun sejumlah fasilitas pusat data di tanah air, agar jika terjadi hal yang tidak diinginkan, dapat dilakukan proses mitigasi secara cepat.

Dari keempat kasus tersebut dapat dilihat bagaimana persoalan yang berada dalam ranah pribadi – yaitu pendapat individu seorang pelanggan rumah sakit, rekaman/koleksi pribadi seorang selebritis, korespondensi antar sejumlah intelijen, dan rekaman transaksi serta interaksi ataupun komunikasi antar pelanggan – dalam waktu sangat cepat dapat memberikan pengaruh dan dampak signifikan ke dalam domain publik karena berbagai hal, mulai dari yang bersifat murni sosial-budaya hingga yang berbau kepentingan bisnis maupun politis. Pada saat inilah maka mulai terjadi “keresahan” publik akan dampak dari teknologi informasi dan komunikasi – terutama internet – yang sudah cukup lama diprediksi oleh sejumlah ahli yang dituangkan dalam berbagai tulisan mengenai dampak teknologi terhadap tatanan sosial kemasyarakatan. Sehingga tidaklah heran jika pertanyaan-pertanyaan yang mendominasi masyarakat saat ini adalah: Mengapa hal tersebut dapat terjadi? Apa yang harus dilakukan dalam menghadapi fenomena ini? Adakah cara efektif untuk menanggulangnya? Bagaimana negara lain menyikapi hal serupa?

Bagi sejumlah komunitas dan praktisi keamanan informasi (internet), keempat kasus besar yang terjadi tersebut dapat dianggap sebagai sebuah “blessing in disguise” dalam arti kata bahwa pada akhirnya pemerintah, pelaku industri, dan masyarakat luas perduli dan “melek” terhadap pentingnya menerapkan prinsip-prinsip keamanan informasi (dan transaksi) dalam kehidupan moderen dewasa ini. Sudah lebih dari lima belas tahun semenjak diperkenalkannya internet ke publik luas, terjadi euforia yang sedemikian besar karena tingginya manfaat dan nilai dari keberadaannya – sementara pada saat yang sama hanya segelintir orang yang mencoba melihat dan perduli dari “sisi mata uang” satunya, yaitu resiko yang menyertainya kehadirannya. Secara prinsip, kedua hal tersebut merupakan sebuah paradoksial, karena semakin banyak orang menggunakan internet, maka akan semakin tinggi nilai dari internet tersebut akibat manfaat yang diberikannya, yang berarti pula akan semakin menarik perhatian para pelaku kejahatan yang ingin menguasai dan memanfaatkan “aset” berupa arena interaksi dan komunikasi publik yang berharga ini (baca: Konsep Cyber-6 dari IDSIRTII di [www.idsirtii.or.id](http://www.idsirtii.or.id)).

Untuk mencari jalan pemecahan terbaik, maka perlu dipilih strategi dan pendekatan yang jitu serta efektif, dalam arti kata mudah diterapkan dan segera menghasilkan keluaran yang diinginkan. Namun demikian, agar strategi yang dipilih benar-benar memecahkan akar permasalahan yang ada – bukan bermain pada tataran simptomik jangka pendek semata – maka perlu dipandang permasalahan yang ada secara utuh, holistik, dan sistemik.

Terkait dengan hal ini, ada tiga langkah utama yang layak untuk dijadikan pegangan dalam menghadapi fenomena keamanan informasi belakangan ini. Pertama adalah sungguh-sungguh memahami mengenai perubahan mendasar yang tengah terjadi akibat perkembangan teknologi dan penerapannya di seluruh sektor kehidupan. Konvergensi antara kemampuan teknologi dalam mendigitalisasikan (merubah suatu entitas menjadi bentuk format file digital atau elektronik) teks, suara, gambar, audio, serta video dan kesepakatan komunitas global untuk mengembangkan format interaksi masyarakat dunia yang lebih terbuka tanpa hambatan melahirkan sebuah arena interaksi bebas yang nyaris tak terbandung maupun terproteksi. Alur data dan informasi dalam beragam format – terlepas dari benar atau salah isinya – secara mudah, bebas, dan cepat mengalir dari satu titik ke titik lainnya di bumi ini dengan biaya reproduksi dan redistribusi yang hampir mendekati nol. Fenomena ini adalah suatu keniscayaan, dan sudah cenderung sulit dikendalikan karena telah membentuk “hyper-network” atau jejaring raksasa kolektif yang tak dapat diatur oleh siapapun juga. Kedua adalah berbasis dengan pemahaman di atas, mencoba untuk merubah pola pikir atau paradigma yang tadinya bersifat protektif-reaktif menjadi adaptif-preventif. Sehingga pertanyaan klasik seperti “bagaimana caranya melakukan proteksi agar dampak buruk internet tidak menimpa anak-anak kita?” harus berganti menjadi “bagaimana caranya mendidik anak-anak kita dalam era internet yang serba terbuka ini agar dapat terhindar dari dampak buruk yang mungkin ditimbulkan?” – atau “bagaimana caranya agar informasi rahasia atau yang bersifat pribadi tidak bocor ke dunia siber” menjadi “bagaimana caranya mengelola informasi rahasia dan pribadi di tengah-tengah kenyataan perkembangan teknologi yang serba canggih dan terbuka seperti saat ini?” – dan seterusnya. Dan ketiga adalah bertindak atau berusaha untuk menerapkan sesuatu berdasarkan pola pikir dengan paradigma baru tersebut. Contohnya adalah sikap orang tua yang memutuskan untuk bekerjasama dengan ahli psikologi anak untuk menerapkan langkah-langkah tertentu agar mekanisme “self censorship” dapat tertanam dalam jiwa sang anak semenjak kecil hingga dewasa (pendekatan edukatif); atau “penanaman sugesti” pada para individu yang memiliki posisi strategis atau penting dengan pemikiran misalnya “anggap saja semua pembicaraan di telepon genggam dan interaksi di email telah disadap” sehingga sang pelaku senantiasa berhati-hati dalam bertutur kata serta melakukan percakapan jika terdapat konten yang bersifat rahasia dan penting untuk dibahas dan dikomunikasikan (pendekatan sugesti); atau memastikan untuk senantiasa melakukan proses penyandian (enkripsi) terhadap data atau file apa pun yang terdapat dalam hard disk terkait (pendekatan prosedural); atau pengembangan desain teknologi yang “memaksa” individu untuk memiliki budaya mengamankan informasi seperti misalnya ATM yang “memaksa” nasabah bank untuk mengganti password-nya secara berkala agar dapat menggunakan pelayanan yang diberikan dari mesin tersebut (pendekatan teknologi); dan lain sebagainya.

Tahun 2011 sudah seyogiyanya dan selayaknya menjadi tahun keamanan informasi di Indonesia, sebagai jawaban terhadap proses pembelajaran menghadapi berbagai kasus keamanan informasi yang dialami pada tahun 2010. Target akhirnya adalah meningkatkan kualitas keamanan informasi di berbagai lembaga dan institusi kritikal, seperti: perbankan, militer, BUMN utama (pertambangan, listrik, transportasi, manufaktur, lembaga keuangan, dan lain sebagainya), dan sejumlah kementerian pemerintahan maupun lembaga strategis di bawah Presiden serta lembaga-lembaga tinggi negara. Diprediksi akan ada 4 (empat) jenis mitigasi keamanan informasi yang akan ditempuh.

Jenis pertama adalah melalui pendekatan teknis, dimana akan semakin banyak diinstalasi piranti lunak anti-virus, perangkat firewall maupun IDS/IPS, migrasi ke IPv6, pembangunan SOC (Security Operation Center), implementasi penyandian (kriptografi), penggunaan biometrik, analisa malware (malicious software), pelaksanaan forensik komputer, dan lain sebagainya. Sementara jenis kedua adalah melalui pendekatan manajerial atau bisnis, dimana upaya yang akan dilakukan antara lain melaksanakan audit keamanan informasi, mengembangkan kebijakan keamanan informasi dan internet di perusahaan, menetapkan model BCP (Business Continuity Planning), membangun DRC (Data Recovery Center), mengangkat CSO (Chief Security Officer), menerapkan sistem manajemen mutu ISO:27001 dan variannya, dan lain sebagainya. Jenis ketiga adalah pendekatan berbasis edukasi dan sosialisasi untuk meningkatkan kepedulian individu terhadap pentingnya memperhatikan dan melaksanakan praktek-praktek mengamankan informasi seperti melalui seminar, lokakarya, workshop, dan pelatihan atau pun melalui buku bacaan, artikel, brosur, flyer, website, email/ mailing list, situs jejaring sosial, atau pun melalui televisi, radio, koran, dan media komunikasi massa lainnya. Dan yang keempat adalah terkait dengan pendekatan politik, hukum, sosial, dan budaya misalnya dengan cara menegakkan hukum melalui penerapan peraturan dan perundang-undangan berlaku (mulai dari level Peraturan Menteri hingga Undang-Undang), pemberlakuan peraturan khusus dalam sektor industri telekomunikasi dan informasi, pelaksanaan standar penerapan keamanan informasi bagi lembaga negara dan pemerintahan, pemberdayaan CSIRT/CERT yang telah beroperasi, pembentukan unit-unit pendukung penegakan hukum terkait, penuntasan penyusunan peraturan yang tertunda, dan lain sebagainya.

Dengan kata lain, setelah diterpa dengan berbagai kasus keamanan informasi di tahun lalu, maka sudah saatnya pada tahun kelinci 2011 ini proses pembelajaran dan pembenahan dilakukan. Peran perguruan tinggi, komunitas TIK, perusahaan keamanan informasi, pemerintah, dan lembaga-lembaga swadaya masyarakat sangatlah diperlukan mengingat masih belum banyaknya SDM dan organisasi yang memiliki sumber daya serta menguasai ilmu/konten terkait dengan keamanan informasi untuk disosialisasikan. Prinsip "your security is my security" menggambarkan bahwa sosialisasi kepedulian dan pemberdayaan masyarakat dalam menerapkan budaya aman hanya akan berhasil jika masing-masing individu memulai mempraktekannya dari diri sendiri dan di lingkungan tempat yang bersangkutan berada serta beraktivitas...

--- oOo ---