JAWABAN TERHADAP PERTANYAAN
TENTANG
RANCANGAN UNDANG-UNDANG KEAMANAN DAN KETAHANAN SIBER (RUU-KSS)

DISCLAIMER :

Mohon dipahami, dihayati, dan direnungkan sebelum dibaca, sebaiknya setelah makan.

Semua (tepatnya : sebagian) yang saya tulis ini adalah hasil pemikiran dan keahlian yang saya miliki (halah!), berdasarkan pengalaman pekerjaan dan proyek, mengamati para pengamat, puluhan tahun menikmati kehidupan, serta beberapa referensi dari luar (yang jelas bukan dari tokobukudion.com).

Istilah bekennya **"MENURUT KEYAKINAN SAYA".**

Pendapat dalam tulisan ini juga bukanlah pernyataan resmi lembaga manapun, bukan pula dari penasihat hukum, saya bukan ahli hukum dan saya juga bukanlah seorang financial advisor.

Jika ada bagian yang perlu diskusikan, silakan didiskusikan, jika ada yang perlu diuji, silakan diuji dengan data, pasal, dan mekanisme uji publik.

KARENA DI DUNIA SIBER, YANG **BENAR DAN ORIGINAL** ITU ADALAH YANG BISA DIBUKTIKAN. BUKAN KARENA YANG SERING MUNCUL, LANTANG SUARANYA, HEBOH THUMBNAILNYA, ATAU BANYAK JUMLAH FOLLOWERNYA SAMPAI MESTI BUAT ACCOUNT BARU.

Catatan :
Apabila setelah membaca artikel ini anda merasa resah, gelisah, gundah-gulana, mual, mules, perih kembung, kepala pusing, susah tidur, mimpi buruk dan perasaan bersalah lainnya, silakan hubungi saya, kemungkinan besar anda perlu beli ganti velg atau upgrade sound system.
Akhir kata, lebih kurangnya demikian, mohon maaf apabila ada kesalahan baik yang disengaja maupun baru niat doang .. (eh, tenang, belum mulai, sabar boss...)

Nama: Belly Rachdianto, saya berasal dari keluarga baik baik.
Profesi: Praktisi Keamanan Siber, sedjak taoen 1988. *ya, anda gak salah lihat: delapan delapan*
Email/kontak: belly@yahoo.com
Nomor WA : (+62)813-192.168.0.1
PIN BB : 2AA2B9E
Nomor ICQ: 40605342

A. Urgensitas dan Landasan Rancangan Undang-Undang Keamanan dan Ketahanan Siber (RUU KKS)

I. Menurut Anda, apa urgensi paling mendasar bagi Indonesia untuk segera memiliki RUU Keamanan dan Ketahan Siber, dibandingkan hanya mengandalkan regulasi sektoral yang ada saat ini?

BR:
Jadi gini bro, kalau ditanya mengenai dasar ke'urgensi'annya, maka jawaban saya adalah: kita perlu satu 'payung' tata kelola nasional (national cyber security governance) yang dapat mempersatukan semua regulasi yg sudah ada, seperti standar keamanan, definisi insiden, mekanisme dan tata cara serta kewajiban untuk melapor, struktur 'komando' dan koordinasi disaat krisis, serta akuntabilitas lintas sektor.

Kenapa? karena yang namanya 'attack' jaman now itu tidak perduli terhadap regulasi mana yang di-applied, mereka bisa masuk dari mana institusi mana aja, dari perangkat vendor, dari aplikasi yang dibuat pihak ke dua, tiga sampai ke sepuluh (tergantung disubcon berapa kali itu, lol).

Regulasi sektoral harus tetap ada dan tetap penting, tapi kalau tidak ada 'payung'nya, kita bakalan sering menghadapi 'fragmentasi', perbedaan standar, mekanisme dan format pelaporan yang tidak konsisten, jalur koordinasi ataupun langkah yang harus diambil disaat terjadi insiden, belum lagi urusan akuntabilitasnya.

Tanpa UU KKS sebagai payung hukum (bahasa kerennya "*Lex Generalis*"), respon negara akan selalu bersifat reaktif dan terkotak-kotak bahkan cenderung adhoc (ini saya lihat dari beberapa kasus insiden siber besar yang udah pernah terjadi lho ya).

Oleh karenanya, kita perlu memiliki landasan hukum / payung yang kuat untuk Keamanan dan Ketahanan Siber.

II. Ancaman siber apa yang paling krusial dan sistemik dihadapi Indonesia saat ini sehingga memerlukan pengaturan setingkat undang-undang, bukan sekadar peraturan teknis atau kebijakan administratif?

BR:

Di Indonesia, ancaman yang sangat dirasakan oleh masyarakat adalah berupa derasnya arus masuk informasi baik yang valid ataupun hoaks/scam di media sosial yang sangat berdampak kepada kehidupan sosial, ekonomi, dan budaya. Terlebih, jika suatu konten disinformasi di 'amplify' di waktu dan lokasi yang tepat, akan meningkatkan resiko terjadinya kepanikan atau bahkan kerusuhan di masyarakat, dan itu sudah sering terjadi. Hal ini sebetulnya sudah sering saya paparkan di beberapa institusi sejak tahun 2012. Pada masa itu, fenomena tersebut masih banyak muncul dalam bentuk propaganda tertentu di media sosial.

Anyway, saya coba uraikan mengenai ancam siber global dengan bahasa yang 'scientific' biar kelihatan lebih keren dan gaya :

"LANDSCAPE ANCAMAN SISTEMIK SAAT INI DIDOMINASI OLEH VEKTOR SERANGAN YANG *HIGH-FREQUENCY* DAN *HIGH-IMPACT*, SEPERTI *SPEAR PHISHING/VISHING, SOCIAL ENGINEERING*, *RANSOMWARE*, *SUPPLY CHAIN ATTACK*, SERTA *INSIDER THREATS*"

Selain itu, semakin maraknya **Advanced Persistent Threats (APT)** yaitu serangan yang siber yang canggih dan persistent (dilakukan terus menerus dalam jangka panjang), sulit terdeteksi, dengan target institusi atau organisasi yang spesifik, vital dan strategis. Umumnya di'sponsori' oleh Negara. Silakan googling tentang : 'WannaCry, 'Flame' Malware, Operation 'Red October', 'Lotus Blossom', dan masih banyak lagi.

Situasi ini semakin diperburuk oleh kemajuan teknologi kecerdasan buatan (AI) dan *agentic AI* yang membuat serangan menjadi lebih cepat, ter-auotomatisasi, advance, high quality of evading and deception, deepfake, akan tapi dengan "cost of attack" yang relatif lebih murah serta efisien.

Tanpa kita sadari, musuh sudah ada di dalam jaringan kita, duduk manis minum kopi, sambil menyalin data rahasia intelijen. Negara kita butuh UU untuk memaksa agar semua melakukan Cyber Threat Intelligence atau bahkan Threat Hunting secara rutin, bukan menunggu viral dulu baru panik. Karena APT yang ada disana adalah" State-Sponsored Hacker", sementara disini masih berupa "State-Sponsored Incompetence". 😉

Jangankan masalah kebocoran data di 'cloud ecosystem', di tahun 2000-an pada sewaktu maraknya 'carding', itu aja udah cukup merepotkan dan melibatkan banyak pihak, mulai dari korbannya, banknya (bank asing pula), merchantnya, hingga aparat penegak hukumnya yang harus bolak balik berhubungan dengan interpol dan FBI (kayak di film film).

Saya masih ingat, pernah turut membantu menelusuri illegal transaction selama berminggu-minggu,

pergi kesana kemari, begadang tiap malam, eh.. ternyata begitu teridentifikasi dan tertangkap, pelakunya adalah anak SMA pelanggan warnet yang sekedar iseng beli kaos Jersey dari Eropa.

Sekarang? cukup searching tool dan tutorial di internet, ketik ketik dan klik sana sini, tunggu beberpaa menit, kelar deh ‘idup’ lu. Yang dulunya cuma jadi korban mama minta pulsa, sekarang si ’mama’ udah menjelma menjadi ’The Nun’ .

Oleh karena itu, kita membutuhkan suatu landasan hukum yang kuat untuk Koordinasi Pertahanan dan Keamanan lintas sektor (bahkan lintas negara) yang hanya bisa diamanatkan oleh Undang-Undang.

Bro, siapapun bisa aja membeli *firewall* paling mahal di dunia, menyewa tentara siber dari planet Mars, atau bikin super-apps dengan vibe-coding dan Agentic AI yang lebih pintar dari Einstein.

Tapi, kalau *password* admin masih "P@ssw0rd123!" , ”vagrant:vagrant”, atau (klasik sih ini) *password* ditulis di post-note ditempel dimonitor, yang ada, UU-KKS ini cuma jadi jilidan kertas mahal dan tumpukan sampah sendok+garpu plastik patah, hasil makan siang setelah paparan berkali-kali.

B. RELASI RUU KKS DENGAN UU SEKTORAL

I. Bagaimana Anda melihat posisi dan relasi RUU KKS dengan undang-undang sektoral yang telah ada, seperti UU ITE, UU Perlindungan Data Pribadi, UU Telekomunikasi, dan UU Perbankan?

BR:
Wah, perasaan gue jadi gak enak nih **,** ini pertanyaan jebakan.

RUU KKS idealnya harus **minim pidana**, yang isinya lebih mengatur kepada **kewajiban administratif & standar kepatuhan**, kecuali kalau ada celah yang benar-benar tidak tercakup di **KUHP/UU ITE**.

Oleh karena itu, sebaiknya **UU KKS** berperan sebagai "L**ex Generalis"** untuk "Cyber Governance And Resilience*"* (baseline controls, incident reporting, crisis coordination, audit/assurance,), sementara UU sektoral tetap sebagai "L**ex Specialis"**.

Beberapa Undang Undang yang sudah ada :

- **UU ITE** : fokus pada kejahatan siber (*cybercrime*).
- **UU PDP** : fokus pada hak privasi dan perlindungan data pribadi subjek data.
- **UU Sektoral (Perbankan/Telko)** : fokus pada standar teknis operasional industri.

Aplikasinya begini, undang undang ITE/Cybercrime harus tetap berada di ranah tindak pidana kejahatan siber (walaupun niatnya mengatur transaksi elektronik, tapi seringnya dipakai untuk menangkap orang yang curhat di medsos).

JIka UU Ketahanan dan Keamanan Siber, dicampur aduk dengan ranah kejahatan siber (walaupun dengan atas nama keamanan negara), hmm.. bakalan ada ada tuh 'pasal karet' baru: karet yang direndem di minyak tanah, dan mayarakat akan takut untuk melakukan riset atau inovasi keamanan. Lantas mau sampai kapan kita bergantung kepada produk dari negara lain ?

Mau bukti, coba cari regulasi tentang aturan export algoritma enkripsi, siapa yang buat?
Bayangin, ALGORITMA aja gak boleh sembarang di export ke negara lain. Keren kan, kok mereka bisa kepikiran ya?

RUU KKS hadir untuk mengisi kekosongan tentang: 'Bagaimana struktur pertahanan nasionalnya', 'Siapa yang akan menjadi komandannya saat terjadi krisis?', 'bagaimana standar minimum ketahanan infrastruktur', dan lain sebagainya. Jadi, posisinya saling melengkapi, bukan menggantikan.

Kalau salah memposisikan, RUU KKS bisa berubah jadi "UU power glue" dan dari situ biasanya awal terjadinya overlap dan kontroversi.

II. Berdasarkan catatan Anda, apa potensi tumpang tindih kewenangan dan norma antara RUU KKS dan UU sektoral, serta bagaimana seharusnya desain normatif RUU KKS untuk menghindari konflik regulasi?

BR:
Hm, pertanyaanya bukan 'berdasarkan catatan', tapi berdasarkan pemahaman saya kali ini.
Potensi tumpang tindih kewenangan di draf RUU KKS yang saya perhatikan ada beberapa disini :

A. Potensi Konflik Kewenangan Investigasi dan Penyidikan
Di draf RUU KKS, Pasal 44 huruf f (ef) dan Pasal 39 memberi ruang kewenangan ke BSSN untuk melakukan "investigasi, penindakan, dan pengenaan sanksi administrasi" atas pelanggaran keamanan siber. Penjelasan terhadap RUU-KSS yang ada di halaman 27, semua pasal tersebut sudah 'cukup jelas' . Nah ini bentrok dengan UU ITE Pasal 43 dan KUHAP, yang menempatkan kewenangan penyidikan tindak pidana siber pada penyidik pejabat Polisi Negara Republik Indonesia dan Pejabat Pegawai Negeri Sipil tertentu.
Kalau batasannya nggak jelas antara "investigasi siber" versi BSSN dan investigasi atau bahkan penyidikan versi aparat penegak hukum, takutnya di lapangan bakalan rebutan: siapa yang duluan pergi ke TKP? siapa yang boleh menyentuh atau membuat copy dari digital evidence, atau kalo mau ekstrim.. 'oh insidennya ternyata di server kantor gue.. ya udah gue WA ke temen ruang sebelah untuk dilakukan forensic investigation...
Ini bukan soal ego Lembaga, ini kepastian hukum. Kalau nggak jelas, yang kena bukan hanya pelaku, yang asalnya patuh dan baik baik, bisa jadi apes karena dianggap 'obstruction'.

B. Potensi Konflik Pengendalian Konten (Penapisan vs Pemutusan Akses)
Di Draft RUU-KKS Pasal 38, memberi kewenangan BSSN untuk melakukan "penapisan terhadap konten dan aplikasi elektronik" yang (dianggap) berbahaya.
Nah, di UU ITE Pasal 40 ayat (2b), memberi kewenangan kepada Pemerintah (biasanya sih, KOMDIGI) untuk melakukan pemutusan akses terhadap informasi elektronik dan/atau dokumen elektronik yang memiliki muatan melanggar hukum. (baca: Konten)
Artinya, ini bakalan ada dualisme kewenangan dan standar definisi konten "berbahaya", yang berisiko 'abuse of power'. Tergantung standar dan definisi pihak mana yang akan digunakan.

Dan masih ada beberapa lagi, misalnya tentang standar keamanan untuk PSE, yang sebetulnya juga sudah ada di UU ITE Pasal 15 (plus aturan turunannya di PP 71/2019), kemudian tentang kerahasiaan dimana UU PDP (UU 27/2022) sudah berlaku sebagai lex specialis yang mengatur rinci soal pemrosesan data, hak subjek data, kewajiban pengendali/prosesor, sampai sanksi kebocoran.
Ada lagi sih beberapa tapi saya ntar jadi ganti profesi nih..

Bayangkan jika UU-KKS datang dengan standar dan audit yang "beda jalur", pelaku industri dan pengguna layanan akan terkena 'compliance fatigue' : diaudit oleh BSSN, Kominfo/Komdigi, dan Lembaga Pengawas PDP dengan interpretasi yang bisa beda-beda.

Ujung-ujungnya nya bukan makin aman, yang ada makin sibuk ngurusin check-list, tapi kontrolnya belum tentu makin bener.

Intinya, kalau UU-KKS mengatur ulang UU / Regulasi yang sudah ada, hasilnya adalah ketidakpastian hukum. Dan itu mahal untuk masyarakat, dunia usaha, dan negara.

Beberapa rekomendasi dan saran dari saya :

1. UU-KKS tidak boleh masuk ranah pidana
2. UU-KKS mengatur mengenai tata Kelola Keamanan dan Ketahanan Negara, Defini Standar Teknis, Manajemen Krisis (Risk Management) dan Incident Respond
3. Batasi wewenang "penindakan" BSSN hanya pada sanksi administratif (seperti pencabutan sertifikat elektronik, dam cukup sampai rekomendasi penghentian sistem)
4. Kalaupun harus melakukan investigasi, tujuannya hanya untuk mencari 'root cause', yang nantinya bisa digunakan oleh semua pihak sebagai bahan utk threat intelligence/threat hunting, membantu mereka melakukan pencegahan. Tidak perlu sampai ke penyidikan untuk memenjarakan orang. Itu udah ada lembaga dengan ranah 'pro-justicia' nya.
5. BSSN (yang saya bada di RUU-KKS) mendingan lebih fokus pada pengamanan infrastruktur vital negara, seperti backbone jaringan nasional (Pipanya, bukan airnya), pusat *data center*, satelit komunikasi, sistem kendali industri (OT/SCADA). Lebih keren kan. Urusan konten konten 'berbahaya' itu biarin aja, udah ada lembaga dengan "Lex Specialis"nya.
6. Saya setuju, BSSN menjadi Pusat Operasi Keamanan Siber Nasional (NSOC), sebagai satu satunya gerbang pelaporan. Baru dari situ, Laporan yang masuk ke NSOC kemudian didistribusikan: aspek pidananya ke Polri, aspek administrasinya ke Kominfo/Sektor, sementara BSSN fokus kembali kepada mitigasi teknis dan pemulihan nasional.

Misal nih, Jika Bank X kebobolan, janganlah mereka disuruh lapor ke 5 instansi (BSSN, OJK, Polisi, TNI, Kominfo, atau BI). Ah kau, kasihan, mereka lagi panik. Cukup lapor ke satu portal nasional, biar sistem di belakang layar yang mendistribusikan laporannya. Efisien, kan? Daripada tau2 ntar karena bingung trus posting aja di IG / X ... biar viralllll..

UU KKS idealnya menjadi payung untuk cybersecurity governance & resilience, yang tujuannya untuk mengayomi dan melayani masyarakat (ehh..), bukan buku jimat yang isinya resep penolak bala untuk mengatasasi semua masalah.

kalau semua lembaga punya wewenang "investigasi", ntar takutnya yang paling sering "diinvestigasi" nanti malah... server/komputernya orang baik-baik.

.

C. ASPEK KEAMANAN SIBER (CYBER SECURITY)

I. Dalam perspektif teknis, elemen minimum apa saja yang harus diatur dalam RUU KKS untuk menjamin keamanan siber nasional secara efektif dan adaptif terhadap perkembangan teknologi?

BR:
Gampang gampang susah nih, ada kata2 'adaptif terhadap perkembangan teknologi.
Tapi saya coba deh:

1. Scope dan Object Pengamanan :

Di RUU-KKS, pasal 10: " infrastruktur siber nasional mencakup **infrastruktur informasi kritikal nasional**, **SPBE**, **perekonomian digital**, dan "sistem elektronik lain", lalu disusun dalam daftar.
Ini udah cukup, tetapi kalau bisa ada ada juga 'daftar' dampaknya terhadap layanan publik, ekonomi, keamanan nasional, dsbnya. Sehingga nanti ada skala prioritas, itu penting, karena kalau semua pada ngaku sistemnya "kritis". Berabe..

2. Mitigasi resiko:

Sudah ada di Pasal 12: backup/salinan, SOC, pengelolaan akses, perubahan berkala kode akses, SOP mitigasi dan simulasi, dll. Hanya saja jangan terlalu 'klasik'.
Tambahin kalimat: adalah elemen minimal yang harus ada, boleh ditambah dengan teknik lain yang tapi tetap didalam koridor mitigasi resiko. Disini bakalan ini terlihat adaptifnya terhadap perkembangan teknologi misalnya cloud, zero trust, managed service, atau malah adaptif juga dengan perkembangan ancamannya.

3. Insident Respond:

Udah ada juga di Pasal 14. Ini kembali ke yang sebelumnya saya bahas, prinsip prioritas dan siapa harus lapor kemana. Oh ya, harus ada 'tresshold dan tahapan laporan'. Untuk mencegah dikit dikit lapor, kirim log, trus lapor lagi, trus kirim log yang lain lagi. Cape deh...

4. Apa lagi ya. Oh, kembali ke pasal 13 : "Standar khusus yang diterapkan oleh BSSN" , ati ati nih. Udah saya bahas di halaman sebelumnya. Harus transparan kalau berubah, dan terbuka terhadap usulan pelaku industri (misalnya, ketinggian standarnya). Iya kalau sanggup, kalau nggak, ada sanksi pula, di pasal berapa tuh.. 22 ya ?

5. Supply chain dan perangkat yang ter'serfitikasi', di pasal 17.

Jangan sampai ini karena harus mengikuti standard BSSN, perangkat yang akan digunakan, mentok di gudang beca cukai.
Biar mikir dikit.. : Helm SNI dan Helm ECE , gak bisa dibandingin secara apple to apple.

6. Yang gak kalah penting nih : Pendanaan & Dana Kontinjensi (biar respon insiden gak modal niat)

Sensitif nih, kata kata 'hibah' di pasal 63. Yang penting akuntabel aja.

Kesimpulannya : wajib transparan dan dipublikasikan / sosialisikan, ada masa transisi, skala priotitas, kriteria yang jelas, dan standar definisinya harus berdasarkan dampak, bukan berdasarkan feeling , alias baperan karena udah rame di medsos..

II. Bagaimana peran standar internasional (seperti ISO/IEC 27001, NIST, atau *framework* EC-Council) sebaiknya diadopsi atau diharmonisasikan dalam RUU KKS?

Intinya (biar nggak muter-muter)
RUU KKS sebaiknya mengganti tulisan "standar khusus ditetapkan BSSN". Kenapa? Karena standar itu dinamis. Sedangkan UU itu statis.

Kalau ada pasal di UU-KKS yang sifatnya teknis dan statis, kemudian besoknya standar acuannya berubah, lusa bisnis pusing, minggu depannya sengketa. Wah ini ngajak berantem namanya, yang ada ntar malah debat kusir tiap minggu. Kerjaan kagak beres beres.

Sekali lagi, Ini review kebijakan & drafting dari perspektif "*cybersecurity governance* dan *resilience implementable"*, bukan nasihat hukum personal.

Menurut dokumen draf RUU KSS RJ2 (29 Mei 2019), problem "standar khusus ditetapkan oleh BSSN" itu memang udah melekat di 3 pasal kunci: Pasal 13 ayat (1), Pasal 16 ayat (1), dan Pasal 19 ayat (2). Ini yang kemudian "diangkat" lagi menjadi dasar sanksi administratif.

Lansung aja deh, saya coba kasih beberapa contoh pasal yang perlu sedikit 'dicoret' (biar keliatan kerja)

A. Pasal 13 ayat (1) — Mitigasi Risiko Ancaman Siber"Mitigasi risiko Ancaman Siber sebagaimana dimaksud dalam Pasal 12 dilaksanakan sesuai dengan standar khusus yang ditetapkan oleh BSSN."
Balik lagi nih. kewajiban + sanksi mengacu ke "standar khusus" tadi. Sehingga, menurut hemat saya, sebaiknya begini :
"Mitigasi risiko Ancaman Siber sebagaimana dimaksud dalam Pasal 12 dilaksanakan berdasarkan profil standar keamanan dan ketahanan siber nasional yang ditetapkan oleh BSSN secara transparan."
Dan supaya lebih bisa 'uptodate' tambahan ayat baru (1a) aturan supaya ada ekuivalensi (disini ISO/NIST/GDPR/dll, biar masuk tuh barang..)
(1a). "Pemenuhan profil standar sebagaimana dimaksud pada ayat (1) dapat dibuktikan melalui penerapan standar nasional dan/atau standar internasional yang diakui dan/atau kerangka kerja lain yang ekuivalen, melalui pemetaan (mapping) yang ditetapkan sesuai ketentuan peraturan perundang-undangan."

B. Pasal 19
(1) Penyelenggara Keamanan dan Ketahanan Siber wajib memanfaatkan sumber daya manusia yang memiliki kompetensi dalam bidang Keamanan dan Ketahanan Siber.
(2) Kompetensi sebagaimana dimaksud pada ayat (1) mengacu pada standar khusus yang ditetapkan oleh BSSN.
Nah, untuk yang ayat 2:
" Kompetensi sebagaimana dimaksud pada ayat (1) mengacu pada standar khusus yang ditetapkan oleh BSSN"
Diganti menjadi:
"Kompetensi sebagaimana dimaksud pada ayat (1) mengacu pada standar kompetensi berbasis peran (role-based) dan tingkat risiko."
Kemudian tambahkan ayat baru, biar gak kena jebakan monopoli.
Pasal 19 ayat (3) – Pengakuan sertifikasi profesi:
"Standar kompetensi sebagaimana dimaksud pada ayat (2) mengakui sertifikasi profesi yang berlaku nasional dan/atau diakui internasional dengan mekanisme pengakuan yang objektif, transparan, dan non-diskriminatif, Temasek melalui pemetaan ekuivalensi."

Sehingga ISO/NIST/EC-Council/GDPR atau apapun itu, hanya digunakan sebagai rujukan yang diakui dan bisa dipetakan, bukan menjadi "standar khusus" yang ntar bisa jadi "pasal karet teknis". Karena kalimat "standar khusus" itu ya.. "khusus" tidak ada 'pagarnya' (Kalo vendor pasti ngerti ini, ahem). Apalagi ada sanksinya administratifnya di pasal 25, gawat itu. Niatnya membuat 'panduan' nanti malah menjadi "alat ketok palu".

Saya kasih contoh 2 Pasal aja dulu ya ..

Ringkasannya gini adopsi referensi standar itu mindsetnya adalah berbasiskan output dan dampak resiko. Jangan berpikir bahwa 'framework" itu harus diikuti plak plek.

Lakukan juga klasifikasi standar/framework untuk tiap area : contoh, untuk ISO27000 utk tata kelola/governanace. NIST CSF bisa digunakan sebagai acuan untuk Cyber Resillience, untuk kompentensi, boleh gunakan ISACA, ISC2, EC-Council, dll. Jangan dibalik bolak, nanti seperti duluan Telur atau Ayam. Proses berikutnya ya tentu di sesuaikan cucok dengan kondisi di Indonesia.

Jangan buat "Standar Nasional Indonesia" yang aneh-aneh dan tidak kompatibel dengan dunia luar. Cukup adopsi NIST Cybersecurity Framework 2.0 atau ISO 27001. Tetap ingat, Standar itu cuma alat bantu, bukan jimat penolak bala.

D. ASPEK KETAHANAN SIBER (CYBER RESILIENCE)

I. Apa perbedaan mendasar antara konsep keamanan siber dan kejahatan siber, dan mengapa aspek ketahanan perlu diatur secara eksplisit dalam RUU KKS?

BR:
Konsepnya begini :

1. Keamanan Siber: Utamanya lebih kepada pencegahan dan pendeteksian : identify – prevent – detect – respond - recover (ref. NIST).
2. Kejahatan Siber: situasi =dimana suatu ancaman (baik natural maupun technical) yang tentunya memiliki resiko (kecil-sedang-besar) dan jika tidak diminimalisasi atau di cegah maka terjadilah insiden/kejahatan, nah, ini sudah masuk ranah pidana dan penindakan.

Situasi yang aman artinya.. ancaman tetap ada, tapi resiko terjadinya kejahatannya kecil, sedangkan arti dari KETAHANAN adalah seberapa kuat kita (eh kita, elu aja lagi...) digebukin orang ampe babak belur, kemudian bisa banguin lagi, dan dagang seperti kayak gak ada apa apa.

Ketahanan siber adalah merupakan hasil dari produk Business Continuity and Recovery Policy. Dimana system/layanan harus tetep berfungsi (secara technical maupun business centric), serta sebisa mungkin meminimalisir dampak yang terjadi. Dengan kata lain, ketahanan siber adalah kemampuan untuk bertahan, merespons, dan pulih saat pencegahan gagal..

Karena konsep 100% aman adalah retorika yang tidak realistis, maka tata cara dalam mewujudkan ketahanan perlu ditulis secara eksplisit, karena dalam dunia siber, kita harus menggunakan paradigma "Assume Breach" (asumsikan sistem akan jebol), maka keamanan Siber adalah upaya pencegahan memperkecil resiko terjadinya insiden.

Tanpa rincian yang detail tentang ketahanan, negara akan gagap dan chaos saat insiden besar terjadi, akan tetapi, rancangan UU KKS harus berimbang antara "mencegah serangan" dan "menjamin keberlangsungan layanan". Ini yang sering kebablasan, kalau hukum hanya fokus pada penanganan, bukan pencegahan.

Intinya begini, “CYBER RESILLIENCE” itu bukan sekedar “MENCEGAH SERANGAN”, tapi yang lebih penting adalah bagaimana jika terjadi insiden, suatu layanan (ingat: bukan cuma sistemnya doang) harus tetap beroperasi, cepat pulih seperti semula, dan yg tidak kalah penting, harus akuntabel.

II. Bagaimana RUU KKS seharusnya mengatur mekanisme kesiapsiagaan, pemulihan, dan keberlanjutan layanan digital pasca-insiden siber berskala besar?

BR:
Nah ini pertanyaan yang kelihatannya teknis, ini kita sebenernya inti dari "ketahanan".
Kalau UU-KKS hanya tentang pencegahan, itu seperti bikin payung tapi lupa bikin atap rumah.
Ya, tentungnya sudah ada dalam UU-KKS mengenai **mekanisme kesiapsiagaan, pemulihan, dan keberlanjutan layanan** yang bisa dijalankan saat kondisi paling buruk.

Dalam skala nasional ketahanan siber artinya **negara tetap bisa melayani warga** walau terjadi insiden / disaster (baik natural, maupun technical), power outage, banjir, lumpuhnya komunikasi, terhentinya transaki keuangan, logistik, dan layanan pemerintahan lainnya.
Caranya banyak, misalnya ada backup system, redundancy, clustering, incident response, disaster recovery, latihan (exercise), dan pemulihan layanan, dan dengan target waktu yang jelas.

Ini penting banget karena semua serba digital, jika layanan publik lumpuh, dampaknya bermacam cama, mulai dari **dampak sosial + ekonomi + kepercayaan publik**.

Didalam UU-KKS harus tertera tentang tata cara :

1. **Business Continuity Plan (BCP)** yang wajib diuji secara berkala, bukan dokumen mati.
2. **Penetapan RTO/RPO:** Target waktu pemulihan (*Recovery Time Objective*) yang jelas untuk layanan publik kritikal.
3. **Protokol Komunikasi Krisis:**

Auran main tentang siapa yang berhak bicara ke publik untuk mencegah kepanikan dan disinformasi saat terjadi serangan nasional.
Komunikasi krisis juga harus diatur: pesan publik yang cepat dan konsisten mengurangi ruang hoaks/panik.

Klasifikasi harus berbasis dampak (impact-based), bukan sekadar label administratif: jika gangguan menimbulkan dampak besar pada keselamatan publik, layanan dasar, ekonomi, stabilitas sosial, atau keamanan nasional—maka itu kritis.

Selain dampak langsung, perlu menilai ketergantungan (vendor/cloud/supply chain) dan efek domino lintas sektor. Dengan cara ini, kewajiban keamanan bisa dibuat proporsional: makin kritis, makin ketat baseline-nya..

Harus ada juga mengenai kewajiban simulasi latihan bencana. Kalau pemadam kebakaran latihan memadamkan api, kenapa orang IT pemerintah tidak pernah latihan memulihkan server yang down?

E. INSIDEN SIBER DAN MANAJEMEN KRISIS

I. Berdasarkan pengalaman Anda, kelemahan utama apa yang terlihat dalam penanganan insiden siber di Indonesia selama ini, baik di sektor publik (layanan publik/eksternal) maupun privat (internal sistem/kelembagaan seperti BSSN dan kementerian/lembaga terkait)?

BR:

Jadi gini bro, diatas kertas, SOP nya bagussss banget. Tapi begitu kejadian, yang ada malah *"ini pada kemana di WA kok gak di reply ?"* trus, semua pura-pura sinyal jelek atau batre abis.

Coba saya ingat ingat lagi ..

1. Proses IR dan Eskalasi masih ADHOC. Jalur komunikasi untuk koordinasi seringkali tergantung dari siapa yang duluan reply di WA.
2. Takut lapor, takut disalahkan, atau takut keburu viral. Akibatnya, bukan proaktif, tapi reaktif. Tenang, di RUU-KSS udah ada kok, konsep wajib lapor insiden.
3. Jarang simulasi / latihan jika ada bencana/insiden. Sibuk dengan pekerjaan, atau scrolling socmed.
4. Kebanyakan CSIRT, tapi tidak terkoordinasi dan merata. Yang simple aja deh, pernah nelpon call centre waktu internet mati di saat hari libur atau weekend ? .. tekan satu jika anda pelanggan, tekan dua... tekan tiga... . By email ? jangan ditanya boss.. replynya bisa 3 hari, itupun cuma dapet jadwal kunjungan teknisi. Teknisi dateng, kita udah keburu pasang internet dari isp laen. (ahem, pengalaman pribadi).
5. Kabar baiknya, kalo di sektor yang 'mature' , misalnya di perbankan, itu biasanya lebih disiplin, karena regulatornya lebih 'galak' serta bisnisnya sensitif. Tapi, ya ada aja sih.. (ntar saya ada buktinya). Ya dah bisa nebak2 deh kira2 warna nya apa..

Bahasa gayanya 'ego sektoral', tapi prakteknya itu cuma alesan doang. Bilang aja gak tau gitu harus ngapain. Beres.

Btw saya ada beberapa contoh nyata, dari mulai layanan pemerintahan, sampai yang 'ketat' tadi. Tapi yah jangan ditulis disini. Cukup dipendam dalam hati aja..

Bukan "gimana biar UP lagi?, tapi "siapa nih yg buruan ngomong kalo itu kesalahan dari system "

II. Apakah Indonesia membutuhkan satu mekanisme nasional terpadu dalam respon insiden siber, jika diperlukan/urgen, bagaimana idealnya mekanisme tersebut diatur dalam RUU KKS?

BR:
Sama seperti jawaban di awal, sudah URGEN bingitsss..
Nah, saran saya , ada hirakri seperti manajemen krisis setingkat nasional. Anggaplah kayak bencana alam. Itu kan udah ada model hirkarkiya, struktur komandonya, koordinasinya seperti apa, atau mungkin kita harus ikuti model bisnis / cara kerja pemadam kebakaran.

Hmm.. saya jadi ada ide nakal, kenapa gak mengikuti prosedur bencana alam atau kebakaran. Cukup telpon 999 misalnya, tim IR dateng, server yang kena ransomware langsung di isolasi, TKP diamankan, barang bukti diambil. Besoknya langsung dimulai kegiatan forensicnya.

(eeh.. kebanyakany nonton film kalo ini..)

Tapi yang jelas, harus ada hirarki dengan dengan struktur komando. Karena ini sifatnya nasional, maka lembaganya juga harus levelnya nasional, dan tentunya memiliki kapabilitas.
Rasanya udah ada deh, ditulis di RUU-KKS.

Dan karena ini ada di ranah siber, dunia yang tidak kasat, dan tidak mengenal batas waktu, batas negara, batas social, tidak mengenal 'identitas', anonim, pelakunya bisa darimana aja, apalagi dengan kecepatan internet yang saat ini yang itungannya udah Gbps lagi (bukan kayak saya dulu masih pake dial up 28.8 bkps.

Bos, di dunia siber tahun 2026 ini, 3 hari itu sama kayak 30 taun di taun 1995. Dulu download 3gp bisa 3 hari, skrg cuma 3 detik (btw masih ada gitu 3gp, lol). Nah sekarang bayangin, berapa ratus GB data rahasia kita bisa sudah keburu di download oleh entah oleh siapa, darimana, dan lewat mana aja.

.... sementara itu, kita masih sibuk rapat 3 hari kesana kemari (itupun kalo pas semuanya), cuma untuk memutuskan harus manggil siapa dan ambil log file darimana...

F. INFRASTRUKTUR VITAL STRATEGIS

I. Bagaimana seharusnya RUU KKS mendefinisikan dan mengklasifikasikan Infrastruktur Vital Kritis dari perspektif keamanan siber?

BR:
Klasifikasi harus melihat dari akibat/dampaknya (impact-based). Karena setiap sektor, setiap industri, itu punya tugas dan fungsi masing masing. Dan punya 'critical asset' masing masing.

Pengalaman saya pernah saat kerja menjadi operator warnet, itu lebih berat dari saat bekerja sebagai Network Administrator di instansi pemerintah. Artinya apa, defnisi 'kritis' di dua sektor itu berbeda.

Ada 2 kategori dampak,
1. Dampak langsung : Jika suatu insiden menimbulkan dampak besar pada keselamatan publik, layanan dasar, ekonomi, stabilitas sosial, atau keamanan nasional, maka itu kritis.

2. Dampak tidak langsung : dampak weekend saat ISP rata rata sedang maintenance, dampak 'hari jumat keramat', dimana tidak ada transaksi sektor financial khusus. Para pelaku trading forex, saham, dan sejenisnya, pasti pernah mengalami ini. Rencananya sabtu-minggu mau jalan2, eh.. malah gak bisa tidur. Karena lampu ONT nyala kelap kelip. Itu bahasa kerennya, Intangible lost.

Nah, di UU-KKS, harus juga mendefinisikain hal tersebut, bagaimana jika pelaku industri sudah mematuhi aturan aturan yang tertera. Tapi jika terjadi kejadian yang diluar SLA, siapa yang harus mengganti untung (bukan rugi).

Juga tidak berarti semua institusi harus selalu menggunakan teknologi paling canggih dan produk yang paling baru dan mahal. Saya kasih contoh, di tahun 2002, saat membangun sistem manajemen koordinasi berbasiskan internet di satu insitusi yang termasuk 'stragis' dan 'vital' , semua resource dikerahkan, bandwidth beli yang paling besar, internet kecepatan tinggi, aplikasi dibangun menggunakan konsep ideal disaa itu, dengan budget yang juga 'unlimited'.

Semua feature di implementasikan, vpn dengan end to end encryption, leased line, tunnelling, vlan, network segmentation, access control list, you name it. 1-3 bulan awal, traffic masih mengalir sesuai rancangan awal. Bulan ke 4, mulai sedikit. Setelah ditelusuri, ternyata tetap lebih efektif menggunakan mesin fax dan radio komunikasi.

PS : pernah baca aturan SLA ISP ? atau.. contoh yg paling mudah, kalua kita kirim paket , kemudian hilang, yang kita peroleh ganti untungnya senilai harga barang yang dikirim, atau senilai harga pengiriamannya.. Jujur..

G. Kebocoran Data dan Akuntabilitas

I. Menurut Anda, dalam berbagai kasus kebocoran data atau kasus insiden siber besar di Indonesia, di mana letak kegagalan utamanya: apakah pada teknologi, sumber daya manusia, tata kelola, atau penegakan hukum?

BR:
Jawabannya : ”KESALAHAN SYSTEM” – LOL.
Hehe. Sorry2 nggak deng, serius. (lho)

Yang saya lihat dari kasus yang pernah terjadi baik yang terpublish ataupun ’diem diem’ aja, masalahnya tidak hanya dari satu faktor, tapi kombinasi (mirip kayak 2 factor authentication).
PPT lah istlahnya. (bukan power point…) People – Process – Technology.
Akan tetapi, selalu ada factor utamanya. Yang jelas, sangat jarang teknologi yang menjadi penyebab utamanya. Oleh karena itulah pentingnya melakukan threat intelligence.

Semua berawal dari Policy, alias kebijakan. Karena policy dibuat berdasarkan tupoksi institusi atau core business dari suatu perusahaan. Nah, disini akar masala. Fungsi tata kelola yang hanya tertulis di kertas/file, tapi tidak dilaksanakan sepenuhnya.

Ya, namanya juga manusia. Teknologi bisa dibeli, ilmu bisa dipelajari, tetapi literasi dan awareness pengguna, budaya/culture keamanan cyber, itu perlu waktu dan disiplin.
Apalagi di era saat ini. Bangun tidur, boro boro buka laptop dan melakukan prosedur incremental backup , mendingan liat status IG atau Tiktok.

Sebagai contoh, Insiden serangan ransomware terhadap Pusat Data Nasional Sementara (PDNS) 2 di Surabaya oleh kelompok Brain Cipher dan kebocoran data pemilih di Komisi Pemilihan Umum (KPU) bukanlah sekadar Vmware yang belum dipatch atau karena hari itu hari apes.

Itu contoh pekerjaan paperwork yang (saya juga mengakui), masih bisa tar sok tar sok… (atau lebih parahanya lebih, ntar aja telpon vendornya).

Itulah jebakan batman dari mengutamakan pengadaan (procurement) di atas pemeliharaan (maintenance), dan mengutamakan kepatuhan administratif (compliance) di atas kompetensi teknis (skill competence)

Anda bisa kasih Ferrari ke orang yang tidak bisa nyetir, pasti nabrak juga. Pemerintah beli alat canggih, tapi operatornya tidak di-training, atau vendornya dipilih karena "koneksi", bukan kompetensi.

I. Bagaimana RUU KKS sebaiknya mengatur pertanggungjawaban negara dan korporasi atas insiden kebocoran data yang berdampak luas terhadap publik dan negara?

BR:

Waduh, kalo ini saya harus hati banget. Salah jawab, berabe.

Harus seimbang boss, ada konsep tanggung Jawab (Strict Liability):

Ini bagian yang harus kritis tapi aman.

1. Untuk Swasta:

Denda uang yang besar. Kalau data bocor, denda sekian persen dari omzet. Biar mereka mikir, "lebih murah bayar keamanan daripada bayar denda."

2. Untuk Pemerintah:

Denda uang itu percuma (uang negara kembali ke negara).
Sanksinya harus Sanksi Jabatan. Jika Dirjen atau Kepala Badan lalai menjaga data rakyat, konsekuensinya harus mundur atau non-job. Kalau tidak ada konsekuensi karier, mereka akan terus menganggap keamanan siber itu urusan "tukang ketik" di ruang server.

Saya lihat di draft RUU-KSS sebagian besar yang ngeri ngeri sedap itu sudah ada kok.

UU-KKS harus berprinsip adil dan berpihak kepada rakyat, tapi juga bijaksana.
tapi UU-KKS juga harus bisa membuktikan. Apakah organisasnya yang lalai, atau sudah sengah mampus ngikutin aturan tapi tetap kena serangan.

Kalau insiden terjadi karena kelalaian, ya wajar kalau ada sanksi administratif yang tegas dan kewajiban benerin sistemnya.
Tapi kalau si korban tersebut bisa membuktikan bahwa dia sudah menerapkan semua kewajiban sesuai dengan UU tapi tetep kena serangan yang sangat canggih (0day misalnya, atau ditodong pistol), pendekatannya ya jangan langsung “menghukum”. Justru harus dibimbing bagaimana cara memulihkannya. Dan janji ya, jangan sampai terulang lagi..

Negara kan harusnya hadir untuk membantu, bukan menambah beban.

Sanksi juga harus bersifat konstruktif mendorong perbaikan sistem dan pencegahan pengulangan, bukan sekadar menghukum administratif tanpa ’merehabilitasi’. Ntar takutnya, di penjara malah ketemu hacker lain yang lebih jago...