BUDAYA PERANCANGAN PEMULIHAN BENCANA
(*DISASTER RECOVERY PLANNING CULTURE*)

Omar Zakaria
(Malaysia)

ABSTRAK

Tidak dapat dinafikan, peranan rancangan kontingensi adalah penting selaku pilihan alternatif sekiranya rancangan utama gagal berfungsi. Contoh rancangan kontingensi di dalam sistem maklumat ialah rancangan pemulihan bencana (*disaster recovery plan* – DRP). Pada peringkat organisasi, institusi kewangan tidak dapat lari daripada menyediakan DRP ini. Ini disebabkan Bank Negara Malaysia (BNM) menyediakan garis panduan yang ditetapkan tentang DRP untuk institusi kewangan yang mana mereka perlu akur dengan polisi ini. Akan tetapi, selain daripada institusi kewangan, statistik menunjukkan kebanyakan organisasi masih tidak mempunyai DRP. Tanpa DRP, sistem maklumat akan terdedah kepada ancaman kesediaan (*availability*) yang berpanjangan sekiranya masa yang diambil untuk memulihkan sistem induknya mengambil masa yang panjang. Jadi kertas kerja ini cuba untuk mengupas kepentingan DRP dalam keselamatan maklumat dan mencadangkan bagaimana hendak membudayakan DRP.

Kata kunci: *Keselamatan maklumat, budaya, kontingensi, rancangan pemulihan bencana.*

PENGENALAN

Di dalam pengurusan keselamatan maklumat, pemiawaian keselamatan maklumat antarabangsa menyediakan panduan tentang kod amalan terbaik keselamatan [1]. Contoh pemiawaian ini ialah ISO /IEC 17799:2000 yang mempunyai sepuluh seksyen (amalan keselamatan) [4]. Seksyen-seksyen ini ialah polisi keselamatan, organisasi keselamatan, kawalan dan pengelasan aset, keselamatan kakitangan, keselamatan persekitaran dan fizikal, pengurusan operasian dan komunikasi, kawalan capaian, penyelenggaraan dan pembangunan sistem, kepatuhan (*compliance*) dan pengurusan kesinambungan bisnes (*business continuity management* - BCM).

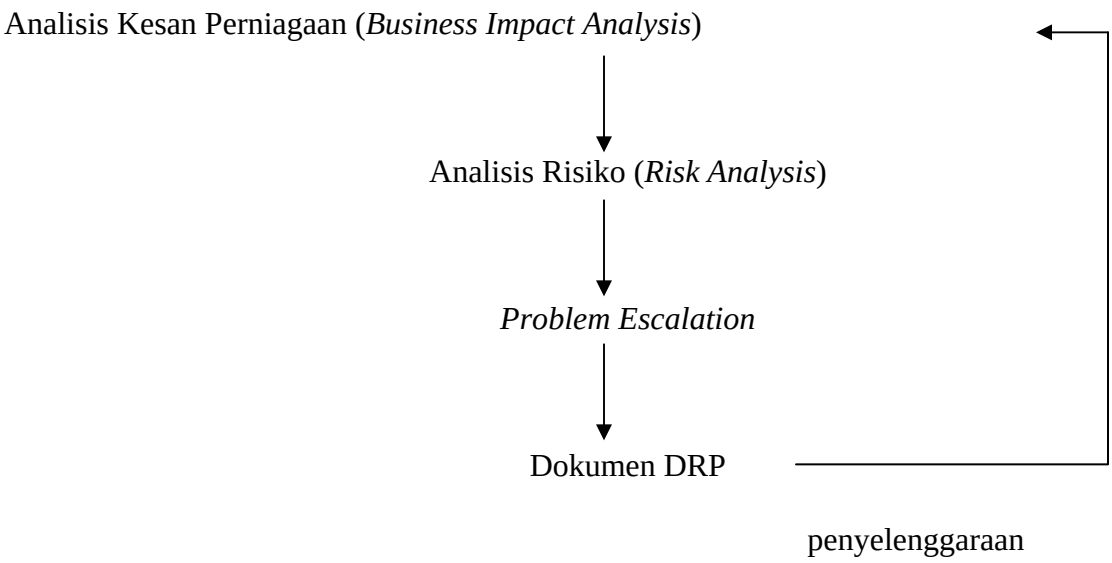
Dalam aspek BCM, komponen DRP merupakan komponen yang terpenting. Ini disebabkan kebanyakan organisasi banyak bergantung kepada sistem maklumat berkomputer dalam urusan harian operasian mereka. Secara ringkasnya, objektif BCM ialah untuk memastikan bahawa operasi perniagaan/perkhidmatan masih boleh diteruskan (secara manual atau dalam talian) walaupun terdapat sampukan atau ancaman bencana pada sistem. DRP hanya memastikan sistem maklumat berkomputer dapat berfungsi pada tempoh pemulihan bencana yang ditetapkan. Kesimpulan BCM melibatkan sistem teknologi maklumat dan bukan teknologi maklumat manakala DRP hanya menumpukan perhatian kepada pemulihan sistem teknologi maklumat semata-mata.

Justeru itu, daripada perenggan sebelumnya, kita dapat lihat bahawa DRP merupakan salah satu aspek penting dalam pengurusan keselamatan maklumat. Tanpa DRP, kita tidak dapat menjamin aspek kesedidaan sistem maklumat yang baik.

RANCANGAN PEMULIHAN BENCANA

DRP merupakan pernyataan-pernyataan yang komprehensif yang dirancang dan didokumenkan, yang mana melibatkan tindakan yang konsisten yang perlu diambil sebelum, semasa dan selepas bencana ke atas sistem maklumat berkomputer [6]. Objektif suatu DRP ialah memastikan operasi pengkomputeran kritikal dapat dipulihkan pada jangka masa yang telah ditetapkan. Ini juga memastikan kepentingan pelanggan, pemegang saham dan kakitangan dilindungi. Dengan adanya DRP, ia dapat meminimumkan masa membuat keputusan semasa bencana dan kehilangan kewangan.

Terdapat pelbagai metodologi dalam membangunkan DRP. Salah satunya ialah metodologi yang boleh digunakan untuk DRP yang dicadangkan oleh Goh Moh Heng [2]. Secara ringkasnya, suatu DRP yang ingin dibangunkan perlu melalui langkah-langkah yang dinyatakan di dalam rajah 1.



Rajah 1 Contoh Metodologi DRP.

Matlamat analisis kesan perniagaan ialah untuk mengenal pasti semua aplikasi-aplikasi kritikal, masa pemulihan suatu aplikasi dan keutamaan aplikasi yang perlu dipulihkan dulu selepas bencana. Ini adalah penting kerana kita tidak dapat memulihkan semua aplikasi pada masa yang serentak selepas suatu malapetaka berlaku.

Tujuan analisis risiko pula dibuat bagi menentukan setiap ancaman dan ketidakkebalan pada aplikasi sistem maklumat. Jadi, ini dapat memastikan kawalan keselamatan yang digunakan merupakan kos-efektif. Di samping itu, analisis ini dapat menyediakan strategi pemulihan yang terbaik dan sesuai pada sesebuah organisasi [6].

Sebelum bencana diuar-uarkan, masalah yang dihadapi mesti melalui fasa *problem escalation*. Sesuatu bencana diisytiharkan apabila masalah tersebut tidak dapat diselesaikan pada masa yang toleran. Pengisytiharan bencana melibatkan kos yang mana proses pemulihan perlu dilakukan. Fasa-fasa ini diperlukan kerana setiap masalah yang

timbul dikatakan boleh diselesaikan mengikut tahap kesukarannya. Apabila suatu masalah tidak dapat diselesaikan pada masa yang ditetapkan, maka barulah bencana diisytiharkan.

Gambaran suatu dokumen DRP menunjukkan ia mengandungi prosedur langkah-demi-langkah pemulihan suatu aplikasi sistem maklumat. Jadi pengujian DRP perlu diadakan bagi membiasakan kakitangan dengan prosedur pemulihan dan tapak alternatif pemulihan. Selain daripada itu, dokumen DRP mempunyai semua maklumat yang dikehendaki semasa kecemasan.

PERMASALAHAN RANCANGAN PEMULIHAN BENCANA

Walaupun kebanyakan pengurus syarikat menyedari tentang kepentingan DRP, tetapi mereka masih tidak menyediakannya. Ada beberapa alasan kenapa DRP ini dipandang mudah. Pertama, mereka beranggapan bahawa sistem maklumat berkomputer mereka adalah lasak (*robust*) dan setakat ini tidak pernah mengalami kerosakan. Kedua, penyediaan DRP ini melibatkan kos yang agak tinggi. Kos-kos ini ialah kos media storan untuk sandaran (*backup*), perkakasan pendua (*duplicate*) dan premis tambahan serta pengujian DRP.

Dalam kes yang lain pula, ada setengah pengurus syarikat prihatin tentang DRP, tetapi tahap kefahaman mereka tentang DRP tidak mendalam. Sebagai contoh, mereka ada menyediakan DRP tetapi premis untuk melakukan sandaran dan sistem maklumat utama ialah pada lokasi yang sama. Sekiranya berlaku kebakaran atau bencana, semua sandaran dan maklumat induk akan termusnah dan DRP yang sedia ada tidak berguna lagi. Pada kes lain, mereka mempunyai prosedur sandaran, tapi tidak mengawasi proses

sandaran secara teliti seperti tiada piawaian storan sandaran, jadual sandaran yang tidak konsisten dan inventori sandaran yang kelam kabut.

Secara ironiknya, penyediaan DRP di dalam organisasi masih tidak menjamin kesediadaan sistem pada tempoh sasaran masa pemulihan, jika kita tidak pernah menguji keberkesanan DRP ini. Aspek pengujian DRP adalah penting kerana kita dapat mengetahui sebarang kepincangan rancangan yang sedia ada dan tempoh masa pemulihan.

Walau bagaimanapun, perlu diingatkan, tanpa DRP dan pengujian DRP, ia akan mewujudkan kekalutan sekiranya berlakunya bencana kepada sistem maklumat berkomputer kita. Kita tidak dapat memulihkan sistem pada masa yang ditetapkan dan reputasi kita dalam kalangan pelanggan akan menurun. Pada hakikatnya, jika kita gagal untuk merancang DRP, maka kita merancang untuk gagal.

Seksyen yang seterusnya cuba untuk mengupas program budaya DRP yang boleh digunakan bagi menyedarkan organisasi atau individu tentang kepentingan DRP dalam keselamatan maklumat.

PROGRAM BUDAYA RANCANGAN PEMULIHAN BENCANA

Ramai orang beranggapan bahawa budaya ialah suatu yang diwarisi daripada genetik dan keturunan. Akan tetapi, sebenarnya budaya merupakan suatu proses yang telah dipelajari [3]. Contoh proses ialah polisi, prosedur, peraturan, tindakan dan senarai semak yang perlu diikuti semasa menyiapkan kerja harian di pejabat. Dengan perkataan lain, budaya terbentuk daripada kelaziman. Kelaziman terbit dari amalan. Amalan datang dari latihan.

Terdapat pelbagai definisi tentang budaya tetapi ia mempunyai ciri-ciri budaya yang biasa (*common*) iaitu interaksi adaptasi, elemen yang telah dikongsi dan dihantar merentasi jangka masa dan generasi. Apabila suatu elemen budaya telah terbukti efektif, maka ia boleh dijadikan penyelesaian masalah sosial dalam rutin kerja harian atau sepanjang hayat [5].

Dengan adanya budaya DRP ini, sesebuah organisasi sudah terbiasa dengan rancangan kontingensi. Jadi sebarang bencana yang akan berlaku, organisasi tersebut tahu untuk bertindak untuk mengatasinya. Selanjutnya dalam kertas ini, penulis cuba mencadangkan budaya DRP pada peringkat individu, organisasi dan nasional.

Peringkat Individu

Dalam dunia digital sekarang, kehidupan kita banyak dipengaruhi oleh sistem teknologi maklumat (IT). Hampir kebanyakan generasi muda kita telah didedahkan sistem komputer di rumah, di kafe sibar, di sekolah mahupun di pejabat. Komputer digunakan untuk melakukan pelbagai aktiviti seperti menyiapkan tugasan, berbual-bual, layaran internet dan sebagainya. Pada masa yang sama juga, kita juga menyimpan semua fail-fail tugasan, tesis, kertas kerja, persembahan dan lain-lain di dalam cakera keras komputer.

Kebanyakan kita yakin bahawa apa yang disimpan dalam komputer adalah selamat dan boleh dicapai pada bila-bila masa. Persoalannya ialah apa yang dapat dilakukan oleh kita jika berlaku nahas sistem (*system crash*) atau serangan virus komputer dan cecacing (*worm*). Jadi kita akan dapat lihat DRP boleh menjadi salah satu penyelesaian pada permasalahan ini.

Dengan perkembangan semasa, ancaman keselamatan semakin meningkat. Lihatlah kehadiran ancaman cecacing yang bernama Sobig, Blaster dan Nachi yang menunggu peluang mengancam kesediadaan sistem komputer kita. Apabila sistem komputer tidak boleh digunakan (sedia ada), maka semua storan komputer tidak dapat dicapai. Di sini kita dapat menyedari bahawa peranan sandaran storan adalah mustahak.

Dengan itu penulis ingin mencadangkan beberapa langkah sandaran yang dapat dilakukan oleh individu. Bagi peringkat individu, proses DRP adalah mudah dan senang kerana hanya melibatkan sandaran pada media storan sekunder dan di lokasi yang berlainan.

Langkah pertama ialah kita hendaklah sentiasa menyimpan fail-fail di dalam pelbagai media storan sekunder atau mudah alih seperti beberapa cakera liut, cakera keras, pemacu pena (*pen drive*) atau cakera zip (*zip disk*). Bagi dokumen yang mustahak, kita menyimpan salinan keras (*hard copy*) atau mencetak fail-fail yang berkenaan.

Langkah kedua ialah semua storan sekunder ini perlu disimpan di lokasi yang berbeza. Sebagai contoh, pemacu pen yang bersaiz kecil boleh diselitkan pada poket seluar/baju. Katakan semua storan utama di simpan di pejabat, maka storan sandaran kita diletakkan di rumah.

Langkah ketiga pula merupakan alternatif langkah pertama dan kedua. Caranya ialah menyimpan fail-fail penting kita di dalam server e-mel di pejabat, atau server e-mel yang percuma seperti Yahoo, Hotmail, GMail, Waumail dan Malaysia.com. Gunalah ruang storan dalam akaun server e-mel kita untuk tujuan storan sandaran.

Langkah-langkah ini perlu diterjemahkan ke dalam bentuk latihan harian. Memang tidak disangkal bahawa untuk mempraktikkan langkah ini memerlukan

kebolehan untuk menyeragamkan pengemaskinian fail-fail tersebut, kerana fail yang dikemas kini mestilah sama pada cakera keras dan media storan sekunder yang lain. Di sini penulis ingin syorkan, apabila proses sandaran dilakukan, semua salinan sandaran hendaklah dilakukan pada masa tersebut dan jangan bertangguh. Apabila latihan ini sering dilakukan, maka ia akan menjadi amalan kita sehari-hari. Apabila amalan menjadi kelaziman kita, maka tercetusnya budaya DRP di dalam diri kita.

Bagi merealisasikan latihan sandaran, tahap kesedaran kita tentang keselamatan maklumat perlu tinggi. Individu perlu peka tentang serangan ancaman keselamatan maklumat semasa yang berlaku, kerana apabila kita sedar kepentingannya, maka kita dengan rela akan melakukan latihan langkah pemulihan atau pencegahan tersebut. Latihan merupakan langkah pertama untuk membudayakan DRP di dalam diri kita. Seksyen yang berikutnya akan menghuraikan program budaya DRP di peringkat organisasi.

Peringkat Organisasi

DRP di peringkat organisasi tidak akan berjaya, jika tiada komitmen daripada pihak pengurusan atasan. Tanpa sokongan mereka, tiada peruntukan untuk DRP. Jadi pihak pengurusan tinggi perlu disedarkan tentang kepentingan DRP. Bagi menyedarkan mereka, usaha individu tidak memadai, jadi penulis mencadangkan bahawa peraturan undang-undang dan keperluan audit DRP merupakan cara yang terbaik untuk mengatasi masalah ini. Sebagai contoh, peraturan DRP yang dibuat oleh BNM untuk institusi kewangan di negara ini. Jadi adalah perlu mewujudkan undang-undang atau akta khusus untuk DRP bagi semua bentuk institusi yang menggunakan sistem IT di Malaysia.

Penyediaan DRP dalam organisasi adalah kompleks, kerana melibatkan pelbagai produk dan sistem. Jadi cara termudah, metodologi DRP yang ditunjukkan di dalam Rajah 1 boleh dibuat panduan. Secara ringkas untuk mengetahui peringkat-peringkat di dalam metodologi DRP, lihat Jadual 1.

Jadual 1 Penerangan Peringkat-peringkat di dalam Metodologi DRP.

Peringkat	**Penerangan**
Analisis Kesan Perniagaan	1. Untuk kenal pasti semua aplikasi-aplikasi kritikal. 2. Untuk tentukan masa pemulihan setiap aplikasi. 3. Untuk kelaskan keutamaan aplikasi kritikal. 4. Untuk tahu tahap toleran pengguna jika sistem di luar talian.
Analisis Risiko	1. Untuk dapatkan pengukuran keselamatan yang kos-efektif. 2. Untuk ketahui tapak alternatif yang kos-efektif.
Problem Escalation	1. Untuk kelaskan suatu masalah yang timbul. Apabila suatu masalah tidak dapat diselesaikan dari satu peringkat ke peringkat yang lebih serius, maka barulah bencana diisytiharkan. Kemudian DRP dilaksanakan.
Dokumen DRP	1. Untuk dokumenkan semua rancangan, prosedur di dalam bentuk pendokumenan.

Peringkat Nasional

Telah diketahui umum, pelan kontingensi di peringkat nasional terutamanya perkara-perkara yang melibatkan bencana alam seperti banjir dan jerebu sudah lama wujud di negara kita. Justeru itu, adalah wajar pelan kontingensi ini juga diperpanjang kepada pelan pemulihan bencana pada sistem maklumat di peringkat kebangsaan. Tidak dapat dinafikan banyak syarikat/individu yang mempunyai kesedaran pelan pemulihan bencana mempunyai pelan ini, tetapi ia bukanlah golongan yang bukan majoriti. Dengan itu adalah bertepatan pihak kerajaan mahupun pihak swasta berganding bahu untuk menyedarkan syarikat dan individu tentang kepentingan pelan pemulihan bencana kepada mereka. Bagi pihak kerajaan, mereka boleh membuat kempen kesedaran pelan kontingensi secara amnya atau pelan pemulihan bencana secara khususnya kepada syarikat dan individu. Di pihak swasta, mereka boleh menaja rancangan televisyen, radio dan sebagainya yang bercorak pelan kontingensi, seperti kepentingan fail sandaran (*backup file*). Dengan adanya komitmen yang baik dari pihak kerajaan dan swasta, masyarakat dapat disedarkan tentang perlunya pelan pemulihan bencana diadakan.

KESIMPULAN

Cuba renung ayat ini, “Jika anda gagal untuk merancang, maka anda merancang untuk gagal”. Apa yang dapat disimpulkan pada ayat ini ialah jika kita gagal untuk mengadakan pelan pemulihan bencana, maka kita akan ditimpa musibah jika kita gagal merancang pelan ini. Tanpa pelan pemulihan bencana, ia akan menyebabkan huru-hara semasa bencana. Sebagai contoh, jika kita gagal untuk merancang kawad kebakaran (salah satu contoh pelan kontingensi untuk kebakaran), maka kita akan mewujudkan suasana kelam

kabut jika kebakaran benar-benar berlaku seperti di mana kita perlu berkumpul atau apa alat pemadam api yang sesuai untuk jenis kebakaran yang berlaku. Justeru itu, dengan adanya cadangan-cadangan yang diajukan pada peringkat individu, organisasi dan nasional, dapatlah memberi maklum balas yang baik dan segera daripada pihak-pihak yang terbabit bagi merealisasikan kepentingan pelan pemulihan bencana.

BIBLIOGRAFI

Blackmore, K., 2002. “Setting standards for information assurance”. Conference on IT Security for The Public Sector, Olympia, London. Section 8: 1–10.

Goh, M.H., 1996. “Developing a suitable business continuity planning methodology”. Information Management & Computer Security. 4/2 (1996): 11–13.

Hofstede, G., 1994. *Cultures and organizations: software of mind*. UK: HarperCollins Publishers.

Kenning, M.J., 2001. “Security management standard – ISO 17799/BS 7799”. BT Technology Journal. 19(3): 132–136.

Triandis, H.C., 1994. *Culture and social behaviour*. USA: McGraw-Hill.

Zakaria, O. dan Mat Kiah, M.L., 2002. *Pengenalan kepada keselamatan komputer*. Kuala Lumpur: McGraw-Hill (M) Sdn. Bhd.