CABARAN KESELAMATAN SIBER BAGI KESEJAHTERAAN UMMAH

Wida Susanty Haji Suhaili
School of Computing and Informatics, Universiti Teknologi Brunei
wida.suhaili@utb.edu.bn

ABSTRAK

Cabaran dunia siber bukanlah sesuatu yang baru. Akses kedunia siber dengan pengunaan ICT mendedahkan kita kepada cabaran ini. Kemajuan dalam alat info-komunikasi teknologi (ICT) seperti komputer, telefon pintar dan tablet telah menjadikan pengaksesan ke dunia siber semakin mudah. Lebih-lebih lagi dengan pengenalan berbagai aplikasi-aplikasi yang memudahkan perhubungan. Peningkatan permintaan untuk memiliki telifon pintar dan 'tablets' oleh masyarakat dalam semua lapisan umur ini juga meningkatkan permintaan akses ke dunia siber, yang akhirnya mencabar pengawalan keselamatan siber. Dalam sektor pendidikan pula, penggunaan ICT sangat ketara dengan adanya keperluan dalam teknik pengajaran dan pembelajaran abad ke 21. Oleh kerana itu, pelajar-pelajar juga terdedah kepada cabaran dunia siber ini.

Kertas simposium ini akan mengupas (i) cabaran dan isu keselamatan siber; (ii) langkah-langkah keselamatan; dan (iii) cara mengatasi dan menangani jenayah siber.

1 PENGENALAN

Akses ke dunia siber kini semakin mudah dengan adanya kemajuan dalam alat teknologi maklumat seperti komputer, telefon pintar dan *tablet* mudah alih yang mempunyai pelbagai aplikasi. Kepesatan dalam alat berkenan telah membuatkan kita sentiasa *connected* kedunia siber dan menjadikan kita seperti tidak boleh berenggang dengan alat tersebut. Cara kita berkomukasi juga telah berubah dengan adanya kepesatan ini yang mana kita sekarang telah mampu berkomunikasi merentas sempadan dengan harga yang murah dan membolehkan kita berkongsi dan berkomunikasi melalui text, suara dan video. Ini secara tidak langsung telah banyak mempengaruhi kehidupan kita dalam pelbagai aspek seperti perhubungan, pendidikan, perdagangan dan pergaulan.

1.1 ANTARA KEMUDAHAN HASIL DARI KEPESATAN TEKNOLOGI ICT

Pengaruh alat dan aplikasi berkenaan pada dasarnya telah memudahkan urusan harian pengguna. Contohnya

i. Dalam aspek perhubungan, dengan menggunakan aplikasi perhubungan seperti *Skype*, pegawai di negara sendiri boleh bermesyuarat dan berbincang dengan pegawai

di luar negara dan mahasiswa tempatan boleh menghadapi *viva* dengan pensyarah di universiti luar negara. Selain itu, salah satu aplikasi perhubungan yang paling popular iaitu *WhatsApp* juga telah terbukti menjadi aplikasi yang merapatkan perhubungan keluarga dan orang-orang yang tersayang.

ii. Dalam sektor pendidikan pula, penggunaan ICT sangat ketara dengan adanya keperluan dalam teknik pengajaran dan pembelajaran abad ke 21. Pencarian data semakin mudah dengan aplikasi-aplikasi seperti *Mendeley* bagi penyimpanan bahan-bahan bacaan secara teratur dan *Google Scholar* bagi pencarian bahan-bahan ilmiah.

iii. Dalam sektor perdagangan, pengunaan aplikasi mudah alih telah menggalakkan banyak peniaga muda berkecimpung melalui ICT dengan memulakan perniagaan kos rendah iaitu mempromosikan produk melalui *Facebook* dan *Instagram*.

Kesemua aplikasi yang digunakan dalam sektor-sektor yang disebutkan di atas adalah menggunakan satu proses yang sama iaitu mengakses data melalui pertukaran informasi antara dua orang pengguna iaitu penghantar ke penerima walaupun mereka berada jauh beribu-ribu kilometer. Yang pasti kedua pengguna ini hendaklah 'connected' melalui akaun bersama aplikasi tersebut atau melalui jaringan aplikasi yang sewaktu dengannya seperti bagi aplikasi emel. Kedua pengguna boleh menggunakan produk yang berbeza sama ada *Microsoft Outlook, hotmail* atau *gmail*, kesemuanya mengikut protokol yang telah diset. Ataupun bagi aplikasi pencarian ('*Search Engine'*), pengguna boleh menggunakan produk seperti *Safari, Mozilla Firefox* atau *Google Chrome*. Dalam dunia tanpa sempadan, walaupun setiap akaun adalah unik bagi setiap pengguna, adakalanya pengguna terbiasa menggunakan nama akaun dan kata laluan yang sama untuk semua aplikasi. Kebiasaan ini secara tidak langsung boleh memberi ruang kepada penjenayah siber untuk menggunakan akaun tersebut bagi jenayah siber tanpa disedari oleh pemilik akaun itu sendiri. Seseorang itu boleh melakukan kerosakan yang besar terhadap individu, masyarakat atau negara lain walaupun mereka berada jauh beribu-ribu kilometer.

Negara Brunei Darussalam dalam usahanya mengawal jenayah siber ini telah membentuk beberapa agensi dengan tujuan untuk menyediakan garispandu bagi menyelamatkan informasi, dan menyelamatkan diri bila melayari dunia siber. Khusus bagi tujuan perkongsian, kertas kerja ini akan mengupas (i) cabaran dan isu keselamatan siber; (ii) langkah-langkah keselamatan; dan (iii) cara mengatasi dan menangani jenayah siber dengan merujuk beberapa sumber seperti laporan pihak-pihak berkenaan.

2 JENAYAH SIBER DI BRUNEI DARUSSALAM

Jenayah siber di negara ini adalah dibawah penghimpunan beberapa agensi seperti IT Protective Security Services Sdn Bhd (ITPSS) yang ditubuhkan pada 2003 dengan tujuan untuk menyediakan garispandu menyelamatkan informasi, *digital forensics, secure event management, IT security training* dan *Incident Response Team* yang ditubuhkan pada tahun 2004 dengan nama Brunei Computer Emergency Response Team (BruCERT). Di bawah adalah peratus serangan siber yang telah dialami dari 2011-2015.

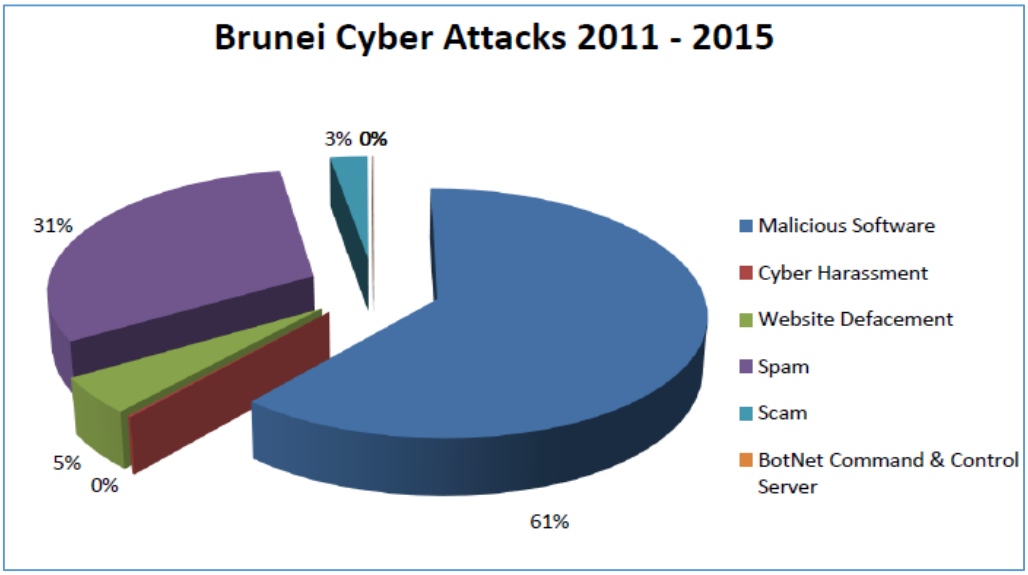

Figure 1: Serangan Siber di Brunei , Source: BruCERT

Dalam kes jenayah siber, peratus jenayah siber di Brunei telah meningkat. Ini berikutan dengan adanya akta kanun yang telah di buat bagi melindungi mangsa disebabkan jenayah siber. Beberapa kes jenayah siber yang telah dapat dikesan dan dihukum telah dikongsikan dalam akhbar tempatan adalah seperti berikut:

Table 1: Rekod kesalahan jenayah siber yang dijatuhkan hukuman. Source: BruneiTimes

Jenayah Siber	Tahun	Hukuman	Kejadian
Hacking dan pencuri data (Kes jenayah siber pertama)	2010	28 bulan penjara	*Wireless Access Point* yang tidak dikunci menyebabkan penjenayah berjaya memperolehi nombor kad kredit dan menggunakannya untuk membayar belian *online* berjumlah $2720.00.
Rogol	2011	14 tahun penjara dan 14 kali sebatan	Kes rogol dibawah umur. Penjenayah telah menceroboh rumah, merogol dan memukul mangsa yang berumur 13 tahun. Perkenalan bermula melalui aplikasi *chat*.
Menyalahgunakan maklumat/Cyber bullying	2012	10 bulan penjara	Bekas kekasih telah mendedahkan gambar dan video sulit dengan kekasih lamanya dengan tujuan untuk memalukan.

Rogol	2015	9 tahun penjara dan 6 kali sebatan	Pesalah berusia 28 tahun, kesalahan 'sexual grooming' dengan dua budak dibawah umur, mengenali mangsa dari Facebook
Ancaman terroris	2015	Dalam sekatan	Melalui jaringan social, keinginan untuk ikut organisasi terrorist

3 CABARAN DAN ISU KESELAMATAN SIBER

Selain jenayah siber yang direkodkan, ancaman-ancaman lain telah dibentangkan dalam Forum Keselamatan Siber pertama pada 5 Februari 2015 yang telah dikendalikan oleh Royal Brunei Technical Services (RBTS). Objektif forum berkenaan adalah untuk mendedahkan kesedaran korporate terhadap keselamatan siber dan memastikan organisasi dilengkapi dengan pengetahuan mengenai keselamatan atas talian. Forum yang bertemakan *Combating Cyber Security Threats* telah membentangkan isu-isu kebergantungan terhadap teknologi yang dapat menjanjikan peluang yang baik tetapi dalam masa yang sama mendedahkan pengguna kepada ancaman-ancaman dunia siber. Forum juga mengambil maklum bahawa ancaman di dunia siber meningkat setiap tahun lebih-lebih lagi dengan meningkatnya perkembangan pengunaan teknologi maklumat. Forum ini juga menekankan kepentingan usaha sama dalam membasmi dan menbenteras ancaman-ancaman siber (RBTS, 2015).

3.1ANCAMAN PENJENAYAH

Jenayah yang paling bahaya ialah menyamar menggunakan alamat IP dan tanpa kita sedari penjenayah ini telah melakukan kesalahan dengan menyamar sebagai anda. Menjejak penjenayah seperti ini adalah sangat mencabar. ICS-CERT (The Industrial Control Systems Cyber Emergency Response Team) telah mengkategorikan penjenayah siber kepada tiga kumpulan. Ancaman dari kumpulan ini adalah melalui proses yang sama, apa yang membezakan ketiga kumpulan ini adalah niat dan sumber yang mereka perolehi. Kumpulan 1 umum, mereka yang mempunyai pengetahuan teknikal, yang memberi ancaman untuk kemasyhuran (*notoriety*); Kumpulan 2 sindiket, mereka ialah penjenayah secara berkumpulan, penggodam, kumpulan activist, orang dalam yang membuka pintu belakang bagi memudahkan serangan. Dan Kumpulan 3 berat, mereka tergolong seperti pengganas, dan mereka yang mengancam keselamatan negara melalui perang siber (Edward, 2015).

Trend isu keselamatan siber sekarang menekankan isu-isu seperti kesahihan maklumat dan pencerobohan yang menyebabkan serangan dan pencurian didunia siber. Lebih teruk lagi bila ia mengugat kestabilan negara dan ugama. Antara perincian isu-isu yang dimaksudkan ialah seperti berikut:

3.2 Kesahihan Maklumat

Cabaran dan isu bagi kesahihan maklumat bukanlah sesuatu yang baru. Semakin pesat teknologi maklumat, semakin mudah dan pesat maklumat dikongsi di dunia siber. Contohnya penggunaan aplikasi *Google* merupakan aplikasi yang sering dilayari oleh pengguna internet termasuklah pelajar. Cabaran dalam menggunakan aplikasi ini ialah:

1. Memastikan maklumat yang diperlukan adalah sahih dan tepat.
2. Memastikan maklumat yang dibaca itu tidak menyesatkan dan memesongkan pengguna untuk mempercayainya hingga menyesatkan agama, kepercayaan dan bangsa.
3. Kesilapan dalam melayari *link* atau laman sesawang yang terpapar dalam *search result*.

Selain *Google*, aplikasi seperti *Email*, *WhatsApp*, *Facebook* juga termasuk dalam cabaran ini. Sekarang *Facebook* atau *WhatsApp* boleh diistilahkan sebagai berita bergerak. Apa jua berita terkini seperti kemalangan, acara-acara keraian dan keramaian akan mudah dan cepat dimuatturun dan dikongsi untuk tatapan. Ada yang akan suka*('like'*) berita-berita ini dan ada juga yang akan mengongsikan berita-berita ini. Tiada masalah jika ia berita baik tetapi jika ia tidak, seperti yang kita lalui mengenai kecelakaan jalan raya, dimana gambar mangsa juga turut disebarkan. Ini sepatutnya tidak dikongsikan dan perlu ditapis.

Antara cabaran lain ialah penyebaran melalui '*Trolling*'. *Trolling* adalah istilah yang terkini dimana pelaku akan membuat kenyataan yang membangkitkan gerak balas negatif. Respond-respond ini akhirnya boleh membangkitkan kemarahan dan boleh mengugat kestabililan sesebuah organisasi mahupun negara, seperti yang berlaku dinegara-negara Arab yang lebih dikenali sebagai the "*Arab Spring*"(Howard, et al, 2011). Kestabilan negara tergugat akibat pengerakkan politik dan pemberontak civil disebabkan penyebaran propaganda jahat. (Knott, 2014). Operasi-operasi ini menyebarkan maklumatyang bersifat untuk memesongkan, mengelirukan dan menjejaskan keupayaan kita berfikira lebih panjang dan bijak. Antara operasi yang mengunakan teknik begini adalah operasi yang dikenali sebagai 'cognitive hacking' (Cybenko, Giani, Thompson, 2002), 'cognitive malware' (Finomore, et al, 2014) atau 'social cyber attacks' (Goolsby, 2012).

Cabaran-cabaran yang disebutkan di atas telah menimbulkan isu keselamatan di mana penyalahgunaan aplikasi boleh mengundang bahaya lebih-lebih lagi jika bertepatan dengan *laman web* yang menjadi 'umpan' penjenayah. Antara kes jenayah ialah mahu menjadikan pelajar remaja sebagai mangsa pornografi, pelacuran, seks bebas, penculikan dan pemerdangangan manusia. Atau jenayah ingin memesongkan atau menyesatkan pelajar dengan *link-link* yang mempunyai propaganda sama ada untuk merosakkan kestabilan sesuatu organisai atau negara mahupun agama. Ini telah terbukti dengan adanya group-group Militant yang merekrut melalui Facebook dan Twitter dan berkomunikasi menggunakan enkripsi untuk merancang dan melaksanakan serangan. Siber Terrorism juga terhasil disebabkan isu ini dimana kes ini telah berlaku di Malaysia, Indonesia, Phillipines dan yang

terkini di Singapore. Ini secara tidak langsung mengugat ketenteraman dan kesejahteraan sesuatu bangsa dan juga negara.

3.3 Pencerobohan

Pencerobohan juga menjadi salah satu cabaran keselamatan siber yang boleh menjurus kepelbagai jenayah siber. Pencerobohan boleh terjadi melalui tiga peringkat. Manusia, proses dan teknologi seperti kecuaian pengguna sendiri yang tidak mengemaskini keselamatan alat ICT atau tidak menukar kata laluan seperti yang disarankan bagi mengurangkan pencerobohan atau kurangnya kawalan keselamatan alat dan aplikasi ICT. Pegawai kanan operasi BruCERT melaporkan bahawa jenayah yang paling banyak direkodkan sejak tahun 2011 ialah *spams dan website defacement* di mana pada tahun 2011 sahaja, sebanyak 160 laman sesawang mengalami *defacement* kerana kurangnya kawalan dan tidak mengunakan *security patch*. Pada 2012 dan 2013, jumlah *website defacement* meningkat kerana penggunaan *3rd party website* tanpa *security control*. Jenayah seumpama ini telah menyebabkan kesukaran pengaksesan informasi dan menghalang operasi harian. Pada tahun 2014, serangan *DDOS(Denial of Service)* direkodkan ke atas institusi kewangan di mana penggodam (hackers) telah mengugut dan melepaskan serangan trafik yang memutuskan perhubungan institusi tersebut.

Cabaran yang terkini ialah melalui kaedah IoT (Internet of Things) (Drubin, 2016; Kolias, Stavrou and Voas, 2015). Kaedah IoT membolehkan sesebuah organisasi atau persendirian untuk mengawal peranti yang berhubung '*connected devices*' melalui hujung jari. Contoh IoT ialah pengawalan lampu elektrik dirumah secara akses jauh/ *remote*. Kemudahan ini boleh diakses ketika kita berada di luar rumah atau negeri yang mana pengawalan elektrik cuma perlu menekan butang melalui aplikasi dalam telipon pintar. Pengaksesan melalui ruang siber ini dalam satu kenyataan dari FBI dalam kenyataan perkhidmatan awam yang telah memberi amaran yang *connected devices* menimbulkan risiko ancaman kerana membuka ruang baru untuk diserang. Ini termasuklah kesemua peranti dari lampu ke *wearables* hingga ke *network connected printers (*Hammond, 2015; Higginbotham, 2015*)*. Rumah yang dipasang CCTV yang dikawal dari luar juga dapat digodam dimana penggodam akan dapat memperoleh data dan mengetahui bila rumah itu benar-benar kosong dan selok belok rumah berkenaan dapat diketahui. Dan cabaran dari trend yang terkini dengan pengunaan aplikasi *Location detection* seperti dalam permainan Pokemon Go. Pengunaan permainan ini adalah ditegah di tempat-tempat sensitif dan bahagian pertahanan, kerana ini boleh mendedahkan organisasi menjadikan tempat itu senang di serang oleh penjenayah yang sentiasa mengambil peluang atas kemudahan-kemudahaan sebegini.

Cabaran yang utama adalah petugas keselamatan ICT. Seseorang yang memegang peranan atau posisi ini perlu sentiasa memastikan cara-cara terkini untuk mengawal dan menghalang jenayah siber dari berlaku. Seterusnya adalah langkah-langkah keselamatan yang dapat diambil bagi menangani dan mengurangkan cabaran ancaman siber.

4 LANGKAH-LANGKAH KESELAMATAN

Langkah-langkah keselamatan yang telah dan terus dilaksanakan ialah penyebaran kesedaran melalui "Talk" yang disampaikan oleh pelbagai agensi seperti dari *Criminal Justice Division of the Attorney General Chambers, BruCERT,Royal Brunei Police Force(RBPF), AITI dan Jabatan Sekolah-Sekolah di bawah Kementrian Pendidikan* terutama sekali kepada pelajar. Antara isu yang dikongsikan adalah kepentingan mengelak dari menjadi mangsa ancaman siber yang sering berlaku kepada para pelajar. BruCERT juga telah melaksanakan pelbagai program kesedaran yang dikenali sebagai "*Secure Verify Connect*" yang bertujuan untuk meningkatkan kesedaran keselamatan bila menggunakan internet. Antara cara untuk mengawal dari menjadi mangsa ialah berhati-hati agar tidak mengongsi maklumat peribadi kepada orang-orang yang baru kita kenali, berfikir sebelum mengongsikan maklumat, bahaya berkawan dengan orang di atas talian dan cyber bullying.

Bagi maklumat-maklumat peribadi seperti kad kredit, numbur keselamatan sosial, akaun bank atau maklumat sensitif sesebuah syarikat atau organisai langkah keselamatan terbaik adalah dengan bergantung kepada enkripsi iaitu satu proses mengekod maklumat supaya hanya mereka yang mempunyai kuncinya saja boleh menyahkod. Atau jika dalam browser, pengguna boleh mengetahui jika mereka menggunakan protokol yang selamat menerusi beberapa cara. Salah satu nya adalah memastikan perkataan *"http"* alamat digantikan dengan *"https"* dan satu symbol manga kecil di *status bar* dibahagian bawah tingkap pelayar. Ini adalah penting terutama sekali bila membuat belian secara online. Antara cara yang lain juga adalah dengan mengunakan "*Two-factor authentication*" dimana untuk mengakses akaun memerlukan dua laluan, satu melalui akaun kata laluan yang biasa kemudian melalui kata laluan yang *dynamically generated* bagi memastikan ianya pemilik yang benar.

Salah satu kelemahan umum ialah disebabkan kecuaian manusia (The Global State of Information Security ® Survey 2016). Kecuaian seperti menggunakan kata laluan yang mudah diteka, tidak menukar kata laluan sekerapnya, membiarkan kata laluan diketahui seperti menampal didepan komputer atau berkongsi kata laluan. Kelalaian seperti ini tanpa di sedari telah membuka pintu bagi penceroboh memasuki sistem atau organisasi berkenaan. Ini secara tidak langsung jika dicerobohi oleh mereka yang memang berniat jahat akan menjadi satu kerugian yang besar lebih-lebih lagi bila ia jatuh kepada penjenayah kumpulan 2 dan 3. Di Brunei bagi sector kerajaan dimana semua warga kerja dibahagian kerajaan telah diisu emel akaun melalui EGNC. Untuk mengatasi kecuaian manusia, antara langkah keselamatan yang telah diambil ialah memastikan sistem pengurusan kata laluan akan diperbaharui setiap 6 bulan. Kata laluan bagi mana-mana akaun yang mengakses ke sistem-sistem atau aplikasi-aplikasi mahupun akses ke dunia siber hendaklah bukan terdiri dari yang mudah diteka, perlulah ia terhasil dari gabungan numbur, huruf besar dan huruf kecil serta simbol dan lebih dari enam gabungan. Langkah keselamatan seterusnya ialah memastikan perisian (*software)* digunakan adalah yang asli (*original*) dan bukannya cetak rompak (*pirated*) bagi mengelakkan virus atau menjadi pintu belakang (*backdoor)* bagi penjenayah siber untuk mencerobohi komputer dan akaun anda. Perisian perlu di kemas kini sentiasa bagi

memastikan pembetulan pepijat atau mengubahsuai fungsi perisian tanpa menyusun semula perisian asal.

5 CARA MENGATASI DAN MENANGANI JENAYAH SIBER

Keselamatan siber akan menjadi isu besar dan serius jika organisasi atau pengguna mempunyai informasi yang sensitif dan berharga. Melindungi dari menjadi ancaman serangan siber juga adalah sangat mahal. Mengikut dari laporan Forbes baru-baru ini yang mana perbelanjaan bagi keselamatan siber dan perlindungan jenama secara atas talian diramalkan meningkat $170 billion pada tahun 2020. Ini adalah bagi produk-produk keselamatan siber seperti *IAM, Encryption, DLP, Risk and Compliance Management, IDS/IPS, UTM, Firewall, Antivirus/Antimalware, SIEM, Disaster Recovery, DDOS Mitigation, Web Filtering dan Security Services* (Morgan, 2016).

Organisasi atau perseorangan, perlu memastikan sistem keselamatan bersesuaian dengan penggunaan dengan mengetahui apa yang perlu dilindungi agar tidak membelanjakan wang yang banyak. Untuk menyelamatkan data, menangani penipuan, dan menghalang penggodam dari melakukan jenayah, kita perlu menangani dan bersedia lebih awal. Kerana bila serangan *Web Applications, hijacking or sniffing wireless communication* terjadi kita mungkin akan terdedah kepada serangan lain seperti pelbagai serangan *DDOS; SYN, TCP* dan *HTTP DDOS* atau menjadi sebahagian dari serangan *botnet/zombie army*.

Jika sesuatu organisasi itu bergantung banyak kepada pengunaan IT maka ia akan terdedah kepada ancaman bila adanya insiden sekuriti berlaku. IBM dan CISCO telah menggunakan rangka kerja Gartner's, dalam penyediaan solusi keselamatan siber. Proses ini melalui 4 langkah: Ramal (*Predict),* Cegah *(Prevent),* Kesan (*Detect) and Bertindak (Respond)* (IBM, CISCO, Thonke, 2016):

5.1 RAMAL (*PREDICT*)

Pengguna mengetahui apa yang perlu diselamatkan dengan membuat *risk analysis* untuk mengetahui apakah kesan jika keselamatan dicerobohi; mengetahui jejak digital agar tidak menjadi pintu pencerobohan bagi serangan penjenayah siber; dan mengetahui *weak spots* agar dapat menyediakan proses utntuk menyelamatkan diri.

5.2 CEGAH (*PREVENT*)

Pengguna yang telah mengetahui *risk* dan *weak spots* boleh mengambil tindakan yang bersesuaian. Seperti mendapatkan *Endpoint Security Solution* yang terdapat *Antivirus* untuk serangan *malicious malware* dan juga dapat memastikan *patch management* yang teratur dan automatik.

5.3 KESAN (*DETECT*)

Pengguna akan menggunakan Endpoint security solution untuk mengesan virus atau malware. Jika organisasi mudah diserang, perlulah memastikan mengesanan diset kepada

advance supaya memastikan ianya dikesan secara menyeluruh. Antara cara perisian anti-virus adalah bila ia mengesan virus ia akan mengasing dan kemudian memusnahkannya. Penambahbaikan perisian perlu dilancarkan secara automatik supaya mendapat himpunan perisian atau skrip yang terkini.

5.4 BERTINDAK(*RESPOND*)

Dan langkah yang terakhir, ialah untuk bertindak jika ada ancaman, dan bertindak mengurangi ancaman, menganalisa dan mempelajari dimana kelemahan dan tempat-tempat yang menjadi ancaman serangan.

Bagi menangani masalah serius, kepakaran menangani insiden di rantau asia perlu bergabung usaha bagi memastikan semua pengguna peka akan ancaman ini dan mengambil langkah berwaspada. Pendekatan secara koloberasi bagi mengangani keselamatan siber diperlukan, dimana perisikan bagi ancaman dan teknik tindak balas adalah dikongsi bersama. Organisasi dan negara telah menyedari akan hal ini dan salah satu usaha sama yang telah dilakukan ialah dengan tertubuhnya Computer Emergency Response Team (CERT). Oleh kerana banyak kebergantungan kita kepada Internet, CERT telah ditubuhkan pada tahun 1988 sejurus selepas Internet diserang dengan ancaman worm. Sekarang CERT memfokus kepada security breach dan insiden denial-of-service (DOS), dan juga menyediakan amaran dan panduan menangani sebarang insiden. CERT juga giat dalam usaha kempen kesedaran awam dan terlibat dalam penyelidikan yang bertujuan untuk memperbaiki sistem keselamatan.

6 KESIMPULAN

Dalam dunia tanpa sempadan, seseorang itu boleh melakukan kerosakan yang besar terhadap individu, masyarat atau negara lain walaupun mereka berada jauh beribu-ribu kilometre. Kita perlu sentiasa berawas dan bersedia atas apa jua pun. Kita perlu faham dan berwaspada bahawa ancaman pengganas siber agak berbeza dengan aktiviti jenayah Internet biasa seperti mencuri kata laluan perbankan internet, penyalahgunaan kad kredit atau penipuan perniagaan laman web. Ancaman pengganas siber perlu ditangani dengan cara yang berbeza. Kesedaran adalah perlu bagi menangani ancaman siber yang datang dari pelbagai corak. Kita perlu membasmi, kerana jika ia tidak ditangani boleh mengugat kesejahteraan ummah. Bagi keselamatan sejagat, dengan tertubuhnya Computer Emergency Response Teams (CERTs), negara-negara dirantau asia telah menubuhkan kempen kesedaran keselamatan siber. Pelan tindakan juga telah di buat untuk mengawal infrastruktur yang kritikal. Ini adalah tindakan-tindakan yang penting bagi memperbaiki siber keselamatan diperingkat kebangsaan. Untuk menangani risiko yang berlandaskan aset digital, satu strategi diperlukan bagi mengabung semua usaha menjadi satu usaha yang koherent, komprehensive dan mapan (ITU, 2016)

Acknowledgements:

Brunei Computer Emergency Response Team – BruCERT, Digibytes, ITPSS/BruCERT
Brunei Times

Rujukan

Assante, M.J. Tobey, D.H. (2011). National Board of Information Security Examiners. Enhancing the Cybersecurity Workforce, *IT Professional, IEEE Computer Society*.

Cybenko. G., Giani, A., & Thompson, P. (2002). Cognitive Hacking: A Battle for the Mind. *Computer* , 35(8), 50-56

Drubin. C. (2016). Booming Opportunities in IoT Cybersecurity. *Microwave Journal*, 59(6), 52

Edward. F. (2015). Cyber Security Challenges: Protecting your transportation management center. *ITE Journal*. Retrieved from: http://library.ite.org/pub/898748dd-0c0c-2cb9-c9db-0cac2bc3bd7d

Finomore, V., Sitz, A.., Blair, E., Rahlil, K., Champion, M., Funke, G., Mancuso, V. & Knott, B. (2013). Effects of Cyber Disruption in a Distributed Team Decision Making Task, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 57, 394-398.

Gavas, E., Memon, N., & Britton, D. (2012). Winning Cybersecurity one challenge at a time. *IEEE Security and Privacy*, 10(4), 75-79 [6265104] DOI: 10.1109/MSP.2012.112

Goolsby, R. (2013). On Cybersecurity, Crowdsourcing, and Social Cyber Attack. *Commons Lab Policy Memo Series*, 1-9.

Hammond, B. (2015). FBI Issues Cybersecurity Alert for IoT Devices. *Cybersecurity Policy Report*.

Higginbotham, S. (2015). The FBI warns citizens to beware of cybercrime and the Internet of things. *Fortune*. Available from: http://fortune.com/2015/09/16/fbi-internet-of-things/

Howard, P.N., Duffy, A., Freelon, D., Hussain, M., Mari, W. & Mazaid, M. (2011). What was the role of Social Media During the Arab Spring? Opening Closed Regimes. *Project on Information Technology & Political Islam (^{P}ITPI)*. Available from: https://www.library.cornell.edu/colldev/mideast/Role%20of%20Social%20Media%20During%20the%20Arab%20Spring.pdf

ITU (2016). The Key ingredients for preparing a comprehensive National Cybersecurity Strategy and its effective implementation. Cybersecurity Workshop, *ITU, Committed to connecting the world*. http://www.itu.int/en/ITU-D/Study-Groups/2014-2018/Pages/side-events/2016/cybersecurity-workshop.aspx

Knott, B. (2014). Cyber Trust and Influence. *Proceedings of the Human Factors and Ergonoics Society Annal Meeting*, 58(1), 415-418. DOI:10.1177/1541931214581985

Kolias,C., Stavrou, A. & Voas, J. (2015). Securely Making "Things" Right. *Computer IEEE Computer Society*, 48(9), 84-88. http://doi.ieeecomputersociety.org/10.1109/MC.2015.258

Mancuso, V.F. (2014). Human Factors in Cyber Warfare II: Emerging Perspectives. *Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting*. 58(1), 415-418. DOI:10.1177/1541931214581085

Morgan, S. (2016). Worldwide Cybersecurity Spending increasing to $170 Billion by 2020. *Forbes #CyberSecurity*. Available from: http://www.forbes.com/sites/stevemorgan/2016/03/09/worldwide-cybersecurity-spending-increasing-to-170-billion-by-2020/#28fc45e576f8

RBTS (2015). Combating Cyber Security Threats, *Cyber Security Forum Brunei*. Available from: https://eiseverywhere.com/ehome/csfbrunei/home/

Thonke, J (2016). The 360 Degree Approach to Cyber Security: Cyber security as a 4-step process: Predict, Prevent, Detect, Respond. *F-Secure Business Security Insider*. https://business.f-secure.com/cyber-security-is-not-a-solution-but-a-process/