JURNAL KETAHANAN NASIONAL
Vol. 26, No. 3, Desember 2020, Hal 359-379
DOI:http://dx.doi.org/ 10.22146/jkn.57322
ISSN:0853-9340(Print), ISSN:2527-9688(Online)
Online sejak 28 Desember 2015 di :http://jurnal.ugm.ac.id/JKN

VOLUME 26 No. 3, Desember 2020 Halaman 359-379

Smartcity : Model Ketahanan Siber Untuk Usaha Kecil Dan Menengah

Ika Riswanti Putranti
Pusat Kajian Ketahanan Siber Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Diponegoro, Semarang
email:ikariswantiputranti@lecturer.undip.ac.id

Anita Amaliyah
Departmen Ilmu Komunikasi Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Diponegoro, Semarang
email: hello.anita13@gmail.com

Reni Windiani
Departemen Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Diponegoro, Semarang
email: reniwindiani@gmail.com

Dikirim: 26-06-2020; Direvisi: 29-12-2020; Diterima; 30-12-2020

ABSTRACT

This article placed an example of a cyber resilience model for smartcity in the context of smart-economy which was currently vulnerable to various cyber attacks. On the other hand SMEs were very limited in access to the development of networks and resources in building cyber resilience that ensured sustainability and increased the competitiveness of their businesses.

Furthermore, this research identified the best practices of other countries, analyzed the readiness of legal instruments in Indonesia, identified the actors involved and analyzed the factors of obstacles in building a model of cyber resilience for SMEs.

The result of this study was that security policy was a big theme with strategic principles in the security strategy of both actors and policies. This could help organizations such as MSMEs to identified, assessed and reduced threats in the cyber world.

Keywords : Smart City; Cyber Attack; Cyber Resilience; SME's,

ABSTRAK

Artikel ini meletakan contoh model ketahanan siber bagi *smartcity* dalam konteks *smart-economy* yang saat ini rentan terhadap berbagai serangan siber. Di sisi lain pelaku UKM sangat terbatas dalam akses pengembangan networking dan sumberdaya dalam membangun ketahanan siber yang menjamin keberlanjutan dan meningkatkan daya saing usahanya.

Selanjutnya penelitian ini mengidentifikasi praktik terbaik negara-negara lain, menganalisis kesiapan perangkat hukum di Indonesia, mengidentifikasi aktor yang terlibat dan menganalisis faktor-faktor hambatan dalam membangun suatu model ketahanan siber bagi UKM.

Hasil dalam pembahasan kajian ini adalah bahwasanya keamanan siber merupakan sebuah tema besar dengan prinsip-prinsip strategis dalam strategi keamanan baik berupa aktor maupun kebijakan. Hal ini dapat membantu organisasi seperti UMKM untuk mengidentifikasi, menilai, dan mengurangi ancaman dalam dunia siber.

Kata Kunci: ***Smart City; Serangan Siber; Ketahanan Siber;UKM.***

PENGANTAR

Diambil dari tulisan Williams and Manhcke Collins menurut Compact Australian Dictionary 1999, resiliensi didefinisikan sebagai "*ability to recover and return to an original state, after some event has occurred to disrupt the original state". Menurut Williams and Manhcke cyber resilience for small businesses is "the ability to defend against and to recover should a cyber incident occur and return to a normal functioning state*" (Firth, Ayoub, dan Nayaz, n.d.)

Secara umum ketahanan siber memiliki unsur tahap yang terdiri dari *identify, protect, detect, respond, recover* dan *evolve* dimana untuk memastikan setiap tahap dilakukan dengan baik maka diperlukan sebuah ekosistem yang mendukung. Dalam hal pembentukan ekosistem yang *adequate* untuk ketahanan siber maka teknologi dan militer (Chotimah, Iswardhana, dan Pratiwi, 2019) bukan merupakan salah satu unsur utama namun ada banyak unsur lain yang juga mempunyai peranan penting seperti sumber daya manusia, budaya (Fitriasari, 2019), organisasi, struktur organisasi, perangkat aturan dan kebijakan, serta kepemimpinan. Ketahanan siber mengacu pada kemampuan entitas untuk terus memberikan hasil yang diinginkan dan mempertahankan operasi bisnis meskipun ada kejadian siber yang merugikan (Rocha, dkk, 2015). Konsep dasarnya menyatukan bidang keamanan informasi, kelangsungan bisnis dan ketahanan (organisasi) bersama. Tujuan dari ketahanan siber adalah untuk mempertahankan kemampuan entitas untuk memberikan hasil yang diinginkan secara terus menerus setiap saat (Herrington dan Aldrich, 2013). Konsep ini juga mencakup kemampuan untuk memulihkan mekanisme yang ada setelah peristiwa serangan serta kemampuan untuk terus mengubah atau memodifikasi mekanisme yang ada jika diperlukan dalam menghadapi risiko baru.

Perkembangan pelayanan publik maupun swasta yang serba digital membentuk apa yang disebut sebagai era informasi ekonomi (Sudaryanto, Ragimun, dan Wijayanti, 2010). Dalam era informasi ekonomi dimana informasi dan data bisa menjadi komoditi yang lucrative bagi pasar untuk mendapatkan keuntungan ekonomi, dimana dibagi menjadi 2 wujud barang yaitu *tangible* (barang berwujud) dan *intangible* (barang tidak berwujud). Barang tidak berwujud seperti informasi, gagasan, dan kekayaan intelektual, terus meningkat dalam nilai absolut dan volume relatif (Putranti, 2015). Tren ini terlihat dari fakta bahwa kapitalisasi pasar entitas terbesar di dunia semakin didasarkan pada nilai aset informasi mereka seperti data pelanggan, data pasien, rahasia dagang, kekayaan intelektual, rahasia dagang, data transaksi, data penelusuran, dan data inovasi produk (Holzheu, dkk, 2019), sehingga saat ini data dan informasi bukan semata-mata asset fisik seperti, tanah, bangunan, peralatan, dan bahan baku. Dalam dunia bisnis, informasi telah berpindah dari peran pendukung ke peran utama dalam menentukan keberhasilan sebuah perusahaansehingga data dan informasi sekarang berada di antara aset, produk, dan layanan bernilai tertinggi. Sehingga data dan informasi dianggap sebagai critical infrastruktur bagi organisasi (Doran dan Fingleton, 2015).

Pada penelitian sebelumnya telah diambil data tingkat ketahanan siber pada Usaha Kecil Menengah (UKM) kerajinan dengan mengambil sampel Kota Semarang. UKM kerajinan dipilih, sebab industri kreatif kerajinan sangat rentan terhadap serangan

siber yang dapat mengancam keberlanjutan usaha dan daya saing produk di pasar. Dalam penelitian tahap pertama sudah dipetakan 43 pelaku UKM kerajinan yang terdaftar dalam *smartcity* Kota Semarang, dimana data yang diambil meliputi pengetahuan umum para pelaku usaha terhadap konsep ketahanan siber, penerapan ketahanan siber dalam proses usaha yang meliputi managemen, produksi, dan pemasaran (Putra, 2016). Dari hasil penelitian tahap pertama pelaku usaha UKM kerajinan Kota Semarang sebanyak 80% masih belum memahami konsep ketahanan siber sedang sisanya sebanyak 20 % hanya memahami namun belum menerapkannya secara komprehensif dalam proses usahanya (Arifin, 2018).

Penelitian ini menggunakan pendekatan analisis hukum dengan metode normatif, dengan tujuan utamanya adalah identifikasi model atau *best practice* negara-negara lain seperti Inggris, Singapura, dan Australia terkait ketahanan siber pada sektor UKM. Tidak hanya itu, identifikasi kesiapan kerangka hukum di Indonesia serta aktor-aktor yang terlibat dan menganalisa hambatan dalam membangun suatu model ketahanan siber bagi UKM.

PEMBAHASAN

Komparasi Model Membangun Ketahanan Siber Bagi UKM.

Pertama, Inggris (United Kingdom)

United Kingdom (UK) dengan sektor UKM mendukung sektor kerja swasta di negara tersebut sekitar 60% dari total bisnis yang menyerap tenaga kerja, dan 99% sebagai populasi bisnis sektor swasta. Namun, pemerintah Inggris menilai bahwa hampir setengah dari populasi tersebut (43%) tidak memiliki bisnis model yang berkesinambungan (*sustain*). Dalam perkembangan era digitalisasi, maka inovasi dan juga kreativitas usaha sebagai satu dari sekian langkah capaian dalam basis pelanggan, meski era digital atau siber memiliki ancaman yang cukup serius dalam sektor UKM di UK (Herrington dan Aldrich, 2013). Dengan mengembangkan sikap ketahanan dunia maya yang didasarkan pada mengikuti beberapa langkah sederhana, UKM tidak hanya dapat bertahan tetapi berkembang di dunia digital baru.

Berdasarkan *Cyber Security Breaches Survey* pada tahun 2019, bahwa 78% U**KM** melihat *cyber security* sebagai salah satu prioritas dalam proses bisnis mereka. namun begitu cara pandang tersebut tidak kemudian diiringi dengan implementasi pembenahan proses manajemen resiko dalam ketahanan siber dalam proses bisnisnya. Inggris UKM selama setahun mendapat serangan sebanyak 7 juta kali secara kolektif. Berdasarkan laporan *Federation Small Businesses* (FSB) serangan ini ini telah membawa kerugian sebesar 5, 26 Milyar Pound Sterling terhadap ekonomi Inggris. dari 93% UKM yang sudah melindungi bisnis mereka dari serangan *cyber* 66% di antaranya telah menjadi korban dari serangan siber dalam 2 tahun terakhir yaitu tahun 2018 dan 2017. Serangan yang paling banyak terjadi yaitu berupa PC yang dilaporkan oleh hampir 49% dari responden. Sebuah temuan menarik di Inggris bahwa hanya 24% dari UKM itu yang menerapkan kebijakan terhadap app keamanan Tinggi sebuah password, 4% nya hanya menulis mengenai prosedur tentang apa yang harus dilakukan apabila terjadi serangan online atau serangan siber dan 2% di antaranya yang paham mengenai standar keamanan siber dalam ISO27001.

Di Inggris khusus untuk UKM telah disediakan *cyber esensials certification*, di mana tujuannya untuk praktik keamanan siber. UKM yang 100% patuh terhadap *cyber esensial certification* 80% di antaranya mampu melakukan mitigasi terhadap risiko keamanan siber seperti *malware, social engineering Attack* dan *hacking*. Sertifikasi ini dilakukan dengan cara yang mudah yaitu UKM bisa melakukannya melalui media virtual atau disebut sebagai *virtual online security officer* (VOSO).

Ketahanan siber yang bagus dapat dibangun seiring sejalan dengan keamanan siber yang baik. Ketahanan siber diperlukan untuk memastikan bahwa bisnis dapat terus beroperasi dan *sustain* meskipun pada saat diserang maupun setelah serangan, sedangkan keamanan siber adalah langkah proaktif untuk melakukan mitigasi risiko.

Sebuah survei di Inggris menyatakan bahwa 52% pembuat keputusan bidang IT tidak memiliki strategi ketahanan siber. Namun begitu 51% persen di antaranya percaya bahwa hal tersebut akan membawa dampak negatif terhadap bisnis mereka. Karena isu terkait dengan ketahanan siber sangat berhubungan dengan keberlangsungan bisnis yang bergantung kepada kepercayaan klien terhadap sistem IT perusahaan. Dimana 40% pembuat keputusan IT melihat *data stolen* sebagai salah satu ancaman selain *phising* atau *scamming,* sehingga 37% di antaranya mengatakan bahwa pengarsipan dan e-discovery adalah salah satu strategi ketahanan siber.

Serangan *malware* yang sangat merusak telah mampu melumpuhkan beberapa sektor penting di UK seperti sektor finansial, sektor kesehatan, sektor pertambangan, maupun *government critical infrastructure* untuk beroperasi. Hal tersebut mendorong untuk pembentukan *legal frameworks* dan *governance* dalam ketahanan siber termasuk adanya sistem *reward* berupa insentif bagi yang patuh dan *punishmen* bagi ketidakpatuhan, sehingga organisasi harus mampu bereaksi dengan cepat dan efektif terhadap serangan siber.

Pada 10 Mei 2018 UK membentuk *The Network and Information Systems Regulations* 2018 atau biasa disebut sebagai *The NIS Regulations*, merupakan implementasi dari *The EU's NIS Directive* (*Directive on security of network and information systems*) tahun 2016 (John, 2018). *The EU's NIS Directive* merupakan undang-undang keamanan siber yang sangat luas di EU. Tujuannya adalah untuk mewujudkan terbentuknya sistem keamanan tingkat tinggi terhadap seluruh infrastruktur kristis di EU. Sedangkan di UK pembentukan perangkat aturan tersebut memperlihatkan perubahan komitmen peran regulator dalam hal ini pemerintah dari hanya pihak pendorong menjadi pengatur dan pengawas yang memaksa peningkatan kepatuhan para pihak yang subjek.

Dengan diberlakukannya aturan tersebut ada 2 subjek hukum yang harus tunduk terhadap standar kepatuhan yang ada yaitu *Operators of Essential Services* (OES) dan *Relevant Digital Service providers* (RDSP). OES (*operators of essential services*) ini mencakup sektor energi, transpor, kesehatan, air, dan infrastruktur digital. Sedangkan RDSPs (*digital service providers*), dibagi menjadi tiga kelompok yaitu *online search engines*, *online marketplaces* dan *Cloud computing services*. Namun begitu aturan tersebut tidak berlaku bagi RDSPs yang merupakan perusahaan kecil atau micro, yang mana mempunyai pekerja kurang dari 50 orang dan laba tahunan atau *balance sheet total* kurang dari 10 juta pound.

Dengan berlakunya *The 'NIS Regulation"* di UK OES dan RDSP harus memastikan *cyber security measures* dalam bisnis mereka untuk mengelola sistem dan fasilitas keamanan, proses bisnis dan prosedur dalam menangani masalah serangan siber dan memastikan keberlangsungan bisnis (European Comission, 2017). Untuk OES wajib mendaftarkan diri ke *Competent Authority* yang berlaku bagi setiap sektor dimulai pada tanggal 20 Agustus 2018. OES dianggap merupakan sektor kritis dan strategis, sehingga mempunyai standar yang jauh lebih tinggi dan ketat serta merupakan subjek audit *Competent Authority.* OES akan diaudit berdasarkan 14 prinsip keamanan dalam *Cyber-assessment framework* yang diterbitkan oleh *UK National Cyber Security Centre* (NCSC). Apabila ditemukan *non-compliance* terhadap *the NIS Regulation* maka berpotensi untuk diberikan sanksi mulai dari peringatan tertulis sampai ke sanksi denda maksimum 17 juta pound.

Sedangkan untuk RDSP tidak akan diaudit, namun jika terjadi serangan siber maka hanya akan dilakukan penyelidikan. RDSP diberikan waktu tenggang yang lebih lama untuk mendaftarkan diri ke *Competent Authority* mulai 1 November 2018. Bagi organisasi atau lembaga yang dikategorikan sebagai OES atau RDSP yang tidak mendaftar dianggap sebagai pelanggaran terang-terangan terhadap Peraturan NIS, dan dapat menyebabkan *non-compliance.*

***Kedua,* Singapura**

UKM atau *Small Medium Enterprises* (SME) berkontribusi hanya di bawah setengah dari Produk Domestik Bruto (GDP) Singapura dan mempekerjakan 70% tenaga kerja. Mereka adalah tulang belakang dari perekenomian Singapura. Berdasarkan *Global Risk Perception Survey* yang dilakukan oleh IMF pada tahun 2019, serangan siber atau *cyberattacks* merupakan resiko global paling penting nomor lima berdasarkan kemungkinan selama 10 tahun, tepat dibelakang "penipuan dan pencurian data besar-besaran" (*massive data fraud and theft*) yang berada di posisi keempat, seperti yang ditulis dalam artikel businesstimes.com Singapura.

Hal ini merupakan tren yang mengerikan bagi Singapura, dimana UKM membentuk 99 persen bisnis dan mempekerjakan lebih dari 70 persen tenaga kerja. UKM menempati posisi yang penting di dalam perkembangan nilai rantai ekonomi dan merupakan bagian dari ekonomi digital. Lebih lanjut, UKM merupakan penghubung pertama dalam rantai pasok bisnis Singapura, dan juga sebagai subkontraktor dan vendor dari perusahaan besar serta agen pemerintah. Banyak dari perusahaan kecil ini menyediakan layanan mulai dari bebersih hingga pemasaran, sumberdaya manusia dan pembuatan konten. Mereka beroperasi pada model ekonomi fleksibel yang menyimpang dari pengaturan jam kerja yang konvensional. Para pegawai dapat bekerja dari rumah, kafe, bahkan dalam perjalanan. Hal ini menciptakan resiko keamanan yang baru dikarenakan banyak dari mereka yang memilih untuk bekerja menggunakan laptop atau *handphone* pribadi, yang tentunya tidak menawarkan enkripsi data dengan kualitas tinggi yang dibutuhkan untuk transaksi bisnis. Dengan semakin banyaknya UKM yang beralih ke digital dalam area industri 4.0, mereka mungkin menemukan diri mereka terpapar oleh ancaman siber yang semakin marak dan terus tumbuh, seperti serangan *phishing*, *defacements*, dan *ransomware* (Rad dan Jahromi, 2014).

Bagi banyak UKM yang melaksanakan *running lean*, ketika sistem mereka diretas berarti operasi normal akan berhenti. Hal ini tidak hanya akan menimbulkan kehilangan pendapatan tetapi juga akan mempengaruhi reputasi bisnis mereka. Serangan malware mungkin akan menjadi awal dari akhir bisnis yang kecil. Lebih lanjut, mereka juga akan dapat menghadapi masalah hukum jika data pribadi dicuri.

Dengan ekonomi Singapura yang menjadi semakin digital, penting bagi bisnis di sini untuk mengembangkan pertahanan keamanan siber mereka. Ini sangat penting untuk usaha kecil dan menengah (UKM), yang saat ini merupakan 99 persen dari perusahaan nasional, dua pertiga dari tenaga kerja kita, dan hampir 50 persen dari Produk Domestik Bruto negara. Hal ini dapat terlihat, dimana Bisnis-ke-Konsumen dan Bisnis-ke-Bisnis dilakukan terutama melalui transaksi digital. Hal ini termasuk melakukan pembayaran online melalui kartu kredit dan bentuk pembayaran smartphone lainnya. Untuk bisnis, pelanggaran data dapat mengakibatkan biaya hukum tinggi dan hilangnya reputasi merek.

Menurut Laporan Ancaman Keamanan Internet 2016 oleh perusahaan *cybersecurity Symantec*, usaha kecil menyumbang 43 persen yang mendapat serangan *phishing* secara global. Selain itu, laporan *Perpustakaan Digital IEEE Computer Society, "Cybersecuring Small Businesses"*, berpendapat bahwa bisnis kecil cenderung menjadi mangsa yang mudah bagi penjahat *cyber* karena jaringan mereka yang tidak terlindungi. Dengan menargetkan bisnis yang lebih kecil, penjahat siber dapat dengan mudah mengeksploitasi celah keamanan mereka untuk mendapatkan akses ke data pelanggan mereka dan juga dari perusahaan besar yang bekerja dengan bisnis kecil ini.

Dengan banyaknya warga Singapura yang bekerja di UKM, serangan *cyber* berskala besar akan berdampak buruk pada perekonomian. Data pelanggan yang dicuri menimbulkan risiko bisnis dan reputasi bagi perusahaan. Bahkan bisa menyebabkan denda yang lumayan dari hukum. Meskipun denda kecil, umumnya kurang dari $ 50.000, *Personal Data Protection Act 2012* (PDPC) dapat mendenda perusahaan hingga $ 1 juta per pelanggaran data.

Bagi banyak UKM, peretasan (*hacking*) berarti operasi normal berhenti. Perusahaan manufaktur tidak akan dapat mengoperasikan dan memantau pabrik mereka. Dan perusahaan desain tidak akan dapat melakukan desain apa pun. Ini semua menyebabkan hilangnya pendapatan. Bagi banyak perusahaan yang tidak memiliki program keamanan siber atau rencana kesinambungan bisnis, peretasan bisa memicu awal dari akhir.

Hampir 40 persen serangan cyber di Singapura menargetkan usaha kecil dan menengah (UKM), menurut *Cyber Security Agency of Singapore* (CSA). Upaya *phishing* dan *ransomware* adalah metode yang paling umum digunakan. Menurut publikasi *Singapore Cyber Landscape* 2017, beberapa 2.040 situs web terdeteksi di Singapura. Mayoritas dari mereka adalah situs web UKM dengan bisnis mulai dari desain interior hingga manufaktur (FSB, 2016). Dalam survei yang dilakukan oleh spesialis Asuransi QBE, 491 UKM di berbagai industri di Singapura disurvei, ditemukan bahwa meskipun 90 persen responden mengaku sadar akan potensi risiko siber, satu dari empat masih tidak memiliki proses internal atau kebijakan untuk melindungi diri mereka sendiri. Untuk UKM berukuran lebih kecil, angkanya mencapai sepertiga. Hal ini terutama disebabkan

oleh fakta bahwa UKM percaya bahwa mereka terlalu kecil untuk ditargetkan oleh penjahat siber karena mereka tidak memiliki sesuatu yang pantas untuk dicuri. Selain itu, kesalahpahaman bahwa *cybersecurity* adalah masalah bagi departemen TI tetap ada. Karena kurangnya anggaran, keahlian dan kemampuan teknis untuk menerapkan langkah-langkah yang efektif, banyak UKM di Singapura terus tidak siap untuk mempertahankan diri dari serangan siber (*cyberattacks*).

Langkah pertama yang perlu diambil oleh UKM untuk memperkuat pertahanan bagi bisnis mereka adalah dengan benar-benar sadar akan ancaman siber yang berisiko. Artinya, mereka perlu tahu, dalam konteks bisnis mereka, kemungkinan bahwa sumber ancaman yang diberikan akan menimbulkan kerentanan tertentu dan dampak yang dihasilkan akan terjadi. Perusahaan juga perlu mengidentifikasi dan memahami aset kritis mereka yang memerlukan perlindungan, dan mengambil langkah-langkah untuk mencegah dan mendeteksi akses ilegal atau tidak sah. Seharusnya kebutuhan bagi setiap individu untuk memahami bahwa keamanan siber menjadi perhatian semua orang, bukan hanya departemen TI. Bahkan jika sistem TI dikelola oleh vendor pihak ketiga, organisasi itu sendiri perlu memastikan bahwa vendor memiliki rencana yang jelas dalam melindungi sistem dan data.

Secara khusus, UKM perlu mengambil langkah proaktif untuk menanamkan kewaspadaan risiko dunia maya dalam staf mereka. Saat Singapura bergerak menuju *Smart Nation*, pemerintah telah, melalui berbagai *Institutes of Higher Learning* (IHLs), serta *Private Continuing Education Training* (CET) atau Pelatihan Pendidikan Lanjutan Pribadi, yang menawarkan harga subsidi yang lebih tinggi untuk kursus kesadaran keamanan siber (*cybersecurity*). Ini telah dilakukan sebagai bagian dari upaya untuk memastikan bahwa karyawan Singapura dan PR memiliki peralatan yang lengkap dan tetap tangguh terhadap serangan siber.

Pemerintah Singapura sudah bekerja pada ketahanan dunia maya. Akhir bulan ini, parlemen akan memperdebatkan (dan tidak diragukan lagi akan meloloskan) Undang-Undang Keamanan Siber. Undang-undang ini akan mengatur Infrastruktur Informasi Kritis, dan menyediakan kerangka kerja bagi pemerintah untuk membantu perusahaan-perusahaan yang menyelenggarakan sistem vital agar lebih tahan terhadap dunia siber *(cyber resillienece)*, yaitu (1). Memberikan subsidi, atau keringanan pajak bagi UKM untuk membeli dan mengimplementasikan perangkat lunak manajemen kerentanan dan anti-virus. (2). Memberikan hibah, atau keringanan pajak bagi UKM untuk menyewa konsultan keamanan TI pihak ketiga untuk mengevaluasi jaringan perusahaan mereka terhadap kelemahan siber. (3). Mengizinkan pelaporan tidak salah (*no-fault*) data pelanggaran ke PDPA. Ini meyakinkan UKM bahwa mereka bisa mendapatkan bantuan ketika mereka dilanggar tanpa dihukum. Ini juga akan membantu CSA melacak jenis-jenis serangan siber yang terjadi di Singapura. (4). Pemerintah mungkin ingin mengembangkan kampanye untuk mendidik UKM tentang risiko ketika tidak menerapkan program *Cybersecurity*. Masalah paling serius adalah banyak orang tidak tahu seberapa rentan mereka.

Singapura adalah negara yang sangat terhubung yang terdiri dari jaringan kuat Usaha Kecil dan Menengah (UKM). Namun, meskipun beberapa upaya telah dilakukan

di masa lalu untuk memperkuat keamanan jaringan ini, UKM ini telah, dan terus rentan terhadap serangan siber. Pada 2017, ada peningkatan yang signifikan dalam kejahatan dunia maya di Singapura, seperti yang dilaporkan oleh Angkatan Kepolisian Singapura atau *Singapore Police Force* (SPF). Lebih dari 5340 kasus kejahatan dunia maya dilaporkan yang merupakan peningkatan 1% dari 2016 dan menjadikan persentase kejahatan dunia maya menjadi 16,6%. Baru-baru ini di bulan Juli, peretas menyusup ke sistem *Sing Health* dan mendapatkan akses ke data pribadi lebih dari 1,5 juta orang (Anto, 2018).

Menurut laporan *Singapore Cyber Landscape 2017* oleh *Cyber Security Agency of Singapore* (CSA), hampir 40% dari semua serangan siber di Singapura menargetkan UKM. Yang lebih mengkhawatirkan lagi adalah bahwa ini hanya kasus yang dilaporkan yang berarti bahwa persentase ini kemungkinan akan jauh lebih tinggi dalam kenyataan. Laporan CSA menyoroti banyak angka dan statistik tentang ancaman siber yang dihadapi UKM di Singapura pada 2017 dan mendesak perlunya mekanisme keamanan yang kuat. Berikut ini adalah rincian bagaimana angka-angka tersebut tampak untuk ancaman siber umum seperti *defacements* situs web, infeksi *malware*, dan *phishing*.

Bisnis, khususnya UKM, adalah target serangan siber paling umum di Singapura. Alasan kerentanan ini adalah karena UKM kekurangan sumber daya dan pengetahuan untuk mengadopsi solusi keamanan siber yang diperlukan. Saat ini, banyak dari UKM ini tanpa rencana kesinambungan bisnis atau program keamanan siber. Perusahaan-perusahaan seperti itu terkena *ransomware*, *malware*, dan berbagai ancaman dunia siber.

Selain organisasi itu sendiri, CSA bekerja sama dengan mitranya untuk meningkatkan ketahanan Singapura terhadap kejahatan dunia siber. Upaya ini memperkenalkan Undang-Undang Keamanan Dunia Maya *(Cybersecurity Act)*, kampanye seperti *GoSafeOnline* dan *SingCERT*, dan pengembangan inisiatif *Smart Nation* untuk meningkatkan kesadaran tentang kejahatan dunia maya.

Ancaman dunia siber terhadap UKM Singapura meningkat selama beberapa tahun terakhir dengan jumlah insiden meningkat secara signifikan. Kurangnya kesadaran ditambah dengan tidak adanya sistem keamanan siber di UKM adalah penyebab utama di balik meningkatnya serangan siber. Langkah selanjutnya untuk UKM adalah bekerja sama dengan CSA untuk meningkatkan ketahanan siber mereka sendiri dan Singapura secara keseluruhan.

Infrastruktur keamanan siber perusahaan dinilai sebagai bagian dari portofolio risiko mereka secara keseluruhan. Infrastruktur keamanan siber yang baik meyakinkan pelanggan dan mempertahankan loyalitas pelanggan. Walaupun UKM menyadari ancaman siber, mereka tidak berbuat banyak untuk melindungi diri mereka sendiri. Salah satu masalah yang mereka hadapi adalah kurangnya keahlian dalam organisasi mereka. Seperti yang diamati oleh Menteri Komunikasi dan Informasi Yaacob Ibrahim dalam Anggaran 2016, perusahaan kecil tidak memiliki kemampuan atau pengetahuan IT yang diperlukan untuk menegakkan praktik keamanan siber dalam bisnis mereka. Dia menambahkan bahwa, pada 2016, masih ada 15.000 lowongan di sektor Teknologi Informasi dan Komunikasi (TIK), tidak berubah dari 2014. Pada 2012, data dari Badan Pengembangan Ekonomi atau *Economic*

Development Board (EDB) menunjukkan bahwa hanya 0,8 persen dari 144.300 pekerja TIK Singapura adalah spesialis keamanan TI. Kurangnya keahlian TI mencerminkan prioritas perusahaan, dengan biaya yang secara alami menjadi salah satu perhatian terbesar mereka. Untuk UKM yang berjuang untuk tetap bertahan di tengah tantangan lokal dan global yang lebih besar, biaya mengadopsi praktik keamanan dunia maya akan menambah tekanan keuangan mereka.

Yaacob Ibrahim, Menteri Komunikasi dan Informasi, telah memberikan poin penting dalam pidatonya pada presentasi Anggaran 2016 di Parlemen. Menteri mencatat bahwa sementara pelanggaran siber *(cyber breaches)* di perusahaan besar dapat menjadi berita utama, UKM juga tidak luput karena kurangnya perlindungan keamanan siber sehingga juga menjadikannya sasaran empuk. Dengan demikian, masuk akal bagi perusahaan untuk melibatkan penyedia keamanan terkelola seperti *StarHub* untuk memberi mereka lapisan perlindungan tambahan saat mereka berkonsentrasi pada lini bisnis mereka.

Menanggapi hal tersebut, Menteri Komunikasi dan Informasi, Yaacob Ibrahim mengatakan bahwa pemerintah menanggung banyak biaya untuk memadamkan keamanan siber dan memperkuat respon terhadap ancaman di tingkat nasional, termasuk latihan keamanan siber reguler dan mengerahkan tim respon insiden siber nasional untuk melawan berbagai ancaman. Otoritas Singapura telah memperkenalkan berbagai inisiatif non-legislatif yang bertujuan untuk meningkatkan standar keamanan siber. CSA juga telah menerbitkan referensi tambahan untuk membantu pemilik CII secara proaktif mengamankan dan membangun ketahanan ke dalam sistem mereka, seperti *Security-by-Design Framework*, yang dikembangkan untuk memandu pemilik CII melalui proses menggabungkan keamanan ke dalam siklus hidup pengembangan sistem mereka. *The Singapore Computer Emergency Response Team* (SingCERT), yang merupakan bagian dari CSA, memfasilitasi pendeteksian, penyelesaian dan pencegahan insiden terkait keamanan siber di internet. Terkadang juga menerbitkan peringatan, saran dan rekomendasi yang merinci prosedur atau tindakan mitigasi bagi organisasi untuk menanggapi ancaman siber baru.

Pemerintah Singapura telah menyatakan secara terbuka bahwa tidak akan menyediakan dana untuk mengimbangi biaya kewajiban CII yang merupakan persyaratan peraturan berdasarkan Undang-Undang Keamanan Siber *(The Cybersecurity Act)*. Namun, pemerintah telah menetapkan beberapa skema untuk meningkatkan kemampuan keamanan siber (*cybersecurity*) UKM, serta perusahaan dan organisasi lainnya. Sebagai contoh, IMDA telah mendirikan *SME Digital Tech Hub*, yang merupakan suatu pusat kegiatan khusus yang menyediakan saran khurus terkait teknologi digital untuk UKM di berbagai bidang termasuk, tetapi tidak terbatas pada, analitik data dan keamanan siber.

Pusat kegiatan ini juga bekerja dengan Pusat UKM dan Asosiasi Dagang & Badan untuk memberikan bantuan dalam menghubungkan UKM dengan vendor dan konsultan teknologi digital, serta mengadakan lokakarya dan seminar untuk meningkatkan kemampuan digital UKM. CSA dan IMDA juga telah menjalin kemitraan dengan organisasi-organisasi swasta melalui Program Sumber Daya Teknologi Informasi Kritis Plus, Skema Profesional Keamanan Siber, program *Cyber Associates and Technologists* dan inisiatif *Tech Skills Accelerator*. Kemitraan

ini membantu untuk melatih dan meningkatkan keterampilan para profesional dengan teknologi *infocomm* (TIK) atau disiplin teknik, yang memungkinkan mereka untuk memiliki peran pekerjaan dalam keamanan siber *(cybersecurity)* melalui pelatihan di tempat kerja yang dipimpin oleh perusahaan.

CSA, melalui *Cyber Security Awareness Alliance*, juga telah menerbitkan panduan dan sumber daya lain tentang berbagai topik seperti mengamankan perusahaan dan mengatasi penipuan *e-commerce*, dan menyediakan panduan untuk UKM seperti *Employee Cyber Security Kit*, yang menampilkan penilaian awal dalam kesiapan keamanan siber perusahaan dan menindaklanjuti dengan program pendidikan keamanan siber yang direkomendasikan. Di bidang sertifikasi dan akreditasi, pemerintah juga telah mengumumkan bahwa akan mengizinkan penyedia layanan kecil untuk mengajukan dana pemerintah guna menutup sebagian biaya untuk menjadi perusahaan anggota *the Certification Registry for Electronis Share Transfer* (CREST). CREST Singapura telah didirikan dalam kolaborasi dan kemitraan dengan CSA, Asosiasi Profesional Keamanan Informasi, MAS, Asosiasi Bank di Singapura dan IMDA, dan menawarkan berbagai sertifikasi untuk layanan keamanan siber di Singapura. Dalam praktiknya, pemerintah biasanya berkonsultasi dengan pihak-pihak terkait dalam mengembangkan standar legislatif dan peraturan.

Sebagai contoh, sebelum pengenalan Undang-Undang Keamanan Siber *(the Cybersecurity Act)*, pemerintah telah melakukan beberapa putaran konsultasi dengan pemilik CII yang potensial, asosiasi industri dan ahli keamanan siber. Pemerintah juga telah mengumumkan bahwa akan terus bekerja dengan industri dan mitra asosiasi profesional untuk membentuk rezim akreditasi bagi para profesional keamanan siber.

Pemerintah telah secara aktif mempromosikan keamanan siber melalui kolaborasi penelitian dan pengembangan (Litbang) antara pemerintah, akademisi dan industri. Pada tahun 2013, pemerintah meluncurkan Program R&D *Cybersecurity* Nasional untuk mempromosikan kolaborasi penelitian tersebut, dengan total dana sebesar 190 juta dolar Singapura yang telah tersedia untuk mendukung program ini hingga tahun 2020. Pemerintah juga telah memulai inisiatif lain seperti *Cybersecurity Consortium* dengan dana sejumlah 1,5 juta dolar Singapura selama tiga tahun sejak 2016, dan Laboratorium R&D *Cybersecurity* Nasional. SingCERT juga bekerja dengan CERT sektoral, jika perlu, untuk memberikan informasi pada perusahaan lokal dan pelanggan yang terpengaruh tentang ancaman dan insiden keamanan siber.

***Ketiga*, Australia**

Laporan dari *the Australian corporate regulator* mengungkapkan bahwa perusahan-perusahan besar di Australia menunjukkan tingkat ketahanan siber yang relatif tinggi. Hal tersebut berdasarkan hasil survei dari 101 perusahaan Australia (29 perusahaan besar dan 72 UKM). Hasil analisis laporan tersebut didapatkan dari hasil penilaian sendiri berdasarkan dari bank investasi, operator pasar, penyedia pasca infrastruktur perdagangan dan lembaga pemeringkat kredit.

UKM telah menemukan manajemen informasi resiko yang menantang. Namun, hampir setengah UKM melaporkan bahwa mereka saat ini mengalami jatuh tempo baik secara parsial ataupun berdasarkan informasi resiko. Laporan ini menjelaskan secara parsial

seperti tidak ada atau tidak diformalkannya suatu kebijakan, dan menjelaskan informasi resiko seperti ketika kebijakan jarang diperbaharui dan tidak diikuti secara konsisten. *User Access Management* (UAM) merupakan area terkuat untuk UKM dengan 83% melaporkan jatuh tempo pada saat ini secara berulang atau adaptif. Berulang disini diartikan ketika secara teratur diperbaharui dan terdapat langkah-langkah dalam memastikan kebijakan berkembang dengan pasar diikuti dan adaptif. Hampir 40% UKM melaporkan lemah dalam praktik pemantauan dan deteksi. Namun, mereka menargetkan adanya peningkatan 32% dalam 12-18 bulan kedepan. 61% kematangan berulang atau adaptif ini membuat UKM bekerja pada bidang lain seperti pendidikan dan kesadaran pengguna.

Bahwa 40% UKM melaporkan tingkat kematangan parsial atau informasi resiko untuk kedua area, sehingga ini merupakan prioritas untuk perusahan besar, yang memiliki 21% di posisi parsial atau informasi resiko. tetapi semua perusahaan menunjukkan bahwa mereka mempunyai rencana untuk memprioritaskan adanya pelatihan kesadaran pengguna kedepannya (Wahid, 2017). Kebijakan dan proses keamanan perlindungan IT merupakan area yang relatif kuat untuk UKM, meskipun masih terdapat ruang untuk perbaikan, terutama seputar keamanan seluler dan media yang dapat dipindahkan. Lebih dari 40% perusahaan saat ini jatuh tempo secara parsial atau informasi resiko, sehingga memerlukan peningkatan secara signifikan di sekitar manajemen respon insiden. Dengan tema umumnya adalah kurangnya proses formal. Menurut laporan, hal yang sama berlaku untuk perusahaan besar.

Cathie Armor, Komisioner ASIC mengatakan bahwa 'ketahanan siber saat ini dianggap secara luas sebagai salah satu kekhawatiran yang paling signifikan untuk sektor pasar keuangan dan ekonomi pada umumnya'. Sementara dalam masalah ini, terdapat laporan kami yang menunjukkan bahwa adanya keterlibatan yang lebih besar oleh perusahaan. Tidak memadainya perusahan dan investasi menyebabkan adanya perbedaan dalam langkah-langkah ketahanan siber. 'Ketahanan dunia bukan hanya masalah IT tetapi juga membutuhkan respon dari seluruh organisasi. Ancaman dunia maya yang bersifat dinamis sehingga membutuhkan komitmen yang komprehensif dan jangka panjang untuk ketahanan dunia maya oleh semua organisasi yang beroperasi di ekonomi Austalia'.

Bisnis kecil adalah bisnis yang mempekerjakan kurang dari 20 orang, dan termasuk bisnis yang tidak mempekerjakan (ABS, 2010). Bisnis yang tidak mempekerjakan (seperti wiraswasta pekerja mandiri) mewakili 61% dari sektor usaha kecil (COSBOA). Artinya, bisnis yang tidak mempekerjakan sering kali merupakan bisnis rumahan satu orang. Akun bisnis kecil menyumbang sekitar 95% dari semua bisis yang beroperasi di Australia. Karena merupakan bisnis rumahan satu orang dan mewakili 61% dari sektor usaha kecil serta menyumbang sekitar 95% dari sema bisnis yang beroperasi di Australia, sehingga perlu untuk mempertimbangkan ketahanan siber usaha kecil tersebut. Komputer di rumah sangat mungkin juga menjadi komputer bisnis kecil yang tidak cukup terlindungi dari ancaman komputer seperti *malware* dan *intrusion.*

Untuk mencegah adanya gangguan yang masuk ke dalam jaringan, maka suatu sistem perlindungan memerlukan beberapa lapis keamanan, baik dalam bentuk fisik seperti perlengkapan keamanan, sampai pada

bentuk non-fisik seperti pembaharuan sistem operasi dan aplikasi perangkat lunak. Dalam usahanya untuk meningkatkan ketahanan siber Australia, maka diperlukan untuk memberikan pengetahuan kepada para pengusaha kecil mengenai beberapa kemungkinan ancaman yang dapat timbul dari internet (Kourtit, dkk, 2014). Mengingat bahwa 90% dari seluruh pengusaha Australia telah memiliki akses terhadap internet dan 42% telah memiliki laman pribadi (ABS, 2010). Hal ini dapat diartikan bahwa hampir seluruh pengusaha Australia rentan terhadap ancaman siber.

Jika dibandingkan dengan suatu organisasi besar, pengusaha kecil berada jauh kekurangan dalam urusan keuangan, waktu dan sumber daya manusia yang tersedia (McDermid, Mahcke dan Williams, 2009). Dengan adanya kekurangan dalam hal waktu dan pengetahuan yang cukup, maka dapat diartikan bahwa pengusaha kecil menunjukkan reaksi yang berbeda jika dibandingkan dengan suatu organisasi besar. Dalam hal ini, pengusaha kecil terlihat tidak melakukan peningkatan dan penyesuaian dalam bidang keamanan informasi mereka, tidak seperti apa yang dilakukan oleh organisasi besar. Pengusaha kecil memilih untuk tidak memperkerjakan seseorang ahli Informasi Komunikasi dan Teknologi (ICT) untuk meningkatkan keamanan meraka, karena di dalam praktiknya sendiri, usaha mereka sudah terlalu sibuk dengan ditambahnya kekurangan sejumlah tenaga kerja (McDermid, Mahcke dan Williams, 2009). Jika Google yang memiliki sistem keamanan tinggi dapat terkena serangan siber, maka setiap pengusaha di Australia juga rentan terhadap serangan siber. Bagaimanapun, terdapat perbedaan yang jauh antara sumber daya yang dimiliki oleh pengusaha kecil dan organisasi besar.

Survei yang dilakukan oleh *Cybersecurity Watch Survey* (Deloitte, 2010), menemukan bahwa hampir seluruh pengusaha yang telah disurvei mengatakan bahwa mereka telah memiliki sistem keamanan yang memadai untuk melindungi usaha mereka, namun mereka memiliki kesadaran yang kurang mengenai serangan siber. Di lain sisi, terdapat sebuah laman *Stay Smart Online* (2010) yang menyediakan pelatihan dan petunjuk mengenai kesadaran akan internet, bahkan pemerintah Australia telah mendanai beberapa program yang berhubungan dengan keamanan perdagangan elektronik. Namun, karena tidak adanya koordinasi dan pendekatan yang jelas oleh pemerintah, menyebabkan pengusaha kecil tidak mengetahui mengenai hal ini. Sama halnya dengan *home user*, pengusaha kecil bertanggungjawab terhadap komputer dan jaringan mereka terhadap dunia luar. Hal ini dapat berarti bahwa tidak terdapatnya cukup ahli di dalam usaha kecil untuk berhadapan dengan kesadaran akan kemanan dan isu ancaman siber. Dan juga, adanya biaya yang harus ditanggung oleh usaha tersebut, yang di mana terkadang sulit untuk memperhitungkan untung rugi antara kemanan yang didapat dan biaya yang dikeluarkan.

Terdapat cara lain yang dapat dilakukan oleh pemerintah untuk melaksanakan kewajibannya dalam meningkatkan keamanan bagi pengusaha kecil, seperti program nasional untuk meningkatkan kesadaran, pendanaan pelatihan melalui berbagai asosiasi atau organisasi seperti Asosiasi Penguasaha Kecil di Australia (Andres dan Round, 2015). Lebih lanjut, perlu adanya intergasi antara teknologi dengan keamanan, dibandingkan dengan menyerahkan tanggung jawab tersebut kepada pengguna untuk menerapkan sistem keamanan berlapis dan melakukan penyerangan, sehingg

para pengembang perangkat keras dan perangkat lunak dapat bekerjasama untuk menemukan teknologi keamanan yang praktis dan efektif. Dalam pandangan yang lebih luas, dorongan penuh untuk dilakukannya penyatuan keamanan ke dalam teknologi komputer dan perangkat lunak dapat menyebabkan adanya batasan terhadap pengetahuan dan akses tersebut terhadap para ahli. Ini menyebabkan keamanan bagi para pengguna seperti membeli mobil baru dan harus menggunakan rem dan kantong udara yang telah disediakan, atau dengan kata lain terdapat biaya tambahan dan ahli yang diperlukan untuk mendapatkan rasa aman dan nyaman.

Sebagai bagian dari *Australian Signals Directorate* (ASD), *Australian Cyber Security Centre* (ASCS) menyediakan berbagai petunjuk, pendampingan, dan tanggapan operasional mengenai keamanan siber untuk mencegah, mendeteksi, dan memulihkan ancaman siber di Australia. Pedoman ini telah dikembangkan untuk dapat membantu pengusaha kecil dalam melindungi usaha mereka dari bentuk ancaman siber yang paling umum. Suatu masalah dalam keamanan siber di pengusaha kecil dapat membawa dampak besar terhadap usaha tersebut. Namun, *Australian Cyber Security Centre* dapat mengetahui dampak yang dihasilkan dari setiap permasalahan keamanan siber, baik itu pada individu, usaha kecil, atau organisasi besar.

Seperti diketahui bahwa pemiliki atau pengurus dalam usaha kecil tidak memiliki waktu yang cukup untuk memahami bagaimana kompleksnya internet atau bahkan mengetahui cara menanggapi beberapa ancaman. Tetapi, juga diketahui bahwa keamanan siber akan mendorong kesejahteraan perekonomian Australia, sehingga diperbolehkan usaha kecil untuk berkembang, berinovasi, dan menemukan teknik yang dapat memberikan nilai terbaiknya kepada konsumen.

Rezim dari masing-masing negara di atas memiliki komponen mutlak, dimana ketahanan siber memiliki prinsip dasar, yaitu kolaborasi pemerintah; strategi pemetaan keamanan; data, keamanan dan teknologi; serta sistem yang berkelanjutan.

Pertama, prinsip kolaborasi pemerintah, yaitu memahami peran sebagai pimpinan daerah dan pejabat yang berwenang dalam pemetaan ancaman-ancaman kejahatan siber baik dalam sektor sipil, ekonomi, maupun pendidikan.

Kedua, strategi pemetaan keamanan, yaitu prinsip dasar dalam pemahaman '*big picture*' dalam melakukan pencegahan, *skill*, untuk membantu memahami gambaran yang lebih besar dan seberapa kuat keamanan dan keterampilan dunia maya, sehingga diperlukan dimensi pemahaman lokal dan kebutuhan organisasi atau sektor secara luas.

Ketiga, data, keamanan dan teknologi, yaitu menyoroti langkah-langkah dan kontrol utama untuk memastikan bahwa badan publik memiliki ketahanan dan sistem yang baik. Sinergi keamanan baik dalam perlindungan sistem dan data mengacu kerangka kebijakan dan standar sesuai dengan keamanan pemerintah pusat. Transformasi digital dan jaminan informasi harus memiliki infrastruktur yang aman dan tepat; dan platform teknologi umum yang akan mendukung ketahanan dunia siber.

Keempat, sistem yang berkelanjutan, yaitu menyadari akan tantangan kelangsungan bisnis dan manajemen risiko dalam berbagai sektor yang ada. Hal ini berkaitan dengan tanggung jawab pemerintah lokal dan pejabat berwenang di bawah pusat. Sistem yang

berkelanjutan berfokus pada dukungan komunitas (sosial) dan bisnis (sektor privat) yang mungkin terpengaruh oleh serangan siber

Kerangka Hukum Dan Kebijakan Ketahanan Siber Di Indonesia

Kebijakan ketahanan siber merupakan amanat konstitusi yang tertuang dalam pasal Pasal 28F dan Pasal 28J Undang-Undang Dasar 1945, dimana menyatakan bahwa setiap orang berhak untuk berkomunikasi dan memperoleh informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, menyimpan, mengolah, dan menyampaikan informasi dengan menggunakan segala jenis saluran yang tersedia. Selanjutnya, setiap orang wajib menghormati hak asasi manusia orang lain dalam tertib kehidupan bermasyarakat, berbangsa, dan bernegara, serta dalam menjalankan hak dan kebebasannya, setiap orang wajib tunduk kepada pembatasan yang ditetapkan dengan undang-undang dengan maksud semata-mata untuk menjamin pengakuan serta penghormatan atas hak dan kebebasan orang lain dan untuk memenuhi tuntutan yang adil sesuai dengan pertimbangan moral, nilai-nilai agama, keamanan, dan ketertiban umum dalam suatu masyarakat demokratis.

Selanjutnya, amanat konstitusi tersebut dituangkan dalam Instruksi Presiden No. 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government. Intruksi presiden ini dikeluarkan untuk merespon beberapa tantangan terkait dengan penggunaan sarana siber dalam pelayanan publik yang berkembang cepat sebagai berikut.

Pertama, menjamin potensi pemanfaatannya secara luas, membuka peluang bagi pengaksesan, pengelolaan dan pendayagunaan informasi dalam volume yang besar secara cepat dan akurat.

Kedua, proses pemerintahan (*e-government*) akan meningkatkan efisiensi, efektivitas, transparansi dan akuntabilitas penyelenggaraan pemerintahan.

Ketiga, menjamin penyelenggaraan pemerintahan yang baik (*good governance*) dan meningkatkan layanan publik yang efektif dan efisien diperlukan adanya kebijakan dan strategi pengembangan *e-government.*

Keempat, perlunya kesamaan pemahaman, keserempakan tindak dan keterpaduan langkah dari seluruh unsur kelembagaan pemerintah, maka dipandang perlu untuk mengeluarkan Instruksi Presiden bagi pelaksanaan kebijakan dan strategi pengembangan *e-government* secara nasional

Sampai dengan saat Indonesia belum mempunyai undang-undang yang mengatur mengenai ketahanan siber, karena isu tersebut mulai ramai muncul keruang publik seiring dengan peningkatan penggunaan teknologi siber dalam kehidupan sehari-hari oleh sebagian besar masyarakat termasuk dalam interaksi sosial. Peraturan yang ada masih banyak memiliki keterbatasan dan kelemahan dalam melindungi infrastruktur siber dan keamanan siber.

Beberapa undang-undang telah diterbitkan seperti Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi, Undang-Undang Nomor 32 Tahun 2002 Tentang Penyiaran, Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik, masih memiliki keterbatasan dalam konteks infrastruktur telekomunikasi, penyiaran dan informatika untuk pelayanan

publik. Undang-undang tentang Informasi dan Transaksi Elektronik juga dianggap belum mampu mencakup seluruh aspek keamanan siber yang begitu luas. Namun begitu terkait dengan *smartcity* ada beberapa peraturan pemerintah yang dapat dijadikan dasar pelaksanaan *e-government* di tingkat daerah ini merujuk pada beberapa peraturan, yaitu (1). Undang -Undang Republik Indonesia Nomor 22 Tahun 1999 Tentang Pemerintahan Daerah. (2). Undang-Undang Republik Indonesia Nomor 25 Tahun 1999 Tentang Perimbangan Keuangan antara Pemerintah Pusat dan Daerah. (3). Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi. (4). Peraturan Pemerintah Republik Indonesia Nomor 25 Tahun 2000 Tentang Kewenangan Provinsi sebagai daerah otonom.

Selanjutnya, beberapa aktor yang diidentifikasi dapat mengambil peran penting dalam pembangunan ketahanan siber UKM di tingkat daerah dan pusat seperti BSSN, Diskominfo, Dinas Koperasi dan Mikro. Secara lebih rinci dapat diikuti uraian berikut.

Pertama, BSSN. Saat ini Indonesia mengalami banyak perubahan dalam kehidupan sosial, ekonomi, politik, dan budaya bahkan juga ruang pribadi karena perkembangan teknologi digital yang sangat pesat, meskipun perubahan tersebut mendorong perubahan masyarakat namun perangkat aturan, kebijakan, bahkan infrastruktur yang ada masih jauh dari memadai. Ketahanan Siber Indonesia tertuang dalam tujuan strategis dari Strategi Keamanan Siber Indonesia adalah tercapainya ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber dan keamanan siber pada ekonomi digital. Berdasarkan Peraturan Presiden Nomor 133 Tahun 2017, telah dibentuk BSSN yang bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber nasional (Badan Siber dan Sandi Negara, 2018). Namun, sampai saat ini di Indonesia belum ditemukan sebuah model ketahanan siber yang dapat diterapkan di *Smart City*.

BSSN (Badan Sandi dan Siber Negara) adalah lembaga pemerintah Republik Indonesia yang didirikan pada tahun 2017. BSSN direncanakan dibentuk sejak tahun 2015 untuk mengonsolidasikan kewenangan, tugas, dan fungsi yang tumpang tindih di antara lembaga terkait siber seperti Kominfo, BIN, Kementerian Luar Negeri, Kementerian Pertahanan, Polri dan institusi lainnya. Sebelumnya, cikal bakal dari lembaga ini ialah Desk Ketahanan dan Keamanan Informasi Cyber Nasional (DK2ICN) yang berada di bawah Kementerian Koordinator Bidang Politik, Hukum dan Keamanan

BSSN mempunyai tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber. Dalam melaksanakan tugas tersebut, BSSN menyelenggarakan fungsi-fungsi, yaitu (1). Penyusunan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi *e-commerce*, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber. (2). Pelaksanaan kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi *e-commerce*,

persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber. (3). Pemantauan dan evaluasi kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian proteksi *e-commerce*, persandian, penapisan, diplomasi siber, pusat manajemen krisis siber, pusat kontak siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan kerentanan, insiden dan/atau serangan siber. (4). Pengoordinasian kegiatan fungsional dalam pelaksanaan tugas BSSN dan sebagai wadah koordinasi bagi semua pemangku kepentingan. (5). Pelaksanaan pembinaan dan pemberian dukungan administrasi kepada seluruh unit organisasi di lingkungan BSSN. (6). Pelaksanaan atas pelaksanaan tugas BSSN. (7). Pelaksanaan dukungan yang bersifat subsantif kepada seluruh unsur organisasi di lingkungan BSSN. (8). Pelaksanaan kerjasama nasional, regional, dan internasional dalam urusan keamanan siber.

Secara mendasar BSSN diharapkan dapat melaksanakan fungsi deteksi, identifikasi, proteksi, penanggulangan, pemulihan dan pemantauan keamanan siber nasional. Dalam lingkup UKM, BSSN berada pada peran edukasi masyarakat. BSSN telah menyusun Panduan Mandiri Keamanan Informasi (Paman Kami) (BSSN n.d.) yang bisa dimanfaatkan oleh pelaku UKM. Paman Kami merupakan *tools* penilaian mandiri keamanan informasi yang berfokus pada 25 langkah keamanan informasi.

Kedua, Diskominfo (Dinas Komunikasi dan Informasi). Berdasarkan Peraturan Walikota Semarang Nomor 76 Tahun 2016 Tentang Kedudukan, Susunan Organisasi, Tugas Dan Fungsi, Serta Tata Kerja Dinas Komunikasi, Informatika, Statistik Dan Persandian Kota Semarang, Diskominfo merupakan unsur pelaksana urusan pemerintahan Bidang Komunikasi dan Informatika, Bidang Statistik, dan Bidang Persandian yang mempunyai tugas dan fungsi, yaitu (1). Merumuskan kebijakan Bidang Pengembangan Komunikasi Publik, Bidang Layanan *E-Government*, Bidang Pengelolaan Informasi dan Saluran Komunikasi Publik, Bidang Pengelolaan Infrastruktur,dan Bidang Statistik. (2). Mengkoordinasikan tugas-tugas dalam rangka melaksanaan program dan kegiatan Kesekretariatan, Bidang Pengembangan Komunikasi Publik, Bidang Layanan *E-Government*, Bidang Pengelolaan Informasi dan Saluran Komunikasi Publik, Bidang Pengelolaan infrastruktur, dan Bidang Statistik. (3). Menyelenggarakan kerjasama Bidang Pengembangan Komunikasi Publik, Bidang Layanan *E-Government*, Bidang Pengelolaan Informasi dan Saluran Komunikasi Publik, Bidang Pengelolaan Infrastruktur, dan Bidang Statistik. (4). Menyelenggaraan program dan kegiatan Bidang Pengembangan Komunikasi Publik, Bidang Layanan *E-Government*, Bidang Pengelolaan Informasi dan Saluran Komunikasi Publik, Bidang Pengelolaan Infrastruktur, dan Bidang Statistik. (5). Menyelenggarakan monitoring dan evaluasi program serta kegiatan Bidang Pengembangan Komunikasi Publik, Bidang Layanan *E-Government*, Bidang Pengelolaan Informasi dan Saluran Komunikasi Publik, Bidang Pengelolaan Infrastruktur, dan Bidang Statistik.

Peran penting yang dapat diambil oleh Diskominfo (Dinas Komunikasi dan Informasi) adalah program pengembangan UMKM seperti program satu juta domain

gratis sebagai pengembangan ekonomi nasional (KKI, 2018).

Ketiga, Dinas Koperasi dan Usaha Mikro. Dinas Koperasi dan Usaha Mikro mempunyai visi yaitu 'Mewujudkan koperasi dan Usaha Mikro sebagai lembaga usaha yang sehat, berdaya saing dan berperan dalam membangun perekonomian menuju masyarakat sejahtera'. Untuk mencapai visi tersebut, dibentuklah beberapa misi, yaitu menumbuh kembangkan kehidupan berkoperasi, meningkatkan pengetahuan dan keterampilan masyarakat, serta memfasilitasi pengembangan usaha dan KUMKM.

Sedangkan tugas pokok Dinas Koperasi dan Usaha Mikro yaitu melaksanakan urusan pemerintahan daerah di bidang Koperasi dan Usaha Mikro berdasarakan asas otonomi dan tugas pembantuan. Selain tugas pokok, Dinas Koperasi dan Usaha Mikro (Wahidin, 2019) juga mempunyai fungsi, yaitu (1). Merumuskan kebijakan teknis di Bidang Pemberdayaan Koperasi, Bidang Pemberdayaan Usaha Mikro, dan Bidang pengawasan dan Pemeriksaan Koperasi. (2). Menyusun, merumuskan, dan menjabarankan teknis Pemberian bimbingan di bidang Koperasi dan Usaha mikro, kecil dan menengah. (3). Melaksanakan kebijakan teknis, memberi bimbingan di bidang koperasi usaha mikro serta memfasilitasi pembiayaan di lingkungan Kota Semarang. (4). Menetapankan kebijakan untuk mendukung pembangunan Bidang Koperasi dan Usaha Mikro. (5). Menyelenggarakan pembinaan dalam melakukan pengawasan yang sesuai standart pelayanan minimal dalam Bidang Koperasi dan Usaha Mikro. (6). Melakukan pengawasan teknis terhadap pelaksanaan bidang Koperasi dan Usaha Mikro yang sesuai dengan peraturan perundang-undangan.

Dalam kaitannya membangun ketahanan dalam dunia siber (*Cyber Resilience*), terlebih dalam sektor industri baik skala besar maupun menengah dan kecil seperti UKM, pemerintah tidak bisa berdiri sendiri, namun harusnya dapat memetakan faktor-faktor penghambat baik berupa prosedural, sistem regulasi, undang-undang maupun aktor yang memmang terlibat di dalamnya (Boyes, 2015). Dalam kajian model ketahanan dalam dunia siber yang berhubungan dengan dunia industri atau bisnis skala menengah dan kecil baik berupa dari hasil kajian literasi komparasi beberapa negara di atas dan juga hasil internal FGD yang dilakukan, maka didapatkan hasil pemetaan apa saja yang menjadi penghambat adanya ketahanan siber itu sendiri, sebagai berikut.

(1). SDM (Sumber Daya Manusia). Sumber daya Manusia erat kaitannya dengan pelaku internal bisnis atau usaha yang ada. Seberapa banyak SDM yang ada belum tentu mencerminkan ketahanan siber yang bagus, yaitu tingkat kesadaran akan gangguan siber atau ancaman siber dan juga pengetahuan akan adanya kebutuhan konsep ketahanan dalam taraf SDM sangat dibutuhkan. SDM merupakan cerminan dari *supply chain* suatu industri yang berjalan baik lingkup organisasi terkecil dalam suatu struktur bisnis atau usaha maupun lingkup besar yang menaungi berbagai industri yang berhubungan erat dengan dunia siber. Banyak di antaranya memahamai konsep ketahanan siber hanyalah kewenangan pemerintah dan juga tim IT suatu organisasi, dimana secara ideal diperlukan pemahaman, kesepakatan secara holistik, top-down atas informasi, kesepahaman, dan juga resiko yang mengintai.

(2). Infrastruktur. SDM tersedia dengan baik, namun secara fasilitas penunjang tidak

diberikan manajemen yang memadai maka tentu menjadi masalah lain. Hubungan dunia digital dalam bisnis proses suatu badan usaha terlebih seperti UKM tentu wajib memiliki fasilitas infrastruktur penunjang yang memadai (Rozikin, 2019). Hal itu tentunya bisa dilihat dari sistem pengamanan IT, sertifikasi standarisasi dalam ketahanan keamanan digital. Sertifikasi Indeks KAMI dengan ISO 27001 yang disediakan oleh pemerintah maupun layanan swasta lainnya hanya dapat mencakup pemain besar dimana skala bisnis seperti *e-commerce* atau perusahaan yang memang memiliki nilai asset minimum, sehingga pemerintah dalam hal infrastruktur UKM perlu diperhatikan dengan baik. Jika dilihat sistem infrastruktur penunjang, maka Singapura bisa dijadikan *benchmark* atas sistem ketahanan siber dalam hal infrastruktur yang harus dimiliki oleh SMEs.

(3). Literasi. Literasi dalam konsep ketahanan siber digunakan sebagai khazanah ilmu pengetahuan atas sejauh mana pemahaman, dan juga ke dalam akses informasi yang dimiliki oleh pelaku usaha dalam kaitannya dengan dunia siber. Tentu saja ragam informasi literasi yang dibutuhkan dimulai dari definisi yang mudah dipahami dan terpadu, pemahaman apa itu kejahatan dalam dunia siber, jenis-jenis ancaman, gangguan, dan juga bagaimana penanggulangan gangguan tersebut. Aspek literasi sangat erat kaitannya dengan SDM dan juga infrastruktur yang saling terhubung

(4). Regulasi. Dalam kaitannya dengan dunia siber, pemerintah selaku regulator harus menjunjung pro yustia dimana patuh atas hukum. Regulasi merupakan rujukan apabila terjadi ancaman, maupun faktor perlindungan akan ragam praktek industri, kegiatan, dan infrastruktur dalam dunia siber.

SIMPULAN

Berdasar penjelasan tersebut di atas dapat ditarik simpulan sebagai berikut.

Pertama, kompleksitas yang berkembang dari sistem dunia maya dan ancamannya memerlukan integrasi proses manajemen risiko dan proses manajemen ketahanan. Seringkali, ancamannya tidak diakui sampai terwujud dalam sistem siber dan karenanya mungkin terlewatkan dalam skenario ancaman yang diperiksa sebagai bagian dari penilaian risiko. Ketahanan siber, sifatnya fleksibel, dapat memberikan kerangka kerja untuk memerangi ancaman siber dan memastikan kelayakan aset dan layanan siber kritis. Mengelola sistem siber yang tangguh menggunakan kerangka ini mengenali dan menekankan interaksi antara masing-masing domain organisasi di setiap tahap acara siklus manajemen, faktor yang telah diabaikan pendekatan ketahanan lainnya.

Kedua, ketahanan sistem siber tergantung pada semua aspek organisasi secara efektif sepanjang siklus manajemen peristiwa di empat domain (SDM, Infrastruktur, Literasi, dan Regulasi) yang diidentifikasi. Selain itu, diskusi ketahanan yang ditemukan dalam literatur sering difokuskan pada satu domain operasional (seperti fisik, informasi, kognitif, atau sosial) dan tidak mewakili interkoneksi antar komponen sistem untuk menginformasikan ke seluruh domain ini. Kolaborasi antara pemerintah dan pihak swasta (*public-pivate partnership*) kiranya dapat menjadi suatu konsep yang akan mewujudkan keamanan siber yang efektif.

DAFTAR PUSTAKA

Andres, Lauren, dan John Round, 2015.,"The Creative Economy in a Context of

Transition: A Review of the Mechanisms of Micro-Resilience." *Cities* 45: hh. 1–6.

Anto, Rusdi, 2018, *Kasus-Kasus Cyber Crime Sebagai Dampak Perkembangan Teknologi Komunikasi Yang Meresahkan Masyarakat.* (July): hh. 0–12.

Arifin, M. Zaenal, 2018, "Litani Minta Pelaku UMKM Kota Semarang Daftarkan Usahanya Di I-Juz Melon "Retrieved November 16, 2018, <http://jateng.tribunnews.com/2018/07/06/litani-minta-pelaku-umkm-kota-semarang-daftarkan-usahanya-di-i-juz-melon>.

Assosiation of Banks in Singapore's (ABS), 2010, *Industry guidelines on cybersecurity,* Retrieved November 14,2018. <https://www.abs.org.sg/>Australia Cybercrime Act 2001.

Boyes, Hugh, 2015, Technology Innovation Management Review Cybersecurity and Cyber-Resilient

Supply Chains. *Technology Innovation Management Review*. 5(4): hh. 28-34

BSSN. n.d., Strategi Keamanan Siber Nasional | *Bssn.Go.Id*.

Chotimah, Hidayat Chusnul, Muhammad Ridha Iswardhana, dan Tiffany Setyo Pratiwi, 2019, "Penerapan Military Confi Dence Building Measures Dalam Menjaga Ketahanan Nasional Indonesia Di Ruang Siber." *Jurnal Ketahanan Nasional* 25(3): hh. 331.

Common Level of Security of Network and Information Systems Across the Union.

Deloitte,2010, *CSO Cyber Security Watch Survey,* Retrieved September,29,2010 from <http://www.deloitte.com/view/en_US/us/Insight/Center-Security-and PrivacySoltion/ bcdc005f1e046210VgnVCM100000ba42f00aRCRD.htm>.

Directive (Eu) 2016/1148 Of the European Parliament and Of the Council, Of 6 July 2016, Concerning Measures for A High.

Doran, Justin, dan Bernard Fingleton, 2015, "Resilience from the Micro Perspective." *Cambridge Journal of Regions, Economy and Society* 8(2): hh. 205–23.

European Comission, 2017, Integration of Digital Technology*, Europe's Digital Progress Report*.

Firth, Clinton. M., Raddad Ayoub, dan Mohammed Nayaz. n.d. *Cyber Resilience in the Digital Age*.

Federation of Small Business (FSB), 2016, *Cyber Resilience : How To Protect Small Firms In The Digital*. United Kingdom.

Fitiriasari, Paramitha Dyah, 2019, "Partisipasi Masyarakat Dalam Kesenian Soreng Guna Meningkatkan Ketahanan Budaya (Studi Di Desa Banyusidi, Kecamatan Pakis, Kabupaten Magelang, Jawa Tengah)." *Jurnal Ketahanan Nasional* 25(3): h. 409.

Herrington, Lewis, dan Richard Aldrich, 2013. "The Future of Cyber-Resilience in an Age of Global Complexity." *Politics* 33(4): hh. 299–310.

Holzheu, Thomas, Patrick Saner, Kulli Tamm, Maurus Rischatsch, dan Roman Lechner, 2019. *Indexing Resilience : A Primer for Insurance Markets and Economies*.

Instruksi Presiden Republik Indonesia, Tahun 2003

John, Swinney, 2018, *A Cyber Resilience Strategy For ScotlandPrivate Sector.*

Kementerian Komunikasi dan Informatika (KKI), 2018. *Kementerian Komunikasi Dan Informatika.* Retrieved November 13, 2018 <https://www.kominfo.go.id/

content/detail/12082/menkominfo-apresiasi-digitalisasi-transaksi-umkm-di-pasar-rakyat/0/berita_satker>.

Kourtit, Karima, Peter Nijkamp, Rachel S. Franklin, dan Andrés Rodríguez-Pose, 2014, "A Blueprint for Strategic Urban Research: The Urban Piazza." *The Town Planning Review; Liverpool* 85(1): hh. 97–126.

McDermid, D., Mahcke, R., dan Williams,P., 2009, Challanges in Improving Information Sesurity Practice Australian GeneralPractice. *Proceeding of The 7th Australia Information Security Management Conference,* hh. 1-5. Peth,WesternAustralia: SECAU_ Securrity Research Centre, ECU.

Peraturan Pemerintah Republik Indonesia Nomor 25 Tahun 2000 Tentang Kewenangan Provinsi Sebagai Daerah Otonom.

Peraturan Presiden Republik Indonesia Nomor Tahun Tentang Badan Siber Dan Sandi Negara.

Peraturan Presiden Republik Indonesia Nomor 133 Tahun 2017 Tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2oi7 Tentang Badan Siber Dan Sandi Negara.

Putra, Adnan Husad, 2016, *Peran UMKM Dalam Pembangunan Dan Kesejahteraan Masyarakat Kabupaten Blora*. Vol. 2016.

Putranti, Ika Riswanti, 2015, "Developing of Cyber Resilience System of the International Trade Facilitations: Specific Reference Indonesia." *UNCITRAL*, hh. 1–28 .

Rad, Z. Besharati, dan A. Eshraghniaye Jahromi, 2014, "A Framework for Resiliency Assessment of Power Communication Networks." *Scientia Iranica. Transaction E, Industrial Engineering; Tehran* 21(6): hh. 2399–2418.

Rocha, Álvaro, Ana Maria Correia, Sandra Costanzo, dan Luís Paulo Reis. 2015. "New Contributions in Information Systems and Technologies." *Advances in Intelligent Systems and Computing* 353(December):III–IV.

Rozikin, Mochammad, 2019, "Memperkuat Ketahanan Masyarakat Berbasis Social Capital Pada Era Otonomi Desa (Studi Di Desa Pandansari, Kecamatan Ngantang, Kabupaten Malang)." *Jurnal Ketahanan Nasional* 25(2): hh. 204–25.

Singapore Cyber Security Act 2018

Sudaryanto, Ragimun, dan Rahma Rina Wijayanti. 2010. "Strategi Pemberdayaan UMKM Menghadapi Pasar Bebas Asean." *Badan Kebijakan Fiskal Kemenkeu RI*.

Undang -Undang Republik Indonesia Nomor 22 Tahun 1999 Tentang Pemerintahan Daerah.

Undang-Undang Republik Indonesia Nomor 25 Tahun 1999 Tentang Perimbangan Keuangan Antara Pemerintah Pusat Dan Daerah.

Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi

Undang-Undang Nomor 3 Tahun 2002 Tentang Pertahanan Negara .

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Wahid, Irfan, 2017, *Digitalisasi UMKM, Keniscayaan Era Modern* - Kumparan. Com. Retrieved November 13, 2018 <https://kumparan.com/ipang-wahid/

digitalisasi-umkm-keniscayaan-era-modern>.

Wahidin, Darto, 2019, "Transformasi Industri Kreatif Batik Dalam Rangka Peningkatan Ketahanan Kerajinan Kain Batik (Studi Di Dusun Giriloyo, Desa Wukirsari, Kecamatan Imogiri, Kabupaten Bantul, Daerah Istimewa Yogyakarta)." *Jurnal Ketahanan Nasional* 25(3): h. 348.