PENGARUH ANALISIS KEBUTUHAN PELATIHAN BUDAYA KEAMANAN SIBER SEBAGAI UPAYA PENGEMBANGAN KOMPETENSI BAGI APARATUR SIPIL NEGARA DI ERA DIGITAL

ANALYSIS CYBER SECURITY CULTURE TRAINING NEEDS AS AN EFFORT TO DEVELOP COUNTRY CIVIL APARATURES COMPETENCY IN DIGITAL ERA

Sri Cahaya Khoironi
Pusat Pendidikan dan Pelatihan Pegawai – Balitbang SDM Kemkominfo
Jalan Raya Kelapa Dua No. 49D, Kota Jakarta Barat, Indonesia
sric001@kominfo.go.id

Diterima tgl. 10/3/2020; Direvisi tgl. 7/5/2020 Disetujui tgl. 18/5/2020

ABSTRACT

The results of Monitoring and Evaluation of Electronic-Based Government Systems (SPBE) that not been optimal, the high incidence of cyber in the government domain. go.id due to system vulnerability as well as the number of government pages with unsafe conditions and not in accordance with existing international standards, show the need for ASN as a manager of digital competence to oversee digitalization in the government environment. To discuss this issue, the method chosen was the study of literature, by reviewing various literature and collection of research results in accordance with the problem. Descriptive qualitative analysis using the technique "PRISMA protocol". The findings of this study are important for designing training programs as part of the development of sustainable digital ASN competencies, specifically related to training in cybersecurity culture in government environments, especially in public services. Given the technology and knowledge of hacking efforts in cybercrime is developing very fast, it is necessary to anticipate investment in human resources through training in cybersecurity culture

Keywords: *Cybersecurity, Cybersecurity Culture, SETA, ASN Competency Development, Cybersecurity Culture Training*

ABSTRAK

Hasil Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (SPBE) yang belum optimal dan tingginya insiden siber pada domain pemerintah.go.id akibat dari kerentanan sistem serta masih banyaknya laman pemerintah dengan kondisi tidak aman dan belum sesuai standar internasional yang ada menyiratkan adanya kebutuhan ASN sebagai pengelola yang berkompetensi digital untuk mengawal digitalisasi di lingkungan pemerintahan. Metode yang dipilih adalah studi kepustakaan dengan meninjau berbagai literatur dan kumpulan hasil-hasil penelitian sesuai dengan permasalahan. Analisis deskriptif kualitatif menggunakan teknik "PRISMA protokol". Temuan dari penelitian ini penting untuk merancang program pelatihan sebagai bagian dari pengembangan kompetensi digital ASN yang berkelanjutan, khususnya terkait pelatihan budaya keamanan siber di lingkungan pemerintahan, terutama dalam pelayanan publiknya. Mengingat teknologi dan pengetahuan tentang upaya peretasan dalam kejahatan siber berkembang sangat cepat, perlu antisipasi investasi sumber daya manusia melalui pelatihan budaya keamanan siber.

Kata Kunci : Keamanan Siber, Budaya Keamanan Siber, SETA, Pengembangan Kompetensi ASN, Pelatihan Budaya Keamanan Siber

1. PENDAHULUAN

1.1 Latar Belakang

Seiring dengan perkembangan teknologi digital yang semakin massif, hal ini juga berdampak pada ancaman keamanan siber atau dunia maya. Perkembangan dunia siber di satu sisi banyak memberikan nilai manfaat, pada sisi yang lain memiliki sisi negatif. Hal ini disebabkan banyak risiko yang terkait di dalamnya. Sisi negatif inilah yang membawa implikasi terhadap upaya untuk penerapan keamanan siber. Harapan untuk menumbuhkan kesadaran budaya keamanan siber

akhirnya menjadi faktor penting menjadi bahan diskusi. Untuk alasan ini, banyak negara bercita-cita menumbuhkan budaya keamanan siber di antara semua pengguna dunia siber (Gcaza, Von Solms, & Van Vuuren, 2015).

Pembahasan keamanan siber juga termasuk di dalamnya tentang kejahatan dunia siber yang terus mengalami perkembangan yang sangat cepat. Pada saat ini serangan siber menjadi sebuah tantangan tersendiri bagi suatu negara modern, termasuk Indonesia. Menghadapi hal tersebut Pemerintah Indonesia mempuyai perhatian dan komitmen yang tinggi terhadap keamanan siber dengan hadirnya institusi yang fokus dalam penanganan keamanan siber, yaitu Badan Siber dan Sandi Negara (BSSN) pada tahun 2017.

Internet telah menjadi bagian tidak terpisahkan dari kehidupan global dan kejahatan yang dilakukan di internet sudah mulai meningkat secara signifikan. Dalam laporan FBI 2019 (Federal Bureau of Investigation, 2019), *Internet Crime Complaint Center* (IC3) pada tahun 2019 pengaduan yang diterima dalam satu hari rata-rata 1.300. Kerugian mencapai lebih dari $3,5 miliar bagi individu maupun korban bisnis. Dari hasil Studi Frost & Sullivan yang diprakarsai oleh Microsoft, potensi kerugian ekonomi di Indonesia akibat insiden keamanan siber dapat mencapai angka US$34,2 miliar. Angka tersebut merupakan 3,7% dari total PDB Indonesia sebesar US$932 miliar (A Frost & Sullivan, 2019)

BSSN menyampaikan dalam Laporan Honeypot 2019 (BSSN, 2019a) dengan data yang diambil dalam rentang waktu Januari 2019 sampai dengan Desember 2019 pada sensor yang aktif menyatakan bahwa Indonesia mendapat serangan siber sejumlah 98.243.896. Dibandingkan dengan data pada tahun 2018 terdapat kenaikan yang sangat signifikan dari angka 12.895.554 serangan (BSSN, 2018). India sebagai negara penyerang terbanyak ke Indonesia dengan 24.460.689 serangan dan Indonesia sendiri menjadi negara terbanyak kedua juga sebagai negara yang menjadi sumber serangan dengan 10.064.615 serangan (BSSN, 2019a). Pada tahun 2019, GOV_CISRT_BSSN (2019) melaporkan tentang aduan yang khusus insiden siber dengan pemerintah (domain .go.id) yang cukup besar, yaitu sejumlah 4241 aduan. Hal ini terjadi karena banyaknya instansi pemerintah yang menerapkan kebijakan Sistem Pemerintah Berbasis Elektronik (SPBE), tetapi kurang peduli atas isu keamanan siber. Selain itu, masih banyak instansi pemerintah yang tidak melakukan mitigasi risiko atas ketersediaan dan keamanan website sehingga terkena insiden siber jenis *web defacement* karena tidak menerapkan *Web Application Firewall* (WAF) (GOV_CISRT_BSSN, 2019). Masih rentannya peretasan pada institusi pemerintah maupun swasta menandakan bahwa keamanan siber menjadi masalah urgen dan serius dalam konteks pelayanan publik.

Salah satu faktor penting dalam sistem keamanan siber yaitu faktor manusia**.** Dalam konteks keamanan siber bahwa faktor manusia sangat terkait dengan peran yang dimainkan sebagai pengguna dalam proses keamanan dan dapat berdampak positif atau negatif terhadap proses keamanan siber (Von Solms & Van Niekerk, 2013). Pengembangan budaya keamanan siber seperti itu tidak mudah karena harus diikuti dengan adanya kesadaran bersama akan ketahanan siber. Penetapan strategi keamanan siber nasional yang merupakan bagian dari strategi keamanan nasional dan di dalamnya termasuk pembangunan budaya keamanan siber sesuai dengan peran pemerintah untuk melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum (Kementerian Kominfo, 2019). BSSN telah menyusun Strategi Keamanan Siber Indonesia sebagai acuan bersama seluruh pemangku kepentingan keamanan siber nasional yang dituangkan dalam visi "Strategi Keamanan Siber Indonesia, yaitu Membangun dan Menjaga Keamanan Siber Nasional dengan Mensinergikan Berbagai Pemangku Kepentingan untuk Ikut Serta Mewujudkan Keamanan Nasional dan Meningkatkan Pertumbuhan Ekonomi Nasional" yang bertujuan untuk

mencapai ketahanan siber, keamanan layanan publik, penegakan hukum siber, budaya keamanan siber dan keamanan siber pada ekonomi digital di Indonesia (Hinsa Siburian, 2018)

Studi terdahulu meneliti tentang *cybersecurity* dalam konteks hukum dan pertahanan nasional. Aspek pembahasannya meliputi sudut pandang hukum, pertahanan nasional, dan hubungan internasional memberikan gambaran tentang bagaimana strategi pemerintah dalam menghadapi tantangan keamanan siber di Indonesia (Rizal & Yani, 2016). Dari hasil pemetaan aspek *people, process, dan technology* dalam studi (Islami, 2018), peluang peningkatan strategi yang dapat dilakukan untuk masa depan adalah dengan rekomendasi yang disarankan berdasarkan identifikasi strategi keamanan siber dan pelatihan profesional keamanan siber bagi Aparatur Sipil Negara terutama yang mengelola data strategis dan tenaga penyidik bidang Informasi dan Transaksi Elektronik (ITE).

Penerapan regulasi tentang Sistem Pemerintahan Berbasis Elektronik atau SPBE (Pemerintah RI.SPBE, 2018) untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya dengan tata kelola dan manajemen sistem pemerintahan berbasis elektronik secara nasional yang membawa konsekuensi atas kehandalan dalam mengantisipasi dan meminimalisir serangan serangan atas SPBE dengan penerapan budaya keamanan siber bagi pengelolanya.

Bertolak dari latar belakang permasalahan keamanan siber tersebut di atas, penelitian bertujuan untuk menjawab masalah terkait banyaknya serangan dan atau insiden siber atas sistem di pemerintahan sehingga dibutuhkan pengelola yang kompeten nantinya sebagai modal mengelola layanan publik yang berbasis internet dan transaksi elektronik dengan pemenuhan pemahaman dan regulasi terkait keamanan siber. Pembahasan dan diskusi dalam studi ini difokuskan untuk menyoroti dan menjelaskan berbagai persoalan yang terkait dengan kebutuhan pelatihan keamanan siber yang khususnya tentang Pelatihan Budaya Keamanan Siber bagi ASN agar dapat mengelola pelayanan publik yang berbasis elektronik dan internet dengan menjalankan standar dan regulasi yang terkait dengan keamanan siber. Secara teori studi ini diharapkan dapat berkontribusi terhadap pemahaman atas kebutuhan pengembangan kompetensi bagi ASN di era digital melalui pelatihan budaya keamanan siber sebagai upaya pengembangan modal sumber daya manusia di lingkungan instansi pemerintah.

1.2 Landasan Teoritis/Konsep

a) Kompetensi

Chouhan & Srivastava (2014) menyatakan bahwa kompetensi berasal dari kata Latin '*competentia*' yang berarti "berwenang untuk menilai" serta "memiliki hak untuk berbicara", sementara Kamus Bahasa Inggris kata *competence* mempunyai arti kemampuan untuk melakukan sesuatu dengan sukses dan atau efisien. Dalam Kamus Besar Bahasa Indonesia kata kompetensi berasal dari kata kompeten yang berarti cakap atau mampu dan kompetensi berarti mempunyai arti kemampuan untuk menguasai dan memutuskan sesuatu. Kompetensi sudah dikenal sejak 3000 tahun yang lalu dalam pemerintahan Cina (Yuanjing Wilcox, 2012) dan dikenalkan pada dunia pendidikan sejak tahun 1953 oleh David McClelland, seorang guru manajemen Amerika untuk pertama kalinya mengakui sifat manusia yang disebut kompetensi (Chouhan & Srivastava, 2014).

Arti dan definisi tentang kompetensi sangat banyak, tetapi penulis lebih sependapat dengan mendefinisikan kompetensi adalah kemampuan menerapkan atau menggunakan pengetahuan, keterampilan, kemampuan, perilaku, termasuk ciri pribadinya agar berhasil dalam melakukan tugas kerja, fungsi spesifik, atau bekerja pada peran atau posisi tertentu. Dengan demikian, kompetensi merupakan karakteristik fundamental atas individu yang menampilkan cara berperilaku atau berpikir dan ditunjukkan dalam pekerjaan atau peran pekerjaan tersebut (Chouhan & Srivastava,

2014). Bahkan secara lebih luas, Wilhelm, Förster, & Zimmermann (2019) menyatakan kompetensi sebagai kemampuan untuk memobilisasi sumber daya untuk menyelesaikan masalah dan tantangan dalam kehidupan dalam konteks tertentu dengan lebih menekankan pentingnya mempertimbangkan kinerja.

Dari hasil memahami berbagai literatur, dapat diambil benang merahnya bahwa kompetensi adalah kemampuan menyelesaikan masalah dan tantangan dalam konteks dan peran tertentu yang ditunjukkan dalam menerapkan atau menggunakan pengetahuan, keterampilan, kemampuan, perilaku, termasuk ciri pribadinya agar berhasil dalam melakukan tugas kerja, fungsi spesifik, atau bekerja pada peran atau posisi tertentu.

b) Kompetensi Digital

Di era digital kemampuan digital adalah prasyarat utama agar bisa bersaing dalam jangka panjang, namun berbagai institusi maupun perusahaan menginginkan *go digital* yang belum memahami mengenai cara terbaik untuk mengatur organisasi dalam proses otomatisasi dan mengembangkan infrastruktur dan talenta yang dibutuhkan dalam pengelolaan informasi digital baik pembangunan, pengembangan, maupun pemeliharaan layanan daring (Daub & Wiesinger, 2015). Ferrari, Editors, Punie, & Bre (2013) menyatakan bahwa bidang kompetensi digital ada lima:

1. Informasi: mengidentifikasi, menemukan, mengambil, menyimpan, mengatur dan menganalisis informasi digital, menilai relevansinya dan tujuannya.
2. Komunikasi: berkomunikasi dalam lingkungan digital, berbagi sumber daya melalui alat daring, terhubung dengan orang lain dan berkolaborasi melalui alat digital, berinteraksi dengan dan berpartisipasi dalam komunitas dan jaringan, kesadaran lintas budaya.
3. Pembuatan Konten: Membuat dan mengedit konten baru (dari pengolah kata hingga gambar dan video); mengintegrasikan dan menguraikan kembali pengetahuan dan konten sebelumnya; menghasilkan ekspresi kreatif, keluaran media, dan pemrograman; berurusan dengan dan menerapkan hak dan lisensi kekayaan intelektual.
4. Keselamatan: perlindungan pribadi, perlindungan data, perlindungan identitas digital, langkah-langkah keamanan, penggunaan yang aman dan berkelanjutan.
5. Pemecahan masalah: mengidentifikasi kebutuhan dan sumber daya digital, membuat keputusan berdasarkan informasi yang merupakan alat digital yang paling tepat sesuai dengan tujuan atau kebutuhan, menyelesaikan masalah konseptual melalui cara digital, secara kreatif menggunakan teknologi, memecahkan masalah teknis, memperbarui sendiri dan kompetensi orang lain.

Mengingat pada penelitian ini erat kaitannya dengan keamanan siber, kompetensi yang dibahas adalah terkait keamanan (Ferrari et al., 2013) meliputi empat kompetensi terkait keamanan, yaitu

1. Melindungi perangkat, untuk melindungi perangkat sendiri dan memahami risiko dan ancaman secara daring serta untuk mengetahui tentang langkah-langkah keselamatan dan keamanan
2. Melindungi data pribadi, untuk memahami ketentuan umum layanan, perlindungan aktif data pribadi, memahami privasi orang lain, melindungi diri dari penipuan dan ancaman daring dan siber
3. Melindungi kesehatan, untuk menghindari risiko kesehatan yang terkait dengan penggunaan teknologi dalam hal ancaman terhadap kesejahteraan fisik dan psikologis
4. Melindungi lingkungan, untuk menyadari dampak TIK terhadap lingkungan.

Dalam pembicaraan global bahwa tahun 2020 masuk dalam era digital dan otomatisasi. Data yang didapat dari hasil survei HR 2025 (Lettink, Garstang Caroline, & Ellimäki, 2020) menyebutkan bahwa setiap individu diperlukan upaya agar mempersiapkan diri mereka dengan kemampuan yang tidak dapat dengan mudah diganti oleh mesin dan robot. Pandangan tentang manusia tidak tergantikan dengan adanya kebangkitan otomasi karena robot atau mesin akan berjalan sesuai instruksi atau program yang dibuat oleh manusia. Menurut survei yang dilakukan (Dell Technologies, 2019) terhadap para pemimpin bisnis global, era terjalinnya kemitraan antara manusia dan mesin pada Tahun 2030 sebanyak 54% orang akan menyerap dan mengelola informasi dengan cara yang sangat berbeda. Bagi pembuat kebijakan, pemimpin bisnis, dan pekerja individu di seluruh dunia, tugas ada di tangan adalah untuk mempersiapkan masa depan yang lebih otomatis dengan menekankan keterampilan baru dan meningkatkan pelatihan (Manyika et al., 2017)**.**

c) Pengembangan Kompetensi ASN

Dalam pengelolaan kepemerintahan, Indonesia telah melengkapi beberapa regulasi terkait dengan Kompetensi dan Pengembangan Kompetensi ASN, yaitu Undang - Undang No. 5 Tahun 2014 Aparatur Sipil Negara (ASN) telah diatur tentang prinsip kompetensi karena ASN adalah profesi bagi pegawai negeri sipil dan pegawai pemerintah dengan perjanjian kerja yang bekerja pada instansi pemerintah. Kompetensi melekat secara individu, manajerial, dan bahkan sebagai tolak ukur dalam pengangkatan dalam suatu jabatan.

Dari Undang Undang dijabarkan dalam Peraturan Pemerintah Nomor 11 Tahun 2017 tentang Manajemen PNS, kompetensi terdiri atas a). Kompetensi Teknis adalah pengetahuan, keterampilan, dan sikap/perilaku yang dapat diamati, diukur, dan dikembangkan yang spesifik berkaitan dengan bidang teknis Jabatan; b). Kompetensi Manajerial adalah pengetahuan, keterampilan, dan sikap/perilaku yang dapat diamati, diukur, dikembangkan untuk memimpin dan/atau mengelola unit organisasi; dan c) Kompetensi Sosial Kultural adalah pengetahuan, keterampilan, dan sikap/perilaku yang dapat diamati, diukur, dan dikembangkan terkait dengan pengalaman berinteraksi dengan masyarakat majemuk dalam hal agama, suku dan budaya, perilaku, wawasan kebangsaan, etika, nilai-nilai, moral, emosi dan prinsip, yang harus dipenuhi oleh setiap pemegang Jabatan untuk memperoleh hasil kerja sesuai dengan peran, fungsi, dan jabatan.

Pada pelaksanaannya terkait pengembangan kompetensi bagi ASN diatur oleh Lembaga Administrasi Negara dalam Peraturan Kepala Lembaga Administrasi Negara Nomor 10 Tahun 2018 tentang Pengembangan Kompetensi Pegawai Negeri Sipil (PNS) yang mengatur Pengembangan Kompetensi PNS yang diartikan sebagai upaya untuk pemenuhan kebutuhan kompetensi PNS dengan standar kompetensi jabatan dan rencana pengembangan karier. Pengembangan Kompetensi dilaksanakan dalam bentuk pendidikan dan atau pelatihan yang berupa pelatihan klasikal dan non klasikal. Menurut (Yaqoot, Noor, & Isa, 2017) dari berbagai penelitian, pelatihan dapat didefinisikan sebagai proses yang memberikan pengaruh terhadap perilaku bagi peserta pelatihan dan merupakan alat bagi organisasi untuk bertahan hidup dan manfaatnya tidak terbatas pada organisasi, tetapi juga bagi karyawan dengan keahlian baru yang diperolehnya untuk diterapkan di lingkungannya guna memenuhi kemajuan pada bidang kerjanya.

d) Keamanan Siber

Organisasi Internasional untuk Standardisasi (ISO), International Telecommunication Union (ITU), Institut Nasional Standar dan Teknologi (NIST), Komite Sistem Keamanan Nasional (CNSS), National Cybersecurity dan Communications Integration Center (NCCIC), NATO, dan ENISA merupakan beberapa organisasi yang telah mengadopsi istilah *cybersecurity* atau keamanan siber. Menurut Fischer, Ave, & Washington (2005), *cybersecurity* merupakan tindakan pencegahan

kerusakan, perlindungan, dan pemulihan komputer, sistem komunikasi elektronik, layanan komunikasi elektronik, komunikasi kawat, dan komunikasi elektronik termasuk informasi yang terkandung di dalamnya untuk memastikan ketersediaan, integritas, otentikasi, kerahasiaan, dan non-penolakan.

Munculnya definisi jenis keamanan siber (Reid & Van Niekerk, 2014) disebabkan saat ini semua pengguna Internet dan TIK dituntut memiliki kesadaran dan pengetahuan keamanan siber tingkat dasar untuk melakukan kegiatan sehari-hari. Hal ini merupakan kebutuhan dalam penanganan masalah keamanan siber di era digital. Kondisi tersebut membutuhkan koordinasi dan kerja sama secara nasional maupun internasional, di sektor pemerintah, masyarakat, dan swasta. Solusi penanganan keamanan informasi tidak cukup hanya dilakukan dalam organisasi. Keamanan informasi tidak hanya berlaku untuk penggunaan informasi dalam konteks pribadi dan dunia telah menjadi semakin lebih berorientasi pada informasi (Reid & Van Niekerk, 2014).

Keamanan siber atau *cybersecurity* adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang dapat digunakan untuk melindungi lingkungan siber dan organisasi aset pengguna. Aset organisasi meliputi perangkat komputasi yang terhubung, personel, infrastruktur, aplikasi, layanan, sistem telekomunikasi, dan totalitas informasi yang dikirim dan / atau disimpan di dunia maya. Secara umum tujuan dari keamanan siber adalah ketersediaan, integritas (yang dapat mencakup keaslian data dan nirsangkal), dan kerahasiaan (International Telecommunication Union, 2008). Penelitian *"Definition of Cybersecurity Gaps and overlaps in standardization"* (ENISA, 2017) memberikan konteks penting yang diperlukan untuk memahami istilah keamanan siber dan penggunaannya. Domain keamanan siber yang lain adalah keamanan komunikasi, keamanan operasi, keamanan informasi, keamanan fisik, keamanan publik/nasional. Di sisi lain dalam tata kelola keamanan siber selalu mempertimbangkan domain-domain ini. Mengorganisir aktivitas tata kelola informasi hanya dari perspektif keamanan informasi saja tidak cukup. Tujuan paling umum dari serangan dunia siber dapat berupa perebutan sistem, penghancuran sistem, kebocoran data, atau mengupayakan sistem yang diserang tidak dapat berfungsi (İlhan, 2015).

e) Budaya Keamanan Siber

Menjaga keamanan siber adalah masalah yang signifikan. Makna signifikan di sini bahwa kejahatan siber terus berkembang seiring dengan perkembangan teknologi juga perilaku tidak aman dari pengguna Internet. Menurut data Digital 2020 per Januari tahun 2020, jumlah pengguna internet di seluruh dunia sekarang telah mencapai 4,54 miliar atau 59% penduduk dunia dan Indonesia pengguna internetnya pada tahun 2020 mengalami kenaikan yang sangat signifikan dari tahun 2019, yaitu kurang lebih 17% menjadi 175,4 juta atau 64% (Digital 2020 Hootsuite 2020, n.d.). Pemahaman tentang perilaku individu ketika dihadapkan dengan ancaman serangan siber adalah bagian dalam menangani keamanan siber dan memitigasi serangan tersebut. Dalam konteks ini komputer sangat rentan terhadap serangan siber jika penggunanya tidak mengadopsi perilaku aman (Coventry, Briggs, Blythe, & Tran, 2014).

Pada keamanan siber orang adalah salah satu elemen utama dan keamanan siber tidak hanya tentang masalah teknis, tetapi juga pertimbangan tentang orang-orang. Hal ini disebabkan peran manusia dalam menangani informasi selalu dianggap sebagai mata rantai terlemah dalam keamanan informasi. Strategi keamanan siber dari sepuluh negara maju, lima organisasi antar pemerintah, dan sebelas kerangka kerja keamanan siber, menemukan bahwa budaya keamanan siber ditempatkan sebagai pilar utama strategi dan kebijakan keamanan siber oleh semua negara, organisasi (Ulum, 2017). Strategi keamanan siber pemerintah Indonesia juga menerapkan pola pikir dan kesadaran

keamanan siber yang sama. Salah satu rekomendasi menekankan perlunya pelatihan keamanan dan program pendidikan masyarakat yang dimulai dari pegawai pemerintah hingga perusahaan kecil-menengah (Ulum, 2017). Dari uraian di atas, dapat asumsikan bahwa budaya keamanan siber dapat dianggap sebagai salah satu strategi keamanan siber yang menempatkan orang sebagai elemen utama untuk mengakumulasi pengetahuan, pengalaman, kepercayaan, nilai – nilai, dan norma dalam tindakan keamanan siber dalam rangka melindungi aset organisasi maupun negara dari serangan siber.

f) Program Pendidikan, Pelatihan dan Kesadaran Keamanan *(Security Education, Training, and Awareness (SETA)*

Program *Security Education, Training, and Awareness* (SETA) atau Program Pendidikan, Pelatihan dan Kesadaran atas Keamanan dapat didefinisikan sebagai program pendidikan dan pelatihan yang dirancang untuk mengurangi jumlah pelanggaran keamanan siber yang terjadi karena kurangnya kesadaran individu terhadap keamanan siber. Program SETA juga dapat didefinisikan sebagai program yang targetnya semua pengguna dalam suatu organisasi untuk membantu mereka menjadi lebih sadar akan prinsip-prinsip keamanan informasi untuk pekerjaan mereka. Program SETA juga membantu organisasi menghadapi risiko penyusupan karena ketidaktahuan para karyawan tentang cara melakukan tugas-tugas berbasis IT yang aman. Hal ini penting bagi setiap karyawan memahami keamanan siber karena dalam pelaksanaan program SETA dibutuhkan partisipasi dan motivasi (Caballero, 2017). Program SETA dalam penerapannya terdiri atas tiga tahap yang merupakan rangkaian pelatihan, yaitu tingkat kesadaran (*awerness*), tingkat pelatihan (*training),* dan tingkat pendidikan (*education*). Pelaksanaan Program SETA diawali dengan tingkat dasar yang bersifat umum untuk semua pengguna dalam hal ini seluruh pegawai yang ada dengan tujuan untuk membangun kesadaran sehingga mampu menciptakan budaya kesadaran keamanan siber di seluruh organisasi dan perlu disampaikan kepada semua pengguna yang berfokus pada akuntabilitas individu. Pada akhirnya, semakin tinggi tingkat risiko yang dikelola oleh individu, semakin tinggi pula tingkat kesadaran dan pelatihan yang harus mereka dapatkan. Tingkat pendidikan keamanan siber biasanya dilaksanakan dalam pendidikan formal yang dibangun untuk mengajarkan semua konsep dasar yang diperlukan untuk membangun karier di bidang keamanan informasi. Sudah banyak di antara universitas dan perguruan tinggi telah mulai membuat kurikulum yang menawarkan gelar sarjana dan magister tentang keamanan informasi.

g) Analisis Kebutuhan Pelatihan

Analisis kebutuhan pelatihan adalah tahap awal dalam proses pelatihan dan melibatkan mekanisme untuk menentukan apakah pelatihan memang akan dapat mengatasi masalah yang sudah diidentifikasi sebelumnya (Bansal & Prakash Tripathi, 2017). Pada dasarnya tujuan pelatihan dapat didefinisikan apabila analisis kebutuhan pelatihan dilakukan secara sistematis terkait dengan pengembangan dalam organisasi yang dilakukan secara profesional. Oleh karena itu, analisis kebutuhan pelatihan dimulai dengan mendefinisikan kesenjangan antara apa yang diketahui dan dapat dilakukan oleh karyawan dan apa yang mereka dan organisasi harapkan dapat lakukan, yang dapat diisi dengan pelatihan (Ludwikowska, 2018). Kegiatan pelatihan dipastikan dari analisis kebutuhan pelatihan agar mendapatkan relevansi sasaran peserta dan untuk menaikkan kualitas kinerjanya berdasarkan keahlian atau jenis keahlian yang dibutuhkan (Bansal & Prakash Tripathi, 2017).

Menurut (Khan & Masrek, 2017), setiap kegiatan pelatihan mewajibkan analisis kebutuhan pelatihan untuk mengenali apa, di mana, bagaimana, serta kapan akan dilaksanakan. Keberhasilan

dan kegagalan pelatihan tergantung pada identifikasi peserta yang tepat untuk program pelatihan dimaksud (Nazli, Sipon, & Radzi, 2014).

2. METODE PENELITIAN

2.1. Systematic Literature Review dengan metode PRISMA

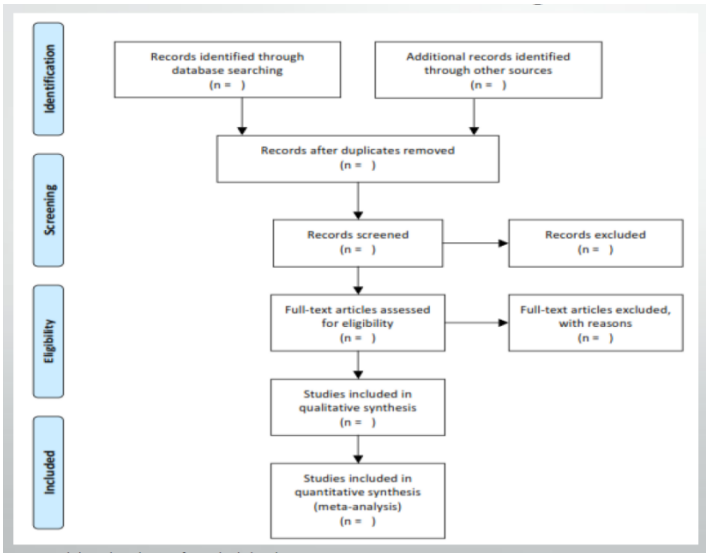
Penyaringan data dalam kajian ini dilakukan dengan *Systematic Literature review* (Cooper, Booth, Varley-Campbell, Britten, & Garside, 2018). Pendekatan kualitatif dalam *systematic review* digunakan untuk mensintesis (merangkum) hasil-hasil penelitian yang bersifat deskriptif kualitatif. Metode sintesis hasil-hasil penelitian kualitatif ini disebut dengan "meta-analisis" yang merupakan teknik melakukan integrasi data untuk mendapatkan teori maupun konsep baru atau tingkatan pemahaman yang lebih mendalam dan menyeluruh (Cooper et al., 2018).

Agar lebih sistematis, studi melakukan *Systematic Literature Review* dengan metode PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-analyses*). PRISMA dapat didefinisikan sebagai teknik penelitian berdasarkan pengumpulan semua bukti yang relevan dalam bidang tertentu secara sistematis dan menilai dengan analisis secara kritis untuk mendapatkan kesimpulan dari rangkuman penelitian, seperti pada Gambar 1. Terdapat empat tahapan yang digunakan untuk melakukan kajian literatur dengan PRISMA, seperti yang dilakukan oleh Kautsarina & Diah Kusumawati dalam penelitian *The Potential Adoption of the Internet of Things in Rural Areas* (Kautsarina & Kusumawati, 2018).

a) Kriteria Kelayakan Literatur

Sumber informasi yang diperoleh penulis secara komprehensif dari pengumpulan makalah yang memiliki hubungan dengan karya tulis ilmiah, seperti jurnal dan artikel serta kebijakan secara *online* yang diterbitkan antara 2013 dan 2020 yang berskala internasional. Pertimbangan periode ini memungkinkan pengambilan sejumlah studi yang sesuai dengan topik dan tren penelitian terkait.

Ruang lingkup batasan kriteria yang digunakan adalah literatur yang diterbitkan berhubungan dengan "Bagaimana Kebutuhan Pelatihan Budaya Keamanan Siber sebagai Upaya Pengembangan Kompetensi ASN Di Era Digital" atau literatur yang terkait dengan kompetensi, kompetensi digital, pengembangan kompetensi ASN, *cybersecurity*, *cybersecurity culture* dan *Security Education Training Awareness* (SETA) serta Analisis Kebutuhan Pelatihan dalam bahasa Inggris (KL1). Selain itu, literatur yang dipilih untuk dapat menjawab pertanyaan penelitian (KL2).



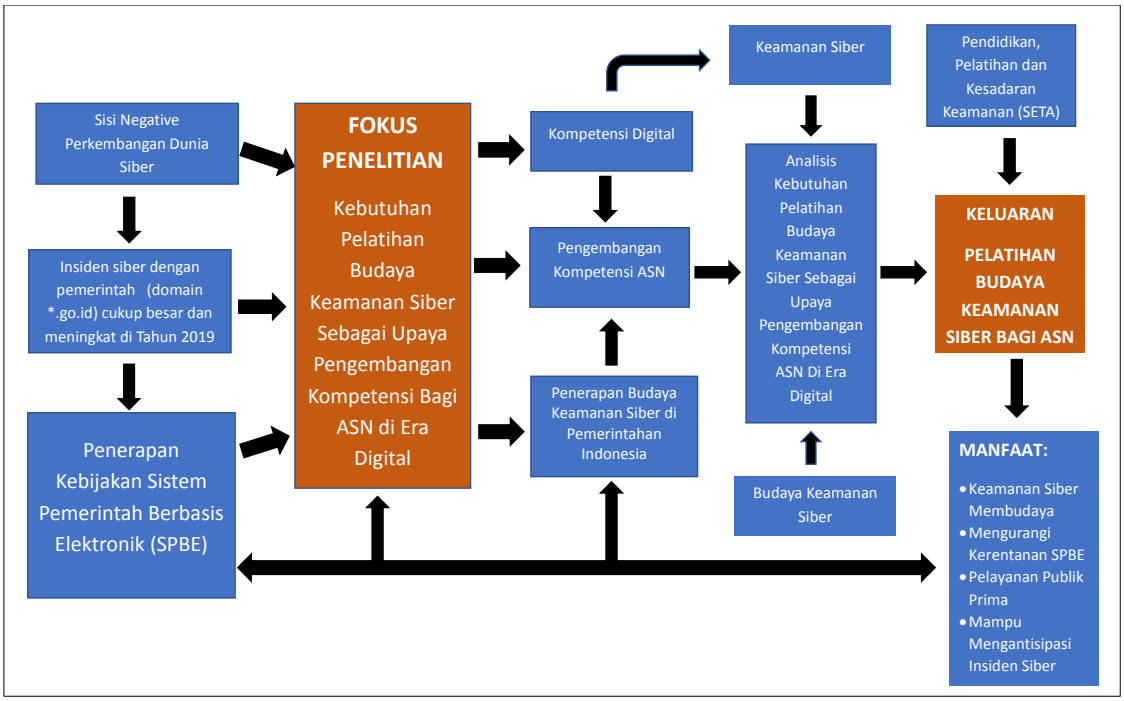
Gambar 1. Diagram Alir PRISMA

b) Pemilahan Literatur/Referensi

Literatur dipilih melalui empat tahapan. *Pertama*, melakukan identifikasi literatur berbasis online yang terkait, yaitu Google Scholar, IEEE Xplore, ScienceDirect, Elsevier serta Researchgate. Pelaksanaan pada tahap ini dilakukan dengan menggunakan kata kunci pencarian yang relevan sebagai berikut: "kompetensi digital" DAN "Pengembangan kompetensi ASN" DAN "*cybersecurity*" DAN "*cybersecurity culture*" DAN "SETA" DAN "Analisis Kebutuhan Pelatihan", yang diadaptasi ke mesin pencari database. *Kedua*, melakukan pencarian atau penggalian judul, abstrak dan kata kunci dari makalah dan artikel dan memilah literatur yang diidentifikasi berdasarkan kriteria kelayakan yang berasal dari kata kunci tersebut. *Ketiga*, membaca secara lengkap atau sebagian literatur atau artikel yang belum dihilangkan pada tahap sebelumnya untuk mempertimbangkan apakah mereka harus dimasukkan dalam ulasan, atau tidak sesuai dengan kriteria kelayakan. Sebanyak 95 dokumen diidentifikasi dan sebanyak 50 di antaranya dipilih untuk diambil sebagai daftar pustaka. *Keempat*, mengambil daftar referensi makalah (*paper*) untuk menemukan studi baru yang kemudian ditinjau sebagaimana ditunjukkan dalam tahap 2 dan 3, tetapi makalah ini harus memenuhi kriteria kelayakan literatur.

2.2. Kerangka Pemikiran

Dalam penulisan karya tulis ilmiah ini, penulis memerlukan kerangka pemikiran yang bertujuan untuk memberikan gambaran mengenai variabel apa saja yang diamati dan menjabarkan secara terstruktur komponen dan cakupan penelitian sehingga dapat menjadi pemandu peneliti ataupun pembaca hasil penelitian untuk mengerti secara cepat keseluruhan penelitian yang dilakukan seperti yang tersebut pada Gambar 2 di bawah ini.



Gambar 2. Kerangka Pemikiran Penelitian

3. HASIL DAN PEMBAHASAN

3.1. Keamanan Website Instansi Pemerintah Pusat dan Daerah

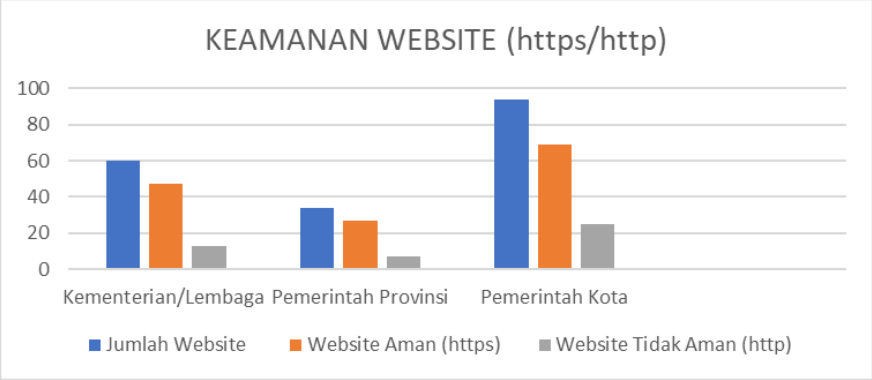
Sebelum menjalankan metode PRISMA, studi ini melakukan observasi dan analisis atas laman website Pemerintah Pusat dan Daerah. Hal ini dilakukan mengingat laman (*website*) merupakan salah satu representasi tampilan organisasi, bahkan menjadi tampilan awal untuk layanan

pemerintah berbasis *online*. Observasi dilakukan pada bulan Januari 2020 dengan melihat tingkat keamanan laman pemerintah dan melakukan validasi kesesuaian dengan standar World Wide Web Consortium (W3C) yang merupakan konsorsium untuk bekerja mengembangkan standar-standar World Wide Web (WWW). Evaluasi dilakukan terhadap laman satuan unit kerja di lingkungan Pemerintah Pusat (Kementerian/Lembaga), Pemerintah Daerah tingkat Provinsi dan Kota. Dari kegiatan ini diperoleh gambaran awal kondisi pemerintahan Indonesia saat ini terkait komitmen terhadap keamanan siber. Proses ini juga dapat melihat sejauh mana perhatian dan sikap pemerintah atas penerapan keamanan siber.

Dari hasil pendataan atas aman (menggunakan HTTPS) dan tidak amannya (menggunakan HTTP) laman atau situs kementerian, lembaga, pemerintah provinsi dan kota diperoleh hasil bahwa penggunaan HTTPS pada kementerian dan lembaga terdapat 60 institusi, yang tidak aman (menggunakan HTTP) sebanyak 13 (21,7%) institusi, sdangkan untuk pemerintah provinsi yang lamannya tidak aman (hanya menggunakan HTTP) sebanyak 7 (20,59%) institusi dari 34 pemerintah provinsi. Sementara untuk pemerintah kota yang hanya menggunakan HTTP pada laman *website*-nya berjumlah 26 institusi atau 27,6% dari 94 pemerintah kota.

Hasil validasi URL laman pemerintah disajikan dalam Gambar 3. dari angka tersebut dapat dipahami bahwa baik instansi pusat maupun daerah masih belum secara penuh menerapkan kesesuaian standar keamanan laman (*website*), padahal laman adalah merupakan tampilan permukaan untuk berbagai sistem pemerintahan berbasis elektronik untuk pelayanan publik. Temuan ini memperlihatkan adanya korelasi banyaknya pengaduan insiden siber dari instansi pemerintah tentang kerentanan sistem (ID-SIRTII, 2018). Dari 105 pengaduan insiden siber, sebanyak 63% adalah tentang kerentanan sistem dan 37 % sisanya tentang Web defacement, Malware Phising, dan lain lain.

Dalam kasus insiden siber yang dimaksud adalah semua instansi pemerintah yang sudah seharusnya melakukan mitigasi risiko dengan memberikan konteks penting yang diperlukan untuk memahami keamanan siber dan penggunaannya karena domain keamanan siber juga meliputi keamanan komunikasi, keamanan operasi, keamanan informasi, keamanan fisik, keamanan publik/nasional (ENISA, 2017).



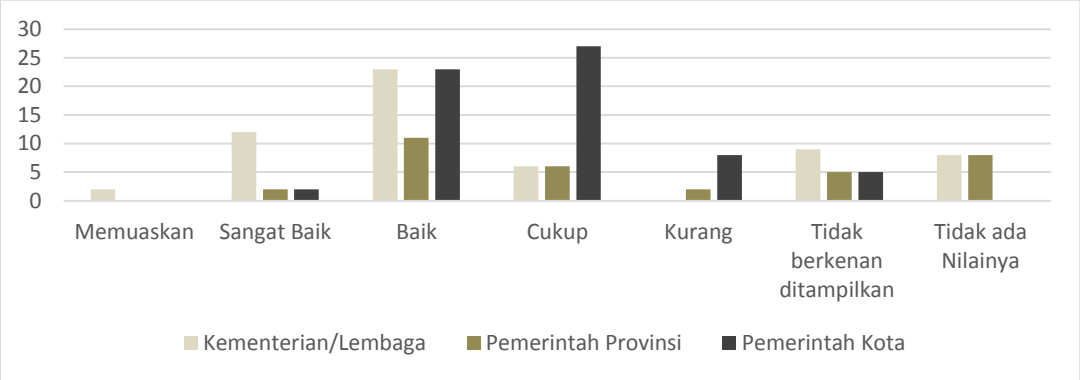
Gambar 3. Bagan Hasil Pendataan atas aman dan tidak amannya Laman atau *Website* Kementerian/Lembaga, Pemerintah Provinsi dan Pemerintah Kota (Sumber Hasil Januari 2020)

3.2. Penerapan SPBE pada Instansi Pusat dan Pemerintah Daerah

Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE (Pemerintah RI.SPBE, 2018). Pelaksanaan penerapan SPBE pada instansi pusat dan pemerintah daerah dapat diketahui dari capaian kemajuan

pelaksanaan SPBE dan Kementerian PANRB melakukan kegiatan Evaluasi SPBE pada tahun 2019. Dengan berpedoman pada Kemenpan RB (2018), dapat diketahui nilai dan predikat SPBE termasuk di dalamnya adalah nilai setiap domain dan aspeknya, yaitu Domain Kebijakan Internal SPBE yang meliputi Aspek Kebijakan Internal Tata Kelola SPBE dan Aspek Kebijakan Internal Layanan SPBE serta Domain Tata Kelola SPBE meliputi Aspek Kelembagaan dan Aspek Strategi dan Perencanaan serta Aspek Teknologi Informasi dan Komunikasi dan Domain Layanan SPBE yang meliputi Aspek Layanan Administrasi Pemerintahan Berbasis Elektronik dan Aspek Layanan Publik Berbasis Elektronik.

Dari hasil Monitoring dan Evaluasi SPBE pada laman http://spbe.go.id/moneval, sebanyak 60 instansi kementerian dan lembaga, 34 pemerintah provinsi, dan 74 pemerintah kota diperoleh informasi bahwa hanya ada di instansi pusat yang mendapatkan penilaian **SANGAT MEMUASKAN,** yaitu Kementerian Keuangan dan Kementerian Perhubungan**.** Selanjutnya terdapat instansi 15% pemerintah pusat yang tidak berkenan nilainya dipublikasikan karena menjadi angka tertinggi dibandingkan pemerintah provinsi yang sebesar 14,71% dan pemerintah kota sejumlah 6,76%. Hal tersebut akan menimbulkan pertanyaan dari publik atas integritas dan transparansi dari suatu instansi seperti tersebut pada Gambar 4 di bawah ini. Di samping itu pula masih terdapat instansi pusat dan daerah yang mendapatkan nilai CUKUP, yaitu kementerian/lembaga sebanyak 10%, pemerintah provinsi sebanyak 14,71% dan pemerintah kota sejumlah 36,49%. Adapun untuk penilaian KURANG hanya pada pemerintah kota (10,81%) dan pemerintah provinsi (5,88%).



Gambar 4. Bagan Nilai SPBE Instansi Pusat dan Daerah (Sumber Olahan Data MenPAN RB)

3.3. Keamanan Siber di Pemerintahan Era Digital

a) Lembaga Pemerintah dan Non Pemerintah Terkait Keamanan Siber di Indonesia

Kehadiran Badan Siber dan Sandi Negara BSSN mengemban seluruh tugas dan fungsi di bidang persandian serta pelaksanaan seluruh tugas dan fungsi di bidang keamanan informasi, pengamanan pemanfaatan jaringan telekomunikasi berbasis protokol internet, serta keamanan jaringan dan infrastruktur telekomunikasi. Kementerian Komunikasi dan Informatika pada nomenklatur Organisasi yang baru untuk menjawab tantangan dunia siber adalah Direktorat Tata Kelola. Direktorat itu menangani kebutuhan regulasi layanan untuk ekonomi digital, sertifikasi elektronik, hingga tata kelola perlindungan data pribadi. Semua itu ditujukan untuk memastikan tidak ada kekosongan dalam perundangan yang berkaitan dengan tata kelola dunia siber dan digital (Kementerian Kominfo, 2018).

ID-SIRTII/CC berada di bawah kewenangan BSSN sebagai lembaga dalam struktur BSSN dan memiliki tugas pokok melakukan sosialisasi dengan pihak terkait tentang keamanan IT, melakukan

pemantauan dini, pendeteksian dini, peringatan dini terhadap ancaman terhadap jaringan telekomunikasi dari dalam maupun luar negeri khususnya dalam tindakan pengamanan pemanfaatan jaringan, membuat/menjalankan/mengembangkan dan database log file, serta statistik keamanan Internet di Indonesia. Indonesia Honeynet Project (IHP) merupakan komunitas keamanan siber dan salah satu chapter dari organisasi nirlaba Honeynet Global (https://honeynet.org) di Indonesia. ID-CERT (https://www.cert.or.id/tentang-kami/id/) adalah tim koordinasi teknis berbasis komunitas yang bersifat independen. ID-CERT berfungsi sebagai koordinasi teknis terhadap komplain yang diterima dan bersifat reaktif, baik di dalam negeri maupun ke luar negeri. ID-CERT bersikap reaktif, yakni melakukan pekerjaan atas dasar masukan dari pihak luar, dalam hal ini melalui pelaporan yang diterimanya. Gov-CSIRT (Government Cyber Security Insiden Response Team)Indonesia (https://govcsirt.bssn.go.id/) merupakan tim respons insiden siber sektor pemerintah yang memberikan layanan respon insiden di sektor pemerintah. Gov-CSIRT Indonesia beranggotakan seluruh staf BSSN pada sektor pemerintah. Gov-CSIRT Indonesia berfungsi membangun, mengoordinasikan, mengolaborasikan, dan mengoperasionalkan sistem mitigasi, manajemen krisis, penanggulangan dan pemulihan insiden keamanan siber di sektor pemerintah.

b) Sikap Pemerintahan Indonesia Terhadap Keamanan Siber di Era Digital

Tuntutan transformasi administrasi publik telah dipenuhi dengan adanya kewajiban penerapan SPBE. Transformasi tersebut meliputi perubahan pada organisasi dalam peningkatan pemberian layanan kepada publik. Penggunaan teknologi informasi untuk menciptakan nilai publik dan meningkatkan responsibilitas dan keterbukaan pemerintah (Lindgren & Van Veenstra, 2018).

Perubahan paradigma dari bentuk pemerintahan birokrasi ke pemerintahan berjejaring membutuhkan akuntabilitas yang lebih besar dari sekedar administrasi publik sehingga hasil evaluasi penerapan SPBE tidak akan dijumpai dalam penerapan SPBE dengan status **"tidak berkenan untuk ditampilkan"** seperti tersebut pada Gambar 4 di atas karena paradoks dengan tujuan dari pemerintahan digital sendiri yang dianggap sebagai fasilitator dan pendorong transformasi birokrasi. Pemerintahan digital sering dipahami sebagai pengembangan digitalisasi layanan publik secara elektronik untuk masyarakat secara umum dan tidak dipahami hanya sebatas wujud laman (website).

Strategi keamanan siber pemerintah Indonesia juga menerapkan pola pikir dan kesadaran keamanan siber yang sama. Salah satu rekomendasi menekankan perlunya pelatihan keamanan dan program pendidikan masyarakat yang dimulai dari pegawai pemerintah hingga perusahaan kecil-menengah (Ulum, 2017). Hal ini membawa konsekuensi terkait perlunya pembudayaan keamanan siber secara masif kalau tidak kita akan mendapatkan kerugian seperti yang dinyatakan oleh (A Frost & Sullivan, 2019) potensi kerugian ekonomi di Indonesia akibat insiden keamanan siber dapat mencapai angka US$34,2 miliar. Angka tersebut merupakan 3,7% dari total PDB Indonesia sebesar US$932.

Dari sikap pemerintah Indonesia terkait keamanan siber dengan kesiapan, kelembagaan pemerintah dan lembaga independen dan regulasinya dapat dikatakan sudah siap. Seperti yang dinyatakan dalam (International Telecommunication Union, 2018), Global Cyber Security Indeks 2019 posisi Indonesia di peringkat global ke 41 dan peringkat ke 9 di tingkat regional masih di atas negara India dan Philipina.

c) Penerapan Budaya Keamanan Siber di Pemerintahan Indonesia

Penerapan SPBE (Pemerintah RI.SPBE, 2018) adalah wujud dari pemerintahan Indonesia di era digital maka mau atau tidak mau, telah menjadi keharusan dan keniscayaan bagi seluruh

instansi pemerintah bauk di pusat maupun di daerah untuk menerapkan tata kelola pemerintah yang. operasionalnya berbasis internet, dan menerapkan keamanan siber. Digitalisasi menjanjikan memberikan partisipasi secara luas kepada warga negara dalam proses bisnis disektor publik. Pemerintahan di era digital identik dengan pemerintahan yang berbasis teknologi digital (Lindquist & Huse, 2017) atau berbasis data dan proses bisnis pemerintahannya dijalankan secara elektronik (McKinsey Global Institute, 2018). Perlindungan infrastruktur nasional yang strategis dalam bidang keuangan, perbankan, transportasi, medis, pendidikan, energi, pemerintahan dan administrasi publik berbasis elektronik, pendidikan dan budaya keamanan dunia maya adalah merupakan tantangan tata kelola keamanan siber (Eugen, 2018).

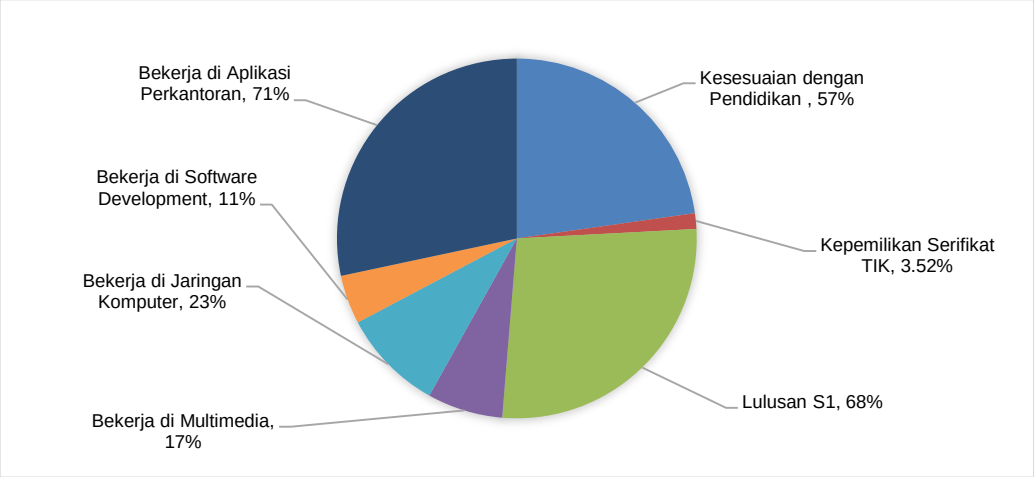
Dari sinilah budaya keamanan siber dapat dipahami sebagai salah satu strategi keamanan siber yang menempatkan orang sebagai elemen utama untuk mengakumulasi pengetahuan, pengalaman, kepercayaan, nilai – nilai dan norma dalam tindakan keamanan siber dalam rangka melindungi aset organisasi bahkan aset negara dari serangan siber.

Penerapan budaya keamanan siber belum sepenuhnya dilaksanakan di lingkungan pemerintahan. Hal ini terlihat dari masih adanya laman pada pemerintah pusat maupun pemerintah daerah yang belum aman juga didapatkan data sejumlah 229 (dua ratus dua puluh sembilan) insiden siber pada sektor pemerintah di tahun 2019 (GOV_CISRT_BSSN, 2019). Dari data tersebut memperlihatkan korelasi dengan hasil evaluasi SPBE dan kesesuaian terkait kondisi instansi pemerintah pusat dengan predikat **"cukup"** 10%, pemerintah provinsi 14,71% dan pemerintah kota sejumlah 36,49%. Instansi pusat tidak terdapat predikat **"kurang"**. Adapun yang terbanyak adalah pada pemerintah kota sebesar 10,81% dan pemerintah provinsi sejumlah 5,88%, seperti data yang ditunjukkan pada Gambar 4.

3.4. Kompetensi Digital ASN

Selain teknologi, keamanan siber juga merujuk pada fakta bahwa orang memiliki keterlibatan akses ke data dan proses aksesnya sehingga mendapatkan status dapat diotorisasi atau tidak sah. Penyerang dunia siber dapat berasal dari individu atau kelompok yang berupaya dengan tujuan mengeksploitasi kerentanan untuk keuntungan pribadi atau finansial dengan melakukan kegiatan kejahatan di dunia siber (Reegård & Blackett, 2019). Dalam kerangka pemikiran kepemerintahan dan untuk mengantisipasinya, diperlukan adanya ASN pengelola data dan aksesnya yang siap dengan datangnya insiden siber sehingga dalam hal ini ASN perlu memiliki kepekaan terhadap keamanan siber di Indonesia.

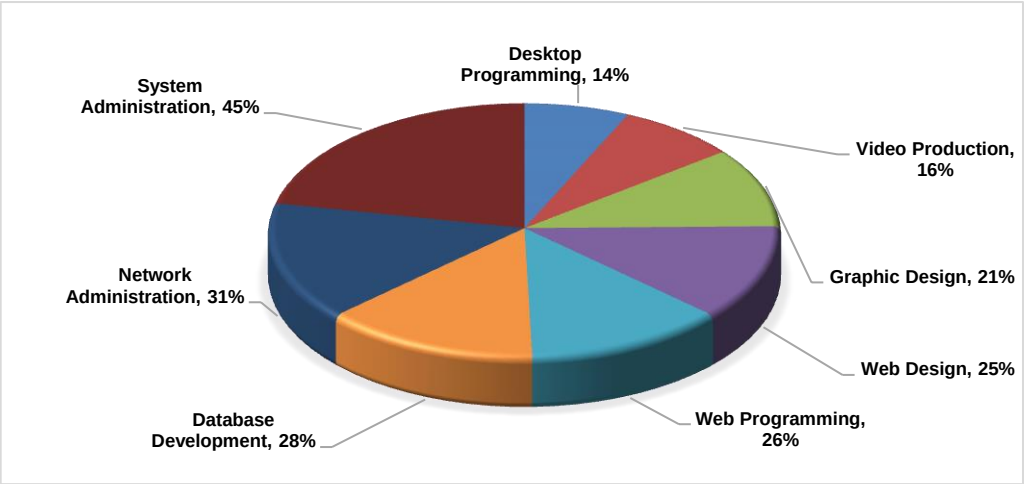
Menurut statistik Badan Kepegawaian Negara per Juni 2019, saat ini total PNS berjumlah 4,2 juta atau pastinya 4.286.918 orang. Dari Survei Balitbang SDM Kominfo (Kementerian Kominfo, 2018) mendapatkan potret dan gambaran tentang kompetensi SDM TIK di 20 Provinsi dengan 1.400 responden ASN yang diperkirakan ASN Bidang TIK sejumlah 13.336 dengan gambaran seperti pada Gambar 5 di bawah ini.



Gambar 5. Bagan Profil dan Pemetaan SDM TIK (Sumber Olahan dari Kementerian Kominfo 2019)

Profil pada Gambar 5 memperlihatkan bahwa kompetensi ASN sangat sederhana apabila dikaitkan dengan kebutuhan kompetensi di era digital karena kompetensi saat ini didominasi pada pekerjaan dengan aplikasi perkantoran sebesar 71%, yang artinya hanya 29% ASN yang bekerja dengan kompetensi di bidang TIK dan yang lainnya. Lebih dari itu, kompetensi yang teruji melalui sertifikasi hanya 3,52% yang menunjukkan masih banyak ASN yang belum teruji kompetensinya. Hal ini menunjukkan bahwa data tersebut berbanding lurus dengan keinginan pelatihan yang disampaikan oleh ASN Bidang TIK, seperti pada Gambar 6.

Ketika kompetensi digital dengan menganalogikan pengembangan profesional guru dengan ASN pendapat Spante, Hashemi, Lundin, & Algers (2018) sehubungan dengan hal tersebut mendefinisikan konsep kompetensi digital tersebut dipertimbangkan dengan kemampuan masing-masing ASN dalam mengimplementasikan TIK pada kegiatan operasionalnya dan untuk meningkatkan pengembangan pengetahuan dan pemahaman bagi ASN itu sendiri.



Gambar 6. Bagan Pelatihan Yang Diinginkan ASN Bidang TIK

Dari gambaran kompetensi ASN pada Gambar 5 saat ini bila dibandingkan dengan 5 bidang kompetensi digital yang dinyatakan oleh Ferrari et al. (2013) terlihat bahwa yang sudah dilakukan oleh ASN adalah kompetensi informasi dan komunikasi, sedangkan kompetensi keamanan informasi belum terlihat, yang meliputi perlindungan pribadi, perlindungan data, perlindungan identitas digital, langkah-langkah keamanan, penggunaan yang aman dan berkelanjutan. Hal ini juga menunjukkan bahwa adanya hubungan antara kompetensi digital ASN dengan tidak amannya

laman website di beberapa instansi pusat dan daerah serta masih adanya yang berpredikat cukup dan kurang sesuai hasil monitoring dan evaluasi SPBE 2019.

3.5. Pengembangan Kompetensi Digital ASN pada area Keamanan Siber

a) Pengembangan Kompetensi Digital pada Area Keamanan

Pada bagian ini pembahasan lebih diarahkan kepada pemahaman area keamanan pada kerangka kompetensi digital. Sehubungan dengan itu, yang menjadi kerangka kerja kompetensi digital pada area keamanan dan kemahiran yang akan diperoleh (Ferrari et al., 2013). Hal ini akan sangat sesuai dengan pembahasan jika dikaitkan dengan pelayanan publik dan bisa dimungkinkan bahwa serangan siber berasal dari orang dalam pada tabel 1.

Tabel 1: Kompetensi Digital dan Kemahirannya Pada Area Keamanan

KOMPETENSI KEAMANAN	KEMAHIRAN
Melindungi Perangkat untuk melindungi perangkat sendiri, memahami risiko dan ancaman *online*, dan mengetahui langkah-langkah keselamatan dan keamanan	• Menggunakan langkah-langkah dasar untuk melindungi perangkat, misalnya, menggunakan anti-virus, kata sandi. • Mengetahui bagaimana melindungi perangkat digital dan memperbarui strategi keamanan. • Sering memperbarui strategi keamanan dan dapat mengambil tindakan saat perangkat terancam.
Melindungi data pribadi Untuk memahami ketentuan umum layanan, perlindungan aktif data pribadi, memahami privasi orang lain, melindungi diri dari penipuan dan ancaman *online* dan intimidasi siber	• Mengetahui hanya dapat berbagi jenis informasi tertentu tentang pribadi atau orang lain di lingkungan daring. • Melindungi privasi daring pribadi dan orang lain dan memiliki pemahaman umum tentang masalah privasi dan pengetahuan dasar tentang bagaimana data dikumpulkan dan digunakan. • Sering mengubah pengaturan *privasi default* layanan daring untuk meningkatkan perlindungan privasi Memiliki pemahaman yang luas s tentang masalah privasi dan mengetahui bagaimana data dikumpulkan dan digunakan.
Melindungi kesehatan Untuk menghindari risiko kesehatan yang terkait dengan penggunaan teknologi dalam hal ancaman terhadap kesejahteraan fisik dan psikologis	• Mengetahui cara menghindari perundungan siber (*cyber bullying*), mengetahui teknologi dapat memengaruhi kesehatan jika disalahgunakan. • Mengetahui bagaimana melindungi diri dan orang lain dari perundungan siber dan memahami risiko kesehatan yang terkait dengan penggunaan teknologi (dari aspek ergonomi hingga kecanduan teknologi). Menyadari penggunaan teknologi yang benar untuk menghindari masalah kesehatan. • Mengetahui cara menemukan keseimbangan yang baik antara dunia daring dan tatap muka
Melindungi lingkungan Menyadari dampak TIK terhadap lingkungan	• Mengambil langkah-langkah dasar untuk menghemat energi. • Memahami aspek positif dan negatif dari penggunaan teknologi terhadap lingkungan. • Memiliki informasi tentang dampak teknologi terhadap kehidupan sehari-hari, konsumsi daring, dan lingkungan.

Dalam rangka meningkatkan profesionalitas sumber daya manusia terkait keamanan siber (*cybersecurity)*, kehadiran Peta Okupasi Nasional dalam Kerangka Kualifikasi Nasional Indonesia pada Area Fungsi Keamanan Siber (BSSN, 2019b) yang terdiri dari berbagai jabatan pekerjaan maupun profesi di birokrasi /pemerintahan dan industri dengan 16 fungsi kunci dan salah satu fungsi kuncinya terkait keamanan siber adalah *IT Security and Compliance.* Ruang lingkup kompetensi bervariasi dari sangat konseptual hingga teknis dari yang teoretis hingga terapan. Dengan demikian, terbuka peluang bagi ASN untuk meniti karier di bidang keamanan siber yang nantinya akan mempunyai pengaruh berganda (*multiplier effect*) di organisasinya sehingga

harapannya dapat menjadi individu yang kuat dalam mengawal keamanan siber di organisasi pada khususnya dan Indonesia pada umumnya.

b) Pengembangan kompetensi Digital ASN pada Area Keamanan Siber

Data Kementerian Kominfo (2018) menyebutkan bahwa ASN yang pernah mengikuti pelatihan sebesar 42,7% dan didominasi dengan ASN yang berada di lokasi di Pulau Jawa. Data ini menunjukkan bahwa ASN Indonesia sangat membutuhkan pengembangan kompetensi digital melalui pelatihan dengan sebaran di seluruh provinsi agar bisa mengelola layanan publiknya sesuai kebutuhan masyarakat di era digital. Menurut Mahmud, Saira Wahid, & Arif (2019), pelatihan adalah proses yang merupakan kunci untuk meningkatkan keterampilan, sikap, dan pengetahuan seseorang yang dalam hal ini terkait dengan kompetensi digital untuk menghasilkan pencapaian hasil organisasi dan sumber daya manusia yang lebih baik.

Pengembangan kompetensi ASN adalah upaya untuk pemenuhan kebutuhan kompetensi dengan standar kompetensi Jabatan dan rencana pengembangan karier (LAN, 2018). Pengembangan kompetensi adalah merupakan hak ASN (ASN, 2014) dan dalam bentuk pendidikan dan pelatihan (LAN, 2018). Semakin banyak pelatihan yang diberikan, semakin banyak manfaat bagi karyawan, semakin meningkat keterampilan dan kemampuan, dan semakin banyak manfaat yang kembali ke organisasi. Pentingnya pelatihan lainnya adalah memberikan kemungkinan adaptasi pada karakteristik daya saing dan perubahan pasar yang cepat. Pelatihan adalah kekuatan yang disimpan untuk mempertahankan organisasi. Pelatihan merupakan hal yang penting karena merupakan wujud dari investasi manusia (Yaqoot et al., 2017).

Era digital adalah era disruptif yang harus diantisipasi oleh pemerintahan berbasis elektronik dalam penerapan SPBE. Sudah menjadi keharusan adanya tuntutan mendesak agar dilakukan pengembangan kompetensi bagi ASN agar mampu mengimbangi perkembangan zaman yang lebih cepat, responsif, dan adaptif terhadap seluruh tuntutan kebutuhan masyarakat yang semakin tangkas. Sementara makin tingginya angka serangan siber pada instansi pemerintah dan kondisi penerapan SPBE pada beberapa instansi pemerintah yang tingkat maturitasnya masih rendah, sangat relevan bila pembahasan akan diarahkan pada upaya pengembangan kompetensi digital ASN dengan fokus pelatihan budaya keamanan siber.

3.6. Analisis Kebutuhan Pelatihan Budaya Keamanan Siber

Berbagai faktor yang dapat mempengaruhi keberhasilan atau kegagalan pelatihan, dimana salah satunya adalah ketika pelatihan yang tidak tepat dilakukan untuk peserta pelatihan atau melaksanakan pelatihan di waktu yang tidak tepat. Di sinilah kebutuhan pelatihan memainkan peran penting untuk memastikan pelaksanaan pelatihan akan berhasil (Nazli et al., 2014) dan dapat diyakini bahwa melakukan analisis kebutuhan akan menjadi strategi yang efektif untuk membuat program pelatihan menjadi efektif juga sebagai bagian dari pengembangan profesional yang berkelanjutan (Mahmud et al., 2019).

Dalam perspektif budaya keamanan siber, SETA yang merupakan program pendidikan dan pelatihan dan dirancang untuk mengurangi jumlah pelanggaran keamanan siber yang terjadi karena kurangnya kesadaran individu terhadap keamanan siber dan dapat membantu organisasi menghadapi risiko penyusupan karena ketidaktahuan para karyawan tentang cara melakukan tugas-tugas berbasis IT yang aman (Caballero, 2017). Hal ini menjadi sangat sesuai apabila SETA ditinjau dari kebutuhan pelatihan budaya keamanan siber sebagai kebutuhan organisasi (Yoo, Sanders, & Cerveny, 2018). Dalam SETA yang utama adalah belajar tentang mengamankan organisasi dan aset informasinya dan dapat memberikan pengalaman kepada karyawan memperoleh kepemilikan psikologis atau rasa ikut memiliki dalam memotivasi untuk berperilaku etis dan

bertanggung jawab dan sisi individu lebih mengarah pada unjuk kinerja yang baik. Dalam konteks ini faktor pendidikan keamanan siber harus bisa memberikan informasi kepada penggunanya serta memberikan umpan balik (Bada et al., 2014). Dalam kenyataannya masih sering didapatkan kasus yang ada di antara mereka yang tidak patuh pada kebijakan terkait keamanan siber dan tidak termotivasi untuk mematuhi praktik keamanan siber. Akibatnya, diperlukan budaya keamanan siber secara efektif dalam praktik dan kebijakan bagi semua pemangku kepentingan. Mereka meningkatkan keterampilan dan pengetahuan untuk mendukung terciptanya budaya keamanan siber. Hal itu untuk mendorong perubahan menuju budaya keamanan siber yang lebih baik dalam organisasi (M.C. Van ‘t Wout, 2019). Bailey, Kolo, Rajagopalan, & Ware (2018) menyatakan terdapat 50 persen pelanggaran terkait ancaman orang dalam melalui pegawai dan pihak ketiga adalah salah satu masalah terbesar yang harus diperhatikan dalam keamanan dunia siber.

4. PENUTUP

Setelah melakukan eksplorasi dan pembahasan atas berbagai ragam literatur terkait keamanan siber, budaya keamanan siber dan Hasil Monitoring dan Evaluasi SPBE yang belum optimal sehingga dapat disimpulkan bahwa temuan ini penting untuk merancang program pelatihan sebagai bagian dari pengembangan kompetensi digital ASN yang berkelanjutan, khususnya terkait pelatihan budaya keamanan siber di lingkungan pemerintah, dalam pelayanan publiknya. Karena teknologi dan pengetahuan tentang upaya peretasan dalam kejahatan siber berkembang sangat cepat, perlu antisipasi investasi sumber daya manusia melalui pelatihan budaya keamanan siber. Keterbatasan studi ini mencakup konsentrasi hanya pada kompetensi digital pada area keamanan saja sehingga bisa diperluas ke pada empat area lainnya, yaitu kompetensi informasi, komunikasi, pembuatan konten, dan pemecahan masalah dengan program pelatihan dan pendekatan yang berbeda. Namun, penelitian ini membahas lebih kepada kebutuhan dan pentingnya pelatihan budaya keamanan siber dan masih sedikit penelitian yang dapat diakses untuk tujuan penelitian dan penyajian yang menarik untuk studi mendalam di masa depan. Manfaat dengan adanya pelatihan budaya keamanan informasi bagi organisasi adalah telah mempunya investasi sumber daya manusia ASN yang siap dan tanggap serta gesit menghadapi insiden siber baik dari dalam atau dari luar karena sudah mempunyai rasa ikut memiliki organisasi dengan memelihara keamanan siber sehingga harapannya berdampak pada pelayanan publik yang lebih baik.

Sebagai penutup, akan menarik untuk melanjutkan studi ini dan melakukan studi serupa dengan metode statistik lainnya, seperti model regresi untuk mendapatkan pemahaman yang lebih baik tentang bagaimana pelatihan budaya keamanan siber yang merupakan bagian dari pengembangan kompetensi digital ASN. Hal ini juga dapat membantu mempersiapkan organisasi satuan kerja untuk menghadapi serangan siber dan mengembangkan program pengembangan kompetensi digital ASN yang berkelanjutan.

Ucapan Terima Kasih

Bersamaan dengan selesainya penulisan artikel ilmiah ini, saya mengucapkan terima kasih kepada penerbit jurnal, semua teman sejawat kami, dan para reviewer serta semua pihak yang telah memberikan bantuan, sumbang saran, dan kritik untuk kebaikan atas tulisan artikel ilmiah saya ini.

DAFTAR PUSTAKA

A Frost & Sullivan. (2019). *Cyberattack could cost a large healthcare organization US*. Retrieved from https://news.microsoft.com/apac/features/cybersecurity-in-asia/

ASN, U. (2014). UU ASN No. 5 tahun 2014. *Undang-Undang Republik Indonesia Nomor 5 Tahun 2014*

Tentang Aparatur Sipil Negara, 1–105. Retrieved from https://peraturan.bpk.go.id/Home/Download/27837/UU Nomor 05 Tahun 2014.pdf

Bailey, T., Kolo, B., Rajagopalan, K., & Ware, D. (2018). Insider threat: The human element of cyberrisk. *McKinsey Quarterly*, (September), 1–8.

Bansal, A., & Prakash Tripathi, J. (2017). "A Literature Review on Training Need Analysis." *IOSR Journal of Business and Management (IOSR-JBM*, *19*(10), 50–56. https://doi.org/10.9790/487X-1910065056

BSSN. (2018). *Laporan Tahunan Honeynet Project BSSN IHP 2018* (p. 40). p. 40. Retrieved from https://bssn.go.id/laporan-tahunan-honeynet-project-bssn-ihp-2018/

BSSN. (2019a). *Laporan Tahunan Honeynet Project 2019 BSSN*. *1*.

BSSN. (2019b). *Peta Okupasi Nasional Dalam Kerangka Kualifikasi Nasional Indonesia Pada Area Fungsi Keamanan Siber*. *112*.

Caballero, A. (2017). Security Education, Training, and Awareness. In *Computer and Information Security Handbook*. https://doi.org/10.1016/b978-0-12-803843-7.00033-8

Chouhan, V. S., & Srivastava, S. (2014). Understanding Competencies and Competency Modeling — A Literature Survey. *IOSR Journal of Business and Management*, *16*(1), 14–22. https://doi.org/10.9790/487x-16111422

Cooper, C., Booth, A., Varley-Campbell, J., Britten, N., & Garside, R. (2018). Defining the process to literature searching in systematic reviews: A literature review of guidance and supporting studies. *BMC Medical Research Methodology*, *18*(1), 1–14. https://doi.org/10.1186/s12874-018-0545-3

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public ' s use of cyber security best practices improve the public ' s use of cyber. *Project Report. Government Office for Science*, 1–20.

Daub, M., & Wiesinger, A. (2015). Acquiring the Capabilities You Need to Go Digital. *McKinsey&Company*, 7. Retrieved from http://www.mckinsey.com/insights/business_technology/acquiring_the_capabilities_you_need_to_go_digital

Dell Technologies. (2019). *Realizing 2030: A Divided Vision of the Future*. 1–10. Retrieved from https://www.delltechnologies.com/content/dam/delltechnologies/assets/perspectives/2030/pdf/Realizing-2030-A-Divided-Vision-of-the-Future-Summary.pdf

Digital 2020 Hootsuite 2020. (n.d.). *PENETRASI INTERNET DI INDONESI per Januari 2020*. Retrieved from https://datareportal.com/reports/digital-2020-indonesia

ENISA. (2017). Cybersecurity Culture in Organisations. In *European Union Agency for Network and Information Security (ENISA), 2017* (Vol. 31). https://doi.org/10.2824/10543

Federal Bureau of Investigation. (2019). FBI Internet Crime Report 2019. In *Federal Bureau of Investigation - Internet Crime Complaint Center*.

Ferrari, A., Editors, A. F., Punie, Y., & Bre, B. N. (2013). *DIGCOMP : A Framework for Developing and Understanding Digital Competence in Europe*. https://doi.org/10.2788/52966

Fischer, E. A., Ave, I., & Washington, S. E. (2005). *Creating a National Framework for Cybersecurity : An Analysis of*.

Gcaza, N., Von Solms, R., & Van Vuuren, J. (2015). An ontology for a national cyber-security culture environment. *Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015*, (Haisa), 1–10.

GOV_CISRT_BSSN. (2019). *Laporan GOV-CSIRT 2019*.

Hinsa Siburian, K. B. (2018). *Strategi Keamanan Siber Nasional* |. Retrieved from https://bssn.go.id/strategi-keamanan-siber-nasional/

ID-SIRTII. (2018). Indonesia Cyber Security Monitoring Report 2018. *Indonesia Security Incident Response Team On Internet Infrastructure*, p. 42. Retrieved from https://www.idsirtii.or.id/halaman/tentang/laporan-kegiatan.html

İlhan, İ. (2015). *Requirement Analysis for Cybersecurity Solutions in Organisations*.

International Telecommunication Union. (2008). OVERVIEW CYBERSECURITY. *ITU-T X.1205 Recommendation*, *1205*(Rec. ITU-T X.1205 (04/2008)), 2–3. Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I

International Telecommunication Union. (2018). Global Cybersecurity Index (GCI). In *ITU Report*. https://doi.org/10.1111/j.1745-4514.2008.00161.x

Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *8*(2), 137. https://doi.org/10.17933/mti.v8i2.108

Kautsarina, & Kusumawati, D. (2018). The Potential Adoption of the Internet of Things in Rural Areas. *Proceeding - 2018 International Conference on ICT for Rural Development: Rural Development through ICT: Concept, Design, and Implication, IC-ICTRuDEv 2018*, 124–130. https://doi.org/10.1109/ICICTR.2018.8706849

Kemenpan RB. (2018). *Pedoman Evaluasi Sistem Pemerintahan Berbasis Elektronik*. Nomor 5 Tahun 2018.

Kementerian Kominfo. (2018). *Potret Dan Pemetaan SDM TIK Dan Kehumasan ASN Provinsi 2018*.

Kementerian Kominfo. (2019). *PP Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik*.

Khan, A., & Masrek, M. N. (2017). Training needs analysis based on mismatch between the acquired and required levels of collection management skills of academic librarians. *Collection Building*, *36*(1), 20–28. https://doi.org/10.1108/CB-06-2016-0012

LAN, P. K. (2018). *Peraturan Kepala LAN No 10 Tahun 2018 Tentang Pengembangan Kompetensi PNS*.

Lettink, A., Garstang Caroline, & Ellimäki, P. (2020). HR 2025 The Future of Work, Talent & Pay. *Survey Report HR 2025*. Retrieved from https://25onhr2025.com/wp-content/uploads/2020/03/hr2025-research-report-2020.pdf

Ludwikowska, K. (2018). The effectiveness of training needs analysis and its relation to employee efficiency. *Zeszyty Naukowe Politechniki Poznańskiej Organizacja i Zarządzanie*, *77*(December 2018), 179–193. https://doi.org/10.21008/j.0239-9415.2018.077.11

M.C. Van 't Wout. (2019). *Develop and Maintain a Cybersecurity Organisational Culture Develop and Maintain a Cybersecurity Organisational Culture Author : M. C. Van ' t Wout ICCWS 2019 14th International Conference on Cyber Warfare and Security Editors : Noëlle van der Waag-Cowl* (L. L. Noëlle van der Waag-Cowling, Ed.).

Mahmud, K. T., Saira Wahid, I., & Arif, I. (2019). Impact of training needs assessment on the performance of employees: Evidence from Bangladesh. *Cogent Social Sciences*, Vol. 5. https://doi.org/10.1080/23311886.2019.1705627

Manyika, J., Lund, S., Chui, M., Bughin, J., Woetzel, J., Batra, P., & Ko, R. (2017). Jobs lost, jobs gained: Workforce transitions in a time of automation. *McKinsey Global Institute*, (December), 1–148.

McKinsey Global Institute. (2018). Public Services Government 4.0 - the public sector in the digital age. *McKinsey &Company*, (March), 1–15.

Nazli, N. N. N. N., Sipon, S., & Radzi, H. M. (2014). Analysis of Training Needs in Disaster Preparedness. *Procedia - Social and Behavioral Sciences*, *140*(June 2015), 576–580. https://doi.org/10.1016/j.sbspro.2014.04.473

Pemerintah RI.SPBE. (2018). Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. *Media Hukum*, p. 110.

Reegård, K. &, & Blackett, C. (2019). *The Concept of cybersecurity culture*. (September), 978–981. https://doi.org/10.3850/978-981-11-2724-3

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference*, (August 2015). https://doi.org/10.1109/ISSA.2014.6950492

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Spante, M., Hashemi, S. S., Lundin, M., & Algers, A. (2018). Digital competence and digital literacy in higher education research: Systematic review of concept use. *Cogent Education*, *5*(1), 1–21. https://doi.org/10.1080/2331186X.2018.1519143

Ulum, M. (2017). Cyber culture and cyber security policy of indonesia: combining cyber security civic discourse, tenets and copenhagen's securitization theory analysis. *Proceeding The 1st International*

Conference on Social Sciences University of Muhammadiyah Jakarta, Indonesia, 1–2 November 2017 Toward Community, Environmental, and Sustainable Development, (November), 1–2.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wilhelm, S., Förster, R., & Zimmermann, A. B. (2019). Implementing competence orientation: Towards constructively aligned education for sustainable development in university-level teaching-and-learning. *Sustainability (Switzerland)*, *11*(7). https://doi.org/10.3390/su11071891

Yaqoot, E. S. I., Noor, W. S. W. M., & Isa, M. F. M. (2017). Factors Influencing Training Effectiveness : Evidence from Public Sector in Bahrain. *Economica*, *13*(2), 31–44. Retrieved from http://journals.univ-danubius.ro/index.php/oeconomica/article/view/3991

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, *108*(February), 107–118. https://doi.org/10.1016/j.dss.2018.02.009

Yuanjing Wilcox. (2012). *An Initial Study to Develop Instruments and Validate The Essential Competencies for Program Evaluators*. Retrieved from https://www.rics.org/south-asia/upholding-professional-standards/standards-of-conduct/ethics/nal-standards/standards-of-conduct/ethics/