White Paper

LANSKAP KEAMANAN INFORMASI SEKTOR PUBLIK DI INDONESIA

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

PENDAHULUAN

Perkembangan teknologi informasi dalam beberapa dekade terakhir telah menghasilkan dampak positif dalam berbagai aspek kehidupan dan industri, tidak terkecuali pada sektor publik di Indonesia. Transformasi digital di sektor publik diketahui berkontribusi dalam meningkatkan kualitas layanan publik, meningkatkan transparansi, dan meningkatkan partisipasi serta kepuasan masyarakat (Mergel et al., 2019). Namun demikian, kerentanan keamanan informasi menjadi salah satu ancaman yang perlu diperhatikan untuk memastikan keberlangsungan layanan publik berbasis teknologi informasi yang diberikan. Sektor publik seperti instansi pemerintahan adalah salah satu sektor yang strategis dan banyak diincar oleh kriminalitas siber, mengingat banyaknya data dan informasi sensitif penduduk yang disimpan oleh instansi (Szczepaniuk et al., 2020).

Pada tahun 2019, berdasarkan laporan dari Badan Siber dan Sandi Negara (BSSN) Republik Indonesia, terdapat 290 juta serangan siber yang menyasar berbagai instansi/organisasi di Indonesia. Badan Reserse Kriminal Kepolisian Negara Republik Indonesia (Bareskrim POLRI) juga mencatat 4586 laporan kejahatan siber pada tahun 2019. Data tersebut mengalami kenaikan sekitar 5% dibandingkan dengan tahun sebelumnya. Kajian yang dilakukan oleh Microsoft memperkirakan kerugian finansial yang ditimbulkan oleh kejahatan siber tersebut sekitar US$ 34 miliar yang terdiri dari kerugian secara langsung seperti kerugian produktivitas, denda, dan biaya perbaikan, maupun kerugian tidak langsung yang mencakup hilangnya kepercayaan pelanggan (Frost & Sullivan, 2018).

Kerentanan keamanan informasi juga semakin meningkat sejak pandemi COVID-19. Pandemi telah memaksa masyarakat untuk banyak melakukan aktivitas seperti pembelajaran, mencari hiburan, hingga menggunakan layanan publik secara daring. Kementerian Komunikasi dan Informatika Republik Indonesia (2020) dalam laporannya menunjukkan terdapat kenaikan 40% penggunaan internet pada masa pandemi. Hal tersebut juga mendorong layanan publik untuk melakukan transformasi digital. Peningkatan lalu lintas pemakaian internet tersebut juga sejalan dengan lebih banyaknya kasus serangan siber di Indonesia (DPR RI, 2021). Beberapa kasus kebocoran data publik di beberapa instansi/organisasi juga menjadi sinyal perlunya instansi sektor publik untuk memberikan perhatian serius pada keamanan informasi.

Riset ini dilakukan untuk menelusuri kondisi terkini dari lanskap keamanan informasi pada sektor publik di Indonesia. Riset dilakukan pada rentang waktu April - Juni 2022. Riset ini memberikan gambaran mengenai pengukuran kesiapan keamanan informasi, kesiapan infrastruktur keamanan informasi dengan pendekatan 7-Layers, kesiapan manajemen insiden, manajemen kelanjutan bisnis, dan regulasi, serta tantangan yang dihadapi oleh sektor publik dalam mengimplementasikan keamanan informasi.

METODOLOGI

Studi ini mencoba untuk mengeksplorasi kondisi terkini terkait kesiapan dan hambatan manajemen keamanan informasi di instansi sektor publik di Indonesia. Mixed method digunakan untuk mengeksplorasi tema-tema tersebut. Studi ini terutama terdiri dari empat tahap: tinjauan literatur, wawancara kualitatif, survei kuantitatif, dan penulisan laporan.

Tinjauan literatur dilakukan untuk mengidentifikasi indikator kesiapan dan tantangan terkini manajemen keamanan informasi di level organisasi. Literatur yang ditelaah meliputi penelitian lima tahun terakhir terkait kesiapan dan tantangan manajemen keamanan informasi beserta standar keamanan informasi yang umum digunakan di industri. Hasil penelaahan tersebut kemudian digunakan untuk mengembangkan instrumen untuk metode pengumpulan data kualitatif dan kuantitatif

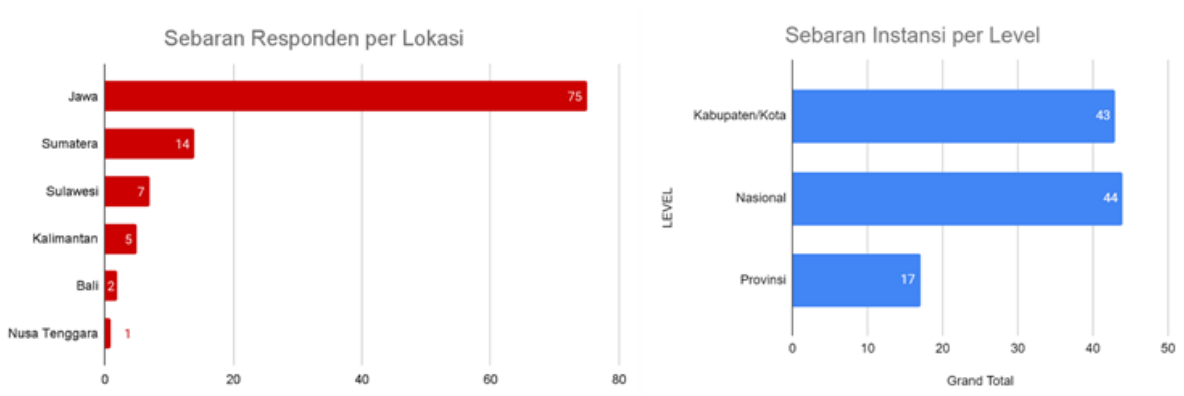
Wawancara kualitatif dilakukan untuk mendapatkan informasi yang lebih kontekstual dari pemangku kepentingan terkait. Tiga kantor pemerintah diwawancarai, mulai dari tingkat nasional dan provinsi. Wawancara secara keseluruhan dilakukan dalam waktu 60 menit. Informasi yang diperoleh kemudian dianalisis menggunakan analisis tematik untuk melengkapi indikator dari literatur. Indikator yang direvisi digunakan untuk survei kuantitatif.

Penelitian kemudian dilanjutkan ke tahap survei kuantitatif. Survei tersebut didistribusikan ke berbagai pejabat pemerintah di berbagai tingkatan, termasuk nasional (kementerian dan non-kementerian), provinsi, kota, dan kabupaten. Penelitian ini mengumpulkan beberapa data, antara lain nama institusi, lokasi (pulau), jumlah pegawai, jumlah staf TI, jumlah pengguna layanan TI, dan penilaian mandiri terkait kesiapan dan tantangan keamanan informasi berdasarkan instrumen yang dikembangkan. Instrumen kuantitatif kemudian dianalisis dengan menggunakan penghitungan perangkingan untuk masing-masing indikator yang dimuat. Hasil perhitungan tersebut kemudian diinterpretasikan menjadi rekomendasi yang relevan bagi para pemangku kepentingan dalam meningkatkan kesiapan keamanan informasi di instansi sektor publik Indonesia.

DEMOGRAFI INSTANSI RESPONDEN

Gambar 1. ***Sebaran Geografis Responden***

Studi ini melibatkan 104 instansi sektor publik pada level nasional, provinsi, dan kabupaten/kota. Data yang diperoleh mencakup instansi dari 21 provinsi di Indonesia yang tersebar di Pulau Jawa, Sumatera, Kalimantan, Sulawesi, Bali, dan Nusa Tenggara. Responden mayoritas merupakan instansi di Pulau Jawa, disusul oleh Pulau Sumatera dan Sulawesi. Ditinjau dari level instansi, sebagian besar responden merupakan anggota instansi level nasional sebanyak 44 instansi, disusul dengan level kabupaten/kota dan provinsi masing-masing sejumlah 43 dan 17 instansi.



Gambar 2. ***Rangkuman Sebaran Lokasi dan Level Instansi***

Secara umum, sebagian besar instansi yang terlibat pada studi ini memiliki ukuran organisasi di bawah 100 orang (35%). Proporsi tersebut didominasi oleh instansi level kabupaten/kota. Sementara itu, sebagian besar instansi level provinsi memiliki personel sebanyak 100 hingga 500 pegawai. Khusus untuk instansi level nasional sebagian besar beranggotakan lebih dari 1000 orang.

Ditinjau dari ukuran tim khusus yang mengelola teknologi informasi (IT), sebagian besar instansi memiliki tim IT dengan ukuran kecil, dibawah 10 orang. Lebih dari 50% instansi level kabupaten/kota dan provinsi memiliki proporsi tim IT tersebut. Instansi level nasional sebagian besar memiliki tim IT beranggotakan 11 hingga 50 personel. Hanya terdapat 6 institusi responden level nasional yang memiliki ukuran tim IT di atas 100 orang.

Studi ini juga mencatatkan bahwa sebagian besar layanan teknologi informasi yang diberikan oleh instansi sektor publik hanya melayani kurang dari 1000 pengguna aktif, khususnya layanan IT untuk instansi berskala provinsi dan kabupaten/kota. Sementara itu, mayoritas layanan IT pada instansi level nasional melayani antara 1000 hingga 10.000 pengguna aktif. Tercatat hanya 7% instansi responden yang melayani di atas 1 juta pengguna.

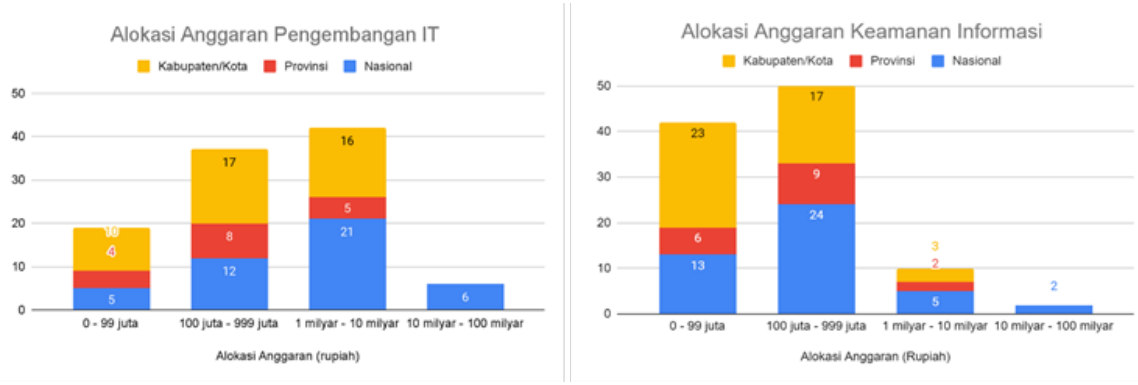
Studi ini juga mengidentifikasi proporsi anggaran yang dikeluarkan oleh masing-masing instansi responden untuk pengembangan dan pengelolaan teknologi informasi, termasuk alokasi khusus untuk keamanan siber. Dari 104 instansi responden yang terlibat, sebanyak 40% instansi menganggarkan sekitar satu hingga sepuluh milyar setiap tahun untuk pengembangan teknologi informasi, khususnya instansi level nasional. Sementara itu, 36% instansi mengalokasikan anggaran antara 100 juta hingga satu milyar per tahunnya. Persentase tersebut didominasi oleh instansi level provinsi dan kabupaten/kota. Hanya terdapat lima instansi level nasional pada studi ini yang mengalokasikan anggaran di atas 10 milyar untuk pengembangan dan pengelolaan layanan teknologi informasi.

Lebih khusus pada anggaran keamanan siber, sebagian besar responden mengalokasikan anggaran ratusan juta rupiah setiap tahun untuk fokus pada keamanan siber. Proporsi tersebut didominasi oleh instansi level nasional dan provinsi. Sementara itu, instansi level kabupaten memiliki alokasi anggaran di bawah 100 juta untuk kegiatan keamanan siber. Sebagai outlier, hanya terdapat dua instansi level nasional yang mengalokasikan anggaran di atas 10 milyar untuk keamanan siber.

Gambar 3. ***Rangkuman Ukuran Instansi dan Layanan IT Responden***

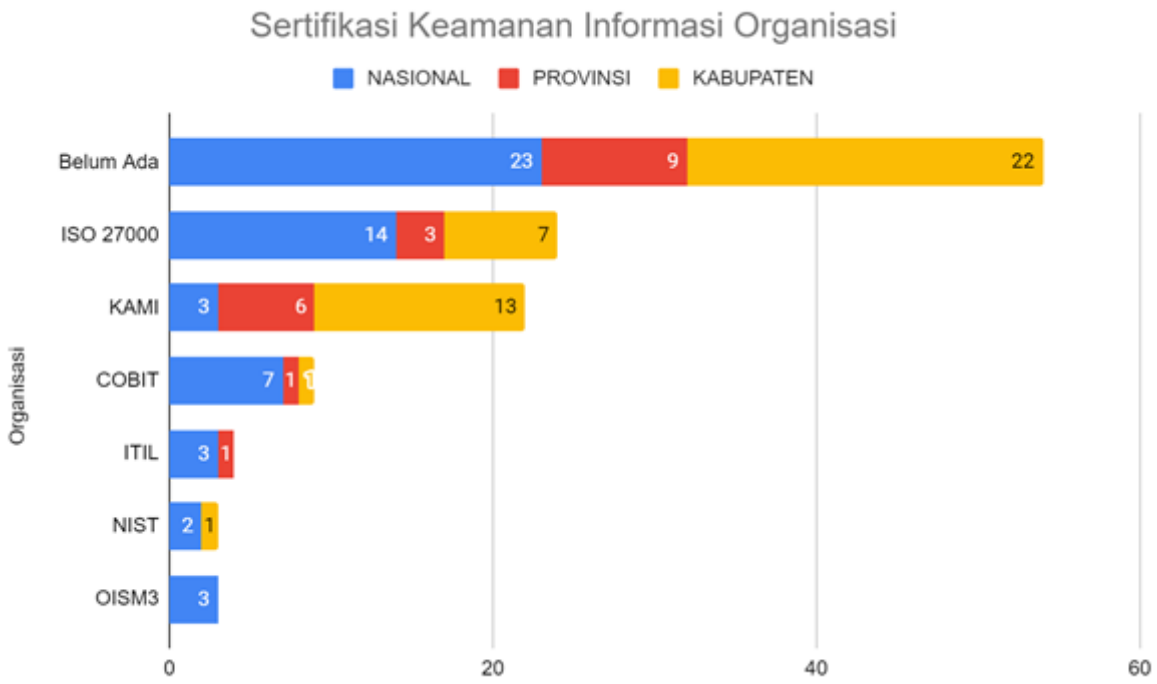
Studi ini juga mengidentifikasi proporsi anggaran yang dikeluarkan oleh masing-masing instansi responden untuk pengembangan dan pengelolaan teknologi informasi, termasuk alokasi khusus untuk keamanan informasi. Dari 104 instansi responden yang terlibat, sebanyak 40% instansi menganggarkan sekitar satu hingga sepuluh milyar setiap tahun untuk pengembangan teknologi informasi, khususnya instansi level nasional. Sementara itu, 36% instansi mengalokasikan anggaran antara 100 juta hingga satu milyar per tahunnya. Persentase tersebut didominasi oleh instansi level provinsi dan kabupaten/kota. Hanya terdapat lima instansi level nasional pada studi ini yang mengalokasikan anggaran di atas 10 milyar untuk pengembangan dan pengelolaan layanan teknologi informasi.

Lebih khusus pada anggaran keamanan informasi, sebagian besar responden mengalokasikan anggaran ratusan juta rupiah setiap tahun untuk fokus pada keamanan informasi. Proporsi tersebut didominasi oleh instansi level nasional dan provinsi. Sementara itu, instansi level kabupaten memiliki alokasi anggaran di bawah 100 juta untuk kegiatan keamanan informasi. Sebagai outlier, hanya terdapat dua instansi level nasional yang mengalokasikan anggaran di atas 10 milyar untuk keamanan informasi.



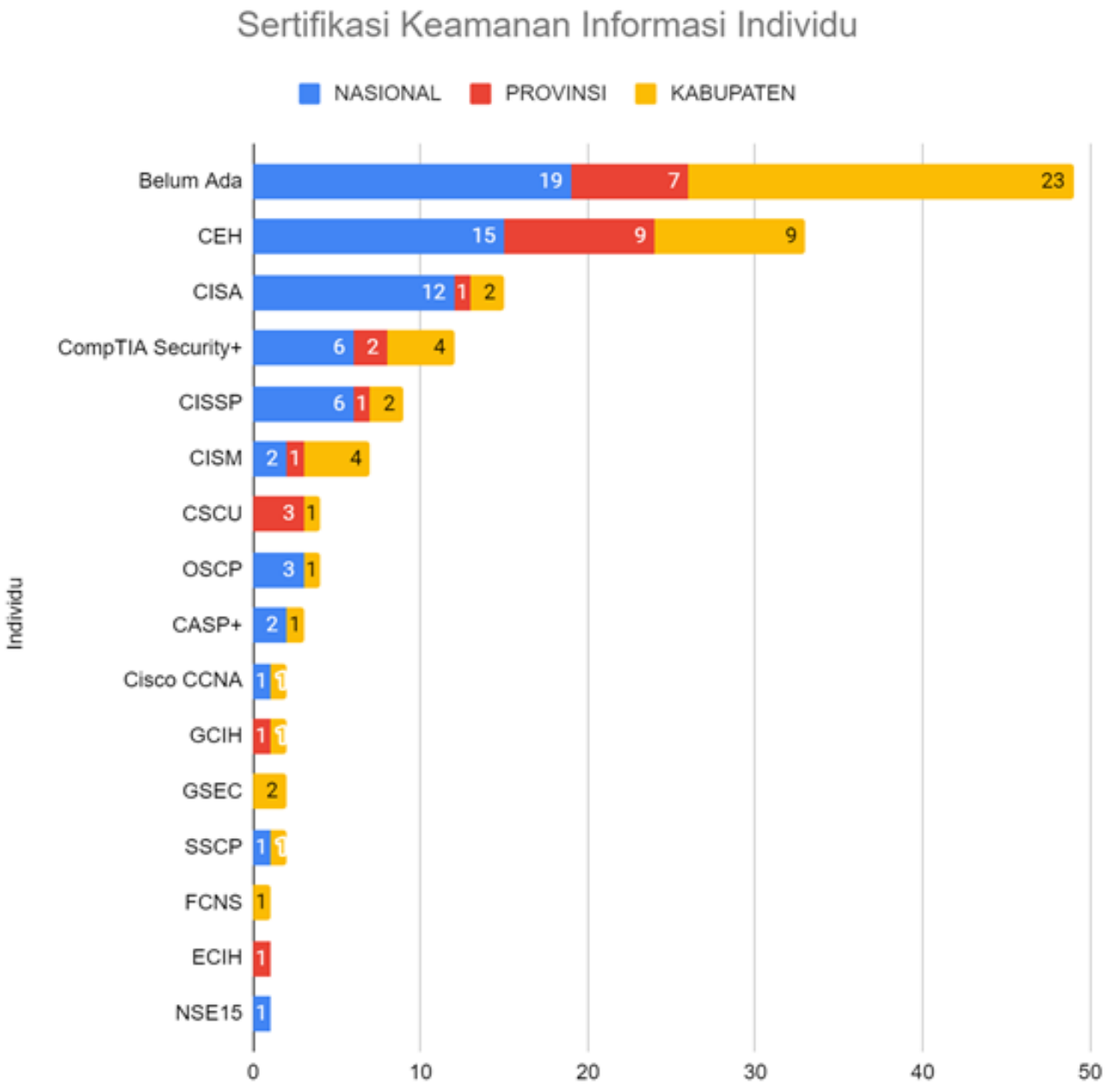
Gambar 4. ***Rangkuman Anggaran IT dan Keamanan Informasi***

Sebagai salah satu indikator kesiapan keamanan informasi di sektor publik, studi ini juga melakukan survei sertifikasi yang dimiliki oleh instansi responden. Sertifikasi yang diidentifikasi pada studi ini meliputi sertifikasi/standar untuk organisasi, maupun sertifikasi individu personel yang ada pada instansi. Secara umum, studi ini menemukan bahwa lebih dari 50% instansi di level nasional, provinsi, dan individu belum memiliki sertifikasi atau mengikuti standar keamanan informasi organisasi. Sertifikasi/standar yang paling banyak diikuti oleh instansi sektor publik pada studi ini adalah standar ISO 27000 beserta turunannya. Kepatuhan pada standar ISO 27000 didominasi oleh instansi level nasional. Sementara itu, indeks keamanan informasi (KAMI) yang disusun oleh pemerintah Republik Indonesia, menjadi instrumen evaluasi tingkat kematangan keamanan informasi terbanyak kedua yang diadopsi oleh 31% instansi sektor publik di Indonesia pada studi ini. Persentase tersebut didominasi oleh instansi level kabupaten dan provinsi, berkebalikan dengan proporsi pada sertifikasi ISO 27000 yang didominasi oleh instansi level nasional. Indeks KAMI sendiri mengadopsi sebagian standar yang ada pada ISO 27000. Indeks pengukuran tersebut hadir sebagai alat bantu bagi instansi untuk mengukur tingkat keamanan informasi sebelum melakukan sertifikasi ISO 27000 secara penuh. Beberapa sertifikasi yang juga diadopsi oleh sebagian kecil instansi sektor publik meliputi: Control Objectives for Information and Related Technologies (COBIT), The Information Technology Infrastructure Library (ITIL), NIST Cybersecurity Framework, dan Open Information Security Management Maturity Model (OISM3).



Gambar 5. ***Proporsi Sertifikasi Organisasi Responden***

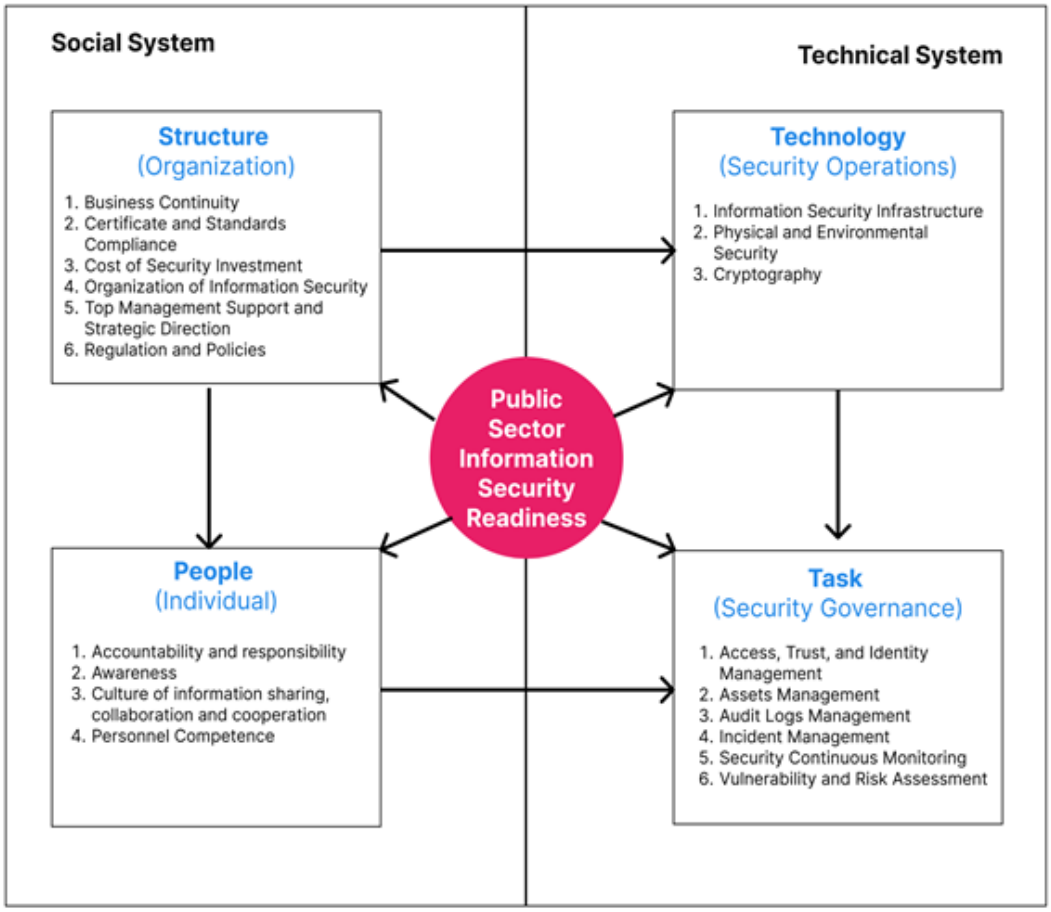
Sebanyak 49 dari 104 instansi sektor publik yang terlibat di studi ini belum memiliki personel dengan sertifikasi individu untuk keamanan informasi, Studi ini mengidentifikasi setidaknya 16 sertifikasi keamanan informasi individu yang dimiliki oleh personel dari 55 instansi pada studi ini. Lima sertifikasi yang paling banyak dimiliki oleh instansi sektor publik berturut-turut di antaranya ***Certified Ethical Hacker*** (CEH), ***Certified Information Systems Auditor*** (CISA), ***Comptia Security+, Certified Information Systems Security Professional*** (CISSP), dan ***Certified Information Security Manager*** (CISM). Terdapat 33 instansi yang memiliki tim yang bersertifikasi CEH. CISA dimiliki oleh 15 instansi pada studi ini dan juga didominasi oleh instansi level nasional. Sementara itu, sertifikasi CompTIA Security+ dimiliki oleh 12 instansi, CISSP 9 instansi, dan CISM sebanyak 7 instansi. Di antara kelima sertifikasi tersebut, secara proporsi seluruhnya didominasi oleh instansi level nasional. Hal tersebut mengindikasikan bahwa kesiapan sumber daya manusia (SDM) di instansi level nasional relatif lebih baik dibandingkan SDM di level provinsi maupun kabupaten/kota. Sertifikasi-sertifikasi lain yang diidentifikasi pada studi ini meliputi, ***Certified Secure Computer User*** (CSCU), ***Offensive Security Certified Professional*** (OSCP), ***CompTIA Advanced Security Practitioner*** (CASP+), ***Cisco CCNA, GIAC Certified Incident Handler*** (GCIH), ***GIAC Security Essentials Certification*** (GSEC), ***Systems Security Certified Practitioner*** (SSCP), dan ***Foresec Certified in Networking Security*** (FCNS).



Gambar 6. ***Proporsi Sertifikasi Individu***

PENGUKURAN KESIAPAN KEAMANAN INFORMASI

Studi ini mengadopsi konsep ***socio-technical system*** (STS) sebagai kerangka kerja (***framework***) penilaian kesiapan keamanan Informasi secara holistik. STS merupakan konsep yang memodelkan interaksi antara ***social system*** (manusia) dan ***technical system*** (Baxter & Sommerville, 2011). Konsep tersebut diadopsi pada studi ini dengan alasan keamanan Informasi tidak hanya berkaitan dengan aspek teknis, melainkan juga melibatkan manusia atau sistem sosial sebagai pengguna teknologi informasi. Social system pada studi ini terdiri dari elemen ***people*** yang berisi faktor terkait individu pada organisasi dan structure yang mencakup faktor-faktor organisasional dan manajerial. Sementara itu, technical system mencakup elemen ***technology*** yang berisi faktor-faktor teknis terkait teknologi keamanan Informasi dan elemen ***structure*** yang mencakup kegiatan-kegiatan tata kelola keamanan Informasi. Gambaran keseluruhan dari ***framework*** pada studi ini dapat dilihat pada Gambar berikut.



Gambar 7. ***Framework Kesiapan Keamanan Informasi***

Framework yang digunakan pada studi ini terdiri dari 19 indikator kesiapan keamanan Informasi yang dibagi menjadi empat elemen berdasarkan kerangka STS. Indikator-indikator tersebut diadopsi dari penelitian-penelitian sebelumnya dan juga standar keamanan Informasi yang sudah ada. Pada elemen ***structure*** terdapat enam indikator untuk

mengukur kesiapan keamanan Informasi suatu organisasi. Keenam indikator tersebut meliputi kesiapan perencanaan keberlanjutan bisnis (***business continuity***), pemenuhan standar dan sertifikasi keamanan Informasi, alokasi anggaran investasi keamanan informasi, pengorganisasian keamanan informasi, dukungan pimpinan, dan keberadaan regulasi dan kebijakan. Elemen people terdiri dari empat indikator, yakni akuntabilitas dan tanggung jawab individu, kesadaran mengenai pentingnya keamanan informasi, kultur berbagi informasi dan kolaborasi terkait pengamanan informasi, dan kompetensi individu terkait keamanan informasi. Sementara itu, elemen task terdiri dari lima kegiatan tata kelola keamanan informasi, di antaranya ***access, trust, and identity management, assets management, audit logs management, incident management, security continuous monitoring***, dan ***vulnerability and risk assessment***. Elemen terakhir yang dievaluasi pada studi ini, yakni ***technology*** terdiri dari tiga indikator di antaranya kriptografi, keamanan fisik dan lingkungan, dan infrastruktur teknologi keamanan informasi.

Tabel 1. ***Peringkat Aspek Kesiapan Keamanan Informasi***

INDIKATOR	ELEMENT	MEAN	STDEV	RANK
Accountability and responsibility	People	3.26	0.76	1
Awareness	People	2.94	0.86	2
Culture of information sharing, collaboration and cooperation	People	2.94	0.90	3
Top Management Support and Strategic Direction	Structure	2.94	0.94	4
Access, Trust, and Identity Management	Task	2.73	0.94	5
Regulation and Policies	Structure	2.65	0.88	6
Physical and Environmental Security	Technology	2.65	0.90	6
Audit Logs Management	Task	2.62	0.98	8
Incident Management	Task	2.59	0.98	9
Assets Management	Task	2.56	0.92	10
Information Security Infrastructure	Technology	2.51	0.95	11
Organization of Information Security	Structure	2.48	1.02	12
Security Continuous Monitoring	Task	2.47	0.99	13
Vulnerability and Risk Assessment	Task	2.47	0.93	13
Business Continuity	Structure	2.46	0.94	15
Cryptography	Technology	2.40	0.96	16
Cost of Security Investment	Structure	2.32	0.91	17
Personnel Competence	People	2.17	0.99	18
Certificate and Standards Compliance	Structure	2.12	1.03	19

Berdasarkan hasil survei yang dirangkum pada Tabel 1, dapat diketahui bahwa lima indikator yang secara umum memiliki tingkat kesiapan lebih baik adalah akuntabilitas dan tanggungjawab individu, kesadaran individu mengenai pentingnya keamanan informasi, kultur berbagi informasi dan kolaborasi terkait pengamanan informasi, dukungan pimpinan, dan ***access, trust, and identity management***. Lima indikator tersebut didominasi oleh elemen ***people***, atau kondisi individu di dalam organisasi. Sementara itu, lima indikator dengan kesiapan paling rendah meliputi ***business continuity***, kriptografi, alokasi anggaran keamanan informasi, kompetensi individu terkait keamanan informasi, dan pemenuhan standar dan sertifikasi keamanan informasi. Elemen ***structure*** atau organisasi mendominasi daftar lima indikator dengan kesiapan terendah tersebut.

Pembahasan Aspek *People*

Salah satu temuan menarik dalam studi ini ada pada elemen ***people*** atau individu pegawai di organisasi. Meskipun tiga indikator mendominasi lima besar indikator kesiapan keamanan informasi dengan rerata tertinggi, satu indikator justru menjadi yang terendah kedua di antara sembilan belas indikator yang ada. Hasil tersebut menunjukkan bahwa meskipun studi ini mencatat bahwa tingkat tanggungjawab dan kesadaran individu mengenai pentingnya keamanan informasi tergolong tinggi, tingkat kompetensi yang dimiliki oleh aparat pada instansi sektor publik di Indonesia masih perlu peningkatan signifikan. Hal tersebut juga didukung oleh data terkait sertifikasi individu pada studi ini yang menunjukkan sebagian besar instansi sektor publik masih belum memiliki aparat yang bersertifikasi keamanan informasi. Dengan demikian, program sertifikasi keamanan informasi individu perlu menjadi prioritas bagi instansi sektor publik untuk mendapatkan aparat dengan kompetensi yang memadai dalam mengelola keamanan informasi.

Berdasarkan ISO 27002 tentang Panduan Praktik kendali Keamanan Informasi, empat indikator pada elemen ***people*** berkaitan dengan kontrol keamanan pada aspek ***Human Resources Security***. Pada aspek ini, perlu dipastikan bahwa karyawan, kontraktor dan pengguna pihak ketiga memahami tanggung jawab sesuai dengan peran mereka, dengan tujuan untuk mengurangi risiko pencurian, penipuan atau penyalahgunaan sistem dan informasi. Secara ideal, aspek ini mencakup kondisi SDM pada waktu sebelum, saat, dan setelah dipekerjakan. Semua calon karyawan/kontraktor harus melalui penyaringan dan pemeriksaan yang sesuai dengan hukum, peraturan, etika, kebutuhan bisnis, klasifikasi informasi yang akan diakses, risiko, serta harus melakukan perjanjian kontrak untuk bertanggung jawab terhadap keamanan informasi organisasi.

Selama karyawan/kontraktor bekerja, mereka wajib menerapkan keamanan informasi sesuai kebijakan dan prosedur organisasi. Semua karyawan yang relevan harus mendapatkan pendidikan kesadaran keamanan informasi, dan terdapat sanksi secara formal apabila terjadi pelanggaran terhadap keamanan informasi. Jika terdapat penghentian atau perubahan karyawan, tanggung jawab dan tugas keamanan informasi tetap berlaku dan harus didefinisikan dalam kebijakan. Tanggung jawab dan tugas yang masih berlaku setelah pemutusan hubungan kerja, harus terkandung dalam syarat dan kondisi kerja karyawan atau kontraktor. Sementara itu, hubungan dengan pemasok (vendor) harus diatur untuk memastikan perlindungan

terhadap aset informasi organisasi. Aspek ini terdiri dari serangkaian persyaratan keamanan informasi untuk mengurangi risiko terkait akses vendor ke aset organisasi.

Pembahasan Aspek *Structure*

Pada elemen ***structure*** atau terkait kesiapan organisasi, studi ini menemukan bahwa elemen tersebut mendominasi jajaran lima besar indikator dengan rerata nilai terendah. Satu-satunya indikator yang berada pada lima besar nilai rataan tertinggi adalah dukungan pimpinan. Indikator terkait regulasi juga menduduki peringkat keenam dalam studi ini. Temuan tersebut menunjukkan bahwa aspek regulasi dan dukungan pimpinan sudah cukup untuk mendukung program keamanan informasi saat ini. Pemerintah Republik Indonesia sendiri juga telah menerbitkan beberapa regulasi dan kebijakan yang mendukung keamanan informasi, meskipun masih belum mencakup keseluruhan aspek keamanan informasi. Keberadaan regulasi formal tersebut membuat instansi sektor publik memiliki panduan formal mengenai proses pengamanan informasi dan sekaligus menjadi pendorong bagi pimpinan untuk memberikan dukungan materil maupun non-materil terhadap upaya pengelolaan keamanan informasi.

Namun demikian, instansi sektor publik perlu menaruh perhatian lebih pada aspek keberlanjutan bisnis (***business continuity***), porsi anggaran keamanan informasi, dan pemenuhan standar/sertifikasi keamanan informasi bagi organisasi. Ketiga aspek tersebut menduduki peringkat lima besar terendah pada studi ini. Aspek ***business continuity*** perlu diperhatikan sebagai langkah persiapan menghadapi disrupsi yang mungkin akan mengganggu sistem layanan teknologi informasi yang disediakan. Alokasi anggaran juga perlu menjadi perhatian untuk meningkatkan kehandalan keamanan informasi. Studi ini mencatatkan bahwa sebagian besar instansi publik, khususnya di level kabupaten/kota menganggarkan kurang dari 100 juta rupiah untuk investasi keamanan informasi. Proporsi tersebut termasuk kecil jika dibandingkan dengan jumlah anggaran pengembangan teknologi informasi yang sebagian besar berkisar antara satu hingga sepuluh milyar rupiah. Proporsi investasi keamanan informasi perlu ditingkatkan oleh instansi sektor publik untuk memberikan pengamanan lebih terhadap sistem layanan IT yang dijalankan. Pemenuhan standar dan sertifikasi keamanan informasi organisasi juga perlu ditingkatkan. Lebih dari 50% instansi sektor publik yang berpartisipasi pada studi ini belum memiliki sertifikasi keamanan informasi. Hanya terdapat 24 dari 104 instansi yang telah memenuhi standar ISO 27000.

Pihak manajemen perlu memperhatikan kesesuaian ***Security Policy*** (Kebijakan Keamanan) dengan persyaratan bisnis organisasi dan peraturan yang relevan. Ketersediaan kebijakan keamanan informasi merupakan hal yang penting, namun peninjauan ulang kebijakan juga perlu diperhatikan. Sekumpulan kebijakan keamanan informasi harus terdefinisi, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak-pihak eksternal terkait. Kebijakan keamanan informasi harus disusun sejalan dengan strategi bisnis, peraturan perundangan, kondisi terkini, dan proyeksi ancaman terhadap keamanan informasi. Jika salah satu kebijakan keamanan informasi didistribusikan ke luar organisasi, perlu dipastikan agar tidak menyingkap informasi rahasia organisasi. Peninjauan ulang kebijakan juga diperlukan pada interval yang telah direncanakan, untuk memastikan kesesuaian, kecukupan, dan efektivitas kebijakan.

Dalam mengelola keamanan informasi pada organisasi, perlu diperhatikan pemrosesan informasi pada internal dan eksternal organisasi. Pada internal organisasi, perlu dibentuk kerangka kerja pengelolaan keamanan informasi yang mengendalikan pelaksanaan dan operasi keamanan informasi. Lalu pada eksternal organisasi, perlu diperhatikan kebijakan tentang penggunaan ***mobile devices*** dan ***teleworking*** untuk mengelola kemungkinan risiko yang timbul serta untuk melindungi informasi yang diakses maupun diproses dari dan keluar organisasi. Organisasi yang memperbolehkan kegiatan teleworking harus mengeluarkan kebijakan yang mendefinisikan kondisi dan pembatasan dalam menggunakan ***teleworking***. Dalam memenuhi kebutuhan Sistem Informasi (***acquisition, development and maintenance***), perlu diperhatikan tiga hal yaitu Persyaratan Keamanan Sistem Informasi, Keamanan dalam Proses Pengembangan, serta Data Uji. Persyaratan Keamanan Sistem Informasi terdiri dari:

1. Analisis dan spesifikasi persyaratan keamanan informasi yang dilakukan berdasarkan manajemen risiko (dapat mengacu pada ISO/IEC 27005).
2. Pengamanan layanan aplikasi pada jaringan publik agar terhindar dari aktivitas penipuan, ***contract dispute*** dan kegiatan pengungkapan yang tidak sah serta modifikasi.
3. Perlindungan transaksi layanan aplikasi untuk mencegah transmisi tak lengkap, ***mis-routing, unauthorized message alteration***, pengungkapan yang tidak sah, dan duplikasi pesan.

Keamanan dalam proses pengembangan sistem informasi diperlukan untuk memastikan bahwa keamanan informasi dirancang dan diimplementasikan dalam ***life cycle*** sistem informasi. Data yang dipergunakan selama uji coba aplikasi juga perlu diperhatikan, misal menghindari penggunaan data pribadi dalam data uji.

Selanjutnya aspek ***Business Continuity Management*** diperlukan untuk menanggulangi proses bisnis dari efek kegagalan sistem informasi atau bencana serta untuk menjamin tidak terjadi kegagalan kembali. Suatu proses manajemen keberlangsungan bisnis harus dilaksanakan untuk meminimalisir dampak pada organisasi dan mempercepat pemulihan dari hilangnya aset informasi. Terdapat dua cakupan pada aspek ini, yaitu keberlangsungan keamanan informasi untuk memastikan kontinuitas keamanan informasi harus tertanam dalam ***business continuity management systems*** dan redundansi untuk memastikan ketersediaan sistem pengolahan informasi.

Organisasi juga perlu memperhatikan aspek ***compliance*** untuk menghindari pelanggaran terhadap hukum, kewajiban hukum, peraturan atau kontrak, dan setiap persyaratan keamanan. Compliance meliputi kesesuaian dengan persyaratan hukum, kontraktual dan tinjauan keamanan informasi. Kesesuaian dengan persyaratan hukum dan kontraktual terdiri dari: 1) Identifikasi persyaratan perundang-undangan dan kontraktual yang berlaku; 2) Hak atas kekayaan intelektual; 3) Proteksi rekaman; 4) Privasi dan proteksi informasi identitas pribadi; dan 5) Regulasi pengendalian kriptografi. Sementara itu, tinjauan keamanan informasi terdiri dari: 1) Tinjauan Independen Keamanan Informasi; 2) Kesesuaian Dengan Kebijakan dan Standar Keamanan; dan 3) Tinjauan Kesesuaian Teknis.

Pembahasan Aspek *Task*

Ditinjau dari elemen ***task***, di antara enam kegiatan tata kelola keamanan informasi, dapat diketahui bahwa ***access, trust, and identity*** management menjadi indikator dengan nilai kesiapan tertinggi, disusul oleh ***audit logs management, incident management,*** dan ***assets management.*** Keempat indikator/kegiatan tersebut menempati sepuluh besar indikator dengan nilai kesiapan tertinggi. Dua indikator dengan nilai rataan terendah pada elemen ini adalah ***security continuous monitoring*** dan ***vulnerability and risk assessment.*** Temuan tersebut dapat menjadi acuan baik bagi instansi sektor publik untuk memfokuskan perhatian peningkatannya sekaligus bagi penyedia jasa layanan keamanan informasi untuk dapat memfokuskan target pemasaran layanannya. Teknologi seperti ***extended detection and response*** (XDR) dapat menjadi solusi yang diprioritaskan untuk dapat diadopsi instansi sektor publik. Hal tersebut berguna untuk membantu pihak instansi memastikan pengawasan sistem secara keseluruhan sehingga dapat membantu proses penanganan insiden keamanan informasi. XDR memungkinkan organisasi untuk melakukan pengawasan secara real-time terkait berbagai aktivitas mencurigakan pada beberapa titik kerentanan seperti ***cloud, server, endpoint***, dan jaringan. Sebagai langkah mitigasi, instansi sektor publik juga perlu berfokus pada deteksi kerentanan dan risiko keamanan informasi. Langkah konkret untuk hal tersebut dapat berupa adopsi paradigma Security Development Operations (SecDevOps) untuk mendeteksi kerentanan secara dini dari tahap pengembangan sistem. Salah satu solusi yang dapat diadopsi adalah ***Static Application Security Testing*** (SAST), untuk mendeteksi kerentanan keamanan sejak dalam fase penulisan kode.

Manajemen aset merupakan aspek yang diperlukan untuk memberikan perlindungan pada aset organisasi. Semua aset harus dipertanggungjawabkan dan terdapat pemilik yang dapat diidentifikasi. Kontrol aset harus didefinisikan ketika proses inventarisasi, penggunaan aset, dan pengembalian aset. Selanjutnya, aset juga perlu untuk diklasifikasikan untuk memastikan bahwa informasi yang terdapat pada aset tersebut mendapatkan tingkat perlindungan yang layak berdasarkan kepentingan informasi aset tersebut dalam organisasi. Selain itu, penggunaan media yang digunakan sebagai perantara aset juga perlu untuk dikontrol demi mencegah terjadinya penyingkapan, modifikasi, pemindahan atau penghancuran tidak sah terhadap informasi aset yang tersimpan.

Organisasi perlu melakukan manajemen operasi dan komunikasi untuk memastikan operasi yang tepat, fasilitas pengolahan informasi yang aman, serta menjamin perlindungan informasi dalam jaringan. Penetapan tanggung jawab dan prosedur untuk pengelolaan dan pengoperasian fasilitas pengolahan informasi harus ditetapkan. Hal tersebut dapat dilakukan melalui proses:

1. Menentukan prosedur dan tanggung jawab operasional (dokumentasi prosedur, manajemen perubahan dan kapasitas, pemisahan lingkungan pengembangan, pengujian, dan operasional).
2. Perlindungan dari ***malware*** (proses deteksi, pencegahan, dan pemulihan terhadap ***malware***).
3. Melakukan pencadangan data (***backup***).
4. Pencatatan (***logging***) dan pemantauan.
5. Kendali perangkat lunak operasional.
6. Manajemen kerentanan teknis (melakukan pembatasan terhadap instalasi perangkat lunak).
7. Pertimbangan audit sistem informasi (persyaratan dan aktivitas audit).

Kontrol terhadap akses (access control) ke informasi juga merupakan hal yang penting. Akses terhadap informasi dan pengolahan informasi harus dikontrol atas dasar proses bisnis dan persyaratan keamanan. Aturan access control harus mempertimbangkan kebijakan penyebaran informasi dan otorisasi. Berikut beberapa aspek access control yang perlu diatur:

1. Persyaratan bisnis untuk ***access control***

   Persyaratan bisnis yang dimaksud adalah kebijakan ***access control*** yang dilakukan harus sesuai persyaratan bisnis dan diberlakukan pembatasan akses ke jaringan dan layanan pada organisasi. Pembatasan tersebut dapat dilakukan dengan memberikan akses ke jaringan dan layanan hanya kepada pihak yang berwenang.

2. Manajemen akses pengguna

   Pengaturan yang dilakukan mencakup proses registrasi atau pembatalan registrasi, penyediaan akses, manajemen hak akses istimewa, manajemen informasi otentikasi rahasia, ***review*** hak akses, dan penghapusan atau penyesuaian hak akses pengguna.

3. Tanggung jawab pengguna

   Pengguna diwajibkan untuk mengikuti aturan organisasi dalam hal penggunaan informasi otentikasi rahasia.

4. Kendali akses sistem dan aplikasi

   Kendali dilakukan dengan membatasi akses ke informasi, menetapkan prosedur ***login*** yang aman, menerapkan sistem manajemen kata kunci (***password***), dan pembatasan akses ke kode sumber.

Aspek manajemen insiden merupakan hal yang tidak kalah penting, aspek ini berguna untuk memastikan kejadian keamanan informasi dan kerentanan yang terkait dengan sistem informasi dapat dikomunikasikan sehingga membantu menentukan tindakan korektif yang akan diambil secara tepat waktu. Semua karyawan, kontraktor dan pengguna pihak ketiga harus diberikan pemahaman akan prosedur pelaporan insiden dan kerentanan yang mungkin berdampak pada keamanan aset organisasi. Mereka harus melaporkan setiap kejadian keamanan informasi dan kerentanan secepat mungkin ke kontak yang telah ditentukan.

Pembahasan Aspek *Technology*

Pada elemen ***technology***, perhatian ekstra perlu diberikan pada aspek kriptografi. Indikator tersebut merupakan salah satu dari lima indikator dengan nilai terbawah pada studi ini. Penyedia layanan keamanan informasi dapat membantu instansi sektor publik di Indonesia untuk dapat menerapkan mekanisme kriptografi untuk mengamankan layanan IT baik dari sisi aplikasi, data, maupun jaringan. Aspek infrastruktur yang meliputi ***hardware*** dan ***software*** untuk keamanan informasi juga perlu peningkatan. Studi ini melakukan penilaian lebih detail terkait infrastruktur bagian apa saja yang perlu mendapatkan perhatian lebih pada bagian terpisah. Sementara itu, indikator dengan nilai kesiapan terbaik dalam elemen ***technology*** adalah pengaman fisik dan lingkungan. Hasil survei studi ini menunjukkan bahwa secara umum instansi sektor publik di Indonesia sudah memiliki mekanisme pengamanan untuk aset fisik yang berkaitan dengan sistem layanan IT.

Keamanan fisik dan lingkungan perlu diperhatikan untuk mencegah akses fisik yang tidak sah, kerusakan, dan interferensi ke lokasi dan informasi organisasi. Fasilitas pengolahan informasi sensitif harus ditempatkan di daerah yang aman, dilindungi oleh perimeter keamanan, dengan keamanan yang sesuai dan terkontrol. Informasi harus secara fisik dilindungi dari akses yang tidak sah, kerusakan, dan interferensi. Perlindungan yang diberikan harus sepadan dengan risiko yang teridentifikasi.

Selanjutnya, perlu diperhatikan aspek kriptografi pada elemen technology. Kriptografi terdiri dari dua cakupan, yaitu kebijakan terhadap penggunaan kriptografi dan manajemen kunci kriptografi. Kebijakan dalam pengambilan keputusan terkait solusi kriptografi harus dilihat sebagai bagian dari proses penilaian risiko dan pemilihan kontrol. Penilaian ini kemudian dapat digunakan untuk menentukan apakah kontrol kriptografi yang digunakan sudah sesuai dengan kebutuhan proses bisnis. Kontrol kriptografi dapat digunakan untuk mencapai tujuan keamanan informasi seperti kerahasiaan, integritas, ***non repudiation***, dan autentikasi. Selanjutnya manajemen kunci kriptografi dilakukan dengan mengikuti siklus ***generating, storing, archiving, retrieving, distributing, retiring, dan destroying keys.*** Dalam manajemen kunci yang tepat, dibutuhkan proses yang aman untuk seluruh siklus yang disebutkan, karena manajemen kunci yang baik akan menentukan efektivitas dari penerapan teknik kriptografi.

Aspek yang tidak kalah penting adalah Keamanan komunikasi. Aspek ini mengatur tentang Manajemen Keamanan Jaringan dan Perpindahan Informasi.

Manajemen keamanan jaringan memperhatikan beberapa aspek, yaitu:

1. Pengendalian jaringan

   Jaringan harus dikelola dan dikendalikan untuk melindungi informasi yang ada pada sistem dan aplikasi.

2. Keamanan layanan jaringan

   Diperlukan kebijakan berisi mekanisme keamanan, tingkat layanan dan persyaratan pengelolaan semua layanan jaringan.

3. Pemisahan dalam jaringan

   Salah satu metode pengelolaan keamanan jaringan untuk jaringan yang besar adalah membaginya menjadi domain jaringan yang terpisah.

Selanjutnya Perpindahan Informasi memperhatikan empat aspek, yaitu:

1. Prosedur dan kebijakan perpindahan informasi

   Kebijakan dan prosedur terkait perpindahan informasi harus melindungi informasi yang ditransfer melalui semua jenis fasilitas komunikasi.

2. Persetujuan perpindahan informasi

   Perjanjian terkait perpindahan informasi harus menjamin transfer informasi yang aman antara organisasi dan pihak luar.

3. Pesan elektronik

   Informasi yang melibatkan penggunaan pesan elektronik harus dilindungi secara tepat.

4. Non-disclosure agreement

   Persyaratan pada non-disclosure agreements harus mencerminkan kebutuhan organisasi dalam melindungi informasi, lalu direviu secara berkala dan didokumentasikan.

KESIAPAN INFRASTRUKTUR KEAMANAN INFORMASI BERDASARKAN PENDEKATAN 7 LAYER

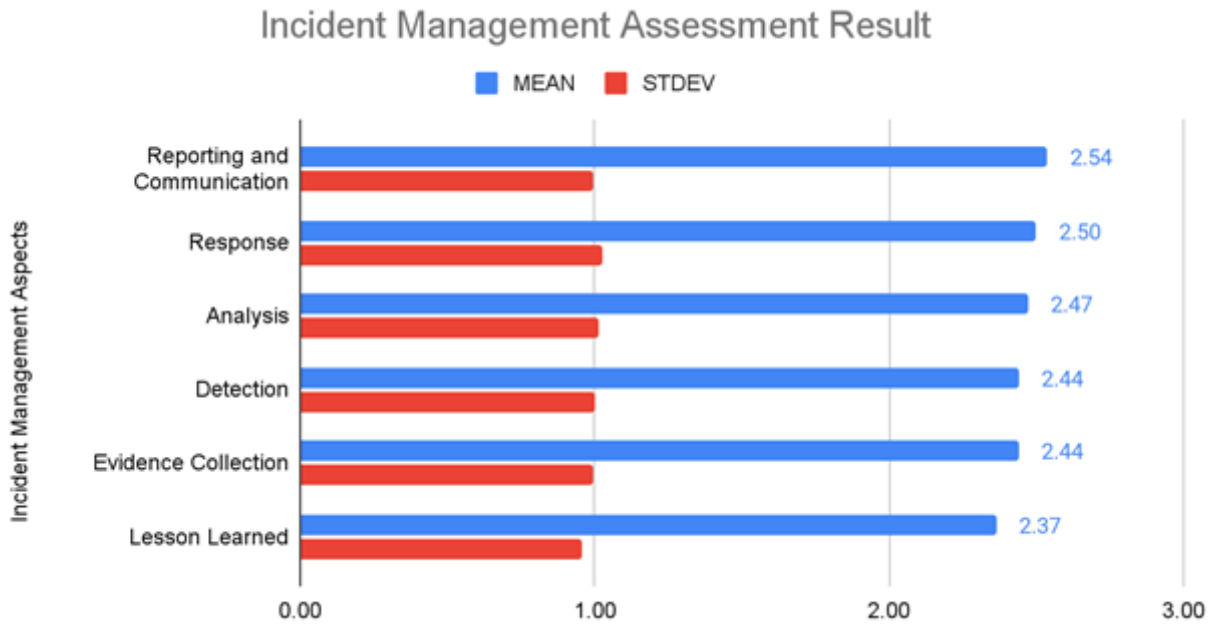
Studi ini juga menganalisis kesiapan infrastruktur keamanan siber berdasarkan pendekatan tujuh lapis keamanan informasi. Tujuh lapis keamanan informasi tersebut meliputi ***human layer, perimeter layer, network layer, endpoint layer, application layer, data layer***, dan ***mission critical assets.*** Human layer berkaitan dengan mekanisme pengamanan manusia dalam organisasi yang juga merupakan salah satu kerentanan dalam keamanan informasi. ***Perimeter layer*** mencakup pengamanan infrastruktur fisik maupun digital yang menjadi lapisan terluar untuk mengakses data, aplikasi, maupun jaringan organisasi. ***Network layer*** berfokus pada pengamanan jaringan dan memastikan hak akses jaringan hanya dimiliki oleh pengguna yang telah ditentukan. ***Endpoint security*** berkaitan dengan perangkat yang digunakan oleh anggota organisasi untuk mengakses jaringan, data, maupun aplikasi. ***Application layer*** berhubungan dengan akses terhadap aplikasi yang dikembangkan. ***Data security*** berfokus pada pengamanan penyimpanan dan transfer data pada sistem. Sementara itu, mission critical assets lebih dikhususkan untuk memproteksi data maupun informasi sensitif dan penting bagi instansi sektor publik, seperti data kependudukan, data rekam medis, dan data sensitif sejenis.

Gambar 8. ***Ranking Kesiapan Keamanan berdasarkan 7 Layers of Security***

Dari hasil survei pada studi ini, tiga lapisan yang relatif memiliki kesiapan pengamanan yang lebih baik adalah jaringan, data, dan aplikasi. Hasil tersebut mengindikasikan bahwa keamanan informasi di sektor publik masih identik dengan pengamanan jaringan, data, kemudian aplikasi. Lebih dari 50% responden di studi ini telah menerapkan solusi pengamanan jaringan dan data. Perhatian khusus perlu diberikan pada pengamanan aset data kritikal (***mission critical assets***). Hanya terdapat 5 dari 104 instansi responden yang secara penuh sudah menerapkan solusi pengamanan data sensitif. Hal tersebut dapat disebabkan oleh kurangnya pemahaman mengenai perlindungan data pribadi yang memang belum terdapat peraturan formal mengenai hal tersebut. Pengamanan pada ***human layer*** juga perlu ditingkatkan. Tidak hanya dengan sosialisasi terkait kesadaran keamanan informasi, namun yang lebih penting adanya ***enforcement*** terkait prosedur kerja yang berisiko menimbulkan kerentanaan keamanan informasi. Di sisi lain, adopsi pengemanan pada ***endpoint*** dan ***perimeter layer*** juga perlu ditingkatkan untuk mendukung keamanan jaringan, data, dan aplikasi yang saat ini sudah menjadi ***top of mind***.

KESIAPAN INCIDENT MANAGEMENT

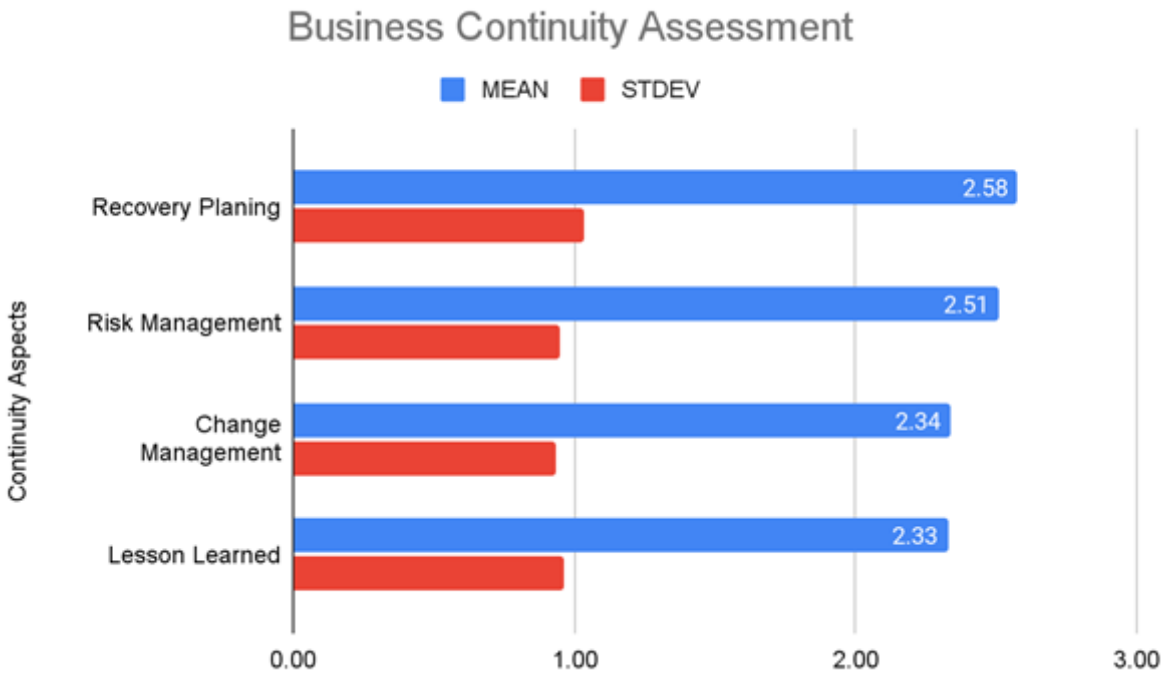
Studi ini juga melakukan evaluasi secara khusus terkait manajemen insiden. Beberapa aspek yang menjadi indikator pada kesiapan manajemen insiden keamanan informasi meliputi deteksi, pengumpulan bukti, analisis, respons, pelaporan dan komunikasi insiden, serta penyusunan ***lesson learned*** dari insiden keamanan informasi yang terjadi. Berdasarkan nilai rataan dari responden pada Gambar 9 di bawah, dapat diketahui bahwa instansi sektor publik di Indonesia memiliki tingkat kesiapan yang lebih baik dalam hal pelaporan dan komunikasi, respon insiden, dan analisis insiden. Perhatian khusus perlu diberikan pada kemampuan instansi sektor publik dalam melakukan deteksi dan pengumpulan bukti insiden mengingat kedua aspek tersebut memiliki nilai lebih rendah dibandingkan dengan ketiga aspek sebelumnya. Adopsi teknologi ***extended detection response*** (XDR) untuk pengawasan sistem secara berkelanjutan dapat dipertimbangkan untuk dapat dengan lebih cepat dalam melakukan deteksi, mengoleksi bukti-bukti insiden, dan melakukan respon terhadap aktivitas mencurigakan. XDR memungkinkan organisasi untuk dapat melakukan analisis secara ***real-time*** terkait aktivitas mencurigakan di berbagai titik seperti ***server, endpoint, cloud,*** dan jaringan sehingga dapat secara proaktif memberikan informasi dini terkait potensi kerentanan informasi pada organisasi. Aspek dengan nilai terendah pada proses manajemen insiden adalah penyusunan pembelajaran (***lesson learned***) dari insiden. Hal tersebut mengindikasikan perlunya organisasi sektor publik untuk dapat membuat mekanisme ***lesson learned*** secara rutin untuk memperkaya aset pengetahuan terkait penanganan kejadian keamanan informasi. Instansi sektor publik perlu mengadopsi mekanisme manajemen pengetahuan secara formal untuk mengoptimalkan penyusunan dan manfaat dari ***lesson learned*** terkait insiden keamanan informasi.



Gambar 9. ***Pemeringkatan Aspek Manajemen Insiden***

KESIAPAN BUSINESS CONTINUITY MANAGEMENT

Business continuity merupakan salah satu aspek organisasional yang menduduki posisi lima terendah di antara sembilan belas indikator kesiapan keamanan informasi yang digunakan pada studi ini. Secara detail, studi ini mengelaborasikan ***business continuity management*** menjadi empat elemen, yakni manajemen risiko, ***recovery planning,*** manajemen perubahan, dan lesson learned. Hasil survei pada studi ini sesuai yang ditampilkan pada Tabel 10, menunjukkan bahwa ***recovery planning*** menjadi aspek dengan nilai rerata tertinggi. Hal ini cukup wajar mengingat kegiatan perencanaan pemulihan pasca insiden keamanan informasi merupakan topik dasar dalam manajemen keamanan informasi. Namun demikian, dengan nilai standar deviasi yang tinggi mencapai lebih dari satu menunjukkan bahwa dimungkinkan adanya ***gap*** kemampuan ***recovery planning*** antar instansi. Dengan demikian, pemerataan pengetahuan pada instansi sektor publik, khususnya instansi di luar jawa terkait ***recovery planning*** juga perlu menjadi perhatian. Perhatian serupa juga perlu diberikan pada kemampuan organisasi dalam melakukan manajemen risiko dan manajemen perubahan. Sementara itu, serupa dengan indikator pada ***incident management, lesson learned*** memiliki nilai paling rendah. Temuan tersebut mengindikasikan urgensi bagi instansi sektor publik untuk memiliki manajemen pengetahuan yang baik, sehingga organisasi tidak hanya berjalan namun juga berkembang secara berkelanjutan, khususnya dalam konteks keamanan informasi berdasarkan akumulasi pengetahuan dari setiap kejadian dan intervensi yang dilakukan.

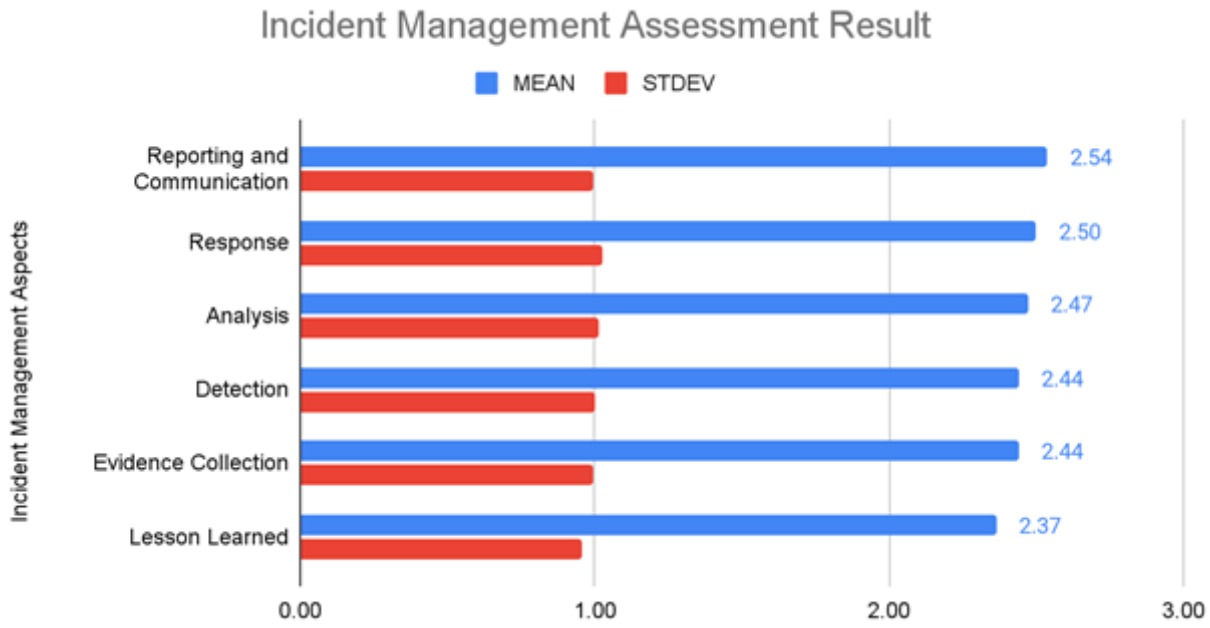


Gambar 10. ***Pemeringkatan Aspek Manajemen Insiden***

KESIAPAN REGULASI

Survei ini mengukur bagaimana kesiapan regulasi pada instansi publik untuk keamanan informasi. Berdasarkan hasil survei yang dirangkum pada Tabel X di bawah, dapat diketahui bahwa tiga indikator yang secara umum memiliki tingkat kesiapan dari sisi regulasi yang lebih baik adalah regulasi terkait akuisisi, pengembangan, dan pemeliharaan sistem, syarat dan ketentuan dari pekerjaan, serta kebijakan/regulasi secara umum. Hal ini mengindikasikan bahwa secara garis besar dan luas, instansi publik telah memiliki kebijakan terkait perencanaan, pengimplementasian, maupun pemeliharaan keamanan informasi.

Di sisi lain, kebijakan terkait hubungan dengan vendor, regulasi terkait keamanan mobile device dan keamanan ***teleworking*** atau yang juga bisa disebut dengan ***remote working*** masih kurang baik dibandingkan dengan tiga indikator sebelumnya. Hal ini mungkin disebabkan karena kebutuhan untuk melakukan pekerjaan dengan menggunakan ***mobile device*** dan secara ***remote*** memang baru dirasakan sejak adanya pandemi Covid-19, sehingga kebijakan yang ada belum mencakup hal-hal tersebut.



Gambar 11. ***Pemeringkatan Aspek Regulasi***

KESIAPAN TANTANGAN IMPLEMENTASI KEAMANAN INFORMASI

Survei ini juga mengukur apa saja tantangan yang dihadapi oleh sektor publik dalam mengimplementasikan keamanan informasi pada instansinya. Pada tabel 2 di bawah, dapat dilihat bahwa komponen terkait sumber daya manusia (***people***) menjadi lima besar tantangan yang menghambat implementasi keamanan informasi. Kurangnya kemampuan keamanan informasi pada sumber daya manusia di instansi menjadi tantangan nomor satu yang mayoritas instansi sebutkan di dalam survei. Hal ini kemungkinan juga terkait dengan tantangan nomor tiga, yaitu ketidakbisaan instansi dalam memberikan kompensasi yang menarik sehingga banyak talenta keamanan informasi yang memilih untuk bekerja di sektor swasta. Hal ini juga besar berhubungan dengan tantangan nomor empat, yaitu karena ada kurangnya alokasi anggaran terhadap keamanan informasi.

Selain itu, hal menarik lainnya yang terungkap dalam survei ini juga terkait sikap dan kesadaran sumber daya manusia di instansi sektor publik tentang keamanan informasi. Pada peringkat dua, terlihat bahwa rasa tanggung jawab terhadap keamanan informasi masih menjadi tantangan yang harus diperhatikan dalam implementasi keamanan informasi. Hal ini mengungkapkan bahwa mayoritas staf pada instansi publik masih menekankan keamanan siber hanya sebagai tanggung jawab divisi TI saja, bukan sebagai tanggung jawab bersama lintas divisi maupun instansi. Hal ini juga kemungkinan terkait pada tantangan nomor lima, yaitu kurangnya kampanye dan/atau sosialisasi terkait keamanan informasi.

Tabel 2. ***Peringkat Tantangan Keamanan Informasi***

NAME	MEAN	STDEV	RANK
Lack of skills	3.2308	0.8728	1
Lack of responsibility towards cyber security	3.2115	0.8666	2
Inability to pay competitive salaries	3.1923	0.8822	3
Lack of cybersecurity technology budget allocation	3.1058	0.9443	4
Lack of cybersecurity awareness campaigns	3.0288	0.8060	5
Talent shortage	2.9808	0.9346	6
No end-user accountability	2.9712	0.8414	7
The silo approach to dealing with cybersecurity-related challenges	2.9135	0.8602	8
Lack of implementation plan	2.8654	0.8819	9
Cyber security technology are moving too fast	2.7885	0.9314	10
Human error	2.7596	0.9190	11
Lack of cybersecurity policies and practices	2.7500	0.9629	12
Lack of support from top officials	2.6731	0.9184	13

Di sisi lain, dapat diketahui bahwa dukungan dari manajemen tingkat atas beserta kebijakan terkait keamanan informasi tidak terlalu menjadi hambatan dalam pengimplementasian keamanan informasi. Hal ini juga terkait dengan tantangan nomor sembilan, yaitu sudah adanya rencana implementasi terkait keamanan informasi. Selain itu, perkembangan teknologi yang cepat beserta unsur kesalahan manusia (***human error***) juga bukan merupakan salah satu tantangan utama dalam melaksanakan implementasi keamanan informasi. Sehingga, dapat dikatakan, dalam pengimplementasiannya, tantangan keamanan informasi banyak bertitik berat pada komponen manusia (***people***), sedangkan untuk komponen teknologi, struktur, dan task tidak menjadi kendala utama.

KESIMPULAN DAN REKOMENDASI

Studi ini telah melakukan perangkingan indikator kesiapan dan tantangan keamanan informasi pada instansi sektor publik di Indonesia. Aspek struktural/organisasi menjadi aspek yang perlu mendapatkan perhatian lebih utamanya terkait business continuity, alokasi anggaran keamanan informasi, dan juga pemenuhan standar sertifikasi keamanan informasi. Instansi sektor publik perlu untuk melihat anggaran keamanan informasi sebagai sebuah investasi untuk menjamin keberlanjutan layanan teknologi informasi yang diberikan. Investasi anggaran keamanan informasi perlu lebih banyak dialokasikan

untuk meningkatkan kompetensi sumber daya manusia dan juga mengadopsi standar maupun solusi-solusi terkini terkait pengamanan informasi. Pemenuhan standar keamanan informasi memiliki urgensi untuk dipenuhi dalam rangka menjamin terlaksananya ***best practice*** dalam mengamankan sistem dan layanan teknologi informasi di instansi sektor publik. Studi ini juga menemukan perlunya instansi sektor publik dalam memiliki mekanisme manajemen pengetahuan mengenai insiden dan kejadian terkait keamanan informasi sebagai langkah untuk mengoptimalkan keberlanjutan layanan dan keamanan informasi.

Terkait aspek sumber daya manusia, peningkatan kompetensi perlu ditingkatkan dengan mendorong aparat pada instansi sektor publik untuk memiliki sertifikasi individu terkait keamanan informasi khususnya untuk instansi di level daerah. Kesadaran akan pentingnya keamanan informasi bagi organisasi perlu juga didukung oleh kompetensi yang mumpuni sehingga setiap personil pada instansi sektor publik dapat secara langsung melakukan kegiatan pengamanan secara proaktif maupun antisipatif. Instansi sektor publik juga perlu untuk mengoptimalkan kegiatan bimbingan teknis (bimtek) kepada para pranata teknologi informasi dengan bekerjasama dengan Badan Siber dan Sandi Negara (BSSN) maupun dengan pihak swasta yang memiliki solusi mutakhir dalam keamanan informasi.

Dari aspek tata kelola keamanan informasi, instansi sektor publik masih memerlukan upaya yang lebih optimal dalam melakukan analisis kerentanan (***vulnerability analysis***) dan juga ***security continuous monitoring***. Adopsi solusi seperti extended response and detection (XDR) dapat menjadi langkah awal untuk meningkatkan pengamanan secara proaktif untuk layanan teknologi informasi di sektor publik. Sebagai langkah mitigasi, instansi sektor publik juga perlu berfokus pada deteksi kerentanan dan risiko keamanan informasi. Langkah konkret untuk hal tersebut dapat berupa adopsi paradigma Security Development Operations (SecDevOps) untuk mendeteksi kerentanan secara dini dari tahap pengembangan sistem. Salah satu solusi yang dapat diadopsi adalah Static Application Security Testing (SAST), untuk mendeteksi kerentanan keamanan sejak dalam fase penulisan kode. Mekanisme kriptografi juga merupakan salah satu aspek yang memerlukan perhatian tersebut mengingat aspek tersebut merupakan salah satu lima indikator dengan rerata terendah. Mekanisme kriptografi tersebut juga dapat mendukung pengamanan ***mission critical assets*** atau aset penting berupa informasi sensitif yang masih tergolong rendah dibanding ***layer*** keamanan lainnya seperti jaringan, data, dan aplikasi.

DAFTAR REFERENSI

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. ***Computers and Security***, 99, 102030. https://doi.org/10.1016/j.cose.2020.102030

Anu, V. (2021). Information security governance metrics: a survey and taxonomy. ***Information Security Journal***, 00(00), 1–13. https://doi.org/10.1080/19393555.2021.1922786

Badan Siber dan Sandi Negara. (2020, March 6). ***Laporan Tahunan 2019 PUSOPSKAMSINAS BSSN | bssn.go.id***. https://bssn.go.id/laporan-tahunan-2019-pusopkamsinas-bssn/

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. ***Interacting with Computers***, 23(1), 4–17. https://doi.org/10.1016/J.INTCOM.2010.07.003

Borgman, B., Mubarak, S., & Choo, K. K. R. (2015). Cyber security readiness in the South Australian Government. ***Computer Standards and Interfaces,*** 37(2015), 1–8. https://doi.org/10.1016/j.csi.2014.06.002

DPR Republik Indonesia. (2021). ***Tantangan Penguatan Keamanan Siber dalam Menjaga Stabilitas Keamanan***.

Frost, & Sullivan. (2018, May 24). ***Ancaman Keamanan Siber Menyebabkan Kerugian Ekonomi bagi Organisasi di Indonesia Sebesar US$34.2 Miliar – Indonesia News Center***. https://news.microsoft.com/id-id/2018/05/24/ancaman-keamanan-siber-menyebabkan-kerugian-ekonomi-bagi-organisasi-di-indonesia-sebesar-us34-2-miliar/

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A Cyber-Security Culture Framework for Assessing Organization Readiness. ***Journal of Computer Information Systems***, 00(00), 1–11. https://doi.org/10.1080/08874417.2020.1845583

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. J***ournal of Information Security and Application***s, 58, 102726. https://doi.org/10.1016/j.jisa.2020.102726

ISO27001. (2022). ISO 27001, ***The Information Security Standard Made Easy***. https://www.isms.online/iso-27001/

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. ***International Journal of Critical Infrastructure Protection***, 15, 47–59. https://doi.org/10.1016/j.ijcip.2016.10.001

Kementerian Komunikasi dan Informatika. (2020). ***Penggunaan Internet Naik 40% Saat Bekerja dan Belajar dari Rumah***. https://www.kominfo.go.id/content/detail/25881/penggunaan-internet-naik-40-saat-bekerja-dan-belajar-dari-rumah/0/berita_satker

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. ***Journal of Enterprise Information Management***, 34(6), 1597–1629. https://doi.org/10.1108/JEIM-06-2020-0240

Mergel, I., Edelmann, N., & Haug, N. (2019). Defining digital transformation: Results from expert interviews. ***Government Information Quarterly***, 36(4), 101385. https://doi.org/10.1016/J.GIQ.2019.06.002

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. ***Journal of Information Security and Applications***, 44, 12–22. https://doi.org/10.1016/j.jisa.2018.11.003

NIST. (2022). ***Cybersecurity Framework*** | NIST. https://www.nist.gov/cyberframework

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. ***Computers & Security***, 90, 101709. https://doi.org/10.1016/J.COSE.2019.101709

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. ***Computers and Security***, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. ***Computers and Security,*** 83, 313–331. https://doi.org/10.1016/j.cose.2019.02.009

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. ***Journal of Computer Information Systems***, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

Lampiran 1. ***Referensi Faktor Kesiapan Keamanan Informasi***

FACTOR	DIMENSION	REFERENCES
Accountability and responsibility	People	(AlGhamdi et al., 2020; Uchendu et al., 2021)
Awareness	People	(AlGhamdi et al., 2020; Anu, 2021; Borgman et al., 2015; Georgiadou et al., 2020; Karabacak et al., 2016; Nasir et al., 2019; Uchendu et al., 2021; Zwilling et al., 2022)
Culture of information sharing, collaboration and cooperation	People	(al., 2021; Karabacak et al., 2016)
Personnel Competence	People	(rabacak et al., 2016)
Business Continuity	Structure	(Anu, 2021; Georgiadou et al., 2020; Nasir et al., 2019; Uchendu et al., 2021) - (NIST Cybersecurity Framework)
Certificate and Standards Compliance	Structure	(AlGhamdi et al., 2020; Anu, 2021; Borgman et al., 2015; Hasan et al., 2021; Kumar et al., 2021; Uchendu et al., 2021; Vitunskaite et al., 2019)
Cost of Security Investment	Structure	Anu (2021); Nasir et al. (2019)
Organization of Information Security	Structure	(ISO 27000)
Top Management Support and Strategic Direction	Structure	(Anu, 2021; Borgman et al., 2015; Hasan et al., 2021; Kumar et al., 2021; Nasir et al., 2019)
Regulation and Policies	Structure	(Anu, 2021; Hasan et al., 2021; Karabacak et al., 2016; Kumar et al., 2021; Nasir et al., 2019; Uchendu et al., 2021) - (ISO 27000)
Access, Trust, and Identity Management	Task	(Anu, 2021; Georgiadou et al., 2020; Nasir et al., 2019)
Assets Management	Task	(Anu, 2021; Borgman et al., 2015; Georgiadou et al., 2020; Nasir et al., 2019)
Audit Logs Management	Task	(Anu, 2021; Borgman et al., 2015; Karabacak et al., 2016; Nasir et al., 2019)
Incident Management	Task	(AlGhamdi et al., 2020; Anu, 2021; Borgman et al., 2015) -(NIST Cybersecurity Framework)
Security Continuous Monitoring	Task	(Nasir et al., 2019; Uchendu et al., 2021)
Vulnerability and Risk Assessment	Task	(AlGhamdi et al., 2020; Anu, 2021)
Information Security Infrastructure	Technology	(Hasan et al., 2021; Karabacak et al., 2016)
Physical and Environmental Security	Technology	(Anu, 2021; Hasan et al., 2021)
Cryptography	Technology	(NIST Cybersecurity Framework)

PENGARAH

Anton Setiawan
Kepala Pusat Pengkajian dan Pengembangan Teknologi Keamanan Siber dan Sandi
BSSN

Laksana Budiwiyono
Country Manager
Trend Micro Indonesia

TIM PENELITI

Prof, A. Nizat Hidayanto, Dr.
Dosen dan Peneliti
Universitas Indonesia

Hafizh Rafizal Adnan
Dosen dan Peneliti
Universitas Indonesia

Fathia Prinastiti Sunarso
Dosen dan Peneliti
Universitas Indonesia

Alex Budiyanto
Ketua Umum
ACCI

Asriza Yolanda
Analis Persandian, Puskajibang Tekkamsisan
BSSN

Adrian Admi
Sandiman Muda, Puskajibang Tekkamsisan
BSSN

Galih Wening Werdi Mukti
Analis Persandian, Puskajibang Tekkamsisan
BSSN

Reza Ilham Zulfahmi
Analis Persandian, Puskajibang Tekkamsisan
BSSN

Muhammad Rakha Rafi Baihaqi
Pengelola Penelitian
BSSN