URGENSI STRUKTUR ORGANISASI KEAMANAN INFORMASI PADA SEKTOR KESEHATAN

Direktorat Proteksi Infrastruktur Informasi Kritis Nasional (IIKN)
Badan Siber dan Sandi Negara

Penyelenggara pelayanan kesehatan menjadi salah satu industri yang paling terancam dengan semakin meningkatnya tren serangan siber. Menurut data dari IBM X-Force Threat Intelligence Index 2019, industri pelayanan kesehatan menjadi industri kedelapan paling ditargetkan dalam ancaman keamanan siber. Hal ini dikarenakan sektor kesehatan memiliki informasi yang dapat menjadi komoditas "komersial" bagi penyerang, diantaranya adalah informasi kesehatan dan data pribadi pasien. Oleh karena itu, implementasi sistem manajemen keamanan informasi sangat diperlukan pada sektor kesehatan. Menurut Peraturan Pemerintah Nomor

46 Tahun 2014 tentang Sistem Informasi Kesehatan, informasi kesehatan yang dilarang untuk dipublikasikan diantaranya:

- salinan kartu pengguna Fasilitas Pelayanan Kesehatan atau bukti identitas lain;
- riwayat kesehatan atau data rekam medis;
- tagihan dan bukti pembayaran biaya penggunaan Fasilitas Pelayanan Kesehatan;
- hasil pemeriksaan diagnostik berupa foto rontgen, pemindaian, analisa laoratorium;
- data dan informasi terkait kegiatan penelitian, meliputi: data identitas subyek penelitian, baik individu, kelompok individu/masyarakat;
- data dan informasi hasil penelitian dan/atau kajian yang apabila dibuka untuk umum akan merugikan subyek, meresahkan masyarakat dan/atau mengancam keamanan negara;
- data dan informasi hasil penelitian yang secara etika atau hasil kesepakatan dengan subyek penelitian bersifat rahasia atau dirahasiakan.

Roohparvar (2017) menyatakan bahwa keamanan informasi pada sektor kesehatan harus menjadi prioritas karena beberapa alasan berikut:

1. **Teknik pencurian data oleh *hacker* semakin bervariasi;**
   Peretas atau *Hacker* senantiasa memperbarui teknik dan pendekatan untuk melakukan eksploitasi terhadap suatu sistem kesehatan, bahkan melalui celah kerawanan terkecil. Data kesehatan sangat bernilai bagi *hacker* karena dapat diperjual belikan di pasar gelap, digunakan untuk pemerasan atau transaksi keuangan ilegal. Selain itu peluang korban di sektor kesehatan untuk membayar tebusan yang diminta oleh pelaku kejahatan siber juga sangat tinggi.
2. **Teknik perlindungan data pasien semakin kompleks;**
   Teknik perlindungan data pasien tidak hanya membutuhkan strategi dan rencana yang matang tetapi juga dana yang tidak sedikit. Hal ini karena sifat perlindungan yang diberikan harus mampu mendeteksi serangan sebelum insiden terjadi. Demikian pula layanan perlindungan dan kontrol akses harus dapat diterapkan secara menyeluruh mulai dari

data diambil, dikumpulkan, digunakan, ditangani, dikirim, hingga disimpan.

3. **Meningkatnya kasus penyanderaan data menggunakan *ransomware*;**

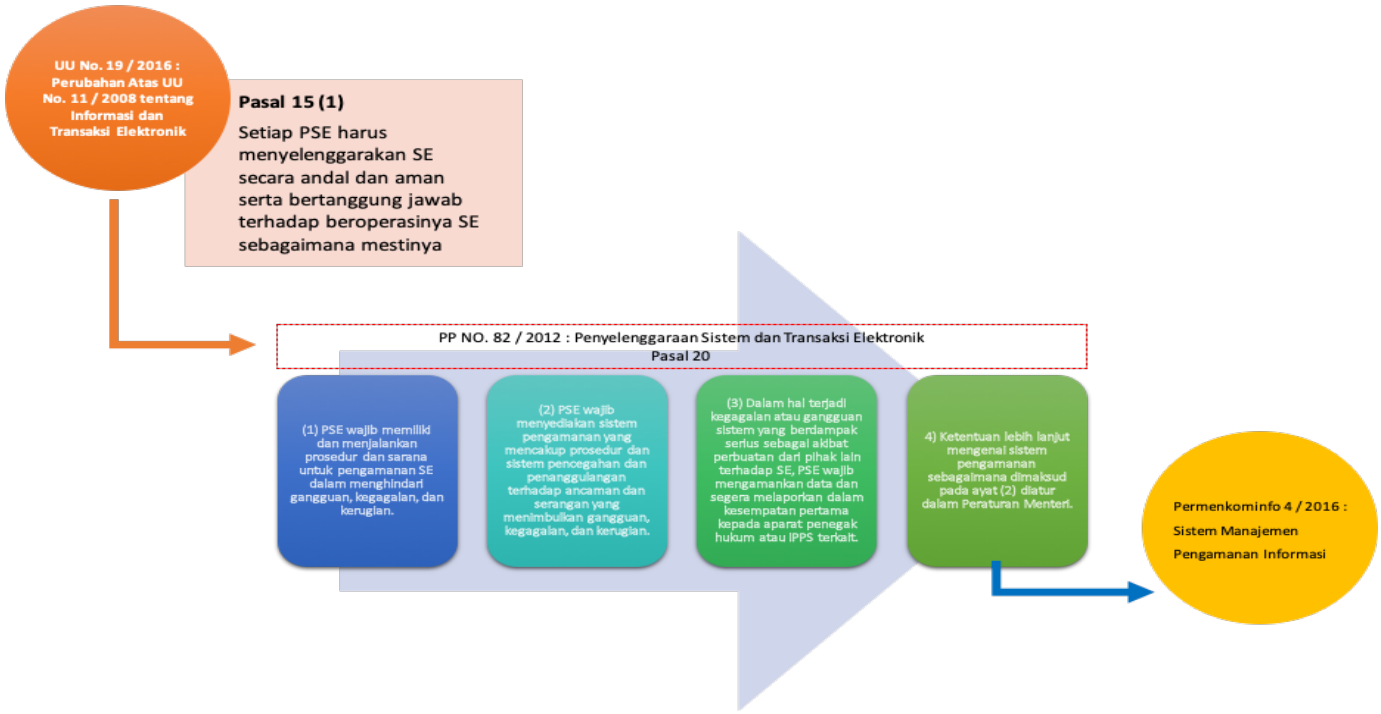
   Ransomware merupakan jenis serangan dimana *hacker* mengenkripsi suatu data sehingga data tersebut tidak dapat diakses, sampai dengan korban membayarkan sejumlah uang tebusan yang dipersayaratkan. Kasus *ransomware* pada sektor kesehatan semakin sering terjadi. Dilapokan oleh situs www.bleepingcomputer.com dalam suatu penelitian yang melibatkan 2700 profesional IT pada tahun 2017 tercatat 76% responden dari sektor kesehatan pernah mengalami serangan *ransomware*.

4. **Risiko dari pihak ketiga;**

   Seringkali layanan kesehatan mengharuskan adanya berbagi informasi dengan pihak ketiga. Hal ini dapat menimbulkan celah kerawanan baru yaitu kemungkinan adanya kebocoran informasi yang disebabkan oleh kelalaian pihak ketiga. Sehingga, dibutuhkan kebijakan keamanan informasi yang jelas tertuang dalam perjanjian kerja agar ketentuan pengelolaan keamanan informasi dipatuhi oleh seluruh pihak yang terlibat.

5. **Kerawanan *email* dan aplikasi bergerak (mobile application)**

   Email dan aplikasi bergerak merupakan kebutuhan perusahaan untuk dapat bertahan di era informasi saat ini. Meskipun demikian, masih terdapat celah kerawanan yang ditemukan pada penggunaan *email* dan aplikasi bergerak. Pengelolaan keamanan informasi pada *email* dan aplikasi bergerak mutlak diperlukan untuk mencegah kebocoran informasi.



Gambar 1 - Regulasi tata kelola keamanan informasi di Indonesia

Implementasi Keamanan informasi tidak hanya terkait masalah teknis saja, tetapi juga harus didukung oleh kebijakan yang dikeluarkan oleh organisasi, berupa tata kelola keamanan informasi (*information security governance*). Tata kelola keamanan informasi dalam tersebut diaplikasikan

dalam wujud sebuah sistem, yaitu *Information Security Management System* (ISMS). Konsep utama ISMS adalah merancang, menerapkan, dan memelihara suatu rangkaian terpadu proses dan sistem untuk secara efektif mengelola keamanan informasi dan menjamin kerahasiaan, integritas, serta ketersediaan aset-aset informasi serta meminimalkan risiko keamanan informasi.

Tata kelola keamanan informasi elektronik di Indonesia telah diatur dalam aturan perundangan, seperti dijelaskan dalam Gambar 1. Setiap Penyelenggara Sistem Elektronik Pelayanan Publik harus menetapkan tata kelola keamanan informasi secara andal dan aman serta bertanggung jawab sesuai dengan ketentuan pasal 15 UU Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan PP Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dengan merujuk pada standar sistem menajemen keamanan informasi. Standar sistem manajemen keamanan informasi yang dimaksud di atas, dijelaskan lebih lanjut dalam Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.

REGULASI TENTANG PERLINDUNGAN DATA PASIEN DI INDONESIA

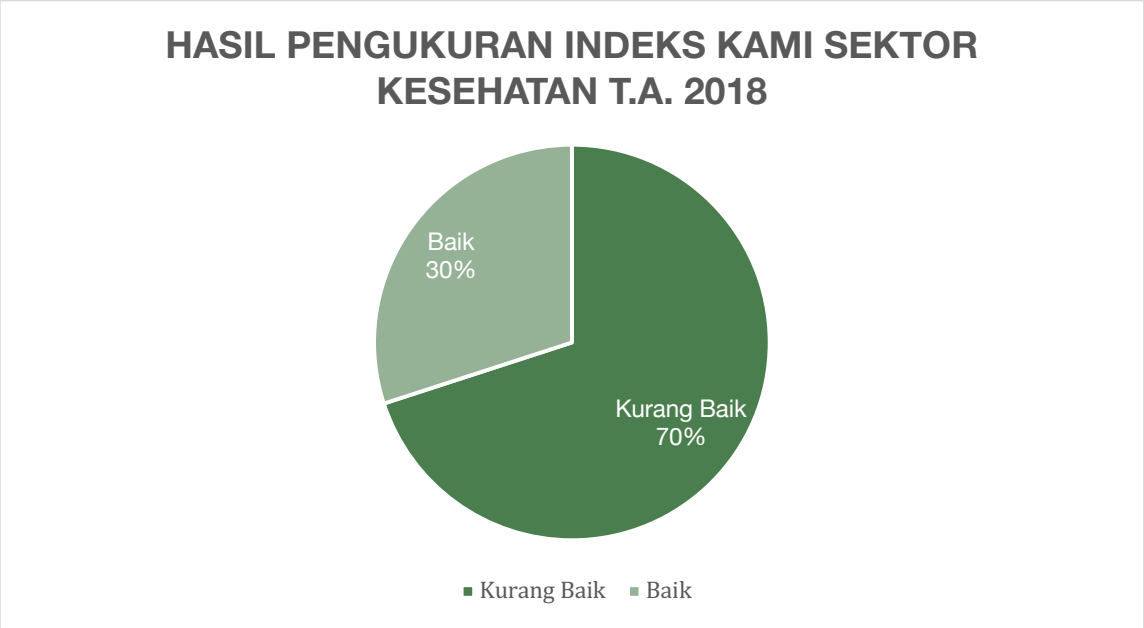
Kebijakan mengenai kerahasiaan informasi kesehatan dalam beberapa aturan perundangan, antara lain:

- Undang Undang Nomor 29 Tahun 2004 tentang Praktik Kedokteran;
- Undang Undang Nomor 36 Tahun 2009 tentang Kesehatan;
- Undang Undang Nomor 44 Tahun 2009 tentang Rumah Sakit;
- Undang Undang Nomor 36 Tahun 2014 tentang Sistem Informasi Kesehatan;
- Peraturan Menteri Kesehatan Nomor 36 Tahun 2012 tentang Rahasia Kedokteran;
- Peraturan menteri Kesehatan Nomor 4 Tahun 2018 tentang Kewajiban Rumah Sakit dan Kewajiban Pasien; dan
- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

Sebagai industri yang memanfaatkan teknologi informasi dalam menunjang proses bisnisnya, sudah seharusnya setiap organisasi di sektor kesehatan berupaya untuk melindungi informasi yang dikelolanya sesuai ketentuan perundangan yang berlaku yaitu melalui pengimplementasian sistem manajemen pengamanan informasi. Berdasarkan laporan pengukuran Indeks Keamanan Informasi (Indeks KAMI) Tahun 2018 yang

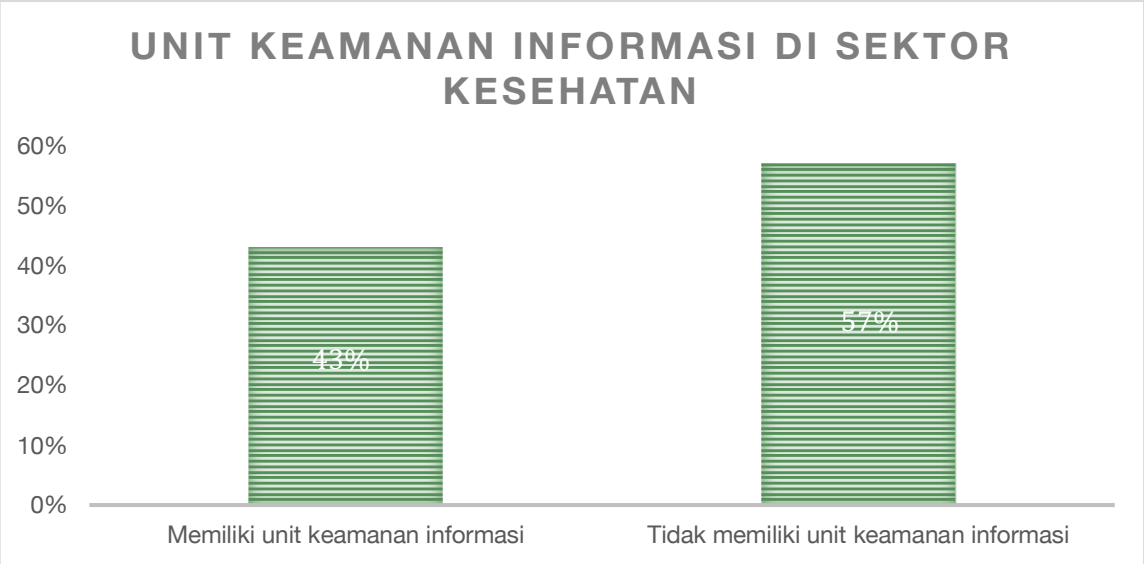
dilakukan oleh BSSN pada 14 (empat belas) organisasi di sektor kesehatan, hanya 30% yang mendapat predikat BAIK atau hanya 4 (empat) instansi yang berhasil mendapat nilai di atas 80.

Hasil ini menggambarkan bahwa penyelenggaraan tata kelola keamanan informasi pada sektor kesehatan di Indonesia **belum optimal dan perlu perbaikan**.



Gambar 2 Diagram hasil Pengukuran Indek KAMI Pada Sektor Kesehatan T.A.2018

Berdasarkan hasil kuesioner yang dibagikan oleh BSSN pada 35 (tiga puluh lima) instansi penyelenggara pelayanan kesehatan di tahun 2018, diperoleh data bahwa seluruh instansi memiliki unit pengelola Teknologi Informasi. Pada 15 (lima belas) instansi tersebut, unit organisasi pengelola Teknologi Informasi memiliki unit yang mengelola keamanan informasi, sedangkan pada 20 (dua puluh) instansi lainnya tidak memiliki unit yang mengelola keamanan informasi namun fungsi keamanan informasi menjadi bagian dari tugas dan fungsi dari unit Teknologi Informasi. Dari data tersebut dapat disimpulkan bahwa organisasi penyelenggara pelayanan kesehatan sudah paham akan urgensi dari struktur keamanan informasi pada sektor kesehatan.



Gambar 3 Diagram Hasil Kuisoner Terkait Unit/Fungsi Keamanan Informasi pada Instansi di Sektor Kesehatan T.A.2018

Dari unit pengelola TI tersebut, sebanyak **43% memiliki unit pengelola keamanan informasi, sedangkan 57% tidak memiliki unit pengelola keamanan informasi.** 57% instansi tersebut menjadikan pengelolaan keamanan informasi sebagai bagian dari tugas dan fungsi dari unit TI-nya.

DAMPAK TIDAK ADANYA UNIT KEAMANAN INFORMASI

Melihat arti pentingnya pengimplementasian sistem manajamen pengamanan informasi untuk menunjang proses bisnis organisasi, maka perlu dibentuk suatu unit pada struktur organisasi yang secara konsisten melakukan pengelolaan terhadap sistem manajemen pengamanan informasi di organisasi tersebut. Dengan adanya unit yang bertanggung jawab dalam pengelolaan sistem manajemen pengamanan informasi dapat meningkatkan tata kelola keamanan informasi dan kesiapan organisasi dalam menghadapi setiap ancaman keamanan siber.

INDEKS KAMI (Keamanan Informasi) BSSN

Indeks KAMI merupakan alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi dan gambaran mengenai tingkat keamanan informasi pada institusi khususnya pengelolaan informasi yang menggunakan Sistem Elektronik yang merujuk pada standar SNI ISO:IEC 27001:2013. Ruang lingkup penilaian Indeks KAMI meliputi: Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi, dan Teknologi dan Keamanan Informasi.

(informasi lebih lanjut mengenai Indeks KAMI BSSN dapat dilihat pada halaman: https://bssn.go.id/indeks-kami/)

Jika sebuah organisasi penyelenggara kesehatan tidak memiliki unit keamanan informasi atau unit tersebut tidak bekerja secara efektif, maka dapat menimbulkan dampak negatif terhadap keberlangsungan bisnis organisasi tersebut, yaitu diantaranya:

1. **Tidak adanya unit yang bertanggung jawab terhadap masalah keamanan informasi;**

Ajit Appari dalam tulisannya berjudul "Information Security and Privacy in Healthcare: Current State of Research" menjelaskan bahwa terdapat dua ancaman terhadap informasi data pribadi pasien yaitu (1) Ancaman organisasi yang muncul dari akses data pasien yang tidak tepat oleh petugas internal kesehatan yang menyalahgunakan hak istimewa mereka atau pihak eksternal yang mengeksploitasi kerentanan sistem informasi, dan (2) Ancaman sistemik yang timbul dari agen dalam rantai aliran informasi yang mengeksploitasi data di luar penggunaan yang dimaksudkan. Ancaman-ancaman tersebut tentu saja sangat merugikan pasien dan penyelenggara kesehatan. Oleh karena itu, sebuah organisasi penyelenggara kesehatan harus memiliki unit keamanan informasi untuk mengatasi dan mencegah ancaman dan insiden keamanan informasi yang muncul.

2. **Keterbatasan sumber daya mengakibatkan pengelolaan keamanan informasi tidak optimal sehingga terjadi insiden;**

Pada sebagian organisasi kesehatan, sumber daya untuk mengelola sistem keamanan informasi masih dikesampingkan sehingga kebutuhan untuk memenuhi keamanan informasi tidak terkelola dengan baik. Hal ini dikarenakan, sumber daya yang dibutuhkan untuk keamanan informasi tidaklah sedikit dan membutuhkan perencanaan yang matang.

Dengan keterbatasan sumber daya untuk pengelolaan keamanan informasi menyebabkan pengelolaan keamanan informasi tidak optimal sehingga terjadi insiden.

3. **Tuntutan hukum akibat kegagalan melindungi data pasien;**

Saat ini perlindungan data pribadi menjadi hal yang diperhatikan oleh negara-negara di dunia. Beberapa negara sudah menggalakkan regulasi terkait perlindungan data pribadi, diantaranya Amerika, Uni Eropa, Korea Selatan, Australia, dll. Salah satu regulasi terkait perlindungan data pribadi

yang sedang hangat diperbincangkan saat ini adalah GDPR. General Data Protection Regulation (GDPR) merupakan peraturan yang berkaitan dengan bagaimana cara melindundi data pribadi penduduk Uni Eropa. Regulasi ini tidak hanya mengatur organisasi yang terdapat di Uni Eropa tetapi juga organisasi/instansi di negara lain yang menyimpan data pribadi penduduk Uni Eropa. Sanksi yang diterapkan pada GDPR adalah denda sebesar EUR 20 Mio atau 4% Global Revenue, sanksi ini dirasa sangat berat dan mengikat agar para pemangku kepentingan patuh terhadap GDPR. Para penyelenggara kesehatan yang menyimpan data pribadi pasien penduduk Uni Eropa tidak luput dari regulasi ini. Oleh karena itu, penyelenggara kesehatan harus dapat melindungi data pribadi pasien agar tidak menyalahi regulasi yang ada.

4. **Penanganan insiden keamanan menjadi terhambat.**

Kasus terbesar terkait perlindungan data pribadi adalah Kebocoran Data SingHealth, dimana penyerang berhasil mendapatkan 1,5 juta data pribadi pasien termasuk data pribadi Perdana Menteri Lee Hsien Loong. Pemerintah Singapura pada awal bulan Januari 2019 mengeluarkan hasil investigasi resmi dari kasus Singhealth yang terjadi pada pertengahan tahun 2018. Hasil investigasi tersebut menjelaskan penyebab terjadinya insiden dan memberikan rekomendasi untuk mengisolasikan dampak serangan yang sudah terjadi serta mencegah terjadinya serangan sejenis. Menurut Alijoyo (2019), kasus serangan siber SingHealth merupakan pembelajaran bagaimana suatu risiko siber dapat terjadi dan menimbulkan kerusakan baik finansial maupun non-finansial terutama terhadap reputasi organisasi dan negara, dan oleh karena itu, pertahanan organisasi terhadap serangan siber perlu diperkuat.

UNIT KEAMANAN INFORMASI PADA ORGANISASI KESEHATAN

Setiap hari serangan siber mengancam informasi digital yang kita miliki. Ancaman tersebut semakin canggih dari hari ke hari dengan cara-cara baru untuk mencuri informasi. Pencurian data pada penyelenggara layanan kesehatan tidak hanya berdampak pada reputasi Rumah Sakit dan masalah finansial namun juga menimbulkan ancaman baru bagi pasien. Identitas pasien dapat dicuri langsung dari organisasi penyelenggara

pelayanan kesehatan atau perusahaan asuransi yang terkait dengan industri perawatan kesehatan atau dari organisasi lain yang terlibat dalam pengelolaan informasi medis. Salah **satu strategi untuk melakukan pencegahan terhadap kejahatan siber yaitu dengan keterlibatan dan partisipasi karyawan dalam kegiatan kesadaran keamanan Informasi.** Kegiatan tersebut menjadi komponen paling efektif dari program perlindungan kesehatan. Kegiatan kesadaran keamanan informasi tersebut merupakan salah satu tugas dari unit keamanan informasi di dalam organisasi. Oleh karena itu, setiap penyelenggara kesehatan perlu memiliki unit keamanan informasi di dalam organisasinya.

Dalam panduan "*Guide to Information Security for the Health Care Sector*" dijelaskan bahwa dalam rangka mengembangkan program keamanan informasi, suatu organisasi perlu menempatkan struktur manajemen keamanan informasi dengan menetapkan peran dan tanggung jawab agar keamanan informasi di seluruh organisasi terjamin.

Manfaat adanya struktur manajemen keamanan informasi diantaranya:

- Terdapat pemahaman yang jelas tentang pemisahan tugas mengenai siapa melakukan apa, kapan, dan dimana.
- Memastikan bahwa kegiatan keamanan informasi diatur secara efektif dan efisien sehingga staf menyadari tugas mereka dan staf mendapatkan pelatihan dan keterampilan yang memadai.

Hal penting yang harus diperhatikan adalah bahwa setiap organisasi memiliki keunikan yang berbeda-beda. Organisasi yang lebih kecil dapat menggabungkan beberapa tanggung jawab menjadi satu peran, sedangkan organisasi menengah dan besar dapat memisahkan area tanggung jawab menjadi beberapa peran. Namun demikian konsep pemisahan tugas (*segregation of duties*) harus diterapkan ketika menggabungkan peran tanggung jawab ini dengan fungsi lainnya.

Unit Keamanan Informasi Organisasi Skala Kecil

Berdasarkan ISO 27799 Tahun 2017 tentang Manajemen keamanan informasi pada sektor kesehatan menggunakan ISO/IEC 27002, dijelaskan

bahwa minimal terdapat **satu orang** yang harus bertanggung jawab atas keamanan informasi kesehatan di dalam organisasi.

Dimana setiap organisasi di sektor kesehatan yang memproses informasi kesehatan pribadi harus melakukan hal berikut:

a) Secara jelas mendefinisikan dan menetapkan tanggung jawab dan wewenang yang diberikan terhadap pihak yang diberi amanah;

b) Memiliki forum manajemen keamanan informasi untuk memastikan bahwa ada arah yang jelas dan dukungan manajemen yang terlihat untuk inisiatif keamanan yang melibatkan keamanan informasi kesehatan.

Unit Keamanan Informasi Organisasi Skala Menengah Ke Besar

Tabel 1 menunjukkan contoh jenis peran dan tanggung jawab yang umum dalam organisasi menengah ke besar. Contoh ini dapat digunakan sebagai panduan untuk menetapkan peran dan tanggung jawab yang relevan di suatu organisasi. Setiap organisasi perlu untuk menyesuaikan, menggabungkan, mengubah atau menghapus untuk mengembangkan organisasi keamanan informasi yang disesuaikan dengan organisasinya masing-masing.

Tabel 1 Peran dan tanggung jawab dalam organisasi menengah ke besar

Peran	Tanggung Jawab
Manajemen keamanan informasi	▪ Ditugaskan kepada seorang individu dengan tanggung jawab Manajemen Bisnis Senior ▪ Meningkatkan kesadaran dan memberikan pelatihan tentang tanggung jawab mereka terkait keamanan informasi kepada staf ▪ Mengembangkan kebijakan, tujuan, dan strategi keamanan informasi ▪ Menentukan ruang lingkup sistem manajemen keamanan informasi (SMKI) ▪ Melakukan penilaian risiko awal dan mengidentifikasi risiko ▪ Mendapatkan persetujuan dari manajemen senior tentang pendekatan organisasi untuk manajemen risiko dan rencana perawatan risiko ▪ Memilih kontrol keamanan yang akan memenuhi tujuan bisnis ▪ Merekam dan menangani insiden keamanan, termasuk menetapkan penyebabnya dan menentukan tindakan korektif dan/atau pencegahan yang tepat ▪ Melaporkan kepada manajemen senior tentang kemajuan pelaksanaan program keamanan informasi, dan juga terkait insiden, masalah, dan ancaman keamanan informasi saat ini.
Penanggungjawab kepatuhan	▪ Harus independen dari program keamanan informasi ▪ Memantau dan meninjau kepatuhan terhadap kebijakan keamanan informasi dan *security best practices* ▪ Memastikan kepatuhan terhadap Undang-Undang dan Peraturan
Manajemen teknologi informasi	▪ Mengidentifikasi ancaman sistem dan batas jaringan ▪ Menerapkan kontrol keamanan sistem yang dipilih (misal *passwords*), jaringan (misal *firewall*) dan fisik (misal kamera keamanan) ▪ Melaporkan kerentanan teknis dan insiden ke manajemen senior ▪ Menyiapkan pemantauan keamanan ▪ Mendeteksi dan merespon ancaman ▪ Merencanakan dan menguji rencana pemulihan bencana ▪ Memastikan bahwa pembaruan virus dan tambalan sistem diterapkan sebagaimana mestinya ▪ Menegakkan persyaratan keamanan dengan penyedia eksternal ▪ Mengelola keamanan untuk fasilitas komputasi

REFERENSI

1. Ash, Judy *et al*., 2010. *Guide to Information Security for the Health Care Sector, Information and Resources for Complex Organizations*. Ontario: eHealth Ontario.
2. Cimpanu, Catalin., 2018. Ransomware Victims Hit on Average by Two Attacks per Year. Retrieved from https://www.bleepingcomputer.com
3. IBM., 2019. *X-Force Threat Intelligence Index 2019*. New York: IBM Security.
4. ISO 27799:2017, *Health informatics – Information security management in health using* ISO/IEC 27002.
5. Roohparvar, Robert., 2017. *Why Is Information Security Important for The Healthcare Sector*. Retrieved from http://www.infoguardsecurity.com

6 TIPS MEMILIH PASSWORD

Gunakan password yang sulit untuk ditebak

Jangan pernah tuliskan passwordmu

Jangan bagikan password kepada orang lain

Gunakan password manager/ password vault untuk menyimpan paswordmu

Ubah passwordmu secara berkala

Aktifkan fitur Multi Factor Authentication

Gantilah passwordmu seperti halnya sikat gigimu….