Journal of Business Administration Vol 3, No.1, Maret 2019, hlm, 162-171, e-ISSN:2548-9909

PENILAIAN PENGAMANAN TEKNOLOGI PADA SISTEM PEMBELAJARAN ELEKTRONIK MENGGUNAKAN INDEKS KEAMANAN INFORMASI DI POLITEKNIK NEGERI BATAM

Muhammad Ramadhan Slamet[1]), Febrina Wulandari[2]), Diah Amalia[3])

1) Prodi Administrasi Bisnis, Politeknik Negeri Batam, Batam, Indonesia, Email: ramadhanslamet@polibatam.ac.id.
2) Prodi Administrasi Bisnis, Politeknik Negeri Batam, Batam, Indonesia, Email: febrina@polibatam.ac.id
3) Prodi Administrasi Bisnis, Politeknik Negeri Batam, Batam, Indonesia, Email: diahamalia@polibatam.ac.id

Abstract

As an electronic learning system organizer State Polytechnic of Batam (Polibatam) must arrange secured electronic learning system. Ministry of Communication and Information of Indonesia expects the organizations which arrange electronic system can perform SNI ISO 27001 certification related to information security. Information security condition on organizations which will perform on certifiation is expected on maturity level at III+ (Directorate of Information Security Team, 2011). On the other hand, there is a gap between expected conditon and actual condition. Information security index (KAMI) is a tool to assess the implementation of information security that has been done. This research is assessed related to technology component because of high dependency of organization on technology. The purpose of research is to identify how far the security of technology at State Polytechnic of Batam by using information security index. Based on research, electronic learning system that is organized by State Polytechnic of Batam is low categorized. The total percentage is 65 or 54,17% out of maximum percentage. Therefore, the maturity level of technology security is on maturity level II which means the maturity level of technology security is under the expected maturity level for minimum readiness certification on III+. It is caused the position of State Polyetechnic of Batam is on a organizational development stage. Moreover, the focus of organization is related on operational, not strategic.

Keywords*: Electronic Learning System, KAMI Index, Information Security, ISO 27001*

Journal of Business Administration Vol 3, No.1, Maret 2019, hlm, 162-171

PENDAHULUAN

Teknologi informasi (TI) merupakan suatu yang penting bagi organisasi saat ini. Mulai dari membantu pekerjaan di level operasional sampai dengan membantu level strategis untuk mengambil keputusan. Hal tersebut mengakibatkan organisasi melakukan pengeluaran terkait TI untuk memenuhi kebutuhannya. Berdasarkan laporan dari Gartner (2018) diketahui bahwa pengeluaran TI secara global diperkirakan mencapai $3,7 miliar di tahun 2018 atau meningkat 4,5% dari tahun 2017.

Pengeluaran TI yang meningkat menandakan semakin tinggi ketergantungan terhadap TI bagi organisasi. Ketergantungan tersebut dapat menjadi sesuatu yang membahayakan. Hal itu dikarenakan banyak ancaman yang dihadapi oleh organisasi sebagai akibat penggunaan TI yang menimbulkan kasus terkait keamanan informasi. Salah satu kasus terkait keamanan informasi adalah kebocoran data. Berdasarkan laporan dari Gemalto (2017) pada semester satu 2017 secara global terdapat 1.901.866.611 data yang bocor. Artinya, setiap hari ada 10.507.550 data yang hilang. Jika didasarkan atas jenis data sekitar 74% merupakan insiden terkait kehilangan identitas (*identity theft*), sedangkan jika didasarkan atas pelaku insiden sekitar 74% merupakan pelaku dari pihak eksternal (*malicious outsider*).

Pada tahun 2017 institusi pendidikan mendapat sorotan bagi dunia internasional karena mengalami peningkatan kebocoran data terbesar dibandingkan dengan sektor lain (Gemalto, 2017). Hal tersebut disebabkan jumlah data yang hilang meningkat secara signifikan, yaitu mencapai 32 juta data atau naik 4.957% (jika dibandingkan dengan semester lalu) di semester pertama tahun 2017. Ada satu kasus yang cukup fenomenal terkait kebocoran data pada tahun 2017 di institusi pendidikan. Persitiwa tersebut terjadi di Cina. Seorang mantan *manager* pemasaran di salah satu pendidikan swasta di Cina menjual jutaan informasi pribadi mahasiswa ke perusahaan. Hasil penjualan tersebut memberikan keuntungan pribadi oleh tersangka sebesar 10.000 Yuan atau US$1.450 (Huizhi, 2017).

Sehubungan dengan itu, organisasi yang terkena dampak kebocoran data harus menangani ataupun menyelesaikan kasus tersebut. Penanganan tersebut membutuhkan sejumlah biaya, seperti biaya untuk melakukan investigasi kasus kebocoran data. Menurut laporan dari Ponemon Institute LLC tahun 2017 dinyatakan bahwa secara global biaya atas kejadian kebocoran data di institusi pendidikan, yaitu $200 per data yang hilang. Institusi pendidikan menduduki posisi ke-4 sebagai sektor dengan biaya tertinggi dalam penanganan kasus kebocoran data. Hal tersebut akan berdampak pada keuangan organisasi bahkan dapat berdampak kepada kepercayaan konsumen. Oleh sebab itu, para pelaku institusi pendidikan di seluruh dunia perlu melakukan tindakan preventif untuk mencegah kejadian kasus serupa termasuk Indonesia.

Indonesia juga mengalami kasus terkait keamanan informasi. Berdasarkan laporan dari ID-CERT *spam* (upaya pengiriman pesan secara beruntun tanpa dikehendaki oleh pihak penerima) merupakah kasus terbanyak sepanjang tahun 2017. Selanjutnya, ID-Cert (2017) melaporkan bahwa telah terjadi *phising* (pencurian identitas pengguna pada saat melakukan *login* di situs palsu) di sebuah situs sekolah di Indonesia terkait *login* palsu ke universitas di luar negeri.

Peristiwa yang terjadi baik pada institusi pendidikan secara global maupun kondisi keamanan informasi di Indonesia perlu menjadi perhatian bagi para pelaku penyelenggara institusi pendidikan di Indonesia. Hal tersebut dikarenakan mayoritas institusi pendidikan sudah mulai memanfaatkan teknologi informasi (TI). Salah satu bentuk pemanfaatan TI di institusi pendidikan, yaitu adanya sistem pembelajaran elektronik atau biasa disebut dengan *elearning*. *Elearning* merupakan

suatu metode pembelajaran menggunakan perangkat elektronik dan media *digital* (Chistensson, 2015).

Berbagai institusi pendidikan di Indonesia umumnya telah menerapkan sistem pembelajaran elektronik atau *elearning*. Politeknik Negeri Batam atau biasa disebut Polibatam merupakan salah satu perguruan tinggi yang telah meimplementasikan sistem pembelajaran elektronik sejak tahun 2007. Berdasarkan pedoman pembelajaran mahasiswa Politeknik Negeri Batam (2016) sistem pembelajaran elektronik dapat mempermudah dalam proses belajar mengajar karena mahasiswa dapat mengakses materi dari setiap mata kuliah di manapun dan kapanpun selama terhubung dengan internet. Selain itu, dapat digunakan untuk mengerjakan tugas, kuis, UTS, dan UAS sampai mengelola nilai. Sistem tersebut akan terus dikembangkan untuk dapat memberikan layanan pembelajaran jarak jauh (LPJJ). Penyelenggaraan sistem pembelajaran elektronik didasarkan atas Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional pasal 15.

Seiring dengan peningkatan jumlah mahasiswa dari tahun ke tahun sistem pembelajaran elektronik harus diselenggarakan secara aman. Salah satu tujuannya untuk meningkatkan kepercayaan publik. Hal tersebut sesuai dengan Undang-Undang (UU) Nomor 11 Tahun 2008 pasal 15 ayat 1 tentang Informasi dan Transaksi Elektronik (ITE) dan Peraturan Pemerintah (PP) Republik Indonesia Nomor 82 tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik pasal 20 ayat 1 dan 2.

Sebagai bentuk implementasi undang-undang yang berlaku pihak Kementrian Komunikasi dan Informatika (Kemkominfo) Republik Indonesia mengharapkan organisasi yang menyelenggarakan sistem elektronik dapat melakukan sertifikasi SNI ISO 27001 terkait keamanan informasi. Kondisi organisasi yang akan melakukan sertifikasi diharapkan berada pada tingkat kematangan III+ (Tim Direktorat Keamanan Informasi, 2011). Dengan kata lain, terdapat suatu *gap* antara kondisi yang diharapkan dengan kondisi sebenarnya. Oleh sebab itu, perlu dilakukan penilaian terkait dengan sejauh mana penerapan keamanan informasi di suatu organisasi.

Ada beberapa alat penilaian yang dapat digunakan terkait keamanan informasi di institusi pendidikan. Misalnya dengan menggunakan ISO 27001:2013 (Candiwan, et al., 2015), COBIT (Khther, et al., 2013), gabungan antara COBIT 4.1, ITIL v.3, dan ISO 27001 (Suwito, et al., 2016), dan Indeks KAMI (Septanto, 2017). Pada penelitian ini akan digunakan alat penilaian yang disusun oleh Kementrian Komunikasi dan Informatika (Kemkominfo) Republik Indonesia, yaitu indeks keamanan informasi (KAMI).

Indeks KAMI didasarkan atas SNI ISO 27001:2013. Terdapat 5 komponen di dalam Indeks KAMI, yaitu: tata keola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, dan teknologi. Pada penelitian ini akan dinilai terkait dengan komponen teknologi karena tingginya ketergantungan organisasi terhadap teknologi. Hal itu mengakibatkan perlu adanya perhatian khusus terkait dengan komponen teknologi. Oleh sebab itu, penting melakukan penilaian atas pengamanan teknologi yang telah dilakukan.

KAJIAN PUSTAKA

Informasi Sebagai Aset

Menurut Hutahaean (2015) terdapat lima jenis utama sumber daya, yaitu *man* (sumber daya manusia), *material* (sumber daya material), *machine* (sumber daya peralatan termasuk fasilitas dan energi), *money* (sumber daya keuangan), dan *information* (sumber daya informasi termasuk data). Sumber daya manusia, material, dan keuangan tergolong dalam sumber daya fisik karena sumber-sumber tersebut memiliki wujud secara fisik, sedangkan sumber daya informasi

Journal of Business Administration Vol 3, No.1, Maret 2019, hlm, 162-171

tergolong dalam sumber daya konseptual karena sumber daya tersebut memiliki nilai dari apa yang diwakilinya.

Konsep Keamanan Informasi

Menurut Andress (2014) terdapat tiga konsep utama dalam keamanan informasi, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Kerahasiaan (*confidentiality*) mengacu pada kemampuan untuk melindungi data dari orang-orang yang tidak berwenang untuk melihatnya. Integritas (*integrity*) mengacu pada kemampuan untuk mencegah dari pengubahan pada pihak yang tidak berwenang dan kemampuan untuk membalikkan perubahan pada pihak berwenang yang perlu dibatalkan. Ketersediaan (*availability*) mengacu pada kemampuan untuk mengakses data ketika data dibutuhkan.

Sistem Pembelajaran Elektronik

Sistem pembelajaran elektronik sering dikaitkan dengan institusi pendidikan. Sistem tersebut diselenggarakan melalui jaringan internet, CD, satelit, dan telepon (Broadbent, 2013). Hal serupa dinyatakan oleh Chistensson (2015) bahwa sistem pembelajaran elektonik merupakan suatu metode pembelajaran menggunakan perangkat elektronik dan media digital. Dengan kata lain, dapat disimpulkan bahwa sistem pembelajaran elektronik merupakan cara pelaksanaan kegiatan belajar dan mengajar yang menggunakan sistem elektronik.

Indeks Keamanan Informasi

Berdasarkan panduan penerapan tata kelola keamanan informasi bagi penyelenggara pelayanan publik (2011) indeks keamanan informasi (KAMI) adalah suatu alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi bagi penyelenggara pelayanan publik, seperti instansi pemerintah intitusi pendidikan. Indeks KAMI tidak diarahkan untuk menganalisis efektifitas keamanan yang sudah berjalan, tetapi diarahkan untuk memberikan gambaran kondisi kelengkapan dan kematangan keamanan informasi kepada pimpinan. Evaluasi ini dilakukan terhadap berbagai area yang menjadi sasaran penerapan keamanan informasi dengan lingkup uraian semua bagian keamanan informasi pada standar SNI ISO 27001:2013 (versi bahasa Indonesia). Evaluasi ini dapat digunakan oleh badan penyelenggara publik (seperti, instansi pemerintahan) dari berbagai ukuran maupun tingkatan. Hasil dari evaluasi ini dapat digunakan untuk memberikan langkah perbaikan terkait keamanan informasi yang sudah berjalan. Selain itu, Indeks KAMI dapat digunakan untuk mempersiapkan organisasi dalam sertifikasi standar SNI ISO 27001:2013.

METODE PENELITIAN

Teknik Pengambilan Sampel

Tipe yang akan digunakan dalam penelitian ini adalah pengambilan sampel berdasarkan pertimbangan tertentu (*judgement sampling*). Pihak yang akan dijadikan sampel pada penelitian ini berjumlah empat orang yang bekerja di UPT-SI Polibatam.

Teknik Pengumpulan Data

Pengumpulan data menggunakan teknik kuesioner dan wawancara. Kuesioner dalam penelitian ini diadopsi dari Indeks Keamanan Informasi (KAMI) versi 3.1 (15 April 2015) yang telah disusun oleh Kemkominfo RI berdasarkan SNI ISO 27001:2013 (Kemkominfo RI, 2015). Dua aspek yang akan dinilai, yaitu kategori sistem elektronik dan pengamanan teknologi. Wawancara dilakukan untuk meninjau lebih dalam terkait pertanyaan kuesioner.

Tahapan Penilaian

1. Penentuan ruang lingkup
2. Penentuan kategori sistem elektronik

3. Proses penilaian tingkat kematangan pengamanan teknologi dan pengkajian hasil indeks keamanan informasi

Hasil dan Pembahasan

Ruang Lingkup Penilaian Pengamanan Teknologi

1. Organisasi dan lokasi
   a. Nama Organisasi
      Politeknik Negeri Batam
   b. Lokasi
      Batam Centre, Jl. Ahmad Yani, Tlk. Tering, Batam Kota, Kota Batam, Kepulauan Riau 29461, Indonesia
2. Aset
   a. Data dan Informasi
      Termasuk data dan informasi yang dihasilkan oleh elearning dari berbagaijurusan di Politeknik Negeri Batam (jurusan teknik mesin, teknik elektronika, teknik informatika, dan manajemen bisnis)
   b. Perangkat Lunak
      Aset perangkat lunak, antara lain, seperti *software tool* (antivirus) dan *operating system* (OS).
   c. Perangkat Keras
      Aset perangkat keras, antara lain, seperti *personal computer* (PC), laptop, dan media penyimpanan data lainnya.
   d. Perangkat Jaringan Komunikasi
      Aset perangkat jaringan komunikasi, antara lain, seperti *firewall* dan *switch*.
   e. Fasilitas Pendukung
      Aset fasilitas pendukung, antara lain, seperti server.
   f. Sumber Daya Manusia
      Aset sumber daya manusia, antara lain, seperti karyawan dan mahasiswa di lingkungan Politeknik Negeri Batam.

Kategori Sistem Elektronik

Ringkasan penilaian kategori sistem elektronik (sistem pembelajaran elektronik) dapat dilihat pada tabel 1.

Tabel 1 Ringkasan Penilaian Kategori Sistem Elektronik

Total Skor			15
Kategori Sistem Elektronik			Rendah
Ketentuan Penilaian			
Kategori Sistem Elektronik	Strategis	Tinggi	Rendah
Total Skor	36-50	16-35	10-15

Sumber: Hasil Olah Data Peneliti

Berdasarkan penilaian kategori sistem elektronik (sistem pembelajaran elektronik) sistem elektronik yang diselenggarakan oleh Politeknik Negeri Batam termasuk kategori rendah dengan nilai 14. Pada Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi Pasal 4 Ayat 3 disebutkan bahwa sistem elektronik rendah merupakan sistem elektronik yang tidak memiliki dampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara atau pertahanan dan keamanan negara serta tidak berdampak juga pada daerah tertentu.

Ada beberapa hal yang mengakibatkan kategori sistem elektronik (sistem pembelajaran elektronik) Politeknik Negeri Batam berstatus rendah, diantaranya sebagai berikut.

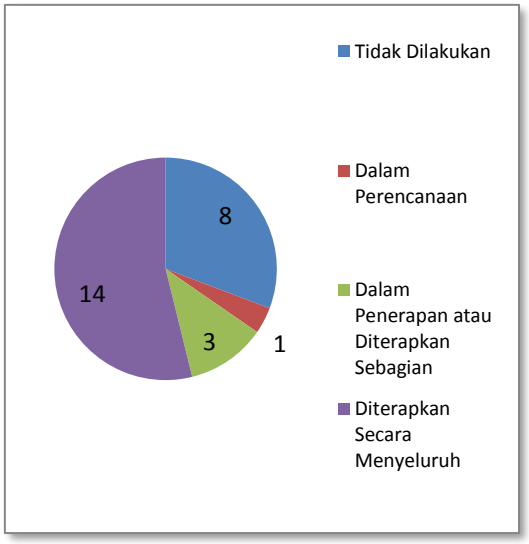
1. Nilai investasi dari sistem pembelajaran elektronik di bawah Rp 3 Miliar.
2. Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan sistem pembelajaran elektronik kurang dari Rp 1 Miliar.
3. Tingkat kekritisan proses yang ada dalam sistem pembelajaran elektronik (jika terjadi upaya penyerangan atau penerobosan keamanan informasi) tidak berdampak bagi kepentingan orang banyak.
4. Dampak dari kegagalan sistem pembelajaran elektronik hanya berdampak kepada internal Politeknik Negeri Batam saja.

Journal of Business Administration Vol 3, No.1, Maret 2019, hlm, 162-171

5. Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem pembelajaran elektronik hanya berdampak pada gangguan operasional saja tanpa membahayakan dan merugikan finansial.

Penilaian Tingkat Kematangan Pengamanan Teknologi

Terdapat 26 komponen pengamanan teknologi yang dinilai, antara lain, yaitu segmentasi jaringan, perlindungan internet lebih dari 1 lapis, konfigurasi standar, penggunaan log, penerapan enkripsi, penggunaan password, instalasi dan pembaruan antivirus, dan audit eksternal terkait keamanan informasi. Ringkasan penilaian pengamanan teknologi sistem elektronik (sistem pembelajaran elektronik) dapat dilihat pada gambar 1.



Gambar 1 Status Pengamanan Tingkat Kematangan Pengamanan Teknologi
Sumber: Hasil Olah Data Peneliti

Berdasarkan pada gambar 1, ada beberapa status pengamanan dari hasil penelitian, yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh. Bentuk pengamanan yang tidak dilakukan berjumlah 8 komponen. Berikut rinciannya.

1. Analisis kepatuhan konfigurasi standar secara rutin.
2. Semua *log* dianalisis secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).
3. Sistem pembelajaran elektronik secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama.
4. Akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis.
5. Ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengonfirmasi bahwa *antivirus*/*antimalware* telah dimutakhirkan secara rutin dan sistematis
6. Setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba.
7. Penerapan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun.
8. Keterlibatam pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.

Bentuk pengamanan dengan status dalam perencanaan hanya 1 komponen terkait dengan keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan sesuai kebutuhan/persyaratan yang ada. Selain itu, 3 komponen pengamanan yang berstatus dalam penerapan atau diterapkan sebagian. Berikut rinciannya.

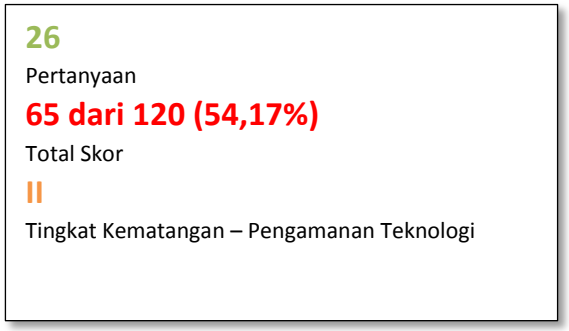
1. Sistem pembelajaran elektronik sudah menerapkan pembatasan waktu akses terkait otomatisasi proses *timeouts*, tetapi tidak menerapkan *lockout* setelah kegagalan login.
2. Penerapan pengamanan akses jaringan nirkabel dari pihak yang tidak resmi sudah dilakukan, tetapi untuk jaringan kabel belum sepenuhnya diamankan.

3. Sistem operasi Windows 10 untuk setiap perangkat *desktop* secara otomatis dimutakhirkan, tetapi perangkat yang masih menggunakan sistem operasi di bawah Windows 10 belum sepenuhnya diamankan.

Terakhir, status pengamanan diterapkan secara menyeluruh berjumlah 14 komponen. Berikut rinciannya.

1. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan.
2. Jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dan lain-lain).
3. Tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
4. Jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
5. Keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
6. Setiap perubahan dalam sistem informasi secara otomatis terekam di dalam *log*.
7. Upaya akses oleh yang tidak berhak secara otomatis terekam di dalam *log*.
8. Penerapan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.
9. Memiliki standar dalam menggunakan enkripsi.
10. Menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya.
11. Menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi.
12. Setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*).
13. Adanya laporan penyerangan virus/*malware* yang gagal/sukses ditindaklanjuti dan diselesaikan.
14. Keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.

Gambar 2 Hasil Tingkat Kematangan



Pengamanan Teknologi
Sumber: Hasil Olah Data Peneliti

Berdasarkan hasil perhitungan tingkat kematangan dengan menggunakan Indeks Keamanan Informasi versi 3.1, total skor yang didapatkan adalah 65 atau 54,17% dari total skor maksimum. Oleh sebab itu, tingkat kematangan pengamanan teknologi berada pada tingkat kematangan II.

Berdasarkan dari hasil tersebut tingkat kematangan pengamanan teknologi sistem elektronik (sistem pembelajaran elektronik) Politeknik Negeri Batam (Polibatam) di bawah tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi, yaitu III+, khususnya terkait dengan pengamanan teknologi. Berdasarkan hasil wawancara posisi Polibatam masih dalam tahap pengembangan organisasi. Selain itu, fokus organisasi masih terkait hal-hal operasional, belum bersifat strategis. Hal tersebut sesuai dengan konfirmasi dari Kepala UPT-SI Polibatam.

"Iya (lebih operasonal level), karena kebutuhan yang kayaknya lebih mendesak adalah diketersediaan, dikonfirmasi sekarang itu sangat mendesak, tapi kalau dilihat di sini itu hampir semua itu

Journal of Business Administration Vol 3, No.1, Maret 2019, hlm, 162-171

ketersediaan yang difokus masih di sana. Kita belum sampai ke, yang ada ini (level strategis) diuji kehandalannya itu enggak sampai, belum fokusnya untuk ke situ. Mungkin nantinya sih ya ada rencana ke depan, ada divisi yang bagian ya development, ada divisi bagian dia uji kehandalan itu idealnya, tapi kita karena terbatas SDM juga." (A, Kepala UPT-SI Polibatam)

Kesimpulan dan Saran

Kesimpulan

Penelitian ini bertujuan untuk mengidentifikasi sejauh mana pengamanan teknologi pada sistem pembelajaran elektronik yang sudah diterapkan Politeknik Negeri Batam dengan menggunakan indeks keamanan informasi. Berdasarkan hasil dan pembahasan dapat disimpulkan sebagai berikut.

1. Sistem elektronik (sistem pembelajaran elektronik) yang diselenggarakan oleh Politeknik Negeri Batam termasuk kategori rendah. Ada beberapa hal yang mengakibatkan kategori sistem elektronik tersebut berstatus rendah, yaitu sebagai berikut:

a. Nilai investasi dari sistem pembelajaran elektronik di bawah Rp 3 Miliar.
b. Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan sistem pembelajaran elektronik kurang dari Rp 1 Miliar.
c. Tingkat kekritisan proses yang ada dalam sistem elektronik elektronik (jika terjadi upaya penyerangan atau penerobosan keamanan informasi) tidak berdampak bagi kepentingan orang banyak.
d. Dampak dari kegagalan sistem elektronik hanya berdampak kepada internal Politeknik Negeri Batam saja.
e. Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik hanya berdampak pada gangguan operasional saja tanpa membahayakan dan merugikan finansial.

2. Berdasarkan hasil penilaian tingkat kematangan pengamanan teknologi total skor yang didapatkan adalah 65 atau 54,17% dari total skor maksimum. Oleh sebab itu, tingkat kematangan pengamanan teknologi berada pada tingkat kematangan II yang berarti tingkat kematangan pengamanan teknologi sistem elektronik (sistem pembelajaran elektronik) Politeknik Negeri Batam (Polibatam) di bawah tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi, yaitu III+ khususnya jika dilhat dari perspektif pengamanan teknologi. Hal ini disebabkan posisi Polibatam masih dalam tahap pengembangan organisasi. Selain itu, fokus organisasi masih terkait hal-hal operasional, belum bersifat strategis.

Saran

Berdasarkan kesimpulan di atas dapat diberikan rekomendasi terkait keamanan informasi, yaitu sebagai berikut.

1. Status rendah pada kategori sistem elektronik (sistem pembelajaran elektronik) mengindikasikan bahwa Polibatam perlu menerapkan keamanan informasi sesuai dengan indeks keamanan informasi (KAMI). Hal tersebut sesuai dengan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi Pasal 7 Ayat 3.
2. Pengamanan teknologi yang berstatus dalam penerapan atau diterapkan sebagian dan dalam perencanaan dapat dimasukkan ke dalam program kerja untuk jangka pendek dan menengah, sedangkan pengamanan teknologi yang berstatus tidak dilakukan dapat dimasukkan ke dalam rencana strategis jangka panjang.
3. Sebagai bentuk *monitoring* terkait peningkatan tingkat kematangan pengamanan teknologi pihak UPT-SI Polibatam dapat menggunakan indeks keamanan informasi (KAMI) secara

berulang. Selanjutnya, pihak UPT-SI dapat melakukan penilaian di area yang lain, seperti tata keola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, dan pengelolaan aset informasi,

4. Bagi penelitian selanjutnya, dapat melakukan evaluasi di area yang lain, seperti mengevaluasi dukungan manajemen terkait keamanan informasi dan kesadaran *end-user* (pengguna akhir) terkait keamanan informasi.

REFERENSI

Andress. (2014). *The Basics of Information Security: Understanding the Fundamentals of Infosec in Theory and Practice.* Waltham: Syngress.

Broadbent, B. (2013). *Summary: ABCs of e-Learning: Review and Analysis of Broadbent's Book.* Canada: Primento.

Candiwan, Sari, P. K., & Nurshabrina, N. (2015). Assessment of Information Security Management on Indonesian Higher Education Institutions. *Advanced Computer and Communication Engineering Technology*, 375-385.

Chistensson, P. (2015, November 5). *Elearning*. Retrieved Maret 7, 2018, from techterms.com: https://techterms.com/definition/e-learning

Gartner. (2018, Januari 16). *Gartner Says Global IT Spending to Reach $3.7 Trillion in 2018*. Retrieved Maret 2, 2018, from Gartner.com: https://www.gartner.com/newsroom/id/3845563

Gemalto. (2017). *Poor Internal Security Practices Take a Toll.* Belcamp: Gemalto.

Huizhi, C. (2017, Mei 22). *Held for selling information on students*. Retrieved Maret 6, 2018, from Shine: https://www.shine.cn/archive/metro/society/Held-for-selling-information-on-students/shdaily.shtml

Hutahaean. (2015). *Konsep Sistem Informasi.* Yogyakarta: Deepublish.

ID-Cert. (2017). *Laporan Akhir Tahun 2017*. Jakarta: ID-Cert.

Indonesia, P. R. (2003). *Undang-Undang Republik Indonesia nomor 20 tahun 2003 tentang Sistem pendidikan nasional.* Jakarta: Pemerintah Republik Indonesia.

Indonesia, P. R. (2008). *Undang-Undang Republik Indonesia. Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.* Jakarta: Pemerintah Republik Indonesia.

Indonesia, P. R. (2012). *Peraturan Pemerintah (PP) Republik Indonesia Nomor 82 tahun 2012* . Jakarta: Pemerintah Republik Indonesia.

Kemetrian Komunikasi dan Informatika (Kemkominfo) RI. (2015). *Indeks Keamanan Informasi versi 3.1 (15 April 2015).* Jakarta: Kemetrian Komunikasi dan informatika RI.

Khther, R. A., & Othman, M. (2013). Cobit Framework As A Guideline Of Effective It Governance In Higher Education: A Review. *International Journal of Information Technology Convergence and Services*, 21-29.

Polibatam. (2016). *Pedoman Pembelajaran Mahasiswa Politeknik Negeri Batam.* Batam: Polibatam.

Ponemon Institute LLC. (2017). *2017 Cost of Data Breach Study.* Michigan: Ponemon Institute LLC.

Septanto, H. (2017). Penilaian Tata Kelola Elearning Kelas Shift DenganMenggunakan Kriteria

StandarIndeks KAMI di STMIK Bina Insani Bekasi. *BINA INSANI ICT JOURNAL*, 67-72.

Suwito, M. H., Matsumoto, S., Kawamoto, J., Gollmann, D., & Sakurai, K. (2016). An Analysis of IT Assessment Security Maturity in Higher Education Institution. *Information Science and Applications*, 701-713.

Tim Direktorat Keamanan Informasi. (2011). *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik.* Jakarta: Direktoat Keamanan Informasi Kementrian Komunikasi dan Informatika Republik Indonesia.