DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Penelitian ini bertujuan untuk menilai dan mengevaluasi implementasi sistem keamanan teknologi informasi yang sudah diterapkan Universitas Nusantara pada sistem penyimpanan elektronik dengan menggunakan indeks keamanan informasi. Serta memahami kontribusi teori sosio-teknis sistem dalam implementasi keamanan teknologi informasi yang sudah diterapkan Universitas Nusantara pada sistem penyimpanan elektronik dengan menggunakan indeks keamanan informasi. Penelitian ini merupakan penelitian yang menggunakan analisis deskriptif baik pada pendekatan kuantitatif maupun kualitatif. Sampel pada penelitian ini adalah sistem penyimpanan elektronik milik Universitas Nusantara yang saat ini masih dikelola secara pribadi oleh organisasi yang disebut dengan Sistem Dokpol. Jumlah pengguna dari sistem ini sebanyak 356 orang. Data dianalisis dengan menilai indeks KAMI selanjutnya dilakukan metode *coding*. Hasil penilaian indeks KAMI terhadap sistem dokpol diperoleh hasil bahwa tingkat kematangan sistem dokpol Universitas Nusantara berada pada tingkat I s/d I+. Artinya, sistem dokpol Universitas Nusantara belum memiliki kematangan yang cukup untuk mencapai SNI ISO 27001:2013. Selain itu, pengevaluasian terhadap tingkat kesiapan sistem dokpol masih dalam lingkup kerangka kerja dasar. Pendalaman informasi dengan tujuan menggali kontribusi teori STS di dalam indeks KAMI diperoleh bahwa dimensi sosial yang terdiri dari struktur organisasi dan manusia memiliki atribut seperti kemampuan, norma dan nilai, pola kebiasaan, budaya, pengetahuan, otoritas, struktur dan kontrol, sistem penghargaan dan kebijakan baik yang berlaku bagi individu, tim atau hubungan antar orang yang terlibat di dalam penggunaan sistem dokpol. Selanjutnya, dimensi teknis terdiri dari teknologi dan tugas yang memiliki atribut hardware, software, peralatan, keamanan fisik, keamanan siber, lingkungan internal, informasi, proses dan teknik yang digunakan dalam menyelesaikan tugas di setiap aktivitas serta pengorganisasian pekerjaan. Analisis penilaian keamanan informasi menggunakan Indeks KAMI masih dapat dijadikan sebagai kerangka penelitian untuk menilai keamanan informasi dari suatu instansi terutama instansi pemerintahan. Selain itu, penelitian mengenai kontribusi teori sosio-teknis sistem dengan menggunakan kerangka keamanan yang tersedia masih terbatas dilakukan di Indonesia.

Kata kunci: Keamanan informasi, Indeks KAMI, Teori sosio-teknis sistem, Tingkat kematangan, Tingkat kelengkapan.

ABSTRACT

This study aims to assess and evaluate the implementation of information technology security systems that have been implemented by Nusantara University on electronic storage systems by using an information security index. In addition, it also aims to understand the contribution of socio-technical system theory in the implementation of information technology security that has been applied by Nusantara University to electronic storage systems by using an information security index. This research is a research that uses descriptive analysis in both quantitative and qualitative approaches. The sample in this study is the electronic storage system belonging to the University of Nusantara which is currently being managed privately by an organization called the Dokpol System. The number of users of this system is 356 people. The data were analyzed by assessing the KAMI index, then the coding method was used. The results of the evaluation of the KAMI index on the docpol system showed that the maturity level of the Dokpol system at Nusantara University was at the I to I+ level. This means that the Nusantara University docpol system does not yet have sufficient maturity to achieve SNI ISO 27001:2013. In addition, evaluating the level of readiness of the Dokpol system is still within the scope of the basic framework. Seeing the in-depth information with the aim of exploring the contribution of STS theory in the KAMI index, it was found that the social dimension consisting of organizational structure and people has attributes such as abilities, norms and values, patterns of habits, culture, knowledge, authority, structure and control, reward systems and good policies that apply to individuals, teams or relationships between people involved in the use of the Dokpol system. Furthermore, the technical dimension consists of technology and tasks that have attributes of hardware, software, equipment, physical security, cyber security, internal environment, information, processes and techniques used in completing tasks in each activity and organizing work. Information security assessment analysis by using the KAMI Index can still be used as a research framework for assessing the information security of an agency, especially government agencies. In addition, research on the contribution of socio-technical systems theory by using available security frameworks is still limited in Indonesia.

Key words: Information security, KAMI Index, System socio-technical theory, Maturity level, Completeness level.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Pemanfaatan teknologi, khususnya internet, secara masif menandakan bahwa teknologi telah mendominasi kehidupan manusia. Internet dianggap sebagai teknologi kunci dari media komunikasi atau jembatan informasi. *Hootsuite We are digital* (2020), sebuah lembaga survei data digital melaporkan bahwa dari populasi manusia di dunia sebesar 7,75 miliar orang, sebanyak 67% orang merupakan *mobile user*. Sekitar 84% di antaranya adalah pengguna yang aktif berinteraksi di media sosial. Dalam datanya juga disebutkan bahwa jumlah pengguna yang memanfaatkan teknologi internet sebanyak 88%. Artinya bahwa teknologi telah menjadi pilihan penting dalam keseharian manusia terutama dalam bidang komunikasi atau pertukaran informasi.

Selain berdampak pada individu, teknologi juga penting bagi organisasi karena teknologi memberikan kemudahan akses informasi yang bermanfaat bagi manajemen atau tata kelola guna merencanakan, mengendalikan, maupun menentukan keputusan (Ramadhan, 2019). Perkembangan teknologi menciptakan lingkungan bisnis yang modern, dinamis, dan kompetitif sehingga organisasi dituntut untuk melakukan pengembangan secara konstan (Coombs & Bierly, 2006). Oleh karena itu, adopsi TI menjadi sangat esensial untuk mendukung keberlangsungan dan pertumbuhan organisasi (Ali *et al.*, 2012; Selig, 2015). Berdasarkan informasi yang diperoleh dari

Gartner (2018), pengeluaran teknologi informasi secara meluas diprediksi menyentuh angka $3,7 miliar pada medio 2018 atau mengalami peningkatan 4,5% dari medio 2017. Data yang dihimpun oleh Katadata (2020) juga menyebutkan bahwa beberapa perusahaan besar seperti Amazon Web Services (AWS) yang dimiliki oleh Amazon meningkatkan pengeluaran di bidang TI untuk mendukung perusahaan dalam transformasi digital. Hasilnya, Amazon melaporkan pendapatan AWS mencapai $10,8 miliar untuk kuartal kedua tahun 2020 atau terjadi pertumbuhan pendapatan sebesar 29%, jika dibandingkan dengan kuartal kedua 2019 sebesar $8,3 miliar. Dampak peningkatan tersebut, secara korporasi menyebabkan peningkatan penjualan Amazon menjadi $88,9 miliar, di mana AWS berhasil menyumbang 12,1% dari pendapatan Amazon. Penjualan ini diperoleh dari pendapatan bersih sebesar $5,2 miliar karena pemanfaatan TI.

Peningkatan pada pengeluaran teknologi informasi memberi sinyal bahwa kian tinggi organisasi, semakin bergantung kepada teknologi informasi. Namun, kebergantungan itu dapat dijadikan sebagai sesuatu yang memicu risiko atau bahaya (Kristiyono, 2015). Perihal tersebut terjadi akibat adanya ancaman yang dialami oleh organisasi atas pemakaian teknologi informasi dengan munculnya berbagai masalah keamanan. Satu dari sekian banyak masalah keamanan informasi, yaitu kebocoran data. Berdasarkan pelaporan dari Gemalto (2017), secara global pada semester satu tahun 2017 terjadi 1.901.866.611 kebocoran data. Hasil itu menandakan bahwa setiap hari terdapat kehilangan data sejumlah 10.507.550. Berdasarkan jenis data, sejumlah 74% kebocoran data terjadi akibat insiden mengenai kehilangan identitas (*identity theft*).

Berdasarkan pada pelaku insiden sekitar 74% kebocoran data terjadi akibat perilaku pihak eksternal (*malicious outsider*).

Pada tahun 2017 lembaga kependidikan memperoleh perhatian internasional akibat terjadi kebocoran data yang cukup meningkat dan berkategori cukup besar dibanding sektor lainnya (Gemalto, 2017). Pada waktu itu jumlah data yang hilang mengalami peningkatan tajam, yakni menyentuh angka 32.000.000 atau mengalami kenaikan 4.957% dari semester pertama tahun 2017.

Permasalahan lain yang pernah terjadi, yaitu kebocoran data pada tahun 2017 di lembaga pendidikan di Tiongkok. Mantan kepala bagian pemasaran di pendidikan swasta di Tiongkok memperjualbelikan jutaan informasi pribadi mahasiswa kepada perusahaan. Hasil dari tindakan itu memberi keuntungan pribadi kepada tersangka sejumlah 10.000 Yuan atau US$1.450 (Huizhi, 2017). Terkait permasalahan tersebut, organisasi yang terdampak dari kebocoran data perlu menangani dan berupaya menuntaskan kasus tersebut. Penanganan memerlukan sejumlah anggaran dana, seperti anggaran untuk menginvestigasi kasus kebocoran data.

Dalam pelaporan Ponemon Institute LLC medio 2017 dijelaskan bahwa secara luas anggaran dana terkait kebocoran data di lembaga kependidikan berkisar sejumlah $200 per data. Lembaga kependidikan menempati posisi keempat sebagai bidang berbiaya tinggi terkait penyelesaian masalah kebocoran data. Perihal itu jelas akan mengakibatkan kondisi finansial organisasi, bahkan berakibat langsung ke tingkat kepercayaan pengguna selaku konsumennya (Malhotra dan Malhotra, 2011). Atas dasar itu, pelaku lembaga kependidikan di semua negara harus menindak atau

melakukan pencegahan terkait kasus yang sama, termasuk Indonesia. Indonesia pun turut mengalami permasalahan perihal keamanan informasi.

Berdasarkan pelaporan yang diperoleh dari ID-CERT *spam* (usaha mengirim secara kontinu tanpa diinginkan penerima) merupakan kasus yang menempati peringkat satu selama 2017. Berikutnya, ID-CERT (2017) menyampaikan laporan bahwa sudah ada upaya mencuri identitas ketika melaksanakan login ke laman *web* palsu (*phishing*) di sebuah laman *web* sekolah di Indonesia, yakni mengenai login palsu ke universitas luar negeri. Kejadian yang menimpa lembaga pendidikan secara global maupun situasi keamanan informasi di Indonesia harus menjadi simpati bagi pihak yang menyelenggarakan lembaga kependidikan.

Peran TI yang esensial menuntut institusi pendidikan menggunakan teknologi informasi. Wujud penggunaan teknologi informasi di lembaga pendidikan, yakni terdapat sistem elektronik yang berfungsi sebagai penyimpanan seluruh data dan informasi terutama untuk kegiatan kearsipan. Universitas Nusantara sebagai perguruan tinggi sudah mengimplementasikan sistem tersebut sejak 2011. Sistem penyimpanan elektronik ini menampung semua data dan informasi milik Universitas Nusantara, meliputi data keuangan, manajemen, mahasiswa, dosen, dan karyawan. Berdasarkan laporan Direktur Universitas Nusantara pada tanggal 29 April 2021 sistem penyimpanan elektronik yang dimilikinya pernah mengalami serangan siber yaitu virus *ransomware*. *Ransomware* ialah nama dari kelas *malware* (*malicious software*), meliputi dua kata: *ransom* (tebusan) dan *malware*. *Ransomware* melakukan penuntutan berupa pembayaran bagi data/informasi pribadi yang sudah tercurinya, atau data

dengan akses yang terbatasi (terenkripsi). Atas kejadian tersebut, Universitas Nusantara mengalami kerugian secara finansial dan beberapa data penting tidak dapat dikembalikan karena sudah terinfeksi virus tersebut. Pihak manajemen Universitas Nusantara telah melakukan investigasi untuk mencari faktor penyebab terjadinya kebocoran data tersebut. Atas investigasi tersebut diperoleh hasil bahwa kebocoran data yang terjadi disebabkan oleh beberapa faktor, yakni kelalaian karyawan dalam membuka pos-el (*e-mail*) masuk termasuk *e-mail phising*, tidak adanya peringatan tertulis dari pihak manajemen bahwa pada saat itu *e-mail* organisasi sudah menjadi target dari para pencuri data, dan tidak ada peraturan untuk membatasi akses jelajah internet saat menggunakan jaringan kampus. Namun, dari beberapa faktor penyebab yang telah disebutkan belum secara terperinci dapat menjelaskan dan mengidentifikasi faktor utama penyebab terjadinya kebocoran data tersebut, baik dilihat dari sudut pandang manajemen maupun sudut pandang teknis. Oleh karena itu, penelitian ini menjadi penting mengingat bahwa pihak manajemen organisasi membutuhkan referensi ilmiah dan perlu melakukan sebuah evaluasi terhadap keamanan informasi dari sistem penyimpanan elektronik tersebut.

1.2 Rumusan Masalah

Keamanan informasi merupakan aspek yang perlu diperhatikan dari sebuah sistem informasi. Menurut Jogiyanto (2005) sistem informasi adalah suatu sistem di dalam organisasi yang dapat mengakomodasi kebutuhan pengolahan transaksi harian, mendukung kegiatan operasional, bersifat manajerial dan strategis dari suatu organisasi serta dapat menyediakan informasi berupa laporan yang diperlukan oleh pihak

eksternal. Dikatakan lebih lanjut bahwa suatu sistem informasi harus memiliki kualitas yang dapat diukur dengan keakuratan, ketepatan waktu, dan relevan. Oleh karena itu, keamanan informasi diperlukan untuk menjaga kualitas dari suatu informasi dan penting untuk diperhatikan dalam setiap implementasi sistem informasi.

Dilihat dari sudut pandang teori sistem teknis-sosial (*socio-technical system*), kegagalan yang terjadi pada keamanan informasi dapat dipengaruhi oleh beberapa faktor yaitu *technology, structure, people*, dan *tasks* (Ada *et al*., 2009). Teori ini dapat menjelaskan tentang bagaimana organisasi dapat mengelola tanggung jawab dengan bantuan teknologi. Tanggung jawab di dalam organisasi ini dibebankan kepada manusia yang dikelompokkan ke dalam beberapa fungsi seperti fungsi strategis dan operasional. Dalam menyelesaikan tugas-tugasnya manusia secara tidak sadar membentuk sebuah perilaku. Perilaku itu dapat menciptakan dampak yang baik atau buruk bagi organisasi. Dengan kata lain, bahwa setiap organisasi mempekerjakan orang dengan kemampuan yang bekerja untuk mencapai tujuan organisasi, mengikuti proses, menggunakan teknologi, beroperasi dalam infrastruktur fisik serta berbagi asumsi dan norma budaya tertentu (Emery, 1959).

Umumnya, teori STS juga menjelaskan bahwa kegagalan proses atau program di dalam sebuah organisasi karena terlalu fokus pada aspek sistem seperti teknologi dan tidak dapat menganalisis dan memahami interdependensi kompleks atas kegagalan yang terjadi (Mumford, 2006; Carayon, 2006). Oleh karena itu, dipacu dari adanya kebocoran data yang terjadi pada Universitas Nusantara, organisasi perlu mengevaluasi

penerapan keamanan informasi pada sistem penyimpanan elektronik dengan melihat empat faktor yang ada di dalam teori STS ini.

Berdasarkan Peraturan Pemerintah No. 82 tahun 2012 Pasal 20 Ayat 1 dan 2 terkait Penyelenggaraan Sistem dan Transaksi Elektronik, sistem penyimpanan elektronik dapat dikategorikan sebagai sistem elektronik karena mencakup serangkaian perangkat dan prosedur elektronik untuk mengumpulkan, menyimpan, dan menampilkan informasi elektronik. UU No. 11 Tahun 2008 Pasal 15 Ayat 1 terkait Informasi dan Transaksi Elektronik (ITE) dan Peraturan Pemerintah No. 82 tahun 2012 Pasal 20 Ayat 1 dan 2 terkait Penyelenggaraan Sistem dan Transaksi Elektronik juga mengharapkan sebagai wujud penerapan perundang-undangan, agar organisasi yang melaksanakan sistem elektronik sudah bersertifikasi SNI ISO 27001 mengenai keamanan informasi. Situasi organisasi yang akan melaksanakan sertifikasi pada sistem elektroniknya dalam hal ini yang akan dibahas adalah sistem penyimpanan elektronik setidaknya ada pada taraf kematangan III+ (Tim Direktorat Keamanan Informasi, 2011). Selain itu, dengan kata lain, ada jarak antara situasi yang diinginkan dengan realitas sesungguhnya. Atas dasar itulah, harus melakukan penilaian awal perihal seberapa jauh implementasi keamanan informasi di suatu organisasi. Terdapat beragam instrumen penilaian yang dapat dimanfaatkan mengenai keamanan informasi, terutama di sektor lembaga pendidikan. Sebagai contoh, melalui penggunaan ISO 27001:2013 (Candiwan, *et al*., 2015), COBIT (Khther, *et al*., 2013), penggabungan antara COBIT 4.1, ITIL v.3, dan ISO 27001 (Suwito, *et al*., 2016), dan Indeks KAMI (Septanto, 2017).

Kajian ini akan menggunakan instrumen penilaian atas penyusunan pihak (Kemkominfo) Republik Indonesia, yakni indeks keamanan informasi (KAMI). Indeks KAMI berdasarkan pada SNI ISO 27001:2013. Ada lima bagian/komponen yang terdapat di dalam Indeks KAMI yang akan digunakan dalam mengevaluasi sistem penyimpanan elektronik di Universitas Nusantara, yakni pengelolaan keamanan informasi pada sistem penyimpanan elektronik, tata kelola risiko keamanan informasi pada sistem penyimpanan elektronik, kerangka kerja keamanan informasi sistem penyimpanan elektronik, tata kelola kelola aset informasi yang berada pada sistem penyimpanan elektronik, dan teknologi dari sistem penyimpanan elektronik. Kajian ini akan dinilai menggunakan komponen teknologi karena tingginya ketergantungan organisasi terhadap teknologi. Atas perihal tersebut harus ada perhatian secara khusus mengenai komponen teknologi. Atas dasar itulah, cukup penting dilakukan penilaian upaya pengamanan teknologi yang sudah terlaksanakan.

1.3 Pertanyaan Penelitian

Sesuai masalah kajian yang sudah tersampaikan, pertanyaan kajian yang terajukan sebagai berikut.

1. Bagaimana penerapan sistem keamanan teknologi informasi pada sistem penyimpanan elektronik yang terimplementasikan oleh Universitas Nusantara dengan menggunakan indeks keamanan informasi?
2. Bagaimana kontribusi teori sosio-teknis sistem dalam penerapan sistem keamanan teknologi informasi pada sistem penyimpanan elektronik yang terimplementasikan oleh Universitas Nusantara dengan menggunakan indeks keamanan informasi?

1.4 Tujuan Penelitian

Kajian ini mempunyai dua tujuan, yaitu:

1. untuk menilai dan mengevaluasi implementasi sistem keamanan teknologi informasi yang sudah diterapkan oleh Universitas Nusantara pada sistem penyimpanan elektronik dengan menggunakan indeks keamanan informasi,
2. untuk memahami kontribusi teori sosio-teknis sistem dalam implementasi keamanan teknologi informasi yang sudah diterapkan oleh Universitas Nusantara pada sistem penyimpanan elektronik dengan menggunakan indeks keamanan informasi.

1.5 Kontribusi Penelitian

Kontribusi yang diinginkan dari kajian ini, yakni dapat digunakan oleh manajemen Universitas Nusantara untuk bahan pertimbangan dalam menentukan keputusan terkait keamanan informasi khususnya pada sistem penyimpanan elektronik. Selain itu, hasil kajian ini dapat berkontribusi bagi para akademisi sebagai referensi yang dapat diandalkan untuk penelitian-penelitian selanjutnya, khususnya mengenai keamanan informasi di sektor pendidikan dengan menggunakan teori sosio-teknis sistem.

1.6 Ruang Lingkup dan Batasan Penelitian

Cakupan dan batasan pada kajian ini terbagi atas dua hal. Pertama, pemilihan standar pengukuran yaitu indeks keamanan informasi (Indeks KAMI) yang dirancang

oleh pemerintah Indonesia. Kedua, pemilihan Universitas Nusantara sebagai perusahaan yang akan dieksplorasi pada penelitian ini.

1.7 Sistematika Penulisan

Sistematika penulisan pada kajian ini meliputi lima bab sebagai berikut.

BAB I: PENDAHULUAN

Bab ini terdiri atas latar belakang permasalahan, rumusan permasalahan, pertanyaan, tujuan diadakan kajian, kontribusi penelitian, cakupan dan batasan kajian, serta sistematika penulisan.

BAB II: LANDASAN TEORI DAN TINJAUAN PUSTAKA

Bab ini terdiri atas landasan teori dan tinjauan pustaka pada kajian ini, serta kajian terdahulu. Bab kedua turut memuat identifikasi gap dan kerangka pemikiran.

BAB III: METODE PENELITIAN

Bab ini berisi paparantentang desain penelitian dengan metode kualitatif.

BAB IV: PEMBAHASAN

Bab ini berisi paparan pembahasan hasil penelitian.

BAB V: PENUTUP

Bab ini terdiri atas kesimpulan, saran, dan keterbatasan penelitian.