BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam lingkungan keamanan informasi yang telah menjadi sangat dinamis, penerapan sistem kontrol dan keamanan yang maju sudah tidak lagi cukup untuk melindungi organisasi dari ancaman yang mengintai. Seiring dengan lingkungan usaha yang terus menerus berubah begitu pula ancaman juga terus berevolusi. Ancaman-ancaman yang dihadapi organisasi-organisasi masa kini jauh lebih maju dibandingkan dengan masa sebelumnya, begitu pula teknologi keamanan informasi dan *framework* keamanan informasi yang terus dikembangkan untuk menghadapi ancaman-ancaman yang muncul [1]. Walaupun demikian, insiden-insiden keamanan informasi yang *high-profile* masih terus terjadi, bahkan sebagian terjadi pada perusahaan-perusahaan multinasional. Sebagai contoh, pada tahun 2011 Sony Corporation mengalami kebocoran data pada jaringan *PlayStation Network* yang dikelola perusahaan dengan sekitar 77 juta data pengguna dicuri, termasuk data kartu kredit (Gambar 1.1).

Millions of internet users hit by massive Sony PlayStation data theft

Sensitive personal details of tens of millions of internet users have been stolen by hackers in one of the biggest ever cases of data theft, it has emerged.

By Shane Richmond and Shanerichmond
26 April 2011 • 11:52pm

Gambar 1.1 Potongan Berita Peretasan Sony Playstation (Sumber: The Telegraph)

Di Indonesia sendiri, insiden peretasan atau kebocoran data sudah terjadi beberapa kali, baik pada sistem milik pemerintah maupun swasta. Salah satu insiden peretasan yang cukup *high profile* adalah kebocoran data pengguna Tokopedia yang terjadi pada tanggal 20 Maret 2020. Pada peristiwa tersebut, data dari sekitar 91 juta akun *user* dan 7 juta akun *merchant* diduga dicuri dan dijual di *darkweb* seharga puluhan juta rupiah (Gambar 1.2).

Gambar 1.2 Potongan Berita Kebocoran Data Tokopedia (Sumber: CNN Indonesia)

Ada banyak faktor yang dapat menjadi penyebab hal ini terus-menerus terjadi, salah satunya adalah penerapan atau implementasi tata kelola keamanan informasi yang tidak efektif yang salah satu penyebabnya adalah para eksekutif perusahaan yang kebanyakan belum berani keluar dari *comfort zone* dan masih menggunakan pendekatan lama pada kerangka *information security* [1].

Agar implementasi *framework* tata kelola keamanan informasi (*InfoSec Governance*) dapat berjalan dengan efektif di perusahaan, implementasi harus didukung oleh budaya keamanan perusahaan (*corporate security culture*) dan sistem pengambilan keputusan yang juga dinamis serta adaptif terhadap kebutuhan

keamanan informasi perusahaan. Saat ini, banyak perusahaan yang masih menerapkan metode pengambilan keputusan yang cenderung sentralistik atau terpusat dan masih menggunakan pendekatan *risk management* yang umum dignakan pada abad ke-20 pada keamanan informasi. Pendekatan seperti ini relatif lebih mudah dikelola karena perusahaan hampir tidak memerlukan tata kelola keamanan dibawah *level* puncak perusahaan dimana mayoritas pengambilan keputusan dilakukan serta masih memberi peran untuk tata kelola tambahan, regulasi-regulasi baru, dan metode-metode baru untuk mengatasi tata kelola keamanan organisasi yang lemah [1].

Akan tetapi, pendekatan semacam ini mungkin sudah tidak lagi relevan pada lingkungan keamanan informasi yang telah menjadi semakin kompleks dan dinamis, serta lebih mengedepankan fleksibilitas dan adaptabilitas. Hal ini disebabkan karena pendekatan ini jika diamati dari penerapannya di berbagai perusahaan, cenderung lebih menekankan pada kepatuhan (*compliance*) dan kontrol dibandingkan dengan keamanan informasi itu sendiri. Hal ini dapat berakibat pada divisi IT, terutama bagian yang bertanggung jawab pada keamanan informasi lebih fokus untuk memenuhi *standard* dan kebijakan organisasi dibandingkan meng-*improve* kualitas keamanan sistem sehingga menyebabkan perusahaan kesulitan untuk merespon dengan cepat jika terjadi perubahan pada lingkungan keamanan informasinya [1].

Dalam implementasi *Information Security Governance* (*InfoSec*), ada beberapa *framework* yang sering digunakan, diantaranya COBIT 5 dan ISO27000 yang merupakan versi terbaru dari COBIT dan ISO serta memberikan *framework* yang lebih komprehensif dibandingkan versi sebelumnya [2]. Tetapi kedua

framework masih belum memberikan informasi mengenai *security objective* atau strategi untuk mengimplementasikannya, serta bagaimana organisasi harus mengembangkan tujuan dan strategi keamanan sebagai bagian dari proses *security governance* [3]. Selain itu, masing-masing *framework* memiliki kelebihan dan kekurangan yang beragam sehingga tidak semua dapat digunakan untuk mengaudit jenis perusahaan tertentu.

Ada beberapa penelitian mengenai hubungan antara pendekatan keamanan informasi perusahaan dengan implementasi tata kelolanya di lapangan serta mengenai audit keamanan informasi dengan *framework* COBIT 5. Salah satunya yang telah dilakukan oleh Terrence C.C. Tan, Anthoine B. Ruighaver, dan Atif Ahmad dengan judul penelitian "*Information Security Governance: When Compliance Becomes More Important Than Security*". Penelitian ini menggunakan metode kualitatif dengan melakukan wawancara pada sebagian staff TI perusahaan dan menghasilkan rekomendasi untuk mengubah pendekatan *information security* perusahaan agar sistem keamanan informasi dapat menjadi lebih dinamis, fleksibel, dan lincah.

Penelitian berikutnya dilakukan oleh Dewi Ciptaningrum, Eko Nguroho, dan Dani Adhipta yaitu "Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5". Penelitian ini melakukan pengukuran terhadap kematangan keamanan sistem informasi pada Pemerintah Kota Yogyakarta dengan kerangka COBIT 5 menggunakan pedoman *assessment* pada *domain* EDM03, APO12, APO13, BAI06, dan DSS05. Hasil dari penelitian ini berupa nilai kapabilitas keamanan SI masing-masing *domain* yang didapat dari perhitungan berdasarkan pengumpulan dan pengolahan hasil kuesioner lalu disusul

dengan mengkaji hasil dan praktek dasar COBIT 5 dengan hasil kuesioner [4], yaitu tidak ada satupun dari semua *domain* yang diukur dapat melewati *level* 1 dengan 4 proses mendapat predikat P dan 1 proses mendapat predikat L.

Sebagaimana hasil pencarian jurnal yang telah dilakukan, sebagian besar jurnal yang ditemukan tidak memberi penjelasan yang lengkap mengenai hubungan antara *information security culture* organisasi dengan kapabilitas keamanan sistem informasi perusahaan. Penelitian ini merupakan kelanjutan dari penelitian yang telah dilakukan oleh Terrence C.C. Tan, Anthoine B. Ruighaver, dan Atif Ahmad (2010) yang berjudul "*Information Security Governance: When Compliance Becomes More Important Than Security*" dengan menambahkan metode kuantitatif menggunakan *framework* COBIT 5 dengan fokus pada *domain* APO13 dan DSS05. Secara kualitatif, jurnal ini cukup baik karena dapat memberi penjelasan yang komprehensif tentang pendekatan *security decision-making* dan dampaknya pada staff TI serta implementasi tata kelola keamanan informasi perusahaan serta memberi saran dan rekomendasi berdasarkan temuan yang didapat selama penelitian. Objek penelitian dalam studi kasus ini adalah sebuah perusahaan *franchise* perhotelan di Indonesia yang bernama PT XYZ.

PT XYZ merupakan sebuah jaringan perhotelan bintang 3 di Indonesia yang berbasis di Makassar, Sulawesi Selatan yang didirikan tahun 2004 dan sampai tahun 2020 telah melakukan ekspansi dengan mendirikan *franchise* di Mataram, Malang, Kendari, Blora, dan Bulukumba. Perusahaan ini mengusung konsep "*Where Luxury is Affordable*" yang berarti menyediakan layanan mewah dengan biaya terjangkau. Hotel pertama perusahaan ini didirikan tahun 2004 dengan nama Banua Hotel Makassar. Pada tahun 2014, perusahaan mulai melakukan ekspansi keluar

Makassar dengan mencoba memanfaatkan momentum program pemerintah yang ingin menggenjot pariwisata Indonesia. Layanan TI perusahaan saat ini dikelola oleh divisi TI dan sebagian besar masih terbatas di lingkungan internal sehingga *customer* belum bisa *booking* melalui *website* perusahaan, tetapi *website* hotel sudah memiliki layanan *chat* yang memungkinkan calon *customer* melakukan kontak dengan *customer services* untuk melakukan *booking*.

Pada penelitian yang dilakukan, pengukuran kapabilitas keamanan informasi akan dilakukan pada layanan TI dari salah satu *franchise* dari perusahaan, yaitu Colonial Hotel. Dalam beberapa tahun terakhir, divisi TI telah melakukan audit secara teratur pada tata kelola TI perusahaan, termasuk pada aspek keamanan informasi namun masih belum menggunakan *framework IT Governance* berstandar internasional. Dari hasil observasi awal (*preliminary observation*) dan diskusi dengan manajer TI perusahaan, ditemukan adanya beberapa permasalahan pada tata kelola keamanan informasi perusahaan seperti yang tercantum pada Tabel 1.1.

Tabel 1.1 Temuan Awal Masalah Pada Keamanan Informasi di PT XYZ

No	Temuan Awal	Dampak
1	Belum diterapkannya *two-way authentication* pada sebagian perangkat	Perangkat rentan terhadap akses yang tidak berizin jika kerahasiaan password ter-*compromised*
2	Kurangnya perlindungan fisik pada ruangan server	Ruangan server mudah dimasuki oleh pihak-pihak tidak bertanggung jawab
3	Adanya *gap* komunikasi antara divisi TI dan manajemen perusahaan	Masukan-masukan dari tim TI kurang diperhatikan dalam proses pembuatan kebijakan keamanan informasi

Berdasarkan uraian dari temuan-temuan awal tersebut, maka pengukuran kapabilitas tata kelola keamanan informasi perusahaan perlu dilakukan dengan lebih mendalam menggunakan standar atau kerangka yang dapat dijadikan acuan untuk mendapatkan hasil yang *valid*, diantaranya adalah ITIL (*Information*

Technology Infrastructure Library), COBIT (*Control Objectives for Information and Related Technology*), dan ISO. Pada penelitian ini, pengukuran hanya berfokus pada departemen TI perusahaan untuk mengukur tingkat kapabilitas keamanan informasi menggunakan *framework* COBIT 5 serta hubungannya dengan pendekatan atau budaya keamanan informasi perusahaan yang sudah berjalan selama ini. *Framework* ini dipilih karena proses-proses yang berkaitan dengan keamanan informasi pada COBIT 5 telah terintegrasi kedalam sebuah kerangka *IT Governance* yang lebih luas dan memiliki pengaruh pada proses-proses COBIT lainnya yang tidak berkaitan dengan keamanan informasi. Hal ini dapat mempermudah penelitian selanjutnya yang ingin menemukan hubungan antara tingkat kapabilitas tata kelola TI pada proses-proses yang diukur pada penelitian ini dengan kapabilitas proses-proses COBIT lainnya yang berkaitan.

Dari hasil penelitian ini, divisi TI diharapkan dapat mengetahui hasil evaluasi dari tingkat kapabilitas keamanan informasi dan hubungannya dengan pendekatan keamanan informasi perusahaan, serta menghasilkan rekomendasi yang dapat digunakan untuk meningkatkan pengelolaan keamanan informasi agar mencapai *level* kapabilitas yang diharapkan.

1.2 Batasan Masalah

Batasan masalah dalam penelitian ini yaitu,

1. Kapabilitas implementasi *Information Security Governance* berdasarkan standar *framework* COBIT 5 dengan fokus *domain* APO13 dan DSS05
2. Hubungan antara pendekatan keamanan informasi perusahaan dan metode pengambilan keputusan dengan tingkat kematangan dan kapabilitas *Information Security Governance* perusahaan.

3. Kuesioner audit IT untuk pengukuran tingkat kapabilitas keamanan informasi dengan skala persentase 0 – 100% yang terbagi dalam 4 kategori, yaitu *Not Achieved, Partially Achieved, Largely Achieved, dan Fully Achieved.*
4. Wawancara dengan *IT manager* untuk mendapatkan penilaian kualitatif mengenai pendekatan *IT security* perusahaan.

1.3 Rumusan Masalah

Dari latar belakang yang telah dikemukakan diatas, rumusan masalah yang didapatkan adalah sebagai berikut.

1. Bagaimana hasil pengukuran tingkat kapabilitas tata kelola keamanan informasi dalam departemen TI PT XYZ menggunakan kerangka kerja COBIT 5?
2. Apakah ada hubungan antara pendekatan dan budaya keamanan informasi yang selama ini diterapkan perusahaan, seperti metode *decision making* dengan tingkat kapabilitas implementasi tata kelola keamanan informasi pada layanan TI perusahaan?
3. Bagaimana rekomendasi yang dapat diberikan untuk digunakan atau menjadi bahan referensi bagi perusahaan berdasarkan hasil pengukuran tingkat kapabilitas tata kelola keamanan informasi?

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, maka tujuan yang inign dicapai pada penelitian ini adalah

1. Mengetahui tingkat kapabilitas keamanan sistem informasi pada divisi IT perusahaan.
2. Menganalisa pengaruh budaya keamanan informasi perusahaan dan metode pengambilan keputusan terhadap kematangan implementasi *Information Security* dalam perusahaan.
3. Memberi rekomendasi pada eksekutif dan divisi IT perusahaan untuk mencegah terjadinya insiden serupa yang sudah pernah terjadi dan membuat pendekatan keamanan informasi perusahaan menjadi lebih dinamis, serta membuat sistem tata kelola keamanan informasi yang sesuai standar COBIT 5.

1.4.2 Manfaat Penelitian

Beberapa manfaat yagn dapat diperoleh dari penelitian ini diantaranya,

1. Menambah wawasan dan pengalaman dalam melakukan *assessment* dan evaluasi pada tata kelola keamanan informasi sebuah perusahaan.
2. Bagi perusahaan, penelitian ini dapat digunakan sebagai referensi untuk mengetahui tingkat kapabilitas *Information Security governance* yang ada serta hubungannya dengan budaya perusahaan yang diterapkan saat ini sehingga perusahaan dapat mengambil langkah-langkah perbaikan yang diperlukan.