

BAB I

PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Penelitian dilakukan pada empat Perguruan Tinggi di Bandung. Objek ini dipilih sebagai penelitian berdasarkan ranking sepuluh teratas Perguruan Tinggi yang terletak di Kota Bandung dari situs webometrics.info. *Webometrics Ranking of World Universities* diprakarsai oleh Cybermetrics Lab, sebuah kelompok riset yang dimiliki *Consejo Superior de Investigaciones Cientificas (CSIC)*, riset publik terbesar di Spanyol. Berikut daftar empat Perguruan Tinggi di Bandung yang menjadi objek penelitian:

1) Universitas Padjajaran

Menduduki peringkat 7 Perguruan Tinggi se-Indonesia dan peringkat 1210 dunia. Universitas Padjajaran merupakan perguruan tinggi negeri yang didirikan 11 September 1957.

Lokasi : Jalan Raya Bandung Sumedang Km. 21 Jatinangor, Bandung

Web : www.unpad.ac.id

2) Universitas Islam Negeri Sunan Gunung Djati

Menduduki peringkat 59 Perguruan Tinggi se-Indonesia dan peringkat 4385 dunia. Universitas Islam Negeri Sunan Gunung Djati merupakan perguruan tinggi negeri yang didirikan tanggal 8 Agustus 1968.

Lokasi : Jalan AH Nasution 105, Bandung

Web : www.uinsgd.ac.id

3) Institut Teknologi Nasional

Menduduki peringkat 68 Perguruan Tinggi se-Indonesia dan peringkat 4552 dunia. Institut Teknologi Nasional merupakan perguruan tinggi swasta yang didirikan pada tanggal 14 Desember 1972.

Lokasi : Jalan PKH Mustofa 23, Bandung

Web : www.itenas.ac.id

4) Universitas Telkom

Menduduki peringkat 78 Perguruan Tinggi se-Indonesia dan peringkat 5192 dunia. Universitas Telkom merupakan perguruan tinggi swasta yang didirikan tahun 1990 sebagai STT Telkom dan MBA Bandung dan resmi menjadi Universitas Telkom tahun 2013.

Lokasi : Jalan Telekomunikasi, Bandung

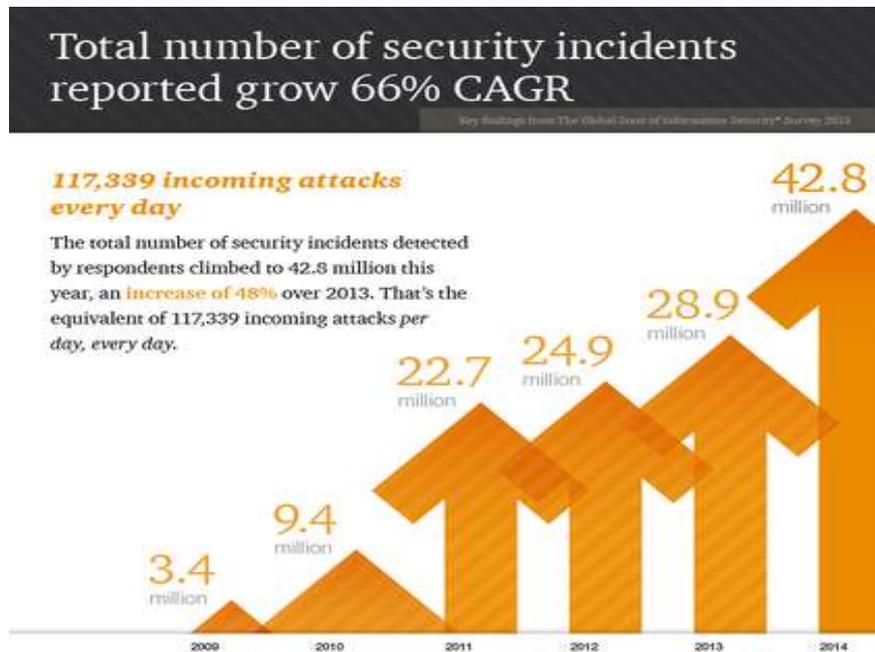
Web : www.telkomuniversity.ac.id

1.2 Latar Belakang Penelitian

Keamanan sistem informasi sangatlah penting bagi organisasi yang menganggap informasi sebagai salah satu asset penting. Menurut PwC, pelanggaran keamanan terus meningkat, baik dari segi jumlah insiden maupun kerugian finansial. Survey PwC pada tahun 2014 menyatakan jumlah insiden pelanggaran keamanan melonjak menjadi 42,800,000 atau 48% lebih besar dari tahun 2013, sedangkan total kerugian finansial mulai dari organisasi kecil hingga organisasi besar meningkat 34% dibanding tahun 2013 (PricewaterhouseCoopers, 2014).

Gambar 1.1

Jumlah Insiden Keamanan Tahun 2009-2014



Sumber: *www.pwc.com* (November 2014)

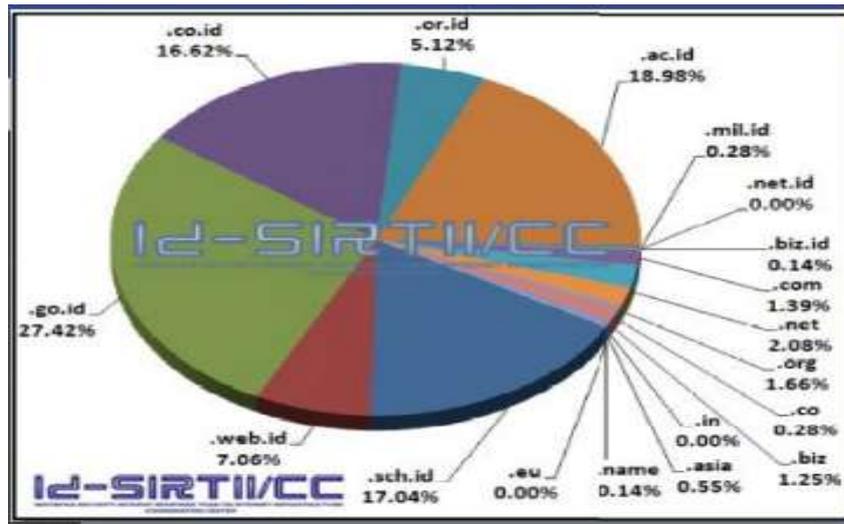
Risiko pelanggaran keamanan, menurut PwC, tidak akan pernah sepenuhnya diatasi. Saat ini lembaga atau organisasi harus tetap waspada dalam menghadapi ancaman yang terus berkembang. Banyak lembaga dan organisasi menyadari pentingnya keamanan informasi sebagai salah satu dari bagian risiko bisnis. Jumlah insiden keamanan dan biaya yang dikeluarkan terus menerus meningkat namun menurut survey yang dilansir PwC menemukan bahwa masih banyak lembaga ataupun organisasi yang tidak memperbaharui baik itu proses keamanan informasi, teknologi dan pelatihan karyawan yang dibutuhkan.

Open Security Foundation dalam *EdTech Magazine* (2014), melansir hasil survey yang menyatakan bahwa sebanyak 35% pelanggaran keamanan terjadi pada institusi pendidikan. Institusi ini dibidik oleh orang-orang yang tidak bertanggung jawab dikarenakan Institusi adalah gudangnya data pribadi. Survey dari *IT leaders* menunjukkan tantangan bagi Institusi pendidikan ke depan, salah

satunya adalah melindungi data pribadi mahasiswa, organisasi dan kekayaan intelektual yang menempati urutan teratas sebesar 79% (Smith, 2014)

Gambar 1.2

Serangan Website Domain Indonesia Tahun 2013



Sumber : Id-SIRTII

Pada gambar 1.2 terlihat bahwa serangan untuk website akademi (ac.id) adalah sebesar 18.98%, angka ini berada di urutan kedua setelah website pemerintahan (go.id) sebesar 27.42%.

Contoh kasus penyerangan keamanan informasi pada institusi pendidikan (A.Yuli, 2010) sebanyak 71 situs yang beberapa diantaranya adalah perguruan tinggi diretas menjelang peringatan kemerdekaan ke 65 Republik Indonesia.

Kasus lainnya (Indonesian Cyber Army, 2014), sebanyak 56 mahasiswa dari Universitas Gunadarma batal diwisuda 19 Oktober 2014 karena terlibat kasus peretasan sistem akademik yang menyebabkan nilai mereka diubah menjadi lebih bagus apabila mereka membayar sejumlah uang.

Kasus peretasan di institusi pendidikan juga terjadi di Universitas Ronggolawe Tuban (Onix, 2014) yang beralamat www.unirow.ac.id, selain

diretas situs ini juga di *deface*. Masih pada sumber yang sama namun di tahun yang berbeda (Onix, 2015), kasus pelanggaran keamanan juga sempat terjadi di kampus IKIP Budi Utomo.

Di Universitas Trisakti, kasus pelanggaran keamanan terjadi pada situs resmi milik universitas tersebut, tim *hacker* Gerandong yang mengaku lebih memilih disebut *security auditor* ketimbang hacker ini menyatakan kalau situs tersebut mudah dibobol dari luar (Sarief, 2010).

Pelanggaran keamanan juga terjadi pada universitas ternama di Indonesia yang terletak di kota Bandung (Onix, 2014), situs Universitas Padjajaran (UNPAD) yang beralamat www.unpad.ac.id berhasil diretas dan di *deface* pada tanggal 18 Juli 2014, bertuliskan pesan sebagai berikut: *"Hacked By PScript with Yuneroz Look Out, Admin is not care about security, you stolen and blame a thieves ! One web got hacked is a tragedy Admin ^_^ We Are : Pscript – Yuneroz – Nabilaholic404 – Bebyyers404 – Panda Dot ID -Papuan ARK- Tsunaomi48 – Gambit – SashiC0de-,"*

Gambar 1.3

Halaman situs UNPAD yang diretas dan di *deface*



Sumber: www.indonesiancyberarmy.com, 2014

Selain UNPAD, Universitas Gadjah Mada juga tidak luput dari serangan hacker (Chandratruna, 2010). Situs portal perpustakaan *online* berhasil di retas. Situs tersebut menyediakan berbagai informasi seputar perpustakaan perguruan tinggi yang telah terhubung.

Selain itu, beberapa praktisi TI bidang Keamanan Informasi juga menyatakan institusi pendidikan rentan terhadap pelanggaran keamanan informasi diantaranya yaitu “*Academic institutions offer a treasure trove of information of interest to cybercriminals. Data is like gold to cybercrooks, universities are like Fort Knox to them.*” (Herold dalam Roman, 2014).

Pernyataan lebih lanjut, “*Securing a university's systems and processes is complex, it requires the institution's management to show a commitment to achieving and maintaining a commercially reasonable level of protection.*” (Brill dalam Roman, 2014) dan “*Universities are prime targets for hackers because they are data-rich environments with multiple access points and a culture of*

collaboration and open sharing of information.” (Lapidus dalam Roman, 2015). Kesimpulan dari ketiga pernyataan praktisi IT tersebut yakni perguruan tinggi menjadi target bagi orang-orang tidak bertanggungjawab termasuk hacker, dikarenakan begitu banyaknya data yang tersimpan maka diperlukan komitmen besar bagi manajemen perguruan tinggi untuk melindungi lingkungan mereka dari berbagai ancaman yang ada.

Untuk dapat meminimalisir ancaman yang terus berkembang, the *International Organization for Standardization (ISO)* dan the *International Electrotechnical Commission (IEC)* mempublikasikan panduan standar bagi keamanan informasi. ISO/IEC menyebut panduan ini sebagai ISMS (*Information Security Management System*) dan menguraikan penjelasannya dalam seri ISO/IEC 27000. ISO seri 27005 khusus membahas *Risk Management*.

Dikarenakan banyaknya ancaman dan pelanggaran keamanan informasi yang terjadi pada institusi pendidikan dan terus meningkat setiap tahunnya serta banyaknya kasus-kasus yang terjadi maka perlu diteliti tentang tingkat risiko keamanan informasi pada Perguruan Tinggi Indonesia khususnya kota Bandung. Adapun fokus dalam penelitian ini adalah risiko-risiko yang terkait Sistem Informasi Akademik (SIA), karena SIA merupakan bagian dari proses bisnis utama sebuah institusi pendidikan.

1.3 Perumusan Masalah

Dari uraian latar belakang di atas, perumusan masalah yang dapat diidentifikasi adalah sebagai berikut:

- 1. Apa saja asset yang terdapat pada masing-masing perguruan tinggi yang berhubungan dengan Sistem Informasi Akademik?*
- 2. Bagaimana potensi, kerentanan dan kemungkinan terjadinya ancaman keamanan yang terkait dengan masing-masing asset perguruan tinggi tersebut?*

3. *Bagaimana tingkat risiko untuk masing-masing asset di tiap perguruan tinggi?*

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan diatas, maka tujuan penelitian yang diinginkan selama penelitian ini adalah:

1. Mengetahui dan menggambarkan jenis asset yang dimiliki perguruan tinggi serta menentukan nilai asset masing-masing
2. Mengetahui dan menggambarkan potensi jenis ancaman dan kerentanan sekaligus menentukan skala nilai kemungkinan terjadinya ancaman keamanan dan kerentanan terhadap asset masing-masing perguruan tinggi
3. Mengetahui dan menentukan nilai tingkat risiko untuk masing-masing asset perguruan tinggi

1.5 Kegunaan Penelitian

Penelitian ini diharapkan dapat berguna dalam:

1. Aspek Teoritis

Diharapkan hasil dari penelitian ini dapat berguna bagi keilmuan bidang Manajemen Keamanan Risiko dan diharapkan temuan-temuan yang diperoleh dapat memberikan pandangan terhadap analisis risiko keamanan informasi bagi penelitian selanjutnya.

Sebagai informasi bagi pihak-pihak yang berkepentingan, baik secara langsung maupun tidak langsung, dimana mereka dapat menggunakan hasil penelitian ini sebagai bahan perbandingan untuk penelitian sejenis dalam konteks analisis risiko keamanan informasi.

2. Aspek Praktis

Bagi institusi pendidikan, sebagai bahan masukan, acuan dan pertimbangan dalam bentuk sebuah laporan analisa tingkat risiko dan dapat juga dijadikan bahan bagi penelitian-penelitian atau perbaikan dalam praktik selanjutnya.

1.6 Sistematika Penulisan Tugas Akhir

Sistematika penulisan dibuat untuk memberi gambaran umum tentang penelitian dan hasil penelitian yang dilakukan. Berikut ini urutan penulisannya :

BAB I PENDAHULUAN

Bab ini bersisi uraian secara singkat mengenai, gambaran umum objek penelitian, latar belakang penelitian, perumusan masalah, tujuan penelitian, kegunaan penelitian, dan sistematika penulisan tugas akhir.

BAB II TINJAUAN PUSTAKA DAN LINGKUP PENELITIAN

Pada bab ini akan diuraikan teori-teori yang melandasi penelitian serta mendukung pemecahan masalah, kerangka pemikiran dan ruang lingkup penelitian.

BAB III METODE PENELITIAN

Pada bab ini akan diuraikan mengenai jenis penelitian, variabel operasional, tahapan penelitian, populasi dan sampel, pengumpulan data, uji validitas dan reliabilitas, dan teknik analisis data.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini akan dijelaskan mengenai cara pengumpulan, pengolahan dan analisa data yang telah melalui proses pengolahan.

BAB V KESIMPULAN DAN SARAN

Pada bab ini akan dijelaskan mengenai kesimpulan dari hasil penelitian yang disertai dengan rekomendasi atau saran bagi Perguruan Tinggi yang diteliti.