BAB I
PENDAHULUAN

1.1. LATAR BELAKANG

Ancaman terhadap keamanan informasi tengah marak terjadi saat ini telah semakin berkembang baik jenis maupun dampak yang ditimbulkannya. Beberapa laporan keamanan yang dikeluarkan oleh *vendor* berkompeten telah menguatkan indikasi tersebut.

Salah satunya adalah laporan yang dikeluarkan oleh perusahaan keamanan Symantec Corp. dirilis pada akhir September 2005. Dimana laporan ini menyampaikan bahwa aksi serangan terhadap jaringan kini bermotif pencarian keuntungan finansial dan mulai mengarah pada tindakan kejahatan seperti penipuan dan pencurian informasi. Ancaman / resiko tersebut dapat muncul dari *hacker*, perangkat lunak berbahaya (*malicious software*), karyawan / mantan karyawan yang kurang puas dengan kebijakan perusahaan, para pesaing maupun sumber-sumber lainnya baik internal ataupun eksternal dari suatu organisasi. Dampak yang ditimbulkannya tentunya dapat berakibat pada hilangnya pendapatan dalam jumlah yang tidak sedikit, privasi hingga rusaknya reputasi dari suatu perusahaan atau organisasi. Oleh karenanya, tidaklah mengherankan jika suatu survey terakhir (Landoll, 2006) menyebutkan bahwa sekitar 78% eksekutif

berpendapat keamanan komputer merupakan atribut kritis dari jaringan komputer atau infrastruktur TI.

Hal ini tentunya mengharuskan banyak perusahaan maupun organisasi untuk memiliki standard aturannya masing-masing terhadap subjek tersebut guna meminimalisir dampak yang ditimbulkannya. Disamping itu, dengan adanya standard yang diturunkan kedalam bentuk kebijakan, prosedur, aturan perusahaan, dan lain sebagainya (yang tentunya *comply* standard internasional) dapat menjadi dasar untuk penetapan SLA (*Service Level Agreement*) suatu perusahaan terhadap partner bisnis.

1.2. PERMASALAHAN

PT. NCS sebagai suatu perusahaan yang bergerak dalam layanan jasa kurir, dalam perjalanan bisnisnya seringkali menemui kondisi dimana para kustomer maupun mitra bisnisnya meminta jaminan standard keamanan informasi yang diterapkan pada perusahaan tersebut. Hal ini biasanya tercantum dalam dokumen MoU (*Memorandum of Understanding*) ataupun RFP (*Request for Proposal*) dimana beberapa poin tertentu menghendaki PT. NCS selaku penyedia layanan memiliki jaminan akan kemanan informasi. Tentunya dibutuhkan suatu standard yang dapat berupa prosedur, kebijakan guna menjawab adanya kebutuhan tersebut.

Kebutuhan akan kebijakan keamanan informasi ini juga semakin diperkuat dengan objektif dari perusahaan yang menyebutkan bahwa “Kerahasiaan data,

ketepatan waktu, serta keakuratan penanganan merupakan prinsip yang tidak bisa ditawar oleh setiap karyawan PT. NCS." Kebutuhan tersebut juga melatarbelakangi suatu *research question* yang akan dijawab melalui penelitian ini, yaitu: "Bagaimanakah bentuk suatu kebijakan keamanan yang sesuai dengan kondisi nyata dari PT. NCS ?"

1.3. TUJUAN PENULISAN

Melalui penelitian dan penulisan tesis ini diharapkan dapat memenuhi beberapa tujuan berikut:

1. Membentuk dokumen kebijakan keamanan sistem informasi berdasarkan standar internasional yang berlaku.
2. Memberikan sejumlah petunjuk serta tata cara khususnya kepada perusahaan yang dijadikan tempat studi kasus dalam proses implementasi kebijakan keamanan sistem informasi.
3. Menjadi bahan referensi terhadap model pengembangan kebijakan keamanan informasi terhadap perusahaan khususnya yang bergerak dalam layanan jasa.

1.4. BATASAN MASALAH

Berhubung besarnya domain dari keamanan sistem informasi (yang diturunkan dari standar internasional yang berlaku), fokus dari penelitian dan

penulisan tesis ini lebih dititikberatkan pada beberapa domain yang menjadi prioritas utama dari perusahaan yang menjadi studi kasus. Adapun rincian dari domain-domain yang menjadi fokus utama dalam penyusunan kebijakan keamanan informasi tersebut akan dibahas pada bab berikutnya.

1.5. SISTEMATIKA PENULISAN

Struktur penulisan tesis ini terbagi dalam beberapa bagian utama dengan ketentuan sebagai berikut:

- Bab I Pendahuluan, memberikan gambaran tentang perumusan masalah akan kebutuhan keamanan informasi secara umum dan secara spesifik terhadap organisasi tempat dijadikan studi kasus (yaitu PT. NCS) berikut tujuan serta sejumlah batasan dimunculkannya penelitian ini.
- Bab II Landasan Teori, menjelaskan sejumlah kerangka teori yang melatari dibentuknya penelitian dan penulisan tesis ini. Bab ini juga memberikan gambaran umum seputar PT. NCS, sebagai organisasi tempat dijadikannya studi kasus dalam penelitian ini.
- Bab III Metodologi Penelitian, memberikan gambaran terhadap metodologi penelitian yang digunakan dalam penyusunan tesis.
- Bab IV Hasil dan Bahasan, menjelaskan bentuk kebijakan keamanan informasi pada perusahaan tempat dijadikannya studi kasus

berdasarkan metodologi penelitian yang telah didefinisikan pada bab sebelumnya.

- Bab V Kesimpulan dan Saran, berisi sejumlah kesimpulan yang penulis peroleh dalam penelitian ini berikut serangkaian solusi saran yang sebaiknya diperhatikan oleh pemegang keputusan pada perusahaan tempat dijadukan studi kasus.