

ABSTRAK

Saat ini keadaan penerapan *IT Security* di Indonesia sebagai infrastruktur pendukung operasional bisnis merupakan kebutuhan yang mulai berkembang seiring dengan berkembangnya teknologi internet di seluruh dunia. Penting bagi para penyedia jasa *IT Security* di Indonesia untuk memahami keadaan pasar di Indonesia.

Melalui analisis kualitatif terhadap hasil survey “*IT Security* di Indonesia” dari sembilan jenis bidang industri yang ada di Indonesia dapat disimpulkan sampai saat ini, bidang industri *Infrastructure, Utility and Transportation* merupakan bidang industri yang paling menarik bagi para penyedia jasa *IT Security* di Indonesia.

Berdasarkan hasil survey diberikan beberapa rekomendasi untuk melakukan pendekatan terhadap para pengguna jasa berdasarkan jenis bidang industrinya.

DAFTAR ISI

PERNYATAAN KEASLIAN KARYA TUGAS AKHIR	ii
LEMBAR PERSETUJUAN.....	iii
LEMBAR PENGESAHAN	iv
KATA PENGANTAR	v
ABSTRAK	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR	xv
DAFTAR TABEL	xviii
Bab 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah.....	1
1.2 Perumusan Masalah	2
1.3 Tujuan Penelitian	2
1.4 Metodologi Penelitian	3
1.4.1 Tipe Penelitian	3
1.4.2 Pendekatan Penelitian	3
1.4.3 Obyek Penelitian	3
1.4.4 Teknik Pengumpulan Data.....	4
1.4.4.1 Teknik Pengumpulan Data Primer	4
1.4.4.2 Teknik Pengumpulan Data Sekunder.....	4
1.4.5 Teknik Pengolahan dan Analisa Data	5
1.4.5.1 Teknik Analisa Data Primer.....	5
1.4.5.2 Teknik Analisa Data Sekunder	5
1.5 Sistematika Penulisan	5
Bab 2 DASAR TEORI	6
2.1 Teori Pendahuluan	6
2.1.1 Apakah <i>Information Security</i> Itu?.....	6
2.1.2 Mengapa <i>Information Security</i> Diperlukan?.....	7

2.1.3	Bagaimana Menentukan <i>Security Requirement</i>	9
2.1.4	Penerapan <i>Risk Assessment</i>	10
2.1.5	Penerapan Kontrol.....	11
2.1.6	<i>Critical Success Factor</i>	11
2.2	10 Domain ISO 17799	12
2.2.1	<i>Security Policy</i>	12
2.2.2	<i>Organizational Security</i>	14
2.2.2.1	<i>Information Security Infrastructure</i>	14
2.2.2.2	<i>Security of Third Party Access</i>	14
2.2.2.3	<i>Outsourcing</i>	15
2.2.3	<i>Asset Classification and Control</i>	15
2.2.3.1	<i>Accountability for Assets</i>	15
2.2.3.2	<i>Information Classification</i>	15
2.2.4	<i>Personnel Security</i>	16
2.2.5	<i>Physical and Environmental Security</i>	17
2.2.5.1	<i>Secure Areas</i>	17
2.2.5.2	<i>Equipment Security</i>	17
2.2.5.3	<i>General Controls</i>	17
2.2.6	<i>Communications and Operations Management</i>	17
2.2.7	<i>Access Control</i>	19
2.2.8	<i>Systems Development and Maintenance</i>	20
2.2.9	<i>Business Continuity Management</i>	21
2.2.10	<i>Compliance</i>	22
Bab 3	REPRESENTASI DATA HASIL SURVEY	23
3.1	Deskripsi Umum	23
3.1.1	Jenis Bidang Usaha Responden	24
3.1.2	Pengalaman Responden Dibidang <i>IT Security</i>	25
3.1.3	Jumlah <i>Device</i> Yang Terkoneksi	25
3.1.4	Jumlah <i>User</i> Yang Dilayani	26
3.1.5	<i>Data Center</i>	26
3.1.6	<i>Remote Access Service</i>	27

3.2	Deskripsi Mengenai Sumber Daya Manusia.....	27
3.2.1	<i>Reported Management</i>	28
3.2.2	Sertifikasi	29
3.2.3	Jumlah Staff <i>IT Security</i> Bersertifikat.....	30
3.3	Deskripsi Mengenai <i>IT Security Policy</i>	30
3.3.1	Implementasi Dari <i>IT Security Policy</i>	31
3.3.2	Ruang Lingkup Dari <i>IT Security Policy</i>	32
3.3.3	Tanggapan Mengenai <i>IT Security Policy</i>	33
3.3.3.1	Kejelasan Dari <i>IT Security Policy</i>	33
3.3.3.2	Kemudahan Untuk Diakses.....	34
3.3.3.3	<i>Enforced</i>	35
3.3.3.4	Secara Reguler Diupdate.....	36
3.3.3.5	Konsistensi Disetiap Organisasi.....	37
3.4	Deskripsi Mengenai Keadaan Saat Ini	38
3.4.1	Perencanaan Mengenai <i>IT Security</i>	38
3.4.2	Hal-hal Yang Sudah Diterapkan	39
3.4.2.1	<i>Network Firewall</i>	39
3.4.2.2	<i>Centralized Data Backup System</i>	40
3.4.2.3	<i>Virtual Private Network (VPN) Untuk Remote Access</i>	41
3.4.2.4	<i>Intrusion Detection</i>	42
3.4.2.5	<i>Active Content Monitoring/Filtering</i>	43
3.4.3	Penerapan Teknologi <i>Wireless LAN</i>	44
3.4.4	Teknologi <i>Wireless LAN</i> Yang Sudah Diterapkan.....	45
3.4.4.1	40-bit <i>Wired Equivalency Privacy (WEP)</i>	45
3.4.4.2	128-bit <i>Wired Equivalency Privacy (WEP)</i>	46
3.4.4.3	<i>Extensible Authentication Protocol (EAP)</i>	47
3.4.4.4	<i>Remote Authentication Dial-In User Service (RADIUS)</i>	48
3.4.4.5	<i>Advanced Encryption Standard (AES)</i>	49
3.5	Deskripsi Mengenai <i>Awareness</i>	50
3.5.1	<i>Awareness</i>	50
3.5.2	Laporan Tentang <i>IT Security Policy</i>	51

3.6	Deskripsi Mengenai <i>Enterprise Process</i>	52
3.6.1	Penerapan Teknologi Otentikasi	53
3.6.1.1	<i>Password</i>	53
3.6.1.2	<i>Kerberos</i>	54
3.6.1.3	<i>Public Key Infrastructure (PKI)</i>	55
3.6.1.4	<i>Smartcards</i>	56
3.6.1.5	Teknologi <i>Biometrics</i>	57
3.6.2	<i>Policy</i> Mengenai <i>Password</i>	58
3.6.3	Pengecekan <i>Vulnerability</i> Baru.....	59
3.6.4	<i>Anti Virus</i>	60
3.6.5	Pencegahan Terhadap <i>Vulnerability</i> Yang Ada	61
3.6.5.1	Pembatasan Protokol.....	61
3.6.5.2	Pembatasan URL.....	62
3.6.5.3	Pembatasan Akses	63
3.6.5.4	Penerapan <i>Software Inventory</i>	64
3.6.5.5	Penerapan <i>Back-Up Plan</i>	65
3.7	Deskripsi Mengenai Penanganan Insiden	66
3.7.1	Prosedur Penanganan Insiden	66
3.7.2	Keterlibatan Pihak Lain Setelah Insiden.....	67
3.7.3	Jumlah Insiden	68
3.8	Deskripsi Mengenai <i>Risk Assessment</i>	69
3.8.1	<i>Risk Assessment</i>	69
3.8.2	Audit Terhadap <i>Vulnerability</i>	70
3.8.3	Pejabat Yang Melakukan <i>Audit</i>	71
3.9	Deskripsi Mengenai Jasa Eksternal.....	72
3.9.1	Jasa <i>IT Security</i>	72
3.9.2	Jasa Yang Dipergunakan.....	73
3.9.2.1	<i>IT Security Architecture Dan Design Services</i>	73
3.9.2.2	<i>IT Security Technical Support Services</i>	73
3.9.2.3	<i>Managed Firewall Services</i>	74
3.9.2.4	<i>Physical Security Audit</i>	74

3.9.2.5	<i>IT Security Policy Setup Services</i>	75
3.9.2.6	<i>Project Management (For IT Security Projects)</i>	75
3.9.3	Keuntungan Penggunaan <i>External IT Security Consultant</i>	76
3.9.3.1	Memberikan Keahlian Teknis	76
3.9.3.2	Metodologi <i>Project Management</i>	76
3.9.3.3	Memenuhi <i>Project Timeline</i>	77
3.9.3.4	Memenuhi <i>Project Budget</i>	77
3.9.3.5	Memberikan Nilai Tambah/Fungsi Baru Kepada Sistem	78
3.9.4	Pertimbangan Memanfaatkan Jasa Konsultan IT Security	78
3.9.4.1	Biaya Aktual Dibandingkan Anggaran	78
3.9.4.2	<i>Knowledge Transfer</i> Kepada Tim Internal.....	79
3.9.4.3	Kerja Sama Dengan Tim Internal	80
3.9.4.4	Pemahaman Terhadap Kebutuhan Pelanggan.....	80
3.9.4.5	Biaya Training Yang Dibeberatkan Kepada Pelanggan.....	81
3.10	Deskripsi Mengenai Dana Anggaran	81
3.10.1	Anggaran	81
3.10.2	Rencana Pengembangan/Efisiensi	83
3.10.2.1	Staf IT.....	83
3.10.2.2	Produk <i>Hardware/Software</i>	84
3.10.2.3	<i>Training</i>	85
3.10.2.4	<i>External Services</i>	86
3.10.3	Alasan Utama Melakukan Pengeluaran	87
3.11	Deskripsi Pendapat Responden.....	88
3.11.1	Penerapan <i>IT Security</i>	88
3.11.2	Pendapat Keadaan <i>IT Security</i>	89
3.11.2.1	Keamanan.....	89
3.11.2.2	Pengukuran Efektivitas	90
3.11.2.3	Perbandingan Dengan 2 Tahun Lalu.....	91
3.12	Deskripsi Mengenai Isu-Isu Lain	92
Bab 4	ANALISA HASIL SURVEY	93
4.1	Analisa Secara Umum.....	93

4.2	Analisa Mengenai Sumber Daya Manusia.....	96
4.2.1	<i>Reported Management</i>	96
4.2.2	Sertifikasi	97
4.2.3	Jumlah Staf <i>IT Security</i> Bersertifikat	97
4.3	Analisa Mengenai <i>IT Security Policy</i>	97
4.3.1	Implementasi Dari <i>IT Security Policy</i>	97
4.3.2	Ruang Lingkup Dari <i>IT Security Policy</i>	97
4.3.3	Tanggapan Mengenai <i>IT Security Policy</i>	97
4.4	Analisa Mengenai Keadaan Saat Ini	98
4.4.1	Perencanaan Mengenai <i>IT Security</i>	98
4.4.2	Hal-Hal Yang Sudah Diterapkan	98
4.4.3	Penerapan Teknologi <i>Wireless LAN</i>	99
4.5	Analisa Mengenai <i>Awareness</i>	99
4.5.1	<i>Awareness</i>	99
4.5.2	Laporan Tentang <i>IT Security Policy</i>	100
4.6	Analisa Mengenai <i>Enterprise Process</i>	100
4.6.1	Penerapan Teknologi Otentikasi	100
4.6.2	<i>Policy</i> Mengenai Password	100
4.6.3	Pengecekan Terhadap <i>Vulnerability</i> Baru.....	101
4.6.4	<i>Anti Virus</i>	101
4.6.5	Pencegahan Terhadap <i>Vulnerability</i> Yang Ada	101
4.7	Analisa Mengenai Penanganan Insiden	102
4.7.1	Prosedur Penanganan Insiden	102
4.7.2	Keterlibatan Pihak Lain Setelah Insiden	102
4.7.3	Jumlah Insiden	103
4.8	Analisa Mengenai <i>Risk Assessment</i>	103
4.8.1	<i>Risk Assessment</i>	103
4.8.2	Audit Terhadap <i>Vulnerability</i>	103
4.8.3	Pejabat Yang Melakukan Audit	103
4.9	Analisa Mengenai Jasa Eksternal.....	103
4.9.1	Jasa <i>IT Security</i>	103

4.9.2	Jasa Yang Dipergunakan.....	104
4.9.3	Keuntungan Penggunaan Eksternal Konsultan <i>IT Security</i>	104
4.9.4	Pertimbangan Memanfaatkan Jasa Konsultan <i>IT Security</i>	104
4.10	Analisa Mengenai Dana Anggaran	104
4.10.1	Anggaran.....	104
4.10.2	Rencana Pengembangan/Efisiensi	104
4.10.3	Alasan Utama Melakukan Pengeluaran	105
4.11	Analisa Mengenai Pendapat Responden	105
4.11.1	Penerapan <i>IT Security</i>	105
4.11.2	Pendapat Keadaan <i>IT Security</i>	105
4.12	Analisa Mengenai Isu-Isu Lain	106
4.13	Analisa per Bidang Industri	106
4.13.1	<i>Banking and Finance</i>	107
4.13.2	<i>Basic and Chemical Industry</i>	108
4.13.3	<i>Consumer Products</i>	110
4.13.4	<i>Farming</i>	111
4.13.5	<i>Infrastructure, Utility and Transportation</i>	113
4.13.6	<i>Manufacturing</i>	115
4.13.7	<i>Mining</i>	117
4.13.8	<i>Property</i>	119
4.13.9	<i>Trading, Services and Investment</i>	120
4.14	Perbandingan Dengan Keadaan Negara Lain	122
Bab 5	PENUTUP.....	126
5.1	Kesimpulan	126
5.2	Saran.....	128
	DAFTAR PUSTAKA	132

DAFTAR GAMBAR

Gambar 2.1 CERT/CC <i>Overview Incident and Vulnerability Trends</i>	8
Gambar 3.1 <i>Screen Capture Web Survey Site</i>	23
Gambar 3.2 Deskripsi Responden Berdasarkan Jenis Industri	24
Gambar 3.3 Pengalaman Dibidang <i>IT Security</i> Secara Umum	25
Gambar 3.4 Jumlah <i>Device</i> Yang Terkoneksi Secara Umum	25
Gambar 3.5 Deskripsi Jumlah <i>User</i> Yang Dilayani Secara Umum	26
Gambar 3.6 Deskripsi <i>Data Center</i> Secara Umum	26
Gambar 3.7 Deskripsi Mengenai RAS Secara Umum	27
Gambar 3.8 Deskripsi Mengenai <i>Reported Management</i>	28
Gambar 3.9 Deskripsi Mengenai Sertifikasi	29
Gambar 3.10 Deskripsi Jumlah Staf Bersertifikasi	30
Gambar 3.11 Implementasi Dari <i>IT Security Policy</i>	31
Gambar 3.12 Ruang Lingkup Dari <i>IT Security Policy</i>	32
Gambar 3.13 Tanggapan Mengenai <i>IT Security Policy</i>	33
Gambar 3.14 Tanggapan Mengenai <i>IT Security Policy</i>	34
Gambar 3.15 Tanggapan Mengenai <i>IT Security Policy</i>	35
Gambar 3.16 Tanggapan Mengenai <i>IT Security Policy</i>	36
Gambar 3.17 Tanggapan Mengenai <i>IT Security Policy</i>	37
Gambar 3.18 Perencanaan Mengenai <i>IT Security</i>	38
Gambar 3.19 Penerapan <i>Network Firewall</i>	39
Gambar 3.20 Penerapan <i>Centralized Data Backup System</i>	40
Gambar 3.21 Penerapan VPN Untuk <i>Remote Access</i>	41
Gambar 3.22 Penerapan <i>Intrusion Detection</i>	42
Gambar 3.23 Penerapan <i>Active Content Monitoring/Filtering</i>	43
Gambar 3.24 Penerapan Teknologi <i>Wireless LAN</i>	44
Gambar 3.25 Penerapan 40-bit WEP	45
Gambar 3.26 Penerapan 128-bit WEP	46

Gambar 3.27 Penerapan EAP.....	47
Gambar 3.28 Penerapan RADIUS	48
Gambar 3.29 Penerapan AES.....	49
Gambar 3.30 Deskripsi Mengenai <i>Awareness</i>	50
Gambar 3.31 Deskripsi Mengenai Laporan Tentang <i>IT Security Policy</i>	51
Gambar 3.32 Deskripsi Mengenai Penerapan Teknologi Otentikasi <i>Password</i> ...	53
Gambar 3.33 Deskripsi Mengenai Penerapan Teknologi Otentikasi <i>Kerberos</i>	54
Gambar 3.34 Deskripsi Mengenai Teknologi Otentikasi PKI	55
Gambar 3.35 Deskripsi Mengenai Teknologi Otentikasi <i>Smartcards</i>	56
Gambar 3.36 Deskripsi Mengenai Teknologi Otentikasi <i>Biometrics</i>	57
Gambar 3.37 Deskripsi Mengenai <i>Policy</i> Tentang <i>Password</i>	58
Gambar 3.38 Deskripsi Mengenai Pengecekan <i>Vulnerability</i> Baru.....	59
Gambar 3.39 Deskripsi Mengenai <i>Anti Virus</i>	60
Gambar 3.40 Penerapan Pembatasan Protokol	61
Gambar 3.41 Penerapan Pembatasan URL	62
Gambar 3.42 Penerapan Pembatasan Akses	63
Gambar 3.43 Penerapan <i>Software Inventory</i>	64
Gambar 3.44 Penerapan <i>Back-Up Plan</i>	65
Gambar 3.45 Deskripsi Mengenai Prosedur Penanganan Insiden	66
Gambar 3.46 Deskripsi Mengenai Keterlibatan Pihak Lain Setelah Insiden.....	67
Gambar 3.47 Deskripsi Mengenai Jumlah Insiden Dalam Setahun Terakhir	68
Gambar 3.48 Deskripsi Mengenai <i>Risk Assessment</i>	69
Gambar 3.49 Deskripsi Mengenai <i>Audit</i> Terhadap <i>Vulnerability</i>	70
Gambar 3.50 Deskripsi Mengenai Pejabat Yang Melakukan Audit	71
Gambar 3.51 Deskripsi Mengenai Pemanfaatan Jasa <i>IT Security</i>	72
Gambar 3.52 Deskripsi Mengenai <i>IT Security Architecture/Design Service</i>	73
Gambar 3.53 Deskripsi Mengenai <i>IT Security Technical Support Services</i>	73
Gambar 3.54 Deskripsi Mengenai <i>Managed Firewall Services</i>	74
Gambar 3.55 Deskripsi Mengenai <i>Physical Security Audit</i>	74
Gambar 3.56 Deskripsi Mengenai <i>IT Security Policy Setup Services</i>	75
Gambar 3.57 Deskripsi Mengenai <i>Project Management</i>	75

Gambar 3.58 Deskripsi Mengenai Keahlian Teknis	76
Gambar 3.59 Deskripsi Mengenai Metodologi <i>Project Management</i>	76
Gambar 3.60 Deskripsi Mengenai <i>Project Timeline</i>	77
Gambar 3.61 Deskripsi Mengenai <i>Project Budget</i>	77
Gambar 3.62 Deskripsi Mengenai Nilai Tambah/Fungsi Baru.....	78
Gambar 3.63 Deskripsi Perbandingan Biaya Aktual Dengan Anggaran	79
Gambar 3.64 Deskripsi Mengenai <i>Knowledge Transfer</i> Kepada Tim Internal	79
Gambar 3.65 Deskripsi Mengenai Kerja Sama Dengan Tim Internal	80
Gambar 3.66 Deskripsi Mengenai Pemahaman Kebutuhan Pelanggan.....	80
Gambar 3.67 Deskripsi Mengenai Biaya Training	81
Gambar 3.68 Deskripsi Mengenai Anggaran.....	82
Gambar 3.69 Rencana Pengembangan/Efisiensi Staf IT	83
Gambar 3.70 Rencana Pengembangan/Efisiensi Produk <i>Hardware/Software</i>	84
Gambar 3.71 Rencana Pengembangan/Efisiensi <i>Training</i>	85
Gambar 3.72 Rencana Pengembangan/Efisiensi <i>External Services</i>	86
Gambar 3.73 Deskripsi Mengenai Alasan Utama Melakukan Pengeluaran	87
Gambar 3.74 Pendapat Responden Mengenai Penerapan <i>IT Security</i>	88
Gambar 3.75 Pendapat Mengenai Keadaan Keamanan <i>IT Security</i>	89
Gambar 3.76 Pendapat Mengenai Pengukuran Efektivitas <i>IT Security</i>	90
Gambar 3.77 Pendapat Mengenai Perbandingan Dengan 2 Tahun Lalu	91
Gambar 3.78 Deskripsi Mengenai Kendala Utama.....	92
Gambar 4.1 Diagram Lingkaran Mengenai jenis Bidang Industri.....	93
Gambar 4.2 Diagram Lingkaran Mengenai Pengalaman Dibidang <i>IT Security</i> ...	94
Gambar 4.3 Diagram Lingkaran Mengenai Jumlah <i>Network Device</i>	94
Gambar 4.4 Diagram Lingkaran Mengenai Jumlah <i>User</i>	94
Gambar 4.5 Diagram Lingkaran Mengenai <i>Data Center</i>	95
Gambar 4.6 Diagram Lingkaran Mengenai RAS.....	95
Gambar 4.7 Ketiadaan Penerapan Teknologi <i>IT Security</i>	123
Gambar 4.8 Tingkat Penerapan Sistem Keamanan IT	123
Gambar 4.9 Implementasi <i>IT Security Policy</i> Berdasarkan Bidang Industri	124

DAFTAR TABEL

Tabel 5.1 Tabel Kesimpulan	127
Tabel 5.2 Tabel Rekomendasi.....	131

