PENYUSUNAN TATA KELOLA KEAMANAN INFORMASI PADA PRODUKSI FILM ANIMASI (Kasus di PT. XX)

Ayu Candra Dewi[1], Eko Nugroho[2], Rudy Hartanto[3]
[1,2,3]*Departemen Teknik Elektro dan Teknologi Informasi, Universitas Gadjah Mada*
Jl. Grafika No.2 Yogyakarta – 55281, Bulak Sumur, Sleman, Yogyakarta, Indonesia
Email : ayu.cio15@mail.ugm.ac.id[1], nugroho@ugm.ac.id[2], rudy@ugm.ac.id[3]

Abstrak

Berjalannya perkembangan teknolgi informasi yang semakin maju dan pesat di era global ini, hal ini berpengaruh terhadap penggunaan teknologi informasi di kalangan perusahaan swasta. PT. XX yang juga beketergantungan erat terhadap teknologi informasi dalam kegiatan produksi film animasi. Namun, permasalahan teknologi informasi yang berperan penting terhadap perusahaan seringkali kurang mendapat perhatian. Akibatnya tidak dipungkiri akan muncul ancaman maupun kelemahan dalam teknologi informasi yang menganggu jalannya kegiatan produksi film animasi. Oleh karena itu diperlukannya pengelolaan teknologi informasi yang dituangkan dalam tata kelola untuk mengelola ancaman maupun kelemahan yang muncul. SNI ISO/IEC 27001:2005 merupakan framework sistem manajemen keamanan informasi yang dapat dijadikan dasar dalam pengelolaan informasi

Kata Kunci : *Keamanan Informasi, SNI ISO/IEC 27001:2009, Produksi Animasi.*

1. PENDAHULUAN

Melalui TI, proses bisnis dapat dilaksanakan lebih mudah, cepat, efisien dan efektif. TI juga menawarkan banyak peluang kepada perguruan tinggi dan organisasi untuk meningkatkan kinerja, mentransformasikan pelayanan, proses kerja, hubungan – hubungan komunitas dan riset. Karenanya, *IT governance* saat ini menjadi salah satu *critical success factor* (CSF) bagi para pemimpin dan mitra perguruan tinggi untuk mengoptimalkan peran TI dalam efektifitas peningkatan aset, capaian kinerja, sasaran, tujuan, visi dan misi organisasi [1]. Demikian juga perusahaan swasta yang dalam kesehariannya melaksanakan kegiatan bisnis perusahaan berkaitan erat dengan dunia teknologi. Oleh karena itu, perusahaan sangat membutuhkan jaminan untuk kerahasiaan, keutuhan dan ketersediaannya data dengan baik sehingga berguna dalam pelaksanaan rencana kegiatan serta melakukan proses bisnis.

PT. XX saat ini berusaha untuk meminimalisir kerawanan dan ancaman yang dapat mengganggu kinerja perusahaan yang disebabkan oleh perkembangan Teknologi Informasi dan Komunikasi yang semakin canggih dan kompleks.

Pembelanjaan TI tersebut meliputi pengadaan perangkat keras, perangkat lunak, dan layanan TI. Peningkatan belanja TI dikarenakan manfaat TI mendukung bisnis semakin nyata seiring dengan kompetisi bisnis yang semakin meningkat dan dinamis. Investasi di bidang TI adalah kunci agar sebuah perusahaan mampu bertahan hidup di lingkungan bisnis yang kompetitif, sehingga mengharuskan sebuah perusahaan berinvestasi di bidang TI [2]. Hal ini juga berlaku pada PT. XXyang dari waktu ke waktu hingga saat ini pengadaan perangkat keras, perangkat lunak semakin meningkat dan ini menyebabkan semakin meningkatnya layanan kinerja yang dilakukan oleh pihak Divisi TI perusahaan.

Menyadari hal tersebut menjadikan tata cara dalam penggunaan teknologi informasi di kegiatan pelaksanaan bisnis perusahaan dengan arahan yang terstandarisasi merupakan hal penting sehingga hal tersebut dapat memicu ketertiban dan keberaturan dalam penggunaannya. Yang pada hal ini diusulkan oleh peneliti untuk menggunakan SNI ISO/IEC 27001:2009 pada perancangan tata kelola keamanan informasi perusahaan.

SNI ISO/IEC 27001:2009 merupakan standar yang mencakup semua jenis organisasi (misalnya usaha komersial, pemerintah, organisasi nir-laba). Standar ini menetapkan persyaratan untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, peningkatan dan pemeliharaan Sistem

Manajemen Keamanan Informasi (SMKI) yang terdokumentasi dalam konteks risiko bisnis organisasi secara keseluruhan. Standar ini menetapkan persyaratan penerapan pengendalian keamanan yang disesuaikan dengan kebutuhan masing-masing organisasi atau bagian organisasi. SMKI didesain untuk memastikan pemilihan pengendalian keamanan yang memadai dan proposional untuk melindungi aset informasi dan memberikan kepercayaan kepada pihak terkait [3]. Penentuan penggunaan SNI ISO/IEC 27001:2009 sebagai acuan perancangan tata kelola keamanan informasi dikarenakan menyediakan kerangka kerja untuk netralitas penggunaan teknologi, termasuk kemampuan mengakses data secara berkelanjutan dengan adanya kerahasiaan dan integritas atas informasi yang dimiliki serta kebutuhan pihak-pihak berkepentingan sesuai dengan hak wewenang yang diperoleh. Penelitian ini bertujuan untuk menyusu tata kelola informasi yang baik untuk PT. XX agar produksi film animasi dapat berjalan dengan baik.

2. METODE PENELITIAN

Metode penelitian yang digunakan secara garis besar terdiri dari 4 (empat) tahapan pengerjaan :

1) Pengumpulan Data,
2) Analisis Data,
3) Pembuatan dokumen tata kelola,
4) Verifikasi dokumen tata kelola.

3. HASIL DAN PEMBAHASAN

3.1 Tata Kelola

Tata kelola Teknologi Informasi didefinisikan sebagai struktur hubungan dan proses untuk mengarahkan dan mengontrol perusahaan agar tujuan bisnis dapat tercapai melalui penambahan nilai sekaligus penyeimbangan risiko terkait dengan pengelolaan proses Teknologi Informasi. Tidak hanya pengelolaan proses, tetapi juga memastikan bahwa proses tersebut telah dipenuhi oleh sumber daya Teknologi Informasi yang memberikan dukungan secara optimal terhadap pemenuhan tujuan bisnis [4]. Sebagai sebuah perusahaan produksi film animasi yang berkaitan erat dengan bidang teknologi informasi sangat diperlukan tata kelola keamanan teknologi informasi untuk mengarahkan dan mengontrol perusahaan agar tujuan bisnis tercapai.

Peningkatan efektivitas dan efisiensi organisasi baik pemerintah maupun bisnis dapat dilakukan melalui upaya penataan organisasi yang baik. Upaya tersebut dilakukan tidak hanya melalui proses pengaturan (*manage*) tetapi lebih luas pada penatakelolaan seluruh proses bisnis (*governance*). Makna mengatur lebih sempit dibanding menata kelola karena mengatur merupakan bagian dari menata kelola [5].

Mengatur teknologi informasi hanya menunjuk pada serangkaian mekanisme di departemen TI untuk menghasilkan suatu spesifik TI, sedangkan menata kelola lebih luas lagi, yaitu serangkaian sistem dan mekanisme yang menentukan pihak-pihak, baik di departemen TI maupun di luar departemen TI, yang membuat dan berkontribusi dalam pembuatan keputusan [6].

3.2 Keamanan Informasi

Keamanan informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki. Mungkin orang akan bertanya, mengapa "keamanan informasi" dan bukan "keamanan teknologi informasi" atau IT security. Kedua istilah ini sebenarnya sangat terkait, tetapi mengacu pada dua hal yang berbeda. "Keamanan Teknoligi Informasi" atau IT security mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan [7].

Beragam bentuk informasi yang mungkin dimiliki oleh sebuah perusahaan meliputi : informasi yang tersimpan dalam computer (baik *desktop* komputer maupun *mobile* komputer, *server* dan *workstation*), segala data yang melintas dijaringan, informasi yang dicetak pada kertas, dikirim melalui fax, data atau informasi yang tersimpan dalam disket, *CD, DVD*, *Flashdisk*, atau penyimpanan data lain termasuk juga informasi yang disampaikan dalam pembicaraan (termasuk hal percakapan melalui

telepon), tersimpan di *mobile phone*, melalui sms, *e-mail*, tersimpan dalam *database*, tersimpan dalam film, dipresentasikan dengan OHP atau media presentasi lain dan metode-metode lain yang dapat digunakan untuk menyampaikan informasi berupa ide-ide baru perusahaan [8].

Keamanan informasi berbeda dengan keamanan teknologi informasi karena mengacu pada dua hal yang berbeda. Keamanan teknologi informasi mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan. Keamanan informasi berfokus pada data dan informasi milik organisasi dengan merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berwenang [7].

3.3 Perlunya Manajemen Keamanan Informasi

Manajemen keamanan informasi diperlukan karena ancaman terhadap *C.I.A* (*triangle model*) aset informasi semakin lama semakin meningkat. Menurut *survey UK Department of Trade and Industry* pada tahun 2008, 49% organisasi meyakini bahwa informasi adalah aset yang penting karena kebocoran informasi dapat dimanfaatkan oleh pesaing, dan 49% organisasi meyakini bahwa keamanan informasi sangat penting untuk memperoleh kepercayaan konsumen. Organisasi menghadapi berbagai ancaman terhadap informasi yang dimilikinya, sehingga diperlukan langkah-langkah yang tepat untuk mengamankan aset informai yang dimiliki [9]. Dalam hal ini diperlukan adanya strategi keamanan informasi yang merupakan detail kebijakan informasi yang berisi tujuan-tujuan, sasaran-sasaran dan tindakan-tindakan yang diterapkan didalam kerangka sebuah kebijakan informasi organisasi yang didukung oleh sistem dan teknologi yang tepat.

3.4 SNI ISO/IEC 27001:2009

ISO/ IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi di perusahaan.

SNI ISO/ IEC 27001 yang diterbitkan pada tahun 2009 dan merupakan versi Indonesia dari ISO/ IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Standar Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol kemanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan [10]. ISO/IEC 27001 mendefinisikan keperluan-keperluan untuk sistem manajemen keamanan informasi. SMKI yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang penting agar terhindar dari risiko kerugian/bencana dan kegagalan serius pada pengamanan sistem informasi. Dalam penerapan SMKI akan memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam masa waktu yang tidak lama.

ISO/ IEC 27001 memberikan gambaran umum mengenai kebutuhan yang dibutuhkan perusahaan/ organisasi dalam usahanya untuk mengimplementasikan konsep-konsep keamanan informasi. Penerapan ISO/ IEC 27001 disesuaikan dengan tujuan, sasaran dan kebutuhan organisasi. Pendekatan proses ini menekankan pada beberapa hal sebagai berikut [11]:

1) Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi,
2) Penerapan dan pengoperasioan kontrol untuk mengelola risiko keamanan informasi dalam bentuk konteks risiko bisnis organisasi secara keseluruhan,
3) Pemantauan dan tinjau ulang kinerja dan efektivitas *ISMS* , dan
4) Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.
   Standar ini mengadopsi model *"Plan-Do-Check-Art" (PDCA)*, untuk membentuk seluruh proses SMKI.

3.5 Hasil Identifikasi

PT. XX merupakan perusahaan yang bergerak dalam bidang pembuatan film animasi yang berdiri sejak tahun 2002. Salah satu badan usaha milik Universitas Amikom ini berlokasi di gedung Universitas Amikom, memiliki visi *"we bring home, hope and happiness"* sehingga salah satu misi yang di ciptakan pun menggambarkan dunia melalui film animasi sesuai dengan visi perusahaan. Dalam kesehariannya PT. XX memproduksi film animasi dalam bentuk 2D dan 3D. Film animasi 2D yang sudah ditayangkan di Indonesia adalah *"Battle of* Surabaya" dan sedang menggarap film dalam bentuk 3D untuk di publikasikan secara *International.* Dalam pembuatannya dilakukan dengan teknologi penggunaan komputer sebagai dasar kinerja para karyawan, termasuk menggambar, merender, penyimpanan data, *tracking* pekerjaan *artist*, meng-*arange instrument music*, administrasi manajemen, administrasi keuangan, administrasi sumber daya manusia, dan pendataan inventaris perusahaan. Maka hal ini berkaitan erat dengan keamanan informasi data maupun kerahasiaan data yang perlu dijaga. Bermula dari perusahaan kecil sehingga berkembang pesat dan mengikuti perkembangan jaman dengan era komputerisasi yang semakin canggih, PT. XX belum memiliki kesiapan untuk menghadapi hal tersebut. Sehingga aset yang dimiliki melimpah, namun untuk prosedur, pengamanan dan pengendalian aset serta informasi belum di tata dengan tepat, bahkan belum memiliki prosedur atau kebijakan untuk tata kelola keamanan informasi sebagai perlindungan dan pencegahan terhadap hal-hal yang tidak diinginkan atau merusak aset milik perusahaan.

3.6 GAP ANALYSIS

Setelah mengetahui kondisi yang sudah ada pada perusahaan, maka penulis mengidentifikasi hal-hal yang sudah ada untuk dijadikan acuan sebagai penentu kebutuhan perancangan kebijakan tata kelola keamanan informasi bagi perusahaan. Sehingga penulis pada sub bab ini akan menjelaskan mengenai domain apa yang akan digunakan, klausul apa, kondisi terkini, kondisi global, dan risiko apa yang akan terjadi apabila tidak adanya kebijakan yang akan dibuat. Hal ini akan dijabarkan melalui tabel berikut :

Tabel 4. 1 Tabel Gap Analysis

Domain	Klausul	Kondisi Terkini	Kondisi Global	Resiko jika tidak ada
A.7 Pengelolaan Aset	A.7.1.3	Belum adanya kebijakan yang mengatur tentang pengelolaan aset yang berbentuk fisik maupun aset informasi. Yang ada hanyalah pendataan mengenai aset fisik secara manual dan data informasi secara tindakan.	• Adanya penentuan siapa pemilik proses yang ada pada proses bisnis. • Adanya Kebijakan yang melindungi aset informasi dan reputasi organisasi serta mempertahankan integritas data.	Apabila tidak terbentuk atau tersedianya kebijakan tersebut maka dapat menimbulkan kerugian terhadap perusahaan, dikarenakan tidak adanya pengelolaan terstruktur untuk menjaga kerahasiaan perusahaan dan yang bertanggungjawab atas tersebarnya data informasi tersebut.
A.10 Manajemen Komunikasi dan Informasi	A.10.7.3	Belum adanya kebijakan yang mengatur tentang penyimpanan data pekerjaan yang sesuai dengan ranah kerja dan divisinya agar tidak terjadi kebocoran informasi dan disalin oleh pihak yang tidak berwenang.	• Adanya kebijakan berbagi informasi dari siapa kepada siapa, hal apa saja yang diizinkan untuk dibagikan secara eksternal maupun internal, serta dimana sebaiknya data informasi tersebut tersimpan.	Apabila tidak terbentuk atau tersedianya kebijakan tersebut maka akan terjadi kerancuan mengenai penempatan penyimpanan data yang dapat mengakibatkan bocornya informasi dari divisi yang seharusnya tidak mengetahui hal tersebut.
A.11 Pengendalian Akses	A.11.1.1, A.11.2.1, A.11.6	Belum adanya kebijakan dan prosedur pengelolaan hak akses	• Adanya penentuan terhadap akses data, program atau sistem	Apabila belum terbentuk dan tersedianya kebijakan tersebut, dapat mengganggu kinerja

Domain	Klausul	Kondisi Terkini	Kondisi Global	Resiko jika tidak ada
		pengguna sistem dan aplikasi. Belum adanya penanganan password pada aplikasi missal aplikasi telah memaksa user untuk mengubah password secara berkala.	hanya diberikan kepada pengguna sesuai dengan hak wewenang. • Adanya arahan untuk batasan koneksi dalam mengakses aplikasi yang berisiko tinggi.	karyawan untuk melakukan pekerjaan lain yang bukan wewenangnya dan hal ini juga berkaitan dengan lisensi *software* yang telah dimiliki oleh perusahaan.

Dengan mengetahui hal yang dibutuhkan oleh perusahaan serta mengetahui dampak apabila hal tersebut tidak tersedia maka, kondisi yang diharapkan dengan adanya kebijakan tersebut adalah :

1. Tata kelola teknologi informasi yang komprehensif dan efektif akan terwujud, dikarenakan adanya pengelolaan infrastruktur TIK.
2. Terdapat disiplin terhadap kinerja karyawan dengan pembatasan penggunaan aplikasi dan akses yang ditentukan oleh perusahaan.
3. Penentuan tanggung jawab serta alur untuk pengelolaan teknologi informasi pada perusahaan.

3.7 Penentuan dan Perancangan Framework

Berdasarkan identifikasi, mengkaji literatur dan pengumpulan data yang telah dilakukan oleh peneliti maka ditentukan SNI ISO/IEC 27001:2009 sebagai model kerangka dasar yang akan diambil untuk merancang kebijakan atau prosedur tata kelola keamanan informasi PT. XX.

Proses yang akan dilakukan pada tahap ini adalah menetapkan batasan dan ruang lingkup dari SMKI yang akan dirancang sesuai dengan karakteristik dan fungsi dari organisasi PT. XX, lokasinya, aset dan teknologi.

Yang dilakukan proses berikutnya adalah menetapkan kebijakan SMKI sesuai dengan karakteristik dan fungsi dari organisasi, lokasinya, aset dan teknologi. Pada tahapan ini penelitian menghasilkan dokumen kebijakan keamanan informasi dan panduan klasifikasi informasi yang akan diajukan sebagai Rancangan Peraturan PT. XX.

Proses penetapan dokumen kebijakan keamanan informasi mengacu kepada beberapa sasaran pengendalian yang terdapat pada standar SNI ISO/IEC 27001:2009. Fokus sasaran pengendalian pada tahapan ini adalah pembuatan dokumen kebijakan keamanan informasi dan panduan klasifikasi informasi seperti yang dilampirkan pada lampiran 3 dan 4.

Tabel 4. 2 Cakupan dokumen pada proses menetapkan kebijakan SMKI

No.	Klausul SNI 27001	Nama Dokumen	Cakupan Dokumen
1.	4.2.1	Kebijakan Keamanan Informasi	Menetapkan ruang lingkup dan batasan sesuai dengan karakteristik bisnis. Mencakup kerangka kerja untuk menyusun sasaran dan menetapkan arahan berkenaan dengan keamanan informasi. Serta persetujuan terhadap kebijakan dan program keamanan informasi.
2.	A.7.2.1	Pedoman Klasifikasi Informasi	Petunjuk mengenai cara melakukan klasifikasi informasi yang ada di perusahaan harus diklasifikasikan sesuai dengan nilai, persyaratan hukum, sensitivitas dan tingkat kritisnya terhadap organisasi.

3.8. Menerapkan dan Mengoperasikan Sistem Manajemen Keamanan Informasi

Pada tahap ini menghasilkan dokumen kebijakan penggunaan *e-mail*, *internet*, komputer/laptop, *temporary*, akses penyimpanan data serta aturan sumber daya informasi yang merupakan bagian dari dokumen kebijakan keamanan informasi yang akan diajukan untuk Rancangan Tata Kelola Informasi.

Dalam proses menerapkan dan mengoperasikan dokumen kebijakan keamanan informasi mengacu kepada beberapa sasaran pengendalian yang terdapat pada standar SNI ISO/IEC 27001:2009. Dan fokus sasaran pengendalian pada tahap ini adalah pembuatan dokumen kebijakan penggunaan aset TIK, kebijakan penyimpanan informasi, kebijakan pengendalian akses, manajemen akses pengguna, manajeman pengendalian akses aplikasi dan informasi.

3.9 Validasi

Validasi yang dilakukan dalam penelitian ini adalah dengan menerapkan member checking untuk mengetahui akurasi dari rancangan kebijakaan yang akan dihasilkan.

Dengan membawa rancangan kebijakan yang sudah dibuat oleh peneliti dan membahasnya dalam diskusi dengan bagian yang berwenang di PT. XX yang memproduksi film animasi dalam kesehariannya. Agar mengetahui teknologi dan informasi sudah tepat, akurat dan sesuai dengan kebijakan yang dibuat oleh peneliti untuk diuji bila nantinya diterapkan di perusahaan.

Dalam pembahasan diskusi dan memberikan daftar pertanyaan tersebut dihadiri oleh *CEO, Chief of HRD-IT-GA, IT Manager* dan para *Lead Production* untuk mengetahui tanggapannya atas rancangan kebijakan tersebut serta menguji apakah rancangan tersebut sudah akurat dan sesuai dengan kebutuhan perusahaan.

4. KESIMPULAN

SNI ISO/IEC 27001:2005 digunakan sebagai dasar penyusunan tata kelola keamanan informasi yang disesuaikan dengan kebutuhan yang diperlukan perusahaan. Berdasarkan hasil analisa penyusunan tata kelola keamanan informasi dengan tahap pengumpulan data, mengidentifikasi tentang perusahaan sehingga ditemukan pengelolaan aset, manajemen komunikasi dan informasi, dan pengendalian akses untuk dirancang kebijakannya sebagai tuntunan perusahaan.

Dihasilkan perancangan kebijakan keamanan informasi dan pedoman klasifikasi. Dan dalam penerapan dan mengoperasikan SMKI dalam penggunaan e-mail, internet, komputer dan laptop serta penyimpanan data. Dan untuk kebijakan yang telah dibuat memverifikasi dengan cara member checking untuk mengetahui akurasi dari rancangan kebijakan yang akan dihasilkan.

DAFTAR PUSTAKA

[1] Henderi, "IT Governance : framework and prototype or higher education," *CCIT*, vol. 3, 2010.
[2] C. . Bacon, *The Use of Decision Criteria in Selecting Information System/ Technology Investment*, 3rd ed. MIS Quaeterly, 1992.
[3] BSNI (Badan Standardisasi Nasional), "SNI ISO/IEC 27001:2009," 2009.
[4] R. Sarno, "Information Technology Security Techniques Informa Security Management System Requirements," in *Audit Sistem & Teknologi Informasi*, Surabaya: ITS Press 2, 2009.
[5] H. Jogiyanto, "Konsep dan Aplikasi Structural Equation Modelling Berbasis Varian dalam Penelitian Bisnis," *UPP STIM YKPN*, vol. 1, 2011.
[6] W. and Ross, "How Top Performers Manage IT Decision Rights for Suoerior Results," in *IT Governance*, Boston: Harvard Business School Press, 2004.
[7] H. Februariyanti, "Standar dan Manajemen Keamanan Komputer," *Teknol. Inf. Din.*, vol. XI No.2.
[8] Calder A, Watkisn S, *A Manager's Guide to Data Security and ISO 27001/ISO 27002*, 4th Editio. IT Governance Publishing, 2008.
[9] BERR ISBS, "Information Security Breaches Survey," 2008.
[10] Kementrian Komunikasi dan Informatika Republik Indonesia, "Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelanggara Pelayanan Publik," 2011.
[11] S. and G. S. Garfinkel, "Practical UNIX & Internet Security2nd edition," *O'Reilly Assoc.*, 1996.