BAYESIAN PROBABILISTIK SEBAGAI PENDEKATAN *HEURISTIC* UNTUK MANAJEMEN RESIKO TEKNOLOGI INFORMASI

Indri Sudanawati Rozas[1], Riyanarto Sarno[2]
[1,2] Jurusan Teknik Informatika, Fakultas Teknologi Informasi,
Institut Teknologi Sepuluh Nopember
Kampus ITS Keputih - Sukolilo Surabaya 60111, Jawa Timur, Indonesia
email : indrisrozas@gmail.com[1], riyanarto@if.its.ac.id[2]

ABSTRAK

Manajemen resiko banyak menjadi bahasan beberapa waktu terakhir ini. Salah satu langkah dari manajemen resiko yang menjadi topik akhir-akhir ini adalah tentang bagaimana cara menghitung resiko (*risk assessment*) dengan baik. *Risk assessment* menjadi bahasan yang penting karena angka yang dihasilkannya akan menjadi rekomendasi bagi langkah-langkah selanjutnya pada manajemen resiko. Untuk itu diperlukan sebuah metode yang tepat dan akurat untuk melakukan *risk assessment*.

Secara mendasar ada dua metode untuk menghitung resiko, yaitu metode kualitatif dan kuantitatif. Masing-masing pendekatan tersebut memiliki kelebihan dan kekurangan. Telah banyak penelitian yang mencoba memperbaiki hasil penghitungan resiko, baik menggunakan metode kuantitatif maupun kualitatif. Pendekatan yang banyak dilakukan akhir-akhir ini adalah menggabungkan metode metode kualitatif dan kuantitatif. Namun dari beberapa penelitian yang menggabungkan kedua metode tersebut terdapat kekurangan yang mendasar, yaitu metode perhitungan yang kompleks.

Penelitian ini mengajukan metode *risk assessment* yang menggabungkan kelebihan-kelebihan metode kuantitatif dan kualitatif dengan model dan cara perhitungan yang sederhana. Hasil penelitian ini diharapkan dapat memberikan pedoman bagi *engineer* yang berkecimpung di dunia manajemen resiko TI untuk melakukan prediksi resiko yang akurat berdasarkan gabungan metode kualitatif dan kuantitatif.

***Kata kunci*:** manajemen resiko, bayesian, *prior*, *posterior*, heuristic

PENDAHULUAN

Manajemen resiko adalah sebuah domain keilmuan yang banyak menjadi bahasan beberapa waktu terakhir ini. Hampir semua disiplin ilmu membahas isu tentang bagaimana melaksanakan manajemen resiko dengan baik. Salah satu langkah dari manajemen resiko yang menjadi topik akhir-akhir ini adalah tentang bagaimana cara menghitung resiko (*risk assessment*) dengan baik. *Risk assessment* menjadi bahasan yang penting karena angka yang dihasilkannya akan menjadi rekomendasi bagi langkah-langkah selanjutnya pada manajemen resiko. Dan tentunya semua organisasi berharap nilai yang dihasilkan dari *risk assesment* mempunyai nilai akurasi yang tinggi. Karena dengan berdasar pada nilai tersebut organisasi akan menentukan sebuah langkah penting untuk menangani resiko yang mungkin muncul di masa mendatang. Untuk itu diperlukan sebuah metode yang tepat dan akurat untuk melakukan *risk assessment*.

Manajemen resiko adalah proses untuk mengidentifikasi resiko, menganalisa resiko dan melakukan penanganan untuk mengurangi resiko[1]. Menajemen resiko

ISBN : 978-602-97491-1-3

meliputi aktifitas: identifikasi informasi, identifikasi ancaman dan kelemahan, analisa dampak bisnis serta penghitungan resiko (*risk assessment*)[1]. Secara mendasar ada dua metode untuk penghitungan resiko, yaitu metode kualitatif dan kuantitatif [1]. Masing-masing pendekatan tersebut memiliki kelebihan dan kekurangan.

Telah banyak penelitian yang mencoba memperbaiki hasil penghitungan resiko, baik menggunakan metode kuantitatif maupun kualitatif. Salah satu penelitian yang mencoba memperbaiki hasil penghitungan metode kualitatif adalah dengan menambahkan pertimbangan terhadap faktor manusianya [2]. Sedangkan penelitian yang mencoba memperbaiki hasil metode kuantitatif yang dilakukan oleh penelitian [3] adalah dengan cara memasukkan semua data empiris yang dimiliki oleh organisasi.

Dan pendekatan yang banyak dilakukan akhir-akhir ini adalah menggabungkan metode metode kualitatif dan kuantitatif, diantaranya penelitian [4, 5, 6, 7]. Penelitian [4] pada tahun 2000 memperkenalkan sebuah kerangka pendekatan baru yang menggabungkan metode kualitatif dan kuantitatif. Namun, dalam publikasi tersebut hanya berhenti sampai pada tahap konseptual. Penelitian [5] menggabungkan metode kuantitatif dan kualitatif pada tahap validasi data kuantitatif. Di sini, data-data kuantitatif yang dimiliki akan dipilah secara kualitatif oleh pakar untuk menentukan data mana yang akan digunakan ke dalam perhitungan akhir. Sedangkan penelitian [6] melakukan penggabungan dari sisi software. Dua buah software *risk assessment* digabungkan, tahap pertama yang dijalankan adalah software kualitatif, kemudian hasil dari perhitungannya dimasukkan ke proses dalam tahap kedua. Dimana tahap kedua menggunakan software kuantitatif. Pada penelitian terakhir [7] dilakukan pendekatan untuk melakukan penggabungan kedua metode dengan komprehensif. Model yang diusulkan bisa menjawab *risk assessment* baik pada contoh kasus sederhana maupun kompleks. Namun model yang dibuat terdiri dari langkah-langkah yang kompleks, bahkan melibatkan peran pakar dengan intens. Hal ini tentu saja tidak menarik bagi organisasi yang memiliki keterbatasan dari sisi sumberdaya manusia maupun finansial.

Untuk itu, penelitian ini mengajukan metode *risk assessment* yang menggabungkan kelebihan-kelebihan metode kuantitatif dan kualitatif dengan model dan cara perhitungan yang sederhana. Makalah dimulai dari dasar-dasar pemikiran dalam dunia *risk assessment* yang mendasari pembuatan model bayesian probabilistik untuk menajemen resiko yang diusulkan. Dilanjutkan dengan pembahasan secara khusus mengenai contoh *risk assessment* menggunakan metode kualitatif dan kuantitatif. Di bagian tiga makalah dibahas mengenai model baru yang diusulkan. Dan yang terakhir adalah *case study* yang diterapkan pada model baru yang diusulkan. Penelitian ini diharapkan dapat memberikan pedoman bagi *engineer* yang berkecimpung di dunia manajemen resiko TI untuk melakukan prediksi resiko yang akurat berdasarkan gabungan metode kualitatif dan kuantitatif.

DASAR TEORI

Bagian dua makalah ini berisi dasar-dasar teori tentang menejemen resiko,resiko teknologi informasi, metode penghitungan resiko kualitatif dan kuantitatif, serta teorema bayes. Dasar-dasar teor tersebut menjadi pengantar ke bagian tiga yang secara khusus membahas tentang bagaimana bayesian probabilistik untuk manajamen resiko teknologi informasi.

ISBN : 978-602-97491-1-3

Manajemen Resiko

Manajemen resiko adalah proses untuk mengidentifikasi resiko, menganalisa resiko dan melakukan penanganan untuk mengurangi resiko[1].

Menurut definisi Wikipedia, tujuan dilakukannya manajemen resiko adalah untuk mengurangi resiko sampai pada tingkat yang dapat diterima. Dikatakan juga bahwa pelaksanaan manajemen resiko melibatkan segala cara yang tersedia bagi manusia, khususnya, bagi entitas manajemen risiko (manusia, staff, dan organisasi)[8]. Secara umum manajemen resiko meliputi tiga tahapan proses [9]:

a. *Risk assessment,*
b. *Risk Mitigation*,
c. *Evaluation and Assessment*.

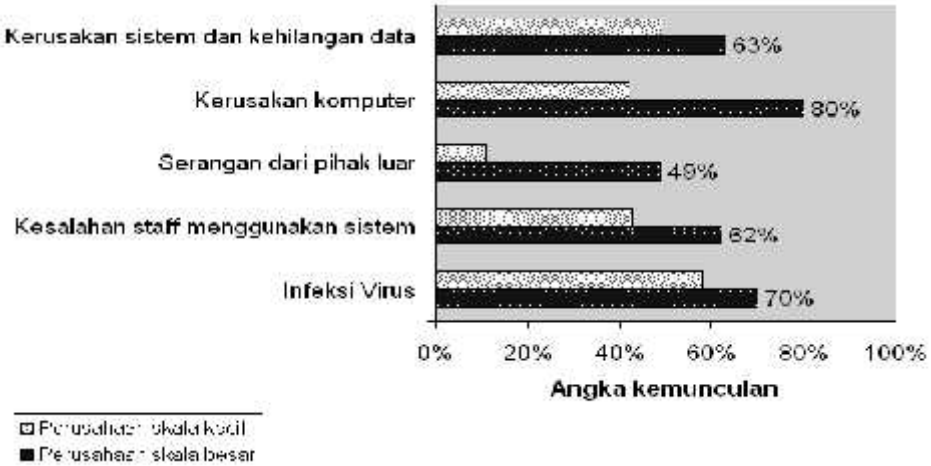
Dan langkah-langkah penghitungan risiko meliputi sembilan langkah utama sebagai berikut: *System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations, Results Documentation*[9].

Secara umum ada dua kelompok pendekatan untuk menentukan nilai resiko, yaitu metode kuantitatif dan kualitatif. Masing-masing pendekatan memiliki kelebihan dan kekurangan. Penelitian [10] dan [11] secara rinci membahas tentang kelebihan dan kekurangan masing-masing metode tersebut.

Resiko Teknologi Informasi

Teknologi Informasi sebagai sebuah alat untuk membantu pekerjaan manusia memiliki dampak pada sisi positif dan negatif. Dampak positif yang secara nyata dirasakan oleh pengguna teknologi informasi adalah efisiensi di berbagai hal, diantaranya adalah waktu, jarak, biaya. Namun di sisi yang lain terbukanya akses informasi sangat berpengaruh atas keamanan data yang dimiliki.

Berdasarkan hasil survey yang dipublikasikan oleh Infosecurity Europe pada 28 April 2010 [12], diperoleh data ancaman keamanan teknologi informasi di Inggris sebagaimana pada Gambar 1.



Gambar 1. Contoh Daftar Gangguan Keamanan

Tingginya angka gangguan keamanan menjadi dasar mengapa manajemen resiko harus dilaksanakan pada setiap perusahaan. Hal ini penting karena menyangkut integritas sebuah perusahaan. Apalagi jika merujuk pada hasil survey di atas yang menyatakan bahwa usaha penyerangan dari pihak luar pada perusahaan mencapai 49%.

ISBN : 978-602-97491-1-3

Analisis Resiko Kuantitatif

Analisis resiko metode kuantitatif adalah sebuah metode penghitungan resiko yang dilakukan berdasarkan hasil perhitungan mengunakan rumus/persamaan matematis [1]. Angka yang diperoleh dalam metode kuantitatif dapat diperoleh dari beberapa *tools* diantaranya: *probability based*, *non-probabilistic models*, dan *bencmarking*[13].

Salah satu rumus yang digunakan untuk *risk assessment* metode kuantitatif dengan input data berupa bencmaring yang tertera pada [1] adalah:

Risk value = NA x BIA x NT, (1)

dimana NA adalah nilai aset, BIA adalah dampak terhadap bisnis, dan NT adalah nilai ancaman. Sebagai ilustrasi bentuk perhitungan nyata dari rumus di atas ada pada Tabel 1.

Tabel 1. Hasil analisis resiko kuantitatif

Jenis Gangguan Keamanan	Nilai Aset (skala 1 s/d 4)	Analisa Dampak Bisnis (skala 1 s/d 4)	Nilai Ancaman (skala 1 s/d 4)	Nilai Resiko
Infeksi Virus	1	1	4	4
Kesalahan staff menggunakan sistem	3	3	2	18
Serangan dari pihak luar	3	4	3	36
Kerusakan komputer	4	4	1	16
Kerusakan sistem dan kehilangan data	2	3	2	12

Nilai pada variabel nilai aset, analisa dampak bisnis, dan nilai ancaman diperoleh dari pendapat pakar keamanan informasi. Nilai yang dimasukkan dari rentang 1 sampai dengan 4, dimana 1 menandakan bahwa pakar memberikan nilai kecil (low) dan 4 bernilai besar (high). Nilai resiko yang dihasilkan melalui persamaan (1) memberikan arti bahwa semakin tinggi nilainya maka semakin serius ancaman tersebut bagi perusahaan. Namun angka yang dihasilkan pada Tabel 1 pada kolom terakhir, yang menyatakan nilai resiko, tidak mudah untuk dipahami.

Analisis Resiko Kualitatif

Berbeda dengan pendekatan kuantitatif yang mengharuskan untuk menghasilkan sebuah angka, metode kualitatif terkait dengan subyektifitas pakar keamanan informasi. Salah satu metode kualitatif yang digunakan adalah menggunakan matriks resiko sebegaimana pada Gambar 2 [14]. Setiap resiko yang ada dipetakan berdasarkan nilai kecenderungan dan dampak yang ditimbulkan. Misalkan, jika pakar mengatakan bahwa infeksi virus memiliki kecenderungan kemunculan 5 (medium) dan nilai dampak 2 (low), maka berdasarkan Gambar 1 nilai resiko virus terhadap perusahaan adalah medium.

Begitu juga jika diterapkan pada jenis ancaman serangan dari pihak luar. Sekalipun menurut pakar kecenderungannya 1 (low), namun jika dampak yang ditimbulkan adalah 5 (high), maka nilai ancaman tersebut berdasarkan Gambar 2 bernilai high.

ISBN : 978-602-97491-1-3

BAYESIAN PROBABILISTIK UNTUK MANAJEMEN RESIKO

Pada Bab 3 makalah ini akan dipaparkan bagaimana model bayesian probabilisitik diusulkan, metodologi penelitian, serta rancangan percobaan untuk desain implementasi model yang diusulkan.

Analisis Metode Penghitungan Resiko

Tabel 1 memaparkan analisa terhadap kedua pendekatan tersebut. Pernyataan diambil dari dua penelitian terbaru tahun 2010 [10] dan 2008 [11] yang membahas tentang kedua jenis pendekatan tersebut. Tabel 1 menjadi dasar pertimbangan untuk membangun sebuah model baru yang menggabungkan kelebihan-kelebihan yang ada sekaligus menghilangkan kekurangan-kekurangan yang dimiliki.

Tabel 1. Kelebihan dan kekurangan metode perhitungan resiko kualitatif dan kuantitatif

Pendekatan	Metode Kualitatif	Metode Kuantitatif
Kelebihan	▪ Mengunakan perhitungan sederhana ▪ Tidak membutuhkan nilai 'rupiah' resiko ataupun frekuensi kemunculan gangguan keamanan ▪ Lebih hemat waktu dan biaya ▪ Selalu menggunakan priotitasi resiko, sehingga lebih mudah dipahami oleh orang awam	▪ Informasi terhadap nilai 'rupiah' bersifat objektif ▪ Pengembalian investasi untuk mengimplementasikan sistem keamanan dapat diukur ▪ Angka yang diperoleh dapat menjadi dasar untuk mengevaluasi kinerja manajemen resiko ▪ Memberikan gambaran yang lebih nyata tentang angka resiko sebuah perusahaan
Kekurangan	▪ Proses pengisian matrik bersifat subjektif ▪ Tidak ada perhitungan nilai menggunakan angka ▪ Tidak ada objektifitas terhadap penghitungan dampak gangguan keamanan ▪ Probabilitas yang muncul terhadap gangguan keamanan tidak dapat diukur secara angka ▪ Analisis untung-rugi perusahaan terhadap penerapan manajemen resiko tidak dapat dilakukan dengan mudah ▪ Hasil akhirnya berupa perkiraan	▪ Perhitungan yang dilakukan kompleks ▪ Membutuhkan data dalam jumlah yang sangat besar ▪ Kurangnya standar yang memberikan daftar ancaman keamanan ▪ Akurasi yang dihasilkan tergantung akurasi pada proses pengukuran data di lapangan ▪ Hasil berupa angka yang ditampilkan tidak bisa langsung dimengerti artinya oleh orang awam ▪ Membutuhkan waktu dan biaya yang tidak sedikit

Sumber: [10, 11]

Metode Hybrid

Kelebihan-kelebihan kedua metode *risk assessment* menarik untuk dijadikan dasar melakukan manajemen resiko. Namun kekurangan-kekurangan yang dimiliki oleh masing-masing metode dkhawatirkan akan menyulitkan mekanisme rekomendasi pada manajemen resiko. Untuk itu, metode hybrid yang menggabungkan kelebihan kedua metode tersebut menarik untuk dijadikan penelitian.

Sebagaimana dibahas pada pendahuluan, ada empat penelitian terdahulu yang telah mencoba melakukan penggabunan metode kualitatif dan kuantitatif [4, 5, 6, 7]. Masing-masing penelitian tersebut memiliki kelebihan dan kekurangan. Penelitian [4] hanya melakukan penelitian pada tahap konseptual. Penelitian [5] menggabungkan metode kuantitatif dan kualitatif pada tahap validasi data kuantitatif secara manual. Sedangkan penelitian [6] melakukan penggabungan dari sisi *software* yang tidak

ISBN : 978-602-97491-1-3

memiliki kepastian kebenaran dari sisi penarikan kesimpulan. Dan penelitian [7] membuat model yang terdiri dari langkah-langkah yang kompleks dan melibatkan peran pakar dengan intens sehingga menyulitkanpada level aplikasi di lapangan. Untuk itu diperlukan pendekatan baru yang dapat menggabungkan kelebihan metode kuantitatif dan kualitatif namun dengan menghilangkan kekurangan-kekurangan yang ditimbulkan.

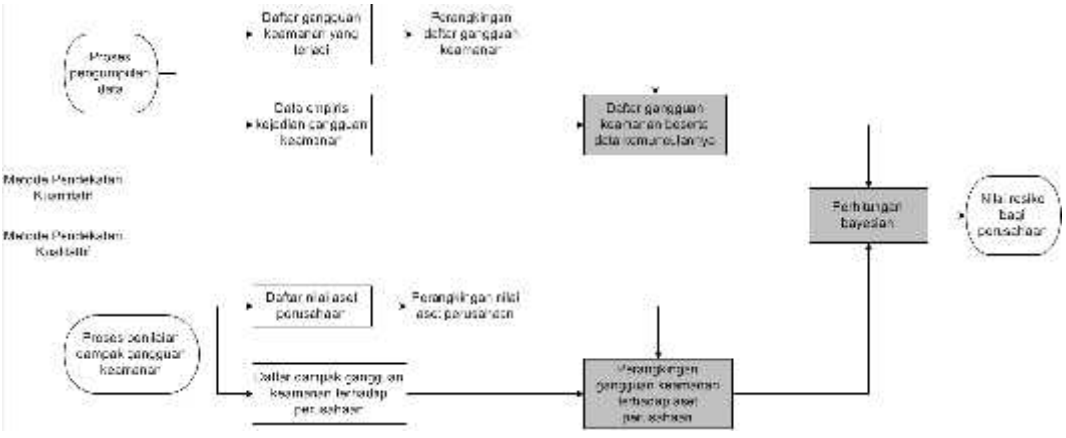
Metodologi Bayesian Probabilistik

Sebagaimana telah dibahas di atas, dibutuhkan sebuah pendekatan baru yang dapat menggabungkan metode kualitatif dan kuantitatif namun memiliki model yang sederhana. Dan model bayesian probabilistik dapat menjawab tantangan tersebut. Menggabungkan metode kualitatif dan kuantitatif inilah yang menjadi kelebihan utama metode bayesian [18]. Kuantitatif yang dimaksud adalah data di lapangan yang digunakan sebagai *input*, dan kualitatif yang dimaksud adalah data *prior* yang datang dari pendapat pakar[16,18].

Untuk melakukan perhitungan bayesian probabilistik untuk manajemen resiko teknologi informasi dilakukan langkah-langkah sebagaimana digambarkan pada Gambar 4. Langkah pertama adalah memperoleh data historikal terkait dengan gangguan keamanan teknologi informasi yang sering terjadi pada perusahaan. Data historikal tersebut merupakan likelihood (data yang dianggap mirip dengan perusahaan yang diteliti). Fase ini mewakili metode kuantitatif. Dalam penelitian ini data yang digunakan adalah hasil survey yang dipublikasikan oleh Infosecurity Europe pada 28 April 2010 [12].

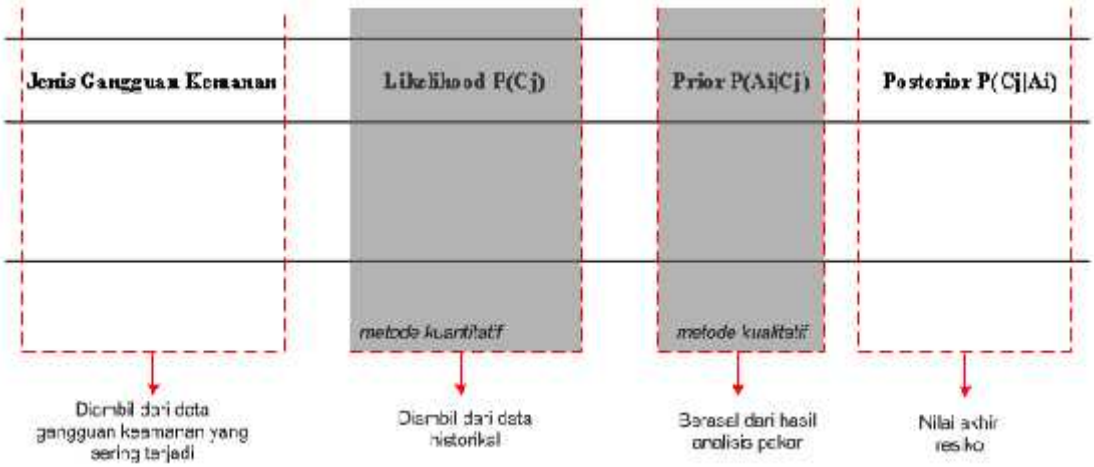
Kemudian dilanjutkan dengan fase berikutnya yaitu metode kualitatif. Kualitatif yang dimaksud di sini adalah penentuan nilai resiko berdasarkan justifikasi pakar. Dalam model bayesian pendapat pakar dinyatakan sebagai nilai prior. Nilai *prior* sebagai representasi dari pendapat pakar tentang sejauh mana impact dari gangguan keamanan berpengaruh kepada aset organisasi.

Setelah fase kuantitatif dan kualitatif dilaksanakan, langkah terakhir adalah perhitungan nilai *posterior* sebagai representasi dari nilai prediksi resiko. Langkah ini menggunakan metode perhitunga berdasarka teorema bayes sebagaimana tertera pada persamaan (2). Untuk lebih jelasnya langkah-langkah dalam melakukan metode bayesian probabilistik disajikan pada Gambar 4. Hasil dari setiap langkah akan menjadi input bagi langkah berikutnya. Dan hasil akhir (posterior) inilah yang akan menjadi angka yang mendasari rekomendasi.



Gambar 4. Langkah-Langkah Bayesian Probabilistik Untuk Menejemen Resiko Teknologi Informasi

ISBN : 978-602-97491-1-3



Gambar 5. Model Perhitungan Bayesian Probabilistik Untuk Menejemen Resiko Teknologi Informasi

Model Penghitungan Resiko pada Bayesian Probabilistik

Berdasarkan langkah-langkah pada Gambar 4, untuk melakukan perhitungan secara nyata diusulkan format perhitungan yang terdapat pada Gambar 5. Tabel yang digunakan relatif sederhana. Hanya terdiri dari empat kolom dengan isi masing-masing sebagaimana keterangan pada Gambar. Pada model bayesian probabilistik hasil akhir nilai resiko (posterior) diperoleh dengan menggunakan persamaan (2)

Jenis gangguan kemanan diisi sesuai catatan historikal yang dimiliki. P(Cj) adalah data historikal berupa banyaknya kejadian gangguan keamanan diperoleh dari catatan kejadian ancaman keamanan informasi perusahaan di tahun-tahun sebelumnya. Atau dapat juga diperoleh dari data resiko perusahaan lain yang sejenis dengan perusahaan yang bersangkutan. Inti dari isi data historikal adalah memberikan variabel yang berisi data-data ancaman yang mungkin muncul di berusahaan tersebut.

Sedangkan nilai prior P(Ai|Cj) adalah penghitungan yang dilakukan oleh pakar berdasarkan pertimbangan sejauh mana gangguan keamanan akan mempengaruhi keninerja perusahaan secara keseluruhan. Nilai prior dapat berupa pertimbangan impact yang akan muncul jika gangguan keamanan terjadi, atau dapat juga pertimbangan pakar atas nilai aset yang mungkin hilang jika gangguan keamanan terjadi, atau gabungan dari keduanya. Sedikit berbeda dengan metode kuantitatif, pada model yang diusulkan pakar dapat menuliskan nilai prior berdasarkan persentase dengan tujuan penekanan yang lebih jelas, atau dapat pula diisi dengan urutan prioritas 1 sampai dengan 4 sebagaimana metode kuantitatif biasa. Setelah kedua variabel tersebut diisikan, maka langkah selanjutnya adalah menghitung total gangguan keamanan yang mungkin terjadi P(A) xjika diketahui data P(C) dan P(A|C). P(A) diperoleh dari sigma hasil perkalian antara P(Cj)* P(Ai|Cj).

Langkah terakhir adalah melakukan perhitungan nilai posterior P(Cj|Ai). Yang menarik, berapapun nilai yang dimasukkan ke dalam likelihood dan prior, hasil nilai posterior dari semua jenis gangguan ini jika ditotal akan bernilai 1. Mengapa hal ini terjadi, dikarenakan nilai posterior merupakan hasil antara P(Cj)* P(Ai|Cj) dibasgi dengan P(A). Secara matematis ini dapat dijelaskan sebagai bentuk normalisasi hasil.

ISBN : 978-602-97491-1-3

Contoh Penggunaan Bayesian Probabilistik untuk Manajemen Resiko Teknologi Informasi

Untuk memberikan gambaran bahwa model bayesian probabilistik yang diusulkan memberikan manfaat dan kontribusi untuk proses perhitungan manajemen resiko, ada tiga contoh perhitungan yang dirancang. Untuk memudahkan pembahasan hasil, perhitungan dilakukan dengan menggunakan set data yang sama. Tiga contoh perhitungan tersebut terdapat pada Tabel 2, Tabel 3 dan Tabel 4.

Tabel 2. Hasil perhitungan resiko menggunakan metode kualitatif.

Jenis Gangguan Kemanan	Nilai resiko
Infeksi Virus	Low
Kesalahan staff menggunakan sistem	Low
Serangan dari pihak luar	High
Kerusakan komputer	Medium
Kerusakan sistem dan kehilangan data	Medium

Tabel 3. Hasil perhitungan resiko menggunakan metode kuantitatif

Jenis Gangguan Kemanan	Nilai Aset (skala 1 s/d 4)	Analisa Dampak Bisnis (skala 1 s/d 4)	Nilai Ancaman (skala 1 s/d 4)	Nilai Resiko
Infeksi Virus	1	1	4	4
Kesalahan staff menggunakan sistem	3	3	2	18
Serangan dari pihak luar	3	4	3	36
Kerusakan komputer	4	4	1	16
Kerusakan sistem dan kehilangan data	2	3	2	12

Tabel 4. Hasil perhitungan resiko menggunakan metode bayesian probabilistik

Jenis Gangguan Kemanan	Data historikal (likelihood)	Nilai prior (pendapat pakar)	Posterior (nilai resiko akhir)
Infeksi Virus	70,00%	7,00%	8,91%
Kesalahan staff menggunakan sistem	62,00%	5,00%	5,64%
Serangan dari pihak luar	49,00%	70,00%	62,36%
Kerusakan komputer	80,00%	8,00%	11,64%
Kerusakan sistem dan kehilangan data	63,00%	10,00%	11,45%

Tabel 2 memaparkan hasil perhitungan jika resiko dihitung mengunakan metode kualitatif. Perhitungan sangat sederhana, hanya berdasarkan justifikasi pakar terhadap masing-masing gangguan keamanan dan kemudian memasukkannya ke dalam tabel pada Gambar 2 untuk menghasilkan klasifikasi. Terlihat bahwa nilai resiko yang dihasilkan hanya berupa klasifikasi low, medium dan high. Tabel 3 memperlihatkan hasil perhitungan dengan metode kuantitatif. Data yang dimasukkan dihitung menggunakan persamaan (1). Sedangkan Tabel 4 adalah hasil perhitungan dengan metode bayesian probabilistik, nilai yang dimasukkan sama dengan nilai data historikal yang diperoleh dari hasil survey [12]. Nilai resiko yang dihasilkan tertera pada kolom terakhir tabel.

ISBN : 978-602-97491-1-3

Perbandingan Metode Kulitatitif dengan Metode BayesianProbabilistik

Apabila Tabel 2 dan Tabel 4 dibandingkan, maka akan terlihat nyata kelebihan metode bayesian probabilistik. Nilai akhir resiko yang berupa persentase nilai kerugian, yang ditimbulkan oleh gangguan keamanan, akan dapat langsung dijadikan rujukan sebagai rekomendasi. Apalagi jika dianalisis dari sudut pandang input untuk proses perhitungan. Justifikasi dampak dan frekuensi kemunculan gangguan yang dilakukan oleh pada metode kualitatif berpotensi menimbulkan ambiguitas. Karena satu pakar dengan pakar yang lain sangat mungkin memberikan nilai yang berbeda. Dan tentu saja akan menghasilkan penilain resiko yang berbeda.

Sedangkan pada metode bayesian probabilistik, walaupun sma-sama ada justifikasi dari pendapat pakar dimasukkan ke dalam proses perhitungan, namun nilai tersebut tidak sepenuhnya dijasikan acuan, karena dilakukan dinormalisasi dengan adanya data historikal di lapangan yang dimasukkan sebagai faktor pengali.

Perbandingan Metode Kuantitatif dengan Metode BayesianProbabilistik

Perbandingan antara metode kuantitatif dan metode bayesian probabilistik dilakukan dengan membandingkan Tabel 3 dan Tabel 4. Secara input data, metode kuantitatif dan bayesian probabilistik relatif lebih obyektif dibandingkan dengan metode kualitatif. Karena nilai input yang dimasukkan sudah berupa data historikal di lapangan. Namun kekurangan metode kuantitatif terletak pada hasil penghitungan resiko. Sekalipun nilai resiko yang dihasilkan oleh perhitungan pada Tabel 3 sudah berbentuk angka, namun angka tersebut masih menimbulkan kemungkinan perbedaan arti bagi pembaca. Sekalipun angka yang dihasilkan menunjukkan skala prioritas, namun untuk melakukan rekomendasi diperlukan langkah tambahan untuk menganalisis arti dari angka tersebut.

Hal ini berbeda dengan angka yang dihasilkan oleh metode bayesian probabilistik. Hasil akhir yang berupa persentase resiko dapat langsung dimengerti oleh pengguna. Selain tidak memungkinkan adanya makna ganda, hasil berupa persentase tersebut dapat langsung digunakan sebagai rekomendasi pada langkah manajemen resiko selanjutnya.

KESIMPULAN

Berdasarkan pembahasan serta contoh perhitungan yang telah diberikan, dapat disimpulkan hal-hal berikut:

- Metode bayesian probabilistik merupakan model yang sederhana untuk dilaksanakan dalam penghitungan resiko, karena hanya terdiri dari sebuah tabel dengan empat kolom (Gambar 5).

Dibandingkan dengan penelitian-penelitian sebelumnya yang menggabungkan metode kualitatif dan kuantitatif, metode bayesian probabilistik memiliki beberapa kelebihan, diantaranya: model yang sederhana sehingga mudah diimplementasikan pada level aplikasi, dan proses penarikan kesimpulan (inferencing) yang dapat dipertanggungjawabkan validitasnya

DAFTAR PUSTAKA

Beakdal, Thomas; Hansen, Kim L.; Todbjerg, Lars; Mikkelsen, Hendrik. (2006) Change Management Handbook. Final Edition.

ISBN : 978-602-97491-1-3

Davidson, Jeff (2002) *The Complete Ideal's Guides: Change Management*. First Edition. Alpha Books.

Spafford, George (2003) *IT Audit Checklist Series: Change Management*. Sixth Edition. IT Compliance Institute.

Government Office for The South West. (2007) *Managing Change: How To Manage Change in an Organisation.* First Edition. Envirowise & Government Office for The South West.

Perumpalath, Binoy P.; Labib, Ashraf W. (2005) *Modelling Business Process: An Integrated Approach.* Portsmouth Business School.

YPT (2009) *Peraturan Dasar Kepegawaian (PDK) Yayasan Pendidikan dan pelatihan Telkom*. YPT, Bandung.

ISBN : 978-602-97491-1-3