PEMODELAN MANAJEMEN RESIKO KEAMANAN JARINGAN MENGGUNAKAN *BAYESIAN NETWORKS* STUDI KASUS DI PT MELVAR LINTAS NUSA

Dafie Buthlan Noorrahman
Program Pascasarjana, Program Studi Magister Sistem Informasi
Universitas Komputer Indonesia
Jl. Dipati Ukur No 112-116, Bandung 40132
email: buthlan@gmail.com

Pengukuran keamanan suatu jaringan pada umumnya difokuskan pada pengukuran suatu ancaman tunggal terhadap aset tanpa mempertimbangkan akibat yang mungkin terjadi dari suatu ancaman terhadap aset lainnya serta kemungkinan terjadinya eksploitasi dari suatu ancaman terhadap aset yang disebabkan oleh ancaman dari tereksploitasnya aset yang lain, sulit untuk diketahui. PT Melvar Lintas Nusa (MELSA) merupakan sebuah perusahan penyedia jasa layanan internet yang memiliki konektifitas perangkat jaringan cukup luas di Bandung. Penerapan sistem keamanan jaringan merupakan langkah perlindungan terhadap ancaman yang mungkin terjadi guna mempertahankan layanan kepada pelanggan dan keberlangsungan proses bisnis. Tingkat keamanan yang berbeda-beda untuk masing-masing perangkat, dapat menimbulkan ancaman yang berbeda-beda. Ancaman tersebut merupakan risiko yang harus dihadapi.

Langkah-langkah pengukuran keamanan jaringan dalam penelitian ini, mengacu kepada tahapan-tahapan dalam manajemen resiko berdasarkan ISO 27005:2008. Katalog aset dan ancaman dari IT Baseline Protection digunakan sebagai panduan dalam melakukan identifikasi aset serta ancamannya. IT Baseline Protection merupakan suatu metodologi audit untuk keamanan teknologi informasi. Bayesian Network digunakan untuk memodelkan dan menghitung probabilitas dari suatu kejadian ancaman terhadap aset yang dapat menimbulkan risiko, dengan memperhatikan hubungan dari masing-masing ancaman yang akan mempengaruhi terjadinya suatu ancaman terhadap aset yang lainnya. Bayesian Network memberikan gambaran keterhubungan antara ancaman dan aset yang direpresentasikan dalam bentuk model grafis. Hasil dari model yang dirancang berupa tingkat keamanan jaringan yang diwakili oleh nilai low, medium dan high.

Kata kunci : keamanan, jaringan, manajemen risiko, Bayesian networks, IT Baseline Protection.

PENDAHULUAN

Laju perkembangan teknologi informasi semakin pesat dalam kurun waktu 10 tahun terakhir, namun seiring dengan perkembangan tersebut, tingkat penyalahgunaan dan kejahatan terhadap sistem informasi semakin meningkat, berdasarkan survey yang dilakukan oleh Computer Security Institute(CSI, 2009) 64.3% ancaman berasal dari *malware*, *financial fraud* 20%, *insider abuse of internet access* 30%, dan lain lain. Jumlah malware yang beredar di internet saat ini mencapai angka kisaran 2 juta *malware* khusus untuk sistem operasi berbasis windows(GData, 2011) dan berdasarkan laporan *Norton Cybercrime Index* 2011(Norton, 2011), setiap 9 detik muncul ancaman baru terhadap sistem komputer, ancaman-ancaman tersebut dapat menimbulkan risiko terhadap aset-aset Untuk menanggulangi, mengalihkan dan mengurangi risiko-risiko tersebut diperlukan manajemen risiko.

PT Melvar Lintas Nusa (MELSA) sebagai perusahaan penyedia jasa layanan internet memberikan layanan akses internet berbayar kepada seluruh pelanggannya, selain itu pun MELSA memberikan layanan internet tidak berbayar (gratis) untuk pengguna umum. Pelanggan dan pengguna umum terhubung ke internet melalui aset jaringan milik MELSA dengan perantara kabel maupun tanpa kabel (*wireless*) dengan tingkat keamanan yang berbeda-beda dari sisi masing-masing pengguna. Perbedaan tingkat keamanan dari masing-masing pengguna tersebut memungkinkan terjadinya ancaman keamanan terhadap jaringan MELSA dan

tidak menutup kemungkinan bahwa ancaman yang akan terjadi berasal dari pihak internal di MELSA yang berdampak terhadap keberlangsungan proses bisnis dan usaha di MELSA.

Dalam melakukan manajemen resiko, IT Baseline Protection(Helmbrecht .U, et.al, 2007) digunakan sebagai acuan untuk mendefinisikan aset-aset(*module*s) yang berhubungan dengan jaringan dan mengidentifikasi ancaman-ancaman (*threat*s) yang mungkin terjadi terhadap masing-masing aset yang merupakan langkah awal dalam manajemen risiko(BSI ISO27005. 2008). *Bayesian Netwok* digunakan untuk menggambarkan model dalam bentuk *directed acyclic graph* (DAG) (Peltier, 2005) dan mengukur ketidakpastian berdasarkan nilai probabilitas dari masing-masing kejadian, kemudian dalam menentukan tingkat resiko dari keamanan jaringan digunakan matrik rentang resiko dengan tingkatan nilai *low*, *medium* dan *high*.

TINJAUAN PUSTAKA

Keamanan Jaringan

Sebuah infrastruktur jaringan bersamaan dengan data dan informasi di dalamnya dikatakan aman(Batelli el al, 2008), jika harus memenuhi 3 syarat berikut ini jika ingin:

a) Kerahasiaan (*Confidentiality*), dimaksudkan sebagai jaminan bahwa data yang diakses, diketahui dan diperlakukan secara eksklusif oleh yang memiliki hak.
b) Integritas (*Integrity*), dimaksudkan sebagai jaminan bahwa data dan informasi yang melalui jaringan tersebut akurat dan bebas dari gangguan, kehilangan atau kerusakan.
c) Ketersediaan (*Availability*), dimaksudkan sebagai jaminan bahwa data dan informasi dapat diakses bila diperlukan. Sistem harus memiliki kapasitas yang cukup untuk memenuhi permintaan akses oleh pengguna.

IT Baseline Protection (IT-Grundschutzhandbuch)

Salah satu metodologi audit yang banyak digunakan adalah BSI - IT Baseline Protection Manual. IT Baseline Protection Manual yang diperkenalkan oleh BSI dan dikembangkan oleh BSI Jerman berisi kumpulan rekomendasi standar kontrol keamanan atau perlindungan. IT Baseline Protection Manual memberikan deskripsi yang luas mengenai kebijakan keamanan informasi, meliputi tanggung jawab manajemen pada kebijakan, menyatukan sebuah tim yang bertanggung jawab pada pengembangan kebijakan, baik dari segi isi kebijakan maupun penyebaran kebijakan.

Struktur dari IT baseline Protection ini terdiri oleh, *Module*s, *Threat catalogue*s dan *Safeguard*s *Catalogues.*

Modules, berisi deskripsi singkat untuk masing-masing komponen sistem teknologi informasi serta gambaran scenario ancaman dan perlindungan yang direkomendasikan. *Module*s ini dikategorikan dalam kalatog berikut ini

1) B 1: Generic aspects of IT
2) B 2: Security of the infrastructure
3) B 3: Security of the IT systems
4) B 4: Security in the network
5) B 5: Security of applications

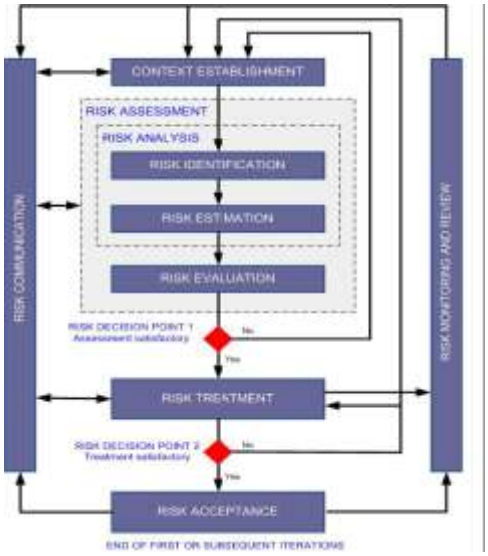
Dalam penelitian ini katalog *module*s yang digunakan yaitu pada bagian B 3 *Security of the IT systems* dan B 4 *Security in the network*.

Threat Catalogues, Bagian ini berisi deskripsi rinci dari ancaman termasuk di dalam skenario ancaman bagi masing-masing *modules*. Ancaman dikelompokkan menjadi lima kategorei katalog:

1) T 1: Force majeure
2) T 2: Organisational shortcomings
3) T 3: Human failure
4) T 4: Technical failure
5) T 5: Deliberate acts

Safeguards Catalogues, Bagian ini menjelaskan perlindungan keamanan yang bersesuainya terhadap ancaman yang terjadi di katalog modules. Namun tidak semua modules memiliki perlindungan, seperti tidak ada perlindungan yang diberikan dalam tahap pengadaan modul-server IIS. Langkah perlindungan ini dikelompokkan menjadi enam katalog, diantaranya:

1) S 1: Infrastructure
2) S 2: Organisation
3) S 3: Personnel
4) S 4: Hardware and software
5) S 5: Communication
6) S 6: Contingency planning



Gambar 1 Proses manajemen risiko keamanan informasi
(Sumber : BSI ISO27005,2008)

Manajemen Resiko

Berikut ini beberapa definisi dari manajemen risiko :

a) Manajemen risiko adalah proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan ekonomi terhadap langkah perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem TI dan data yang mendukung misi organisasi(S. Gary, 2002).
b) Manajemen risiko adalah proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang digunakan oleh organisasi dalam mencapai tujuan bisnis dan memutuskan penanggulangan atau kontrol seperti apa, jika ada, yang akan dilakukan dalam mengurangi risiko sampai pada tingkat yang dapat diterima(CISA, 2010).

Analisis Risiko

Analisis risiko adalah teknik yang digunakan untuk mengidentifikasi dan menilai faktor-faktor yang dapat membahayakan keberhasilan suatu proyek atau pencapaian tujuan organisasi(Peltier, 2005).

Identifikasi Aset

Aset adalah segala sesuatu yang memiliki nilai bagi perusahaan dan membutuhkan perlindungan(BSI ISO27005. 2008). Aset yang berkaitan dengan penelitian ini ialah aset yang termasuk kedalam infrastruktur jaringan. Dalam menentukan daftar aset tersebut, digunakan IT Baseline Protection(Helmbrecht .U, et.al, 2007) sebagai katalog panduan. Dari kalatog tersebut didapatkan daftar aset sebagai berikut ini:

1) B 3.301 Security gateway (Firewall)
2) B 3.302 Routers and switches
3) B 3.303 Storage systems and storage networks
4) B 4.1 Heterogeneous networks
5) B 4.2 Network and system management
6) B 4.3 Modem
7) B 4.4 Remote access
8) B 4.5 LAN integration of an IT system via ISDN
9) B 4.6 Wireless LAN

Identifikasi Ancaman

Ancaman memiliki potensi untuk membahayakan aset seperti informasi, proses dan organisasi itu sendiri. Sumber ancaman mungkin terjadi akibat alam atau manusia yang bersifat disengaja ataupun tidak disengaja. Satu ancaman dapat berdampak negatif terhadap banyak aset, tergantung jenis ancaman tersebut. Di dalam penelitian ini daftar ancaman yang disusun mengacu kepada IT Baseline Protection(Helmbrecht .U, et.al,

2007). didalam katalog tersebut, daftar ancaman terbagi atas 5 kategori diantaranya sebagai berikut :

a) Keadaan Terpaksa (*Force Majuere*)
b) Kelemahan Organisasi (*Organizational Shortcomings*)
c) Kesalahan Manusia (*Human Failure*)
d) Kesalahan Teknis (*Technical Failure*)
e) Tindakan yang disengaja (*Deliberate Acts*)

Bayes Theorems

Teorem Bayes dikemukakan oleh seorang pendeta presbyterian Inggris pada tahun 1763 yang bernama Thomas Bayes . Teorema Bayes ini kemudian disempurnakan oleh Laplace. Teorem Bayes digunakan untuk menghitung probabilitas terjadinya suatu peistiwa berdasarkan pengaruh yang didapat dari hasil observasi. Berikut ini rumusan umun dari Teorema Bayes :

$$P(Y \mid X) = \frac{P(X \mid Y)\, P(Y)}{P(X)} \qquad (1)$$

dimana P(Y|X) menyatakan peluang suatu kejadian Y bila diketahui kejadian X terjadi. P(X) merupakan *marginal probability*(Pearl, 1999) dari kejadian X yang didapatkan dengan cara menjumlahkan peluang X yang dipengaruhi oleh Y dengan kondisi *true* dan peluang X yang dipengaruhi oleh Y dengan kondisi *false*.

Bayesian Network

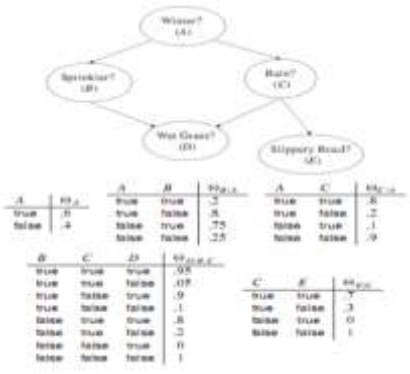
Bayesian Networks adalah sebuah "*directed acyclic graph*" (DAG) dengan sebuah tabel probabilitas untuk setiap simpul. Simpul yang terdapat pada *Bayesian Networks* merupakan representasi atribut proporsional dalam suatu domain dan garis menunjukkan hubungan ketergantungan di antara varibel-atribut. Dalam hal kaitannya dengan jaringan, pada *Bayesian Networks*, simpul merupakan representasi dari kumpulan ancaman, kategori ancaman, dan aset-aset didalam jaringan.

Dalam membuat / menyusun sebuah Bayesian Network, terdapat 3 langkah utama diantaranya(Darwiche A, 2009):

a) Menentukan atribut yang relevan dan nilai probabilitas dari masing-masing atribut tersebut.
b) Menyusun jaringan grafik asiklik terarah (*directed acyclic graph*) DAG
c) Menentukan tabel peluang kondisi atau CPT (*conditional probability Tabel*)

Beberapa istilah yang digunakan dalam *Bayesian Networks*:

a) Notasi graf yang menyatakan peluang bersyarat dalam suatu domain.
b) Simpul menyatakan sebuah atribut acak.
c) *Arc* (*directed edge*) menyatakan hubungan kausal langsung (*direct influence*).
d) Arah sebuah Arc yaitu dari atribut "sebab" ke atribut "akibat"(*causal reasoning*) atau arah sebaliknya (*diagnostic reasoning*).
e) Simpul *sibling* menyatakan atribut yang conditionally independent karena *parent*-nya.
f) Distribusi peluang untuk setiap simpul terhadap *parent*-nya: P(Xi |*Parents*(Xi))
g) Tidak ada siklus berulang di dalam *Bayesian Network*



Gambar 2 Contoh Notasi Grafik dari *Bayesian Network* (Sumber : Darwiche A, 2009)

Gambar 2 merupakan contoh dari Bayesin Network, atribut dari contoh Bayesian Network tersebut diantaranya; *Winter*(A), *Sprinkler*(B), *Rain*(C), *Wet*

Grass(D) dan *Slippery Road*(E). Masing-masing atribut terhubung oleh panah yang menunjukan hubungan sebab-akibat dan masing-masing atribut memiliki tabel peluang kondisi dengan nilai awal yang telah ditentukan.

Matrik Risiko

Matrik Risiko adalah alat grafis sederhana yang memetakan peluang terjadinya suatu peristiwa dan konsekuensi jika peristiwa tersebut terjadi (Barringer, 2006). Jumlah perkalian matrik yang digunakan tergantung dari situasi kebutuhan dalam penilaian risiko yang diinginkan. Penentuan nilai dan tingkat risiko dapat dilakukan secara subjektif(S. Gary, 2002).

Tabel 1 Contoh Matrik Rentang Risiko

(Sumber : S. Gary, 2002)

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Dari contoh tabel diatas, nilai risiko untuk kategori *High* berada pada rentang >50 sampai dengan 100, *Medium* >10 sampai dengan 50 dan *Low* 1 sampai dengan 10.

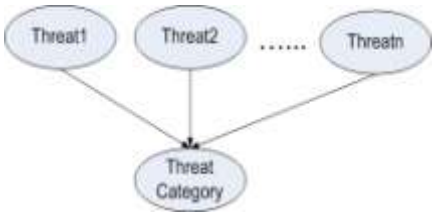
PEMBAHASAN

Dari hasil wawancara yang dilakukan dengan pihak MELSA dalam menentukan aset-aset yang termasuk ke dalam aset jaringan berdasarkan IT Baseline Protection dan langkah dalam manajemen resiko, didapatkan daftar sebagai berikut:

1) B 3.301 Security gateway (Firewall)
2) B 3.302 Routers and switches
3) B 3.303 Storage systems and storage networks
4) B 4.1 Heterogeneous networks
5) B 4.2 Network and system management
6) B 4.6 Wireless LAN

Model Bayesian Network Untuk Threat

Dari masing-masing kategori ancaman terhadap aset di dalam IT Baseline Protection, dilakukan penggabungan ancaman dimana masing-masing ancaman tersebut saling tidak mempengarui (*independent*). Berdasarkan rumusan awal Bayesian Network mengenai peluang terjadinya suatu kejadian dari gabungan beberapa kejadian (*Convergent connection*), didapatkan model jaringan bayes untuk masing-masing kategori sebagai berikut :



Gambar 3 Jaringan Bayesian untuk Threat

Dengan formulasi perhitungan dari model tersebut :

$$\mathbf{P(TC)} = \sum_{T1,T2,\ldots,Tn \in T,F} \mathbf{P(TC \mid T1, T2, \ldots, Tn)} \qquad (2)$$

Dimana TC = Threat Category, terdiri dari *Force Majuere*, *Organisational Shortcomings, Human Failure, Technical Failure,* dan *Deliberate Act*, kemudian T1...Tn merupakan kumpulan ancaman-ancaman yang mungkin terjadi didalam kategori tersebut dan P(TC) merupakan kodisi probabilitas dari kategori terhadap kumpulan ancaman yang bernilai *true.*

Model Bayesian Network Untuk Aset dan Kategori Ancaman

Model di bawah ini merupakan jaringan bayes yang menggambarkan keterhubungan antara kemungkinan terjadinya ancaman-ancaman terhadap aset, dimana ancaman tersebut dikelompokan berdasarkan 5 kategori ancaman, yaitu *Force Majeure(FM), Organizational Shortcomings(OS), Human Failure(HF), Technical Failure(TF),* dan *Deliberate Acts(DA).* Total nilai peluang dari ancaman untuk masing-masing kategori didapatkan melalui wawancara dengan pihak MELSA.

Sehingga formulasi untuk model tersebut yaitu :

$$\mathbf{P(Asset)} = \sum_{FM,OS,HF,TF,DA \in T,F} \mathbf{P(Asset \mid FM, OS, HF, TF, DA)} \quad (3)$$

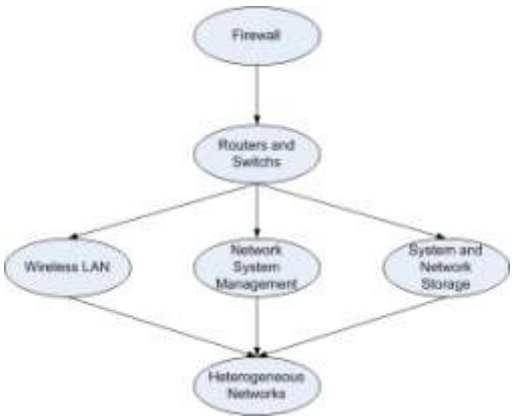


Gambar 4 Notasi grafik Aset dan Ancaman

Dimana P(Aset) merupakan kodisi probabilitas terjadinya ancaman untuk aset yang bernilai *true* terhadap kategori-kategori ancaman ; *Force Majeure(FM), Organizational Shortcomings(OS), Human Failure(HF), Technical Failure(TF)*, dan *Deliberate Acts(DA)*

Model Bayesian Network Untuk Aset

Aset-aset jaringan yang termasuk didalam penelitian ini, mengadopsi dari katalog IT Baseline Protection[ITGrundschutz, 2007], kemudian dilakukan validasi dengan pihak MELSA mengenai keberadaan aset tersebut di lapangan, pembuatan jaringan

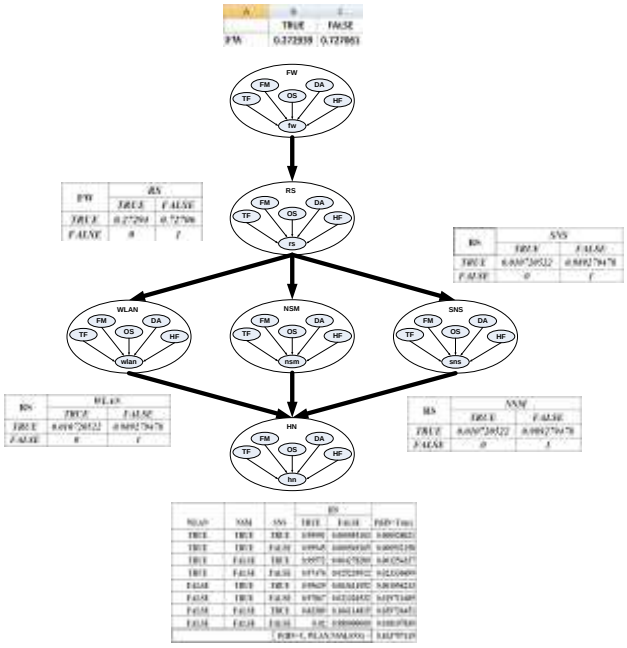


Gambar 5 Jaringan Bayes Untuk Aset Jaringan

Bayesian network untuk aset-aset jaringan berdasarkan hubungan aset secara topologi jaringan yang berada di MELSA. Aset-aset tersebut diantaranya : *Firewall*(FW), *Routers and Switches* (RS), *Wireless LAN* (WLAN), *Network and System Management* (NSM), *Storage Network and System* (SNS), *Heterogeneous Networks* (HN).

Model Bayesian Network Untuk Manajemen Risiko Keamanan Jaringan

Gambar 5 menunjukan keterhubungan antara aset yang satu dengan yang lainnya, dari 3 model dasar sebelumnya yaitu model Bayesian Network untuk threat, model Bayesian Network untuk aset dan kategori Threat dan model Bayesian network untuk aset, dihasilkan suatu model yang merepresentasikan model manajemen risiko keamanan jaringan secara umum.



Gambar 6 Notasi grafik untuk Manajemen Risiko Keamanan Jaringan

Dari gambar 6 didapatkan perhitungan sebagai berikut :

$$P(FW, RS, WLAN, NSM, SNS, HN) = P(HN \mid WLAN, NSM, SNS) * P(WLAN \mid RS) * P(NSM \mid RS) * P(SNS \mid RS) * P(RS \mid FW) * P(FW) \quad (4)$$

$P(FW, RS, WLAN, NSM, SNS, HN)$, merupakan distribusi peluang gabungan dari model manajemen risiko keamanan jaringan yang menyatakan nilai probabilitas dari tingkat risiko keamanan jaringan.

Dari model tersebut diatas dapat dihitung peluang gabungan terjadinya ancaman terhadap keamanan jaringan, Contoh jika: Terjadi Ancaman Terhadap Firewall P(FW), Terjadi Ancaman Terhadap Router dan Switch P(RS|FW), Tidak Terjadi Ancaman Terhadap Wireless LAN P(⌐WLAN|RS), Terjadi Ancaman Terhadap Storage Network System P(SNS|RS), Tidak Terjadi Ancaman Terhadap Network System Management P(⌐NMS|RS), Terjadi Ancaman Terhadap Heterogeneous Network P(HN|WLAN,NSM,SNS) ?

$$P(FW, RS, \neg WLAN, SNS, \neg NMS, HN) = P(FW) * P(RS|FW) * P(\neg WLAN|RS) * P(SNS|RS) * P(\neg NSM|RS) * P(HN|\neg WLAN, \neg NSM, SNS)$$
$$= 0{,}272939 * 0{,}27294 * 0{,}989279478 * 0{,}010720522 * 0{,}989279478 * 0{,}83389 = 0{,}0006518$$

Maka peluang gabungan terjadinya ancaman terhadap aset jaringan yang mungkin terjadi sebesar 0,0006518.

Tabel 2 Rentang Risiko

Peluang Risiko	Interval
Low	{0,0 – 0,3}
Medium	{0,4 – 0,6}
High	{7.0 – 1.0}

Dari tabel 2 diatas, maka dapat disimpulkan bahwa peluang terjadinya suatu ancaman terhadap aset-aset di dalam jaringan berada pada tingkat risiko *Low*.

Kesimpulan

Dari hasil penelitian ini didapatkan beberapa kesimpulan sebagai berikut :

1) Dengan menggunakan *IT Baseline Protection*, identifikasi risiko suatu ancaman terhadap aset yang berkaitan dengan jaringan menjadi lebih terarah dan mudah.
2) *Bayesian networks* dapat digunakan sebagai model untuk manajemen risiko keamanan jaringan, visualisasi grafik dari model jaringan yang terbentuk dapat mempermudah mengklasifikasikan risiko ancaman terhadap aset-aset jaringan.
3) *Bayesian networks* sebagai model untuk manajemen resiko keamanan jaringan mampu memberikan gambaran keterhubungan dari nilai peluang suatu ancaman dimasing-masing kategori ancaman, kategori ancaman terhadap masing-masing aset dan aset satu dengan yang lainnya di dalam jaringan.
4) Model manajemen risiko keamanan jaringan yang dirancang, mampu memberikan penilaian risiko suatu ancaman terhadap aset, serta tingkat risiko dari aset tersebut.

DAFTAR PUSTAKA

[1]. *CSI. 2009.14th Annual CSI Computer Crime and Security Survey*.

[2]. GData 2011 *Security Survey. 2011. How do users assess threats on the Internet?*.

[3]. Norton. 2011. Cyber Crime Index. Melalui : http://us.norton.com/?cci=on [07/02/2011]

[4]. Peltier, Thomas R. 2005. *Information Security Risk Analysis, Second Edition*, Auerbach Publications, USA.

[5]. S. Gary, G. Alice, and F.Alexis. 2002. *Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology

[6]. BSI. 2008. *Information technology — Security techniques — Information security risk management*. British Standard

[7]. ISO-IEC 73. 2002. *Risk management Vocabulary : Guidelines for use in standards*. British Standard

[8]. Helmbrecht .U, et.al. 2007. *IT Baseline Protection (IT-Grundschutz)*. German

[9]. J. Pearl. 1999. *Casuality Models Reasoning And Inference*. Cambridge University Press.

[10]. Kondakci S. 2010. *Network Security Risk Assessment Using Bayesian Belief Networks. Social Computing / IEEE International Conference*

on Privacy, Security, Risk and Trust, 2010 IEEE International Conference on, pp. 952-960, 2010 IEEE Second International Conference on Social Computing.

[11]. Kamat M. 2009. *Matrices for Aset Valuation and Risk Analysis*. ISO 27001 Implementer's Forum

[12]. ISACA. 2010. *CISA® Review Manual 2010*. ISACA

[13]. Pandian R. 2007. *Applied Software Risk Management – Guide For Sofware Project Managers*. New York. Auerbach Publication.

[14]. Darwiche A. 2009. *Modeling and Reasoning with Bayesian Networks*. UK. Cambrige University Press.

[15]. Stefan Fenz. 2011. "*An Ontology- and Bayesian-based Approach for Determining Threat Probabilities*," in *ASIA CCS '11: 6th ACM Symposium on Information, Computer and Communications Security*.

[16]. Uffe B. Kjaerulff and Anders L.Madsen.2 008. *Bayesian Networks and Influence Diagrams*.USA. Springer Science

[17]. Karl-Rudolf Koch. 2007 . *Introduction to Bayesian Statistics Second Edition. Berlin*. Springer-Verlag.

[18]. Wheeler, Evan. 2011. *Security Risk Management :Building an information Security Risk Management Program from the Ground Up*. USA. Syngress.

[19]. Kouns J, Minoli D. 2010. *Information Technology Risk Management In Enterprise Environments*. New Jersey. Wiley & Sons.

[20]. Batelli F, Bruchi D, et el. 2008. *Network Security: From Risk Analysis to Protection Strategies.* Italy.ISACOM Stampa:PrintArt

[21]. Krawetz Neal. 2007. *Introduction to Network Security.* Boston. Charles River Media

[22]. Frigault M, Wang L. 2008. *Measuring Network Security Using Bayesian Network-Based Attack Graphs*. Annual IEEE International Computer Software and Application Conference. IEEE Computer Society.

[23]. Bonafede C.E, Giudici P. 2007. *Bayesian Network for Enterprise Risk Assessment*. Italy. Elsevier