

SKRIPSI
KAJIAN HUKUM *CYBER INSURANCE*
DALAM E-BUSINESS



Oleh :

GRACIA PRAMESI KALYADHARANI
NIM. 030115220

FAKULTAS HUKUM
UNIVERSITAS AIRLANGGA
SURABAYA
2005

KAJIAN HUKUM *CYBER INSURANCE* DALAM E-BUSINESS

SKRIPSI

**Diajukan Untuk Melengkapi Tugas Dan Memenuhi Salah Satu
Syarat Guna Memperoleh Gelar Sarjana Hukum**

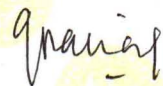
Pembimbing



Zahry Vandawati Chumaida, S.H., M.H.

Nip : 132162030

Penyusun



Gracia Pramesi K.

Nim : 030115220

**FAKULTAS HUKUM
UNIVERSITAS AIRLANGGA
SURABAYA
2005**

Skripsi ini telah diuji dan dipertahankan dihadapan panitia penguji pada hari Jum'at, 5 Agustus 2005.

Panitia Penguji Skripsi :

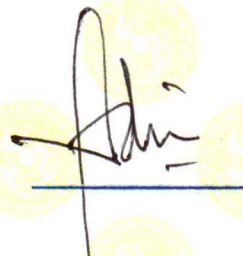
Ketua : Samzari Buntoro, S.H.



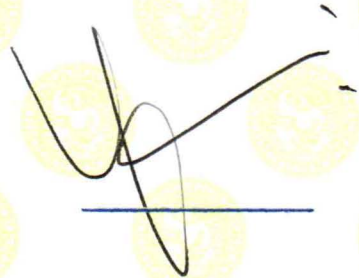
Anggota : 1. Zahry Vandawati Chumaida, S.H., M.H.



2. L. Budi Kagramanto, S.H., M.H., M.M.



3. Wuri Adriyani, S.H., M.Hum.



MOTTO

TO LOVE SOMETHING

TO BE LOVED SOMETHING

TO LOVE AND TO BE LOVED IS EVERYTHING

" KEBAIKAN DALAM KATA-KATA

MENCIPTAKAN PERCAYA DIRI "

" KEBAIKAN DALAM BERPIKIR

MENCIPTAKAN KEBIJAKAN "

" KEBAIKAN DALAM MEMBERI

MENCIPTAKAN CINTA "

(Lao-Tze)

*Skripsi ini saya persembahkan untuk
Kedua orang tuaku dan kakakku yang sangat saya cintai
Dan juga sangat mencintai saya.
Tanpa mereka saya bukanlah apa-apa dan bukanlah siapa-siapa.*

KATA PENGANTAR

Puji Syukur saya panjatkan kepada Allah SWT, karena atas ijin-Nya-lah skripsi ini dapat terselesaikan meski jauh dari sempurna. Meskipun jauh dari sempurna, tetapi dengan itikad baik saya memberanikan diri untuk menulis skripsi ini dengan harapan dapat membagi pengetahuan sekaligus dapat mempelajari lebih dalam mengenai *Cyber Insurance* yang merupakan topik utama dalam skripsi ini.

Tak lupa saya ucapkan terima kasih untuk segala bentuk dorongan dan kritikan yang bertujuan agar skripsi ini dapat menjadi lebih baik lagi.

Saya juga ingin mengucapkan terima kasih yang sedalam-dalamnya untuk semua pihak yang telah membantu dalam proses pengerjaan skripsi ini sehingga dapat terselesaikan dengan baik, yaitu :

1. Allah SWT, karena tanpa ijin-Nya skripsi ini tidak akan dapat terselesaikan dengan baik.
2. Kedua orang tuaku yang telah menyayangi aku dari kecil hingga sekarang, tanpa mereka aku takkan bisa berdiri tegar. Aku sayang kalian.
3. Kakakku tersayang, meskipun *Mbak* sudah tidak ada di kota ini, di dekatku, tapi aku yakin *Mbak* selalu mendoakan kesuksesanku. Terima kasih *Mbak*, jujur aku kangen kamu.

4. Mas Hendra, orang yang selalu mendampingi aku, selalu ada disisiku dan memberikan dorongan juga kritikan ke aku, aku tahu itu untuk kebaikanku. Terima kasih. *Love u always* ^_^
5. Ibu Zahry Vandawati Chumaida, S.H., M.H., selaku dosen pembimbing. Terima kasih atas bimbingan yang selama ini telah diberikan kepada saya. Terima kasih atas kesabaran ibu dalam menghadapi saya. Terima kasih....
6. Seluruh Panitia Penguji Skripsi, Bapak Samzari, Bapak Budi, Ibu Wuri dan Ibu Vanda. Terima kasih atas seluruh masukan yang telah diberikan kepada saya agar skripsi saya dapat menjadi lebih baik lagi.
7. Kepada seluruh dosen Fakultas Hukum Universitas Airlangga. Terima kasih telah memberikan saya tambahan ilmu pengetahuan selama saya belajar di Fakultas Hukum Universitas Airlangga.
8. Bapak Gregorius Singgih Budiarto, selaku *Branch Manager* PT. Staco Jasa Pratama Semarang. Terima kasih atas seluruh masukan dan nasihat yang telah diberikan kepada saya dalam proses pengerjaan skripsi ini.
9. Sdr. Joko Winarko, S.E. dari PT. *Asia Reliance General Insurance*. Terima kasih atas pendapat yang telah diberikan demi kesempurnaan skripsi ini.
10. Ithak 'n Reni. Makasih sudah menjadi sahabatku selama 4 tahun kita belajar di FH Unair. Saling memberikan dorongan dan tak jarang kritikan. Tapi kita tahu bahwa semuanya demi kemajuan kita. Semoga kita tidak saling melupakan. Amin..

11. Lina. Tutuk, Rini, Ekary, Dian. Terima kasih telah menjadi teman-temanku.

Aku bangga mempunyai teman seperti kalian.

12. Semua pihak yang telah membantu yang tidak bisa aku sebutkan satu-persatu.

Terima kasih. Aku sayang kalian semua.

Semoga isi dari skripsi ini dapat memberikan manfaat kepada semua pihak yang membacanya.

Surabaya, 10 Agustus 2005

Penulis

Gracia Pramesi Kalyadharani

DAFTAR ISI

LEMBAR JUDUL.....	i
LEMBAR PERSETUJUAN.....	ii
LEMBAR PENGESAHAN.....	iii
HALAMAN MOTTO.....	iv
HALAMAN PERSEMBAHAN.....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	ix
DAFTAR LAMPIRAN.....	xi
BAB I : PENDAHULUAN	
1. Latar Belakang Dan Rumusan Masalah.....	1
2. Alasan Pemilihan Judul.....	9
3. Penjelasan Judul.....	9
4. Tujuan Penulisan.....	10
5. Metode Penelitian	
a. Pendekatan Masalah.....	11
b. Sumber Bahan Hukum.....	11
c. Analisa.....	11
6. Pertanggungjawaban Sistematika.....	12
BAB II : HUBUNGAN HUKUM PARA PIHAK DALAM <i>CYBER</i>	
<i>INSURANCE</i>	
1. Dasar Hukum Berlakunya <i>Cyber Insurance</i>	14
2. Ruang Lingkup Perlindungan <i>Cyber Insurance</i>	22
3. Hubungan Hukum Para Pihak Dalam <i>Cyber Insurance</i>	30
BAB III : MEKANISME DAN PERTANGGUNGJAWABAN <i>CYBER</i>	
<i>INSURANCE</i>	
1. Terjadinya Penutupan Perjanjian <i>Cyber Insurance</i>	39

2. Sistem Pertanggungjawaban <i>Cyber Insurance</i>	44
3. Cara Pengajuan Klaim.....	45
BAB IV : PENUTUP	
1. Kesimpulan.....	50
2. Saran.....	51
DAFTAR BACAAN	53

DAFTAR LAMPIRAN

1. Form Aplikasi Permohonan *Cyber Insurance*
2. Form *information Security Self Assessment* .

BAB I

PENDAHULUAN

Rahayu

BAB I

PENDAHULUAN

1. Latar Belakang Dan Rumusan Masalah

Sejak dahulu orang selalu mencari cara baru untuk memenuhi kebutuhannya, dari cara yang paling tradisional, yaitu pada saat orang belum mengenal uang. Ketika orang belum mengenal uang, mereka dalam memenuhi kebutuhannya menggunakan cara saling mempertukarkan barang yang mereka miliki untuk ditukar dengan barang milik orang lain yang sedang dibutuhkannya. Cara ini dikenal dengan istilah *barter*. Setelah manusia mengenal uang, mereka menemukan cara baru lagi untuk memenuhi kebutuhannya yaitu dengan uang sebagai alat tukar sekaligus sebagai alat pembayaran yang sah atas suatu barang yang mereka butuhkan. Cara ini kemudian dikenal dengan istilah jual beli dimana sampai sekarang cara jual beli masih digunakan. Jual beli inilah yang menjadi cikal bakal adanya dunia bisnis dimana orang mulai memikirkan suatu keadaan dimana ia tidak hanya menjadi seorang penjual saja atau hanya menjadi seorang pembeli saja. Sang penjual mulai berupaya untuk memproduksi sendiri barang yang akan dijualnya, menjalin kerjasama dengan penjual yang lain, dan usaha-usaha yang lain yang dapat mendatangkan keuntungan maksimal bagi dirinya. Sedangkan pembeli juga demikian. Tidak sedikit pembeli yang membeli suatu barang dari penjual untuk kemudian dijual lagi kepada pihak lain, meskipun tidak sedikit pula pembeli yang membeli barang untuk dirinya sendiri.

Dari aktivitas jual beli yang sederhana dengan tujuan yang sederhana pula berkembang berbagai macam aktivitas-aktivitas manusia yang dilakukan dengan tujuan selain untuk memenuhi kebutuhannya juga untuk mendapatkan keuntungan yang maksimal dari apa yang diusahakannya tersebut. Aktivitas-aktivitas semacam itulah yang dinamakan aktivitas bisnis.

Dalam dunia bisnis, sebagaimana yang telah kita ketahui bersama manajemen resiko cukup penting untuk dipertimbangkan dalam menjalankan sebuah usaha (bisnis). Resiko merupakan aspek mendasar dalam dunia usaha. Resiko usaha dan ketidakpastian yang menimbulkan kerugian dapat terjadi tanpa dapat diprediksikan sebelumnya. Inilah alasan yang mendorong kaum intelektual dan orang-orang yang bergerak dalam dunia usaha untuk mengasuransikan aset-aset yang berhubungan dengan kegiatan usahanya. Selain itu pula dengan tujuan mencegah kerugian yang terlalu besar bila resiko dan berbagai bentuk ketidakpastian yang merugikan menyimpannya. Dengan kebutuhan-kebutuhan diatas, berbagai produk asuransi kerugian saat ini telah banyak tersedia di pasaran guna mengurangi berbagai resiko seperti kebakaran, pencurian, gempa bumi, maupun banjir dan segala bentuk resiko lain.

Perkembangan era teknologi informasi saat ini, ditandai dengan berkembangnya teknologi komputer serta jaringan internet yang menyebabkan hampir sebagian besar bisnis yang dilakukan sehari-hari memanfaatkan kedua hal tersebut. Aktivitas bisnis yang dilakukan melalui internet disebut dengan istilah *e-business (electronic business)*. Aktivitas bisnis semacam ini mampu terkoneksi dari berbagai penjuru dunia secara langsung dan memungkinkan dilakukannya

transaksi secara *real time*. Dengan demikian, sistem baru dalam dunia usaha tampak jelas di depan mata. Namun tidak hanya sistem perekonomian baru yang dijumpai, tapi juga suatu bentuk resiko yang baru yang sebagian besar berkaitan dengan masalah keamanan dan *privacy*. Akibatnya dari perkembangan ini, resiko usaha menjadi semakin kompleks saja.

Internet merupakan jaringan terbuka (*open network*) yang memungkinkan pihak lain baik yang berkepentingan maupun yang tidak berkepentingan ikut berpartisipasi di dalamnya. Terhubungnya jaringan komputer suatu perusahaan dengan dunia maya melalui internet membuka peluang terjadinya kejahatan, karena pihak luar saat ini sangat potensial untuk melakukan serangan maupun manipulasi *database* suatu perusahaan yang pada akhirnya menimbulkan kerusakan.

Kejahatan dalam dunia internet atau yang biasa disebut dengan *cybercrime*, seperti bentuk pencurian kartu kredit, *hacking*, *cracking*, penyadapan transmisi data merupakan suatu bentuk kejahatan yang sangat potensial yang mampu menimbulkan kerugian finansial. Namun, bentuk umum serangan yang terjadi dari jaringan internet adalah *virus invasion*, instruksi *hackers*, maupun upaya memacetkan *website* melalui serangkaian upaya membanjiri *server* dengan sejumlah informasi dalam skala besar. Berbagai bentuk tersebut berimplikasi pada kerugian yang tidak sedikit bagi sasaran/obyek.¹

¹ Dian Siska Herliana, "*Peluang Baru Industri Cyber Insurance Dalam Era Teknologi Informasi*", hal 2
www.lkht.net

Berbagai bentuk proteksi yang diterapkan perusahaan-perusahaan yang terhubung dengan internet dewasa ini, cukup memberikan perlindungan atas propertinya, yaitu terhadap sistem komputasi dan data elektronik perusahaan. Namun sistem keamanan yang diterapkan tersebut tidak selamanya memberikan perlindungan total. Seperti yang telah disebutkan sebelumnya, perusakan sistem keamanan (*security breaches*) dapat terjadi, antara lain dikarenakan faktor *unauthorized access*, maupun adanya penggunaan sistem komputasi dan data perusahaan oleh pihak luar atau pihak dalam (*insider or outsider*).

Seperti contoh kasus yang menimpa *Yahoo!*, *Amazon*, *CNN.com* dan *ebay.com*, beberapa situs internet yang paling populer, telah diserang oleh *hackers*, memenuhi jaringan kerja mereka dan membuat situs mereka tidak dapat digunakan atau menjadikannya lebih lambat untuk diakses oleh para pengunjung situs tersebut. Serangan seperti ini dikenal dengan nama “Penolakan Pelayanan” (*Denial of Service*). Kasus semacam ini dapat *discover* dengan asuransi *e-business*. Tapi serangan seperti ini dan resiko-resiko *e-business* lainnya tidak dapat dilindungi atau *discover* oleh asuransi bisnis yang bersifat tradisional atau konvensional. Hal inilah yang menjadi penyebab munculnya suatu fenomena baru dalam dunia perasuransian yang dinamakan dengan *Cyber Insurance*.

Cyber insurance sebagai suatu bentuk produk asuransi yang menutup resiko-resiko yang terkait dengan sistem keamanan jaringan komputer. Jaringan

komputer yang terhubung dengan jaringan internet berimplikasi mendatangkan kerugian baik dikarenakan serangan *hackers* maupun *virus*.²

Menurut Ty Sagalow, *cyber insurance* merupakan bentuk khusus dari asuransi yang menyediakan baik layanan produk asuransi maupun manajemen resiko untuk melindungi dari berbagai macam jenis resiko digital. Dalam bentuk yang paling kakunya, asuransi tersebut memberikan ruang lingkup perlindungan berupa liabilitas isi dari situs internet (*website content liability*), liabilitas kegagalan keamanan jaringan (*network security failure liability*), liabilitas atas kelalaian dan kesalahan profesional (*professional errors and omissions liability*), liabilitas untuk mengcover kerugian finansial yang merupakan hasil dari kerusakan data dan menurunnya pendapatan akibat dari kegagalan keamanan jaringan. Sebagai tambahan asuransi tersebut dapat memberikan tambahan ruang lingkup berupa *cyber-extortion*, biaya hubungan publik setelah insiden (*post incident public relation fees*), dan bahkan pembayaran kembali dana penghargaan sebagai akibat dari tindak kriminal (*a criminal reward fund reimbursement*). Sebagai tambahan pada topik ini, penanggung yang berkualitas akan memberikan secara gratis atau dengan memberikan potongan biaya layanan manajemen resiko.³

² *Ibid*, hal 2

³ Ty Sagalow, "Chief Operating Officer And Executive VP of New York City based AIG eBusiness Risk Solution".
Cyber Insurance Definition , Ask The Expert, hal 1
www.cio.com

Secara umum, bentuk-bentuk asuransi tradisional seperti asuransi properti dan CGL (*Corporate General Liability*) diciptakan untuk dunia batu bata dan adukan semen. Misalnya dalam kata “properti” pada sebuah polis asuransi properti diartikan sebagai properti dalam bentuk nyata (*tangible property*) dan secara umum tidak akan *tercover* dalam bentuknya yang tidak nyata (*intangible property*) seperti data atau informasi. Pada CGL ruang lingkup perlindungan yang utama adalah mencakup kerusakan secara fisik dan kerugian properti secara nyata. Mereka tidak akan *mengcover* mengenai tanggung gugat hukum yang muncul dari sebuah transmisi virus komputer atau pencurian informasi konsumen dari suatu jaringan kerja komputer pada suatu perusahaan seperti pada *cyber insurance*.⁴

Akan tetapi pendapat dari Ty Sagalow tersebut kurang tepat dengan adanya penyebutan bahwa obyek dari *cyber insurance* yang berupa data atau informasi bersifat tidak nyata (*intangible*) karena sebenarnya data atau informasi tersebut adalah nyata (*tangible*) yang menggunakan media elektronik, yakni komputer.

Bila kita lihat lebih jauh, *cyber insurance* yang mencakup lingkup komputasi dibagi menjadi dua tipe, yaitu : tipe pertama berkaitan dengan *first party* atau *cyber property* yang meliputi penutupan resiko kerugian akibat tindak kejahatan, pencurian, perusakan perangkat lunak (*software*) maupun *database*, rehabilitasi data, pemerasan (*extortion*), dan *business interruption*. Sedangkan tipe

⁴ *Ibid*, hal 2

kedua adalah berkaitan dengan *third party* (pihak ketiga) atau sering disebut dengan *cyber liability* yang meliputi pencemaran nama baik yang terkait dengan materi suatu situs internet termasuk juga pelanggaran hak cipta.⁵

Sebelum munculnya *cyber insurance*, dalam dunia perasuransian lebih dahulu dikenal asuransi khusus untuk peralatan elektronik khususnya komputer yang dikenal dengan nama Asuransi Peralatan Elektronika (*Electronic Equipment Insurance*). Meskipun sama-sama berkaitan dengan komputer tetapi sebenarnya antara *cyber Insurance* dengan asuransi peralatan elektronika mempunyai beberapa perbedaan yang mendasar yaitu :

1. Pada *cyber insurance* obyek perlindungan adalah data-data, informasi-informasi, sistem dan/ atau program dalam komputer atau sering disebut dengan istilah *software*. Sedangkan untuk asuransi peralatan elektronika khusus untuk komputer, obyek perlindungan adalah perangkat keras (*hardware*) dari komputer tersebut seperti : CPU, *keyboard*, *monitor*.
2. Pada *cyber insurance* resiko yang mengancam adalah merupakan resiko digital seperti : *virus*, *hackers*. Sedangkan pada asuransi peralatan elektronika, resiko yang mengancam adalah merupakan resiko yang bersifat eksternal dan konvensional seperti : bahaya kebakaran, banjir, pencurian.
3. Pada asuransi peralatan elektronika khusus untuk komputer, kerugian akibat kerusakan atau kehilangan data dalam jaringan kerja komputer merupakan suatu hal yang dikecualikan, maksudnya tidak ikut *tercover* dalam

⁵ Dian Siska Herliana, "*Peluang Baru Industri Cyber Insurance Dalam Era Teknologi Informasi*", *loc.cit*

perlindungan asuransi tersebut. Pengecualian tersebut biasanya dituangkan dalam suatu klausula dalam polisnya.

Beberapa *cyber insurance* yang tersedia dan cukup terkenal saat ini antara lain adalah *American Internatinal Group (AIG)* , *Marsh, St. Paul* dan *Zurich American Insurance Company*. Perusahaan-perusahaan asuransi tersebut telah menawarkan penutupan resiko pemanfaatan teknologi informasi. Misalnya *AIG* dengan polisnya yang disebut dengan *ProTech Technology Liability Insurance*, *St. Paul* dengan polis *Cybertech + Liability*. Selain itu ada pula perusahaan reasuransi terkemuka yang memberikan perlindungan terhadap resiko internet seperti *Munich Re* dan *Swiss Re*.⁶

Sebagai bahan analisa dalam skripsi ini, penulis menggunakan *Cyber Insurance* dari *AIG e-business, Risk Solution*.

Dari latar belakang diatas, dapat ditemukan beberapa permasalahan, yaitu :

1. Apakah dengan keberadaan *cyber insurance* tidak bertentangan dengan hukum positif yang ada di Indonesia ? Serta bagaimanakah hubungan hukum para pihak dalam *cyber insurance* ?
2. Bagaimanakah mekanisme terjadinya penutupan perjanjian *cyber insurance* dan bagaimana pula sistem pertanggungjawaban dari *cyber insurance* ?

⁶ *Ibid, hal 3*

2. Alasan Pemilihan Judul

Pada skripsi ini, penulis memilih judul “Kajian Hukum *Cyber Insurance* Dalam *E-Business*”. Judul ini sengaja dipilih dengan alasan bahwa pokok pembicaraan dalam skripsi ini adalah mengenai *Cyber Insurance* yang dikaji melalui kacamata hukum. Sedangkan pemilihan kata *E-Business*, berkaitan dengan ruang lingkup dari *cyber insurance* itu sendiri yaitu dimana dibicarakan dalam ruang lingkup aktivitas bisnis melalui internet yang terdiri dari bermacam-macam aktivitas atau kegiatan usaha yang meliputi dan tidak terbatas pada aktivitas perdagangan melalui internet saja.

Dengan demikian, diharapkan judul yang telah dipilih oleh penulis tersebut mampu merefleksikan keseluruhan isi skripsi ini.

3. Penjelasan Judul

Seperti yang telah disebutkan pada sub bab sebelumnya bahwa judul skripsi ini adalah “Kajian Hukum *Cyber Insurance* Dalam *E-Business*”. Pada sub bab ini akan dijelaskan satu persatu definisi kata-kata pada judul tersebut.

- Kajian Hukum adalah suatu cara pembelajaran terhadap sesuatu hal ditinjau dari sisi hukumnya.
- *Cyber Insurance* adalah suatu tipe khusus dari asuransi yang selain menyediakan asuransi, juga menyediakan jasa manajemen resiko untuk menghadapi berbagai macam resiko *digital*.⁷

⁷ Ty Sagalow, “*Cyber Insurance Definition, Ask The Expert*”, *loc.cit*

- *Cyber Insurance* adalah suatu bentuk produk asuransi yang menutup resiko-resiko yang terkait dengan sistem keamanan jaringan komputer.⁸
- *E-Business* adalah segala aktivitas bisnis yang memanfaatkan teknologi komputer serta jaringan *internet*, sehingga mampu terkoneksi dari berbagai penjuru dunia secara langsung dan memungkinkan dilakukannya transaksi secara *real time*.

Jadi “Aspek Hukum *Cyber Insurance* Dalam *E-Business*” adalah suatu sudut pandang hukum terhadap suatu bentuk asuransi yang menutup resiko-resiko yang terkait dengan sistem keamanan jaringan komputer atau dapat disebut dengan resiko digital dalam segala aktivitas bisnis yang memanfaatkan teknologi komputer serta jaringan *internet*.

4. Tujuan Penulisan

Tujuan penulisan skripsi ini adalah untuk memenuhi tugas akhir sebagai persyaratan kelulusan dan juga untuk menerapkan ilmu pengetahuan di bidang hukum yang diperoleh selama masa perkuliahan ke media tulisan yang dapat berguna bagi masyarakat.

Selain itu penelitian hukum ini juga bertujuan untuk memberikan sumbangan pemikiran dalam bidang hukum perdata, khususnya untuk pengembangan hukum asuransi Indonesia.

⁸ Dian Siska Herliana, “*Peluang Baru Industri Cyber Insurance Dalam Era Teknologi Informasi*”, *op.cit*, hal 1

5. Metode Penelitian

a. Pendekatan Masalah

Pendekatan pada penulisan skripsi ini dilakukan dengan metode yuridis normatif dan pendekatan perundang-undangan (*statute approach*) yaitu mengumpulkan norma-norma hukum yang tertulis untuk kemudian diteliti untuk mencari suatu konklusi atau kesimpulan terhadap permasalahan yang ada.

b. Sumber Bahan Hukum

Sumber bahan hukum yang digunakan dalam penulisan skripsi ini adalah :

- Sumber Bahan Hukum Primer :

1. Kitab Undang-undang Hukum Dagang (*Wetboek van Koophandel*)
2. Kitab Undang-undang Hukum Perdata (*Burgerlijk Wetboek*)

- Sumber Bahan Hukum Sekunder :

Bahan-bahan tulisan, buku, majalah, makalah, pendapat para pakar yang mempunyai relevansi kuat dengan bidang hukum yang akan diteliti.

c. Analisa Bahan Hukum

Penulisan skripsi ini dianalisa secara induktif yaitu pola berpikir untuk mencari konklusi atas permasalahan dengan mendalilkan secara umum. Atau mendalilkan secara umum permasalahan tersebut untuk kemudian ditarik kesimpulan atau konklusi.

6. Pertanggungjawaban Sistematika

BAB I, Pendahuluan. Pada bab ini akan dijelaskan mengenai latar belakang dan rumusan masalahnya, alasan pemilihan judul, penjelasan judul, tujuan dan manfaat penulisan, metode penelitian, pendekatan masalah, sumber bahan hukum, analisa, serta pertanggungjawaban sistematika.

BAB II, Aspek Hukum *Cyber Insurance* Dalam *E-Business*. Dalam bab ini akan dijelaskan mengenai dasar hukum berlakunya *cyber insurance*, ruang lingkup perlindungan *cyber insurance* (khususnya *cyber insurance* dari *AIG eBusiness Risk Solution*) serta hubungan hukum para pihak dalam *cyber Insurance* sesuai dengan masing-masing ruang lingkup perlindungan *cyber insurance*.

BAB III, Mekanisme dan Pertanggungjawaban *Cyber Insurance*. Dalam bab ini akan dijelaskan mengenai mekanisme dan prosedur terbentuknya perjanjian *cyber insurance*, mulai dari pengisian aplikasi sampai dengan pengajuan klaim pada saat terjadinya peristiwa tidak pasti. Kemudian akan dijelaskan pula mengenai pada keadaan dan kondisi serta skenario yang bagaimana dapat diajukan klaim atas peristiwa tidak pasti yang menimpa tertanggung untuk mendapatkan pertanggungjawaban dari pihak penanggung, yang dalam hal ini adalah *AIG eBusiness Risk Solution*.

BAB IV, Penutup. Dalam hal ini akan diuraikan mengenai kesimpulan yang dapat diambil oleh penulis dari keseluruhan isi dari skripsi ini. Dan akan

diuraikan pula mengenai saran-saran yang dapat diberikan oleh penulis berkaitan dengan isi dari skripsi ini

BAB II
HUBUNGAN HUKUM PARA PIHAK
DALAM *CYBER INSURANCE*

Rahayu

BAB II

HUBUNGAN HUKUM PARA PIHAK

DALAM *CYBER INSURANCE*

1. Dasar Hukum Berlakunya *Cyber Insurance*

Menurut pasal 246 KUHD asuransi atau pertanggungan adalah suatu perjanjian, dengan mana seorang penanggung mengikatkan diri kepada seorang tertanggung, dengan menerima suatu premi, untuk memberikan penggantian kepadanya karena suatu kerugian, kerusakan, atau kehilangan keuntungan yang diharapkan, yang mungkin akan dideritanya karena suatu peristiwa yang tidak menentu.

Dari isi pasal 246 KUHD dapat terlihat unsur-unsur dari asuransi, yaitu:

1. Tertanggung
2. Penanggung
3. Pembayaran Premi
4. Peristiwa tidak pasti
5. Pembayaran Ganti Rugi

Kelima unsur ini bersifat mutlak dan kumulatif, maksudnya unsur-unsur tersebut harus dipenuhi semua untuk dapat disebut sebagai suatu perjanjian asuransi, tanpa adanya salah satu unsur diatas, tidak dapat dikatakan sebagai suatu perjanjian asuransi.

Sedangkan dalam pasal 247 KUHD disebutkan bahwa pertanggungan itu antara lain dapat mengenai : bahaya kebakaran, bahaya yang mengancam hasil-hasil pertanian yang belum dipanen, jiwa, satu atau beberapa orang, bahaya laut dan perbudakan, bahaya yang mengancam pengangkutan di daratan, di sungai-sungai, dan di perairan darat.

Dalam pasal 247 KUHD tersebut jenis-jenis asuransi yang disebutkan merupakan asuransi yang bersifat konvensional, dimana di dalam perkembangannya sekarang, jenis-jenis asuransi tersebut telah banyak berkembang mengikuti perkembangan jaman yang diikuti dengan perkembangan kebutuhan manusia. Di dalam kenyataannya sejak pasal tersebut dibentuk sampai sekarang sudah banyak sekali jenis-jenis asuransi yang dikenal di dalam praktek seperti halnya *Cyber Insurance* yang muncul karena kebutuhan teknologi pada dewasa ini.

Oleh karena itulah ukuran atau dasar pembagian atau pembedaannya (ruang lingkup) yang dipakai oleh pembentuk undang-undang di dalam pasal 247 KUHD itu kurang tepat. Sebab juga sifat dari pokok asuransi atau kepentingan yang melekat pada peristiwa yang diasuransikan itu memegang peranan penting. Akan tetapi penentuan seperti dalam pasal 247 KUHD itu secara juridis adalah tidak membatasi atau menghalangi timbulnya jenis-jenis asuransi lain menurut kebutuhan masyarakat. Hal ini dapat kita dasarkan pada kata-kata “antara lain” yang terdapat di dalam pasal 247 KUHD tersebut. Dengan demikian sifat dari pasal 247 KUHD itu hanyalah menyebut beberapa contoh saja atau sifatnya pasal tersebut adalah numeratif, bukan limitatif. Dengan demikian para pihak dapat

memperjanjikan adanya asuransi dalam bentuk lain. Hal ini juga sangat dimungkinkan berdasarkan pasal 268 KUHD yang menentukan bahwa semua kepentingan pada dasarnya dapat menjadi pokok pertanggungan asalkan memenuhi persyaratan yaitu : dapat dinilai dengan uang, diancam oleh suatu bahaya, dan tidak dikecualikan oleh undang-undang.⁹

Apabila dikaitkan dengan *cyber insurance*, maka dapat diambilkan contoh sebagai berikut:

“ Perusahaan X yang bergerak dalam bidang otomotif menjalankan bisnisnya dengan menggunakan media internet dan menggunakan jaringan kerja komputer dan menyimpan data elektronik yang dianggap penting untuk mengendalikan bisnisnya. Karena menyadari bahwa data elektronik yang disimpan dalam jaringan kerja komputer tersebut mempunyai peranan yang penting untuk mengendalikan bisnisnya, maka untuk melindungi data tersebut dari serangan resiko *digital* yang mungkin sekali terjadi, maka perusahaan X tersebut memutuskan untuk memproteksi data elektroniknya dengan *cyber insurance* dari *AIG eBusiness Risk Solution*. Antara perusahaan X dengan *AIG* mengikat suatu perjanjian asuransi dengan klausula *all risk* dengan jangka waktu selama 3 tahun, dengan nilai pertanggungan sebesar US\$ 10 juta dan premi sebesar US\$ 75.000 per tahun. Pada tahun kedua terjadi suatu peristiwa tidak pasti yaitu data-data elektronik yang disimpan dalam jaringan kerja komputer perusahaan X dicuri oleh *hacker*. Akibat dari pencurian tersebut perusahaan x menderita kerugian sebesar US\$ 6

⁹ Emmy Pangaribuan Simanjuntak, “*Hukum Pertanggungan dan Perkembangannya*”, hal 22

juta. Dengan adanya kerugian tersebut, maka perusahaan x mengajukan klaim ganti kerugian kepada *AIG* sebagai pihak penanggung. Oleh *AIG*, perusahaan x diberikan ganti kerugian sebesar kerugian yang diderita yaitu sebesar US\$ 6 juta”.

Apabila kasus tersebut terjadi di Indonesia, maka yang perlu ditinjau adalah mengenai perjanjian asuransinya, apakah perjanjian asuransi tersebut telah memenuhi unsur-unsur asuransi dalam pasal 246 KUHD.

1. Adanya tertanggung, dalam kasus ini yang menjadi pihak tertanggung adalah Perusahaan X.
2. Adanya Penanggung, dalam kasus ini yang menjadi pihak penanggung adalah Perusahaan asuransi *AIG*.
3. Adanya pembayaran premi dari tertanggung kepada penanggung, dalam kasus terlihat adanya penentuan besarnya premi yang harus dibayar oleh tertanggung yaitu sebesar US\$ 75.000 per tahun
4. Adanya peristiwa tidak pasti, suatu peristiwa tidak pasti dapat terjadi karena adanya suatu resiko yang mengancam obyek asuransi tersebut. Dalam kasus ini resiko yang mengancam adalah berupa resiko *digital* seperti *virus* dan serangan *hacker*. Disini terlihat adanya serangan dari *hacker*. Dengan begitu serangan tersebut dapat dikatakan sebagai suatu peristiwa tidak pasti.
5. Adanya pembayaran ganti rugi dari penanggung kepada tertanggung. Dengan adanya kerugian dari pihak tertanggung maka pihak penanggung akan memberikan ganti rugi kepada pihak tertanggung. Dalam kasus pihak penanggung memberikan ganti rugi kepada pihak tertanggung sebesar kerugian yang diderita yaitu sebesar US\$ 6 juta.

Dari hasil tinjauan tersebut dapat terlihat bahwa perjanjian *cyber insurance* tersebut telah memenuhi semua unsur-unsur asuransi yang terkandung dalam pasal 246 KUHD. Jadi dapat dikatakan bahwa perjanjian *cyber insurance* tersebut memang merupakan suatu perjanjian asuransi.

Selanjutnya yang perlu ditinjau adalah mengenai obyek asuransi yang akan ditinjau berdasarkan pasal 268 KUHD.

Di dalam kasus yang menjadi obyek asuransi adalah data-data elektronik yang tersimpan dalam jaringan kerja komputer perusahaan X. menurut pasal 268 KUHD pada dasarnya semua kepentingan dapat diasuransikan asalkan memenuhi syarat: dapat dinilai dengan uang, diancam oleh suatu bahaya dan tidak dikecualikan oleh undang-undang. Data-data elektronik milik Perusahaan X merupakan sesuatu yang dapat dinilai dengan uang. Hal ini ditunjukkan bahwa data-data tersebut mempunyai peranan penting untuk mengendalikan bisnis perusahaan X yang dapat diartikan bahwa data-data tersebut dapat menentukan untung rugi perusahaan tersebut. Unsur yang kedua adalah diancam oleh suatu bahaya. Bahaya yang mengancam data-data elektronik adalah berupa serangan dari resiko *digital* seperti *virus* dan serangan *hacker*. Dan yang terakhir adalah tidak dikecualikan oleh undang-undang. Data-data elektronik tersebut bukanlah sesuatu yang dilarang atau dikecualikan oleh undang-undang sepanjang data-data elektronik tersebut mempunyai hubungan yang kuat dengan bidang bisnis yang dijalankan oleh perusahaan tersebut, dengan syarat bidang bisnis yang dijalankan oleh perusahaan tersebut bukanlah suatu bisnis yang dilarang atau dikecualikan oleh undang-undang. Dalam kasus data-data elektronik tersebut berhubungan kuat

dengan bidang bisnis yang dijalankan oleh perusahaan yaitu otomotif, jadi bukan merupakan suatu hal yang dikecualikan oleh undang-undang

Dari hasil tinjauan ini dapat terlihat juga semua unsur dalam pasal 268 KUHD telah terpenuhi. Dengan begitu keberadaan *cyber insurance* ini tidak bertentangan dengan KUHD.

Dasar hukum lain yang dapat dikemukakan sebagai dasar hukum berlakunya *Cyber Insurance* adalah ada pada sifat utama dari asuransi itu sendiri sebagaimana telah dikemukakan di atas yaitu bahwa pada dasarnya asuransi atau pertanggungan merupakan suatu perjanjian atau dengan kata lain asuransi atau pertanggungan timbul karena adanya perjanjian. Di dalam Kitab Undang-undang Hukum Perdata (*Burgerlijk Wetboek – BW*) terdapat satu asas yang mempunyai peranan yang sangat penting dalam pembuatan suatu perjanjian yaitu “Asas Kebebasan Berkontrak” yang diatur dalam pasal 1338 BW. Asas kebebasan berkontrak yang diatur dalam buku III BW tersebut mempunyai sifat terbuka.

Sifat terbuka dari buku III BW ini lebih banyak berlandaskan pada aspek perikatan yang bersumber pada perjanjian. Ini memang mengandung makna bahwa masyarakat diberi keleluasaan untuk mengadakan perjanjian apa saja, dengan siapa saja dan dengan isi sebagaimana kehendak mereka. Para pihak dapat membuat perjanjian di luar apa yang dikenal oleh undang-undang. Ini dapat dipahami karena sudah demikian beragam dan pesatnya perkembangan bisnis di dalam masyarakat itu yang kadangkala memerlukan perangkat-perangkat hukum yang baru sebagai penunjang. Dengan adanya asas kebebasan berkontrak yang tercantum dalam pasal 1338 BW, maka masyarakat akan selalu dapat

mengembangkan aneka kebutuhan yang diperlukan, juga dalam lapangan bisnis, tanpa harus dihadang oleh aturan yang kaku.¹⁰

Akan tetapi asas kebebasan berkontrak yang diatur di dalam pasal 1338 BW harus juga memperhatikan ketentuan pasal 1320 BW mengenai syarat sahnya suatu perjanjian. Meskipun para pihak diberikan kebebasan untuk membuat perjanjian sesuai dengan kehendak para pihak, tetapi jika tidak memenuhi syarat sahnya perjanjian dalam pasal 1320 BW maka berakibat hukum dapat dibatalkan jika syarat yang tidak dipenuhi adalah syarat kesepakatan dan kecakapan atau batal demi hukum jika syarat yang tidak dipenuhi adalah suatu hal yang tertentu dan suatu sebab yang halal.

Sebenarnya ketentuan mengenai keberlakuan *Cyber Insurance* diatur di dalam *UNCITRAL Model Law on Electronic Commerce* yaitu:¹¹

Chapter I: General Provisions

Article I : Sphere of Application

- *This law applies to any kind information in the form of a data message used in the context of commercial activities.*
- *The "term" commercial should be given a wide interpretation so as to cover matters arising from all relationship of a commercial nature, whether commercial or not. Relationship of commercial nature include but are not limited to, the following transaction: any trade for transaction for supply or exchange of goods or services, distribution agreement, commercial representation or agencies, factoring, leasing , contruction of works, consulting, engineering, licensing, investment, banking, insurance, exploitation agreement or concession, joint venture, and other form of industrial or business cooperation, carriage of goods or passenger by air, sea, road or rail.*

¹⁰ Naniek Endang Wrediningsih, S.H., "*Kebebasan Berkontrak Sebagai Azas Hukum Perjanjian*", *Makalah Penelitian Hukum Kotrak Fakultas Hukum Universitas Airlangga*, hal 2

¹¹ *UNCITRAL, Model Law on Electronic Commerce, Chapter I General Provision, Article 4 Variation by Agreement.*

Dalam bagian I mengenai ketentuan umum, artikel I mengenai ruang lingkup penerapan disebutkan bahwa ketentuan atau undang-undang ini diterapkan untuk segala jenis informasi yang berbentuk pesan data yang digunakan dalam konteks perdagangan. Kemudian dijelaskan lagi bahwa istilah perdagangan tersebut harus diinterpretasikan secara luas untuk *mengcover* segala persoalan yang timbul dari hubungan dagang yang bersifat alami baik yang bersifat kontraktual maupun yang tidak bersifat kontraktual. Hubungan dagang tersebut termasuk dan tidak terbatas pada transaksi-transaksi sebagai berikut : segala bentuk transaksi untuk memasok atau untuk mempertukarkan barang dan/ atau jasa, perjanjian distributor, perjanjian keagenan, anjak piutang, sewa guna usaha, jasa konstruksi, jasa konsultasi, teknologi, lisensi, investasi, pembiayaan, asuransi, perjanjian eksploitasi atau konsesi, joint venture, dan bentuk-bentuk kerjasama industrial atau bisnis lainnya; pengangkutan barang atau penumpang melalui darat, air atau udara.

Belum adanya ketentuan Undang-undang yang mengatur secara tegas mengenai *Cyber Insurance* di Indonesia, karena di Indonesia sendiri belum menjadi suatu yang fenomenal bagi perusahaan asuransi untuk mengembangkan usahanya dalam bentuk *Cyber Insurance*. Hal ini karena kurangnya dorongan kebutuhan masyarakat yang ditunjukkan rendah atau bahkan kurangnya tingkat permintaan masyarakat di bidang ini. Namun diprediksikan dalam rentang waktu yang relatif singkat permintaan untuk proteksi *Cyber Insurance* di Indonesia akan meningkat dan terdapat kecenderungan akan semakin berkembang. Dari hasil survey penulis, hal-hal lain yang menjadi penyebab bahwa *Cyber Insurance* belum menjadi suatu yang fenomenal bagi perusahaan asuransi adalah:¹²

1. Masih kurangnya pengetahuan dari pihak perusahaan asuransi mengenai *Cyber Insurance* tersebut.

¹² Joko Winarko, S.E., "*PT. Asia Reliance General Insurance*".

2. Tingginya resiko yang harus ditanggung oleh perusahaan *Cyber Insurance* tersebut yang juga didukung dengan lemahnya kekuatan pembuktian dari pihak tertanggung untuk dapat membuktikan bahwa telah terjadi peristiwa tidak pasti terhadap obyek asuransinya. Atau dengan kata lain rumitnya prosedur administrasi klaim.

Tetapi sekali lagi disini ditegaskan bahwa dengan tidak adanya ketentuan perundang-undangan mengenai *Cyber Insurance* bukan berarti tidak dapat diterapkan atau tidak dapat diberlakukan di Indonesia.

2. Ruang Lingkup Perlindungan *Cyber Insurance*

Pada prinsipnya *Cyber Insurance* merupakan salah satu jenis asuransi kerugian karena *cyber insurance* mengcover segala resiko akan terjadinya kerugian yang mengancam aktivitas-aktivitas *e-business*. Pada *AIG eBusiness Risk Solution* terdapat beberapa macam lingkup perlindungan yaitu :

1. *Internet Media Liability Coverage*

Yaitu suatu bentuk perlindungan yang ditujukan untuk segala informasi yang ditampilkan dalam suatu situs internet termasuk judul-judul iklan. Dimana informasi maupun judul-judul iklan tersebut diancam oleh suatu bahaya yang memungkinkan bagi pihak ketiga untuk melakukan pencemaran nama baik atau fitnah, pelanggaran hak-hak cipta atau merek, atau pelanggaran atas privasi. Di sisi lain, isi dari situs internet dimunculkan secara statis atau dinamis, kadang terlihat kadang tersembunyi. Hal tersebut merupakan resiko dimana seseorang dalam mengakses informasi tersebut dimungkinkan untuk

mengalami serangan atau gangguan. Jadi disini obyek perlindungannya adalah segala informasi termasuk judul-judul iklan yang ditampilkan dalam suatu situs internet.

2. *Internet Professional Liability*

Dengan disediakannya jasa pelayanan *Internet Professional*, untuk klien dan pengguna situs internet, maka perusahaan tersebut terbuka untuk diancam suatu resiko yang signifikan. Misal dalam kasus sebagai berikut:

“Seorang *retailer* mengajukan gugatan melawan sebuah perusahaan penyedia jasa layanan aplikasi untuk menuntut ganti kerugian atas kerusakan-kerusakan yang dialami oleh *retailer* tersebut berkaitan dengan kegagalan dari sistemnya (*System Failure*). Gugatan tersebut menyatakan bahwa penyedia jasa aplikasi tersebut karena kelalaiannya dalam melakukan pemeliharaan terhadap sistem manajemen inventaris milik *retailer* membawa hasil bahwa *retailer* tersebut mengalami kerugian (*Loss of Profit*).”

Bentuk-bentuk jasa pelayanan profesional yang ditawarkan untuk media internet membawa implikasi hukum yang sama dengan bentuk-bentuk jasa pelayanan profesional yang bersifat tradisional yang telah ada sebelumnya.

Jasa pelayanan *Internet Professional* meliputi :

1. Penyedia jasa pelayanan aplikasi
2. *Domain name registration services*
3. *E-Commerce transaction services*
4. *Electronic exchange and action services*
5. *Internet hosting*

6. *Internet media services*
7. *Internet service provider services*
8. *Managed network and network security services*
9. *Search engine service*
10. *Web portal service.*

Dari jasa-jasa yang disediakan oleh suatu perusahaan untuk kliennya atau untuk pengguna situs internet, maka akan timbul suatu resiko seperti contoh kasus yang telah disebutkan diatas. Untuk itulah diperlukan suatu perlindungan untuk mengcover semua kemungkinan resiko yang akan timbul atas jasa pelayanan *Internet Professional* yang telah diberikan oleh perusahaan kepada klien atau pengguna. Jadi disini obyek perlindungannya adalah jaminan atas jasa yang diberikan suatu perusahaan jasa layanan internet kepada kliennya apabila timbul suatu kerugian yang disebabkan oleh adanya kegagalan dalam sistemnya.

3. *Network Security Liability*

Sebagian besar dunia bisnis menggunakan jaringan kerja komputer dan menyimpan data elektronik yang dianggap penting untuk mengendalikan bisnis mereka. Menyediakan keamanan untuk data yang telah disimpan dalam jaringan komputer, dapat merupakan data perusahaan itu sendiri, data dari klien, atau data dari supplier akan membawa suatu tantangan baru. Virus-virus komputer yang baru dibuat secara berkesinambungan dan disebarkan melalui internet dan *e-mail*. Serangan dari sistem “Penolakan Pelayanan” (*Denial of Service*) bukanlah suatu hal yang luar biasa lagi. Telah banyak cerita tentang

pembobolan suatu sistem komputer oleh *hacker*,¹³ mencuri data-data tersebut, bahkan terkadang menjual kembali atau menggunakannya untuk tujuan dari para hacker itu sendiri. Resiko seperti ini dapat menciptakan pertanggungjawaban hukum yang sangat besar. Sebuah pelanggaran dari sistem keamanan suatu jaringan kerja dapat mengakibatkan terjadinya pencurian suatu identitas dan menimbulkan adanya suatu klaim dari pelanggan yang merasa informasinya telah dicuri, klaim dari pelanggan yang mengalami penolakan pelayanan sehingga tidak dapat mengakses sistem tersebut dan juga klaim dari setiap pihak kepada siapa perusahaan tersebut secara tidak sengaja, menularkan sebuah virus komputer yang potensial.

Sebagai contoh kasus dari resiko ini adalah :

Seorang *hacker* melakukan pencurian terhadap 300.000 (tiga ratus ribu) nomor kartu kredit dari sebuah *online retailer*. Berdasarkan penolakan yang tegas untuk melakukan kerja sama, *hacker* tersebut memasang 23.000 (dua puluh tiga ribu) nomor kartu kredit secara *online*. Sebagai akibat dari pembatalan kartu kredit dan penerbitan kembali, *online retailer* tersebut mengalami kerugian sebesar \$2.000.000 (dua juta dolar Amerika) dan serangan dari pihak ketiga. Jadi disini obyek perlindungannya adalah keamanan jaringan kerja suatu komputer tempat dimana data-data suatu

¹³ *Hacker* adalah seorang ahli komputer yang pekerjaannya adalah menyusup ke dalam komputer orang lain dengan tujuan-tujuan tertentu.

Kurniawan Nugroho, *Analisa Resiko dan Merancang Bentuk Asuransi Untuk Resiko Digital*, hal 26

perusahaan itu disimpan, bukan hanya data perusahaan, juga data dari kliennya.

4. *Cyber Extortion Coverage*

Hacker yang telah dikenal sebagai pencuri data dari kartu kredit pelanggan atau menggunakan informasi yang telah dicurinya untuk kemudian dipublikasikan kepada umum bahkan sangat dimungkinkan bahwa informasi yang telah dicuri tersebut akan diberikan ke tangan perusahaan pesaing, kecuali pihak yang menjadi korban pencurian tersebut bersedia membayar *hacker* tersebut sebagai suatu tebusan. Sebagai contoh kasus adalah :

Seorang *hacker* komputer melakukan pemerasan sebanyak \$10.000 (sepuluh ribu dolar) terhadap sebuah bank di *United States* dengan cara melakukan pembobolan pada situs internet milik *Oline Resources Corporation*, yang merupakan sebuah perusahaan yang menawarkan pelayanan aplikasi *internet-banking, bill payment, dan e-finance* untuk institusi keuangan. *Hacker* tersebut mempublikasikan detail dari 1500 (seribu lima ratus) rekening secara *online* untuk memperkuat ancamannya. Jumlah kerugian total dari perusakan aset-aset informasi dan biaya-biaya yang dikeluarkan untuk pemerasan tersebut adalah sejumlah \$250.000 (dua ratus lima puluh ribu dolar)

Dengan adanya kasus seperti inilah, ancaman atas tindakan pemerasan oleh *hacker* perlu dilindungi oleh asuransi sebagai usaha untuk mengalihkan resiko kerugian. Jadi disini obyek perlidungannya adalah jumlah dana yang dikeluarkan oleh suatu perusahaan sebagai uang tebusan untuk mendapatkan kembali informasi-informasi yang telah dicuri oleh *hacker*.

5. *Criminal Reward Fund Coverage*

Dewasa ini kejahatan dalam dunia komputer atau sering disebut dengan *Cyber-crime* mulai muncul di permukaan. Baik beraksi untuk mendapatkan keuntungan pribadi atau hanya sekedar untuk “menyombongkan keahliannya”, para *hacker* melihat suatu jaringan kerja yang aman sebagai suatu tantangan yang menggiurkan. Sebagai contoh kasus untuk menunjukkan pentingnya suatu ancaman *Cyber-crime* perlu diasuransikan adalah :

Dua orang hacker melakukan perusakan terhadap sistem kerja komputer dari sebuah perusahaan induk penelitian pasar dan kemudian mendapatkan catatan rahasia dari perusahaan tersebut. Arsip-arsip yang telah dicuri tersebut termasuk foto-foto dari para pegawai, kata kunci jaringan kerja, dan nomor kartu kredit pribadi dari beberapa *senior manager*. Para *hacker* tersebut mengancam untuk melakukan pelanggaran terhadap sistem keamanan milik klien perusahaan tersebut kecuali pihak Direktur Utama membayar mereka sejumlah “*Consulting fee*” sebesar \$200.000 (dua ratus ribu dolar). Bentuk perlindungan asuransi dalam bentuk “*Reward Fund*” diadakan untuk membantu menahan para penjahat internet (*cyber criminals*) tersebut.

6. *Crisis Communication Management Fund*

Ketika sistem jaringan kerja tersebut diserang, peristiwa tersebut dapat menyebabkan tidak hanya krisis secara finansial tetapi juga suatu mimpi buruk terhadap hubungan antara perusahaan dengan masyarakat. Tekanan yang buruk yang disebabkan oleh gangguan dalam bisnis atau kegagalan sistem keamanan jaringan kerja lebih jauh lagi dapat membahayakan bisnis itu

sendiri. Krisis manajemen yang berat akan mengakibatkan perusahaan tersebut untuk mengambil tindakan untuk memperingatkan para pelanggan, pegawai, dan pemegang saham tentang situasi tersebut sebelum tekanan itu terjadi dan menciptakan “lingkarannya” sendiri.

Dari kasus penyerangan sistem jaringan kerja yang dilakukan oleh *hacker*, biasanya perusahaan akan menyewa jasa investigator ahli khusus untuk penjahat internet (*cyber criminals*) dengan begitu diharapkan para penjahat internet tersebut dapat ditangkap dan ditahan serta diproses secara hukum. Biasanya perusahaan dalam usahanya untuk melakukan pencarian menghabiskan biaya sejumlah \$1.000.000 (satu juta dolar) untuk melakukan investigasi dan juga untuk pembayaran upah untuk seorang humas (*Public Relation*).

Bagi perusahaan biaya yang dikeluarkan tersebut pastilah merupakan kerugian tersendiri. Untuk itulah diperlukan suatu bentuk perlindungan asuransi untuk mengcover biaya-biaya yang dikeluarkan dalam rangka usaha pencarian para penjahat internet tersebut.

7. *Network Business Interruption*

Sebagian besar bisnis moderen menggunakan sistem jaringan kerja komputer dan melakukan penyimpanan data. Bentuk bisnis dimana sistem kerjanya tergantung pada jaringan kerja komputer membutuhkan keamanan, dan infrastruktur yang kuat. Serangan virus komputer seperti “*Love Bug*” atau “*Denial of Service*” dapat mengakibatkan rusaknya jaringan kerja dan

terhentinya aktivitas bisnis. Serangan pada komputer dapat mengganggu aktivitas bisnis dan membawa dampak kerugian yang sangat serius, termasuk :

- Berkurangnya pendapatan yang nyata-nyata diperoleh
- Biaya ekstra yang dikeluarkan dalam usahanya untuk menemukan dan menghentikan gangguan pada aktivitas bisnis.
- Biaya ekstra yang dikeluarkan dalam usahanya untuk menemukan sumber dari serangan pada komputer.

Contoh kasus dari pentingnya bentuk perlindungan "*Network Business Interruption*" adalah :

Seorang *hacker* membanjiri beberapa situs besar dengan cara menyebarkan serangan sistem "*Denial of Service*". *Hacker* tersebut melakukan pembajakan terhadap aneka jenis komputer di seluruh dunia dan kemudian memprogram sistem tersebut untuk menyerang target yang dituju dengan berpura-pura melakukan permintaan yang sah atas suatu data. Hal ini menunjukkan perkiraan serangan dari sistem "*Denial of Service*" yang telah mengacaukan situs tersebut, mempunyai kemampuan untuk mengendalikan aktivitas bisnis, dikarenakan kerugian yang diderita oleh perusahaan yang melebihi \$10.000.000 (sepuluh juta dolar).¹⁴

¹⁴ *Keseluruhan data berasal dari AIG eBusiness Risk Solution.*

3. Hubungan Hukum Para Pihak Dalam Cyber Insurance

Pada prinsipnya hubungan hukum yang terjadi dalam suatu perjanjian asuransi adalah antara penanggung dan tertanggung. Hal ini tersirat dari pasal utama dari perjanjian asuransi yaitu pasal 246 KUHD yang dapat diartikan bahwa pada prinsipnya perjanjian asuransi adalah terjadi antara pihak penanggung dengan pihak tertanggung.

Pada perkembangannya hubungan hukum tersebut dapat meluas hingga bersangkut paut dengan pihak ketiga seperti disebutkan dalam pasal 264 KUHD yaitu :

“Suatu pertanggungan tidak saja dapat ditutup atas tanggungan sendiri, tetapi juga dapat ditutup atas tanggungan seorang ketiga, baik berdasarkan suatu kuasa umum atau khusus, maupun di luar pengetahuan si berkepentingan sekalipun, dan demikian itu dengan mengindahkan ketentuan-ketentuan yang berikut”.

Hubungan hukum dalam perjanjian asuransi yang menyangkut pihak ketiga tidak hanya seperti yang digambarkan dalam pasal 264 KUHD saja, tetapi juga dapat terjadi dalam hal adanya pihak reasuransi dalam perjanjian asuransi tersebut. Reasuransi merupakan suatu cara yang dipakai oleh pihak penanggung pertama untuk mendistribusikan resiko-resiko yang dipikulnya dengan jalan menyerahkan semua atau sebagian dari resiko-resiko tersebut kepada pihak reasuransi (penanggung kedua) dengan tujuan mengurangi jumlah kerugian yang mungkin akan diderita oleh penanggung pertama tersebut.¹⁵

¹⁵ Djoko Prakoso, S.H., *Hukum Asuransi Indonesia*, hal 88.

Untuk reasuransi di dalam KUHD diatur di dalam pasal 271 KUHD yang berbunyi “Si penanggung selamanya berkuasa untuk sekali lagi mempertanggungkan apa yang telah ditanggung olehnya.”

Dalam hal terjadinya reasuransi terbuka peluang yang sangat luas untuk masuknya pihak keempat maupun pihak kelima dan seterusnya, yaitu bilamana pihak reasuransi (penanggung kedua) mereasuransikan lagi kepada pihak reasuransi kedua (dalam konteks ini ia berperan sebagai penanggung ketiga) dan begitu seterusnya. Peluang tersebut diberikan oleh pasal 271 KUHD yang telah tersebut diatas.

Selain reasuransi, masuknya pihak ketiga dalam perjanjian asuransi dapat terjadi dalam suatu kondisi terjadinya peristiwa tidak pasti disebabkan oleh kelalaian pihak ketiga. Dalam hal ini pihak ketiga juga ikut bertanggung jawab untuk mengganti kerugian kepada pihak tertanggung. Kondisi semacam ini disebut dengan subrogasi. Mengenai subrogasi diatur di dalam pasal 284 KUHD.

Pada sub-bab ini penulis mencoba untuk menganalisa hubungan hukum para pihak dalam *cyber insurance* ditinjau dari ruang lingkupnya masing-masing sebagaimana telah djabarkan di pada sub-bab sebelumnya, yaitu :

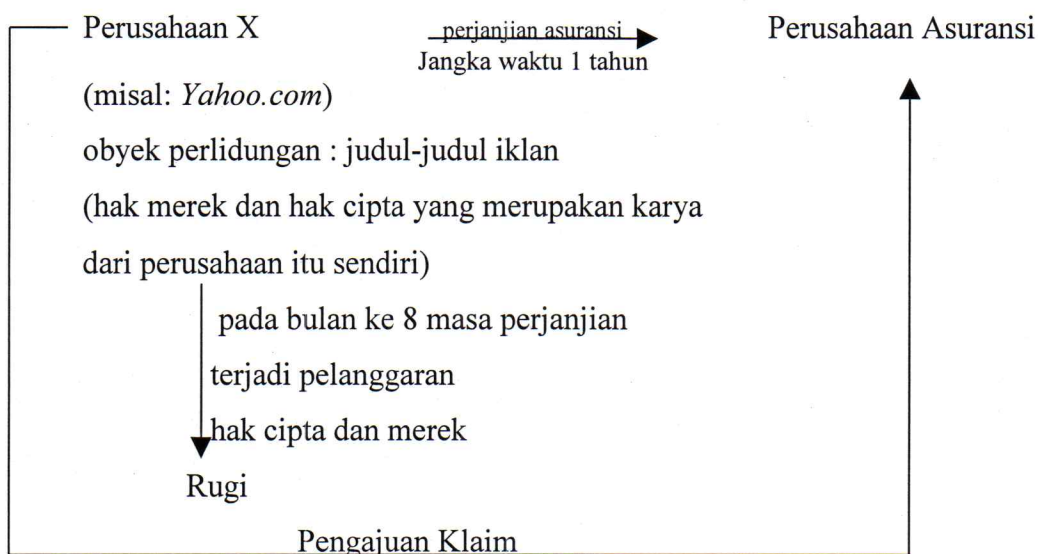
1. Hubungan Hukum Para Pihak Dalam *Internet Media Liability Coverage*

Jenis perlindungan ini memberikan perlindungan terhadap semua informasi yang ditampilkan di dalam suatu situs internet termasuk judul-judul iklan. Pada bentuk perlindungan yang seperti ini, pihak ketiga bisa terlibat, bisa juga tidak terlibat (pihak ketiga disini adalah pihak yang ikut dirugikan atas

terjadinya suatu peristiwa tidak pasti) karena resiko yang mengancam dapat berbentuk pelanggaran hak cipta atau merek.

Hubungan hukum yang terjadi hanyalah antara dua belah pihak saja yaitu perusahaan X sebagai tertanggung dan perusahaan asuransi sebagai penanggung. Disini pihak ketiga tidak terlibat karena kerugian hanya diderita oleh perusahaan X saja. Untuk lebih jelasnya mengenai hubungan hukum para pihak dalam jenis perlindungan ini, dapat digambarkan sebagai berikut :

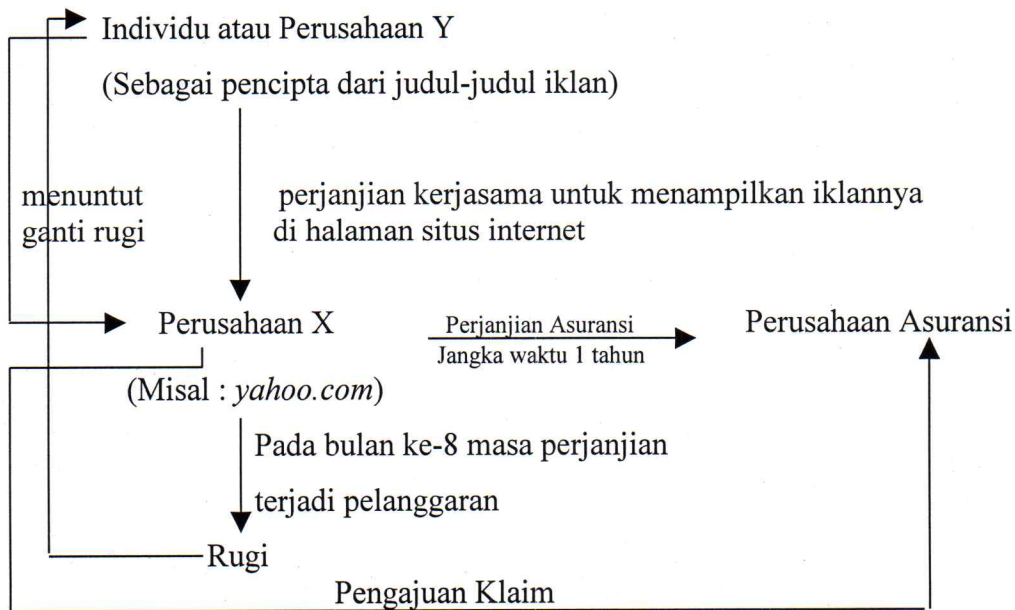
a. Hubungan Hukum Yang Tidak Melibatkan Pihak Ketiga (Secara Sederhana)



b. Hubungan Hukum Yang Melibatkan Pihak Ketiga

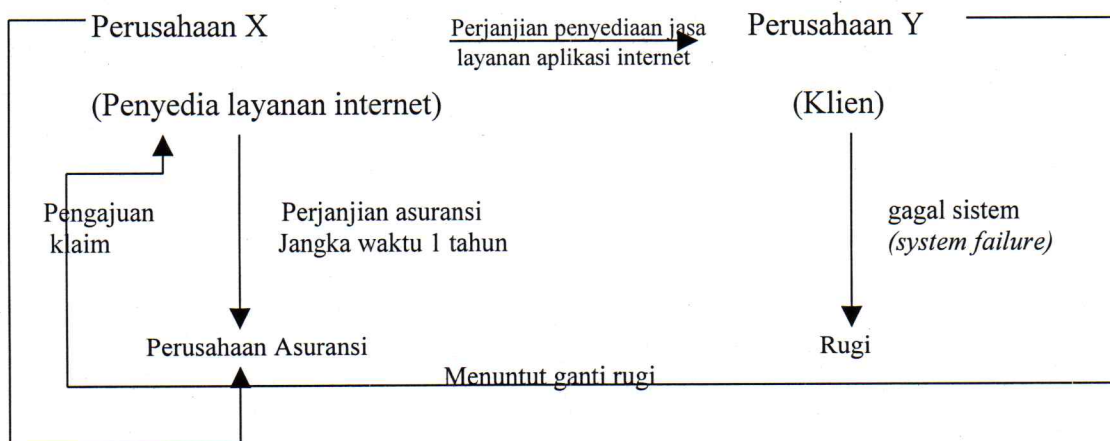
Disini pihak ketiga terlibat karena pihak ketiga sebagai pencipta dari iklan tersebut merasa dirugikan atas terjadinya pelanggaran hak cipta dan hak merek atas iklannya. Disini pihak ketiga berposisi sebagai pihak yang terpisah dari perusahaan X sebagai pihak tertanggung. Meskipun nantinya

ganti rugi yang diberikan oleh pihak asuransi akan diberikan kepada pihak ketiga tersebut. Hubungan tersebut dapat digambarkan sebagai berikut :



2. Hubungan Hukum Para Pihak Dalam *Internet Professional Liability Coverage*

Bentuk perlindungan ini memberikan perlindungan atas jasa yang diberikan oleh perusahaan jasa pelayanan internet kepada kliennya terhadap resiko adanya kegagalan dalam sistemnya. Salah satu contoh dari jasa pelayanan internet ini adalah jasa pelayanan aplikasi internet. Hubungan hukum pada bentuk perlindungan seperti ini dapat digambarkan sebagai berikut.



Pada hubungan hukum yang demikian perusahaan X mempunyai dua posisi yaitu di satu sisi sebagai tertanggung dalam hubungannya dengan perusahaan asuransi (perjanjian asuransi) dan sebagai penanggung dalam hubungannya dengan perusahaan Y (perjanjian kerjasama). Antara perusahaan asuransi dan perusahaan Y (klien perusahaan X) tidak mempunyai hubungan hukum meskipun yang menderita kerugian adalah perusahaan Y.

3. Hubungan Hukum Para Pihak Dalam *Network Security Liability Coverage*

Hubungan hukum yang terjadi pada jenis perlindungan ini adalah antara :

1. Perusahaan X dengan Perusahaan Asuransi yang diikat dengan perjanjian asuransi.
2. Perusahaan X dengan Klien atau *Supplier* yang diikat dengan perjanjian kerjasama.

Bilamana terjadi pencurian informasi oleh *hacker* terhadap data milik Klien atau *Supplier* yang menimbulkan kerugian bagi mereka maka Klien atau *Supplier* tersebut menuntut ganti rugi kepada Perusahaan X. Atas ganti rugi yang dibayarkan oleh Perusahaan X kepada Klien Atau *Supplier* yang menderita kerugian akibat dicurinya informasi data milik mereka yang disimpan di jaringan komputer Perusahaan X, Perusahaan X sebagai pihak tertanggung dalam perjanjian asuransi dapat mengajukan klaim ganti rugi kepada pihak asuransi sebagai pihak penanggung. Jadi disini antara pihak asuransi dengan klien atau *supplier* tidak ada hubungan hukum. Dan seperti jenis perlindungan asuransi sebelumnya, Perusahaan X mempunyai dua posisi yaitu sebagai penanggung dalam perjanjian kerjasama dengan klien atau

supplier dan sebagai tertanggung dalam perjanjian asuransi dengan perusahaan asuransi.

4. Hubungan Hukum Para Pihak Dalam *Cyber Extortion Coverage*

Hubungan hukum disini dapat terjadi dalam dua bentuk yaitu :

1. Hubungan hukum yang terjadi hanyalah antara Perusahaan X sebagai pihak tertanggung dengan Perusahaan Asuransi sebagai pihak penanggung yang diikat dengan perjanjian asuransi. Pada hubungan hukum seperti ini pihak ketiga tidak dilibatkan karena untuk memperkuat ancamannya untuk melakukan pemerasan terhadap perusahaan yang informasinya telah dicuri, *hacker* tidak ikut mencuri data pihak ketiga dalam hal ini adalah pelanggan.
2. Hubungan hukum yang terjadi adalah antara Perusahaan X dengan Perusahaan Asuransi yang diikat dengan perjanjian asuransi dan Perusahaan X dengan Pihak Ketiga dalam hal ini adalah pelanggan yang diikat dengan perjanjian jual beli dengan menggunakan kartu kredit . Pada pola hubungan seperti ini pihak ketiga dilibatkan karena untuk memperkuat ancamannya, *hacker* ikut mencuri data pihak ketiga.

5. Hubungan Hukum Para Pihak Dalam *Criminal Reward fund Coverage*

Hubungan hukum yang terjadi hanyalah antara Perusahaan X sebagai pihak tertanggung dengan Perusahaan Asuransi sebagai pihak penanggung yang diikat dengan perjanjian asuransi. Tetapi hubungan hukum tersebut tidak semata-mata berkait dengan Perusahaan itu saja, tetapi juga berkait dengan individu-individu yang ada di dalam perusahaan tersebut. Kerugian yang

diderita bukan hanya dialami oleh perusahaan secara umum, tetapi juga dialami oleh individu-individu yang ada di dalam perusahaan. Untuk lebih jelasnya dapat dilihat pada contoh kasus yang telah dituliskan pada sub-bab sebelumnya.

6. Hubungan Hukum Para Pihak Dalam *Crisis Communication Management Fund*

Hubungan hukum yang terjadi disini adalah antara :

1. Perusahaan X sebagai pihak bertanggung dengan Perusahaan Asuransi sebagai pihak penanggung yang diikat dengan perjanjian asuransi.
2. Perusahaan X dengan Pihak Investigator dan pihak *Public Relation* yang diikat dengan perjanjian kerjasama dengan pembayaran sejumlah upah.

Munculnya investigator disini adalah untuk menangkap penjahat internet yang telah melakukan serangan untuk kemudian ditahan dan dapat diproses secara hukum. Sedangkan munculnya *public relation* adalah untuk mengkomunikasikan kepada masyarakat, para pelanggan, para pegawai dan para pemegang saham akan ancaman bahaya yang akan menimpa perusahaan tersebut.

Disini peran asuransi adalah untuk mengganti semua biaya-biaya yang telah dikeluarkan oleh perusahaan untuk membayar upah dari investigator dan *public relation* tersebut.

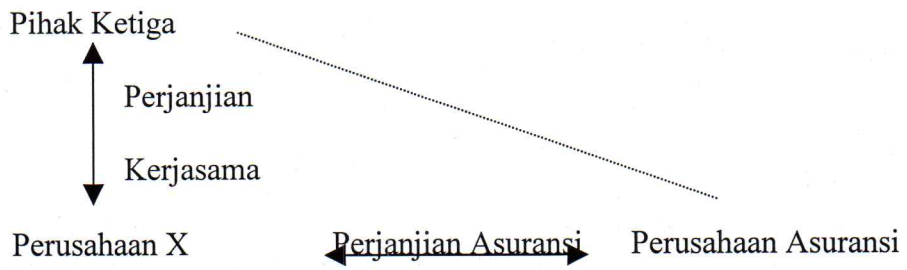
Antara perusahaan asuransi dengan investigator dan *public relation* tidak terdapat hubungan hukum.

7. Hubungan Hukum Para Pihak Dalam *Network Business Interruption*

Hubungan hukum yang terjadi disini adalah murni antara Perusahaan X sebagai pihak bertanggung dengan Perusahaan Asuransi sebagai pihak penanggung yang diikat dengan perjanjian asuransi. Dalam jenis perlindungan ini hanya ada satu hubungan hukum karena kerugian yang muncul nyata-nyata diderita oleh Perusahaan X tersebut bukan pada pihak ketiga. Meskipun pihak ketiga ikut merasa dirugikan, tetapi kerugian yang dirasakan mereka tidak secara langsung dan tidak nyata-nyata diderita. Misal dalam situasi sebagai berikut :

Suatu situs internet diserang oleh suatu virus komputer. Disini yang nyata-nyata merasakan dampak negatifnya adalah perusahaan pemilik situs tersebut bukan pelanggan atau pemakai dari situs tersebut, meskipun ia juga sedikit dirugikan.

Kesimpulan yang dapat diambil dari analisa diatas adalah bahwa hubungan hukum yang terjadi pada pokoknya atau perjanjian utama yang terjadi adalah perjanjian asuransi antara Perusahaan X dengan Perusahaan Asuransi. Dan tidak ada satupun dari jenis-jenis perlindungan tersebut yang menyatakan bahwa antara pihak ketiga dengan Perusahaan asuransi terdapat hubungan hukum. Terkaitnya pihak ketiga dengan perusahaan asuransi adalah karena dihubungkan dengan Perusahaan X sebagai pihak bertanggung dalam perjanjian asuransi. Masuknya pihak ketiga diikat dengan perjanjian yang berbeda, bukan perjanjian asuransi. Secara global hubungan hukum tersebut dapat digambarkan sebagai berikut :



BAB III
SISTEM PERTANGGUNGJAWABAN
CYBER INSURANCE

Rahayu

BAB III

SISTEM PERTANGGUNGJAWABAN

CYBER INSURANCE

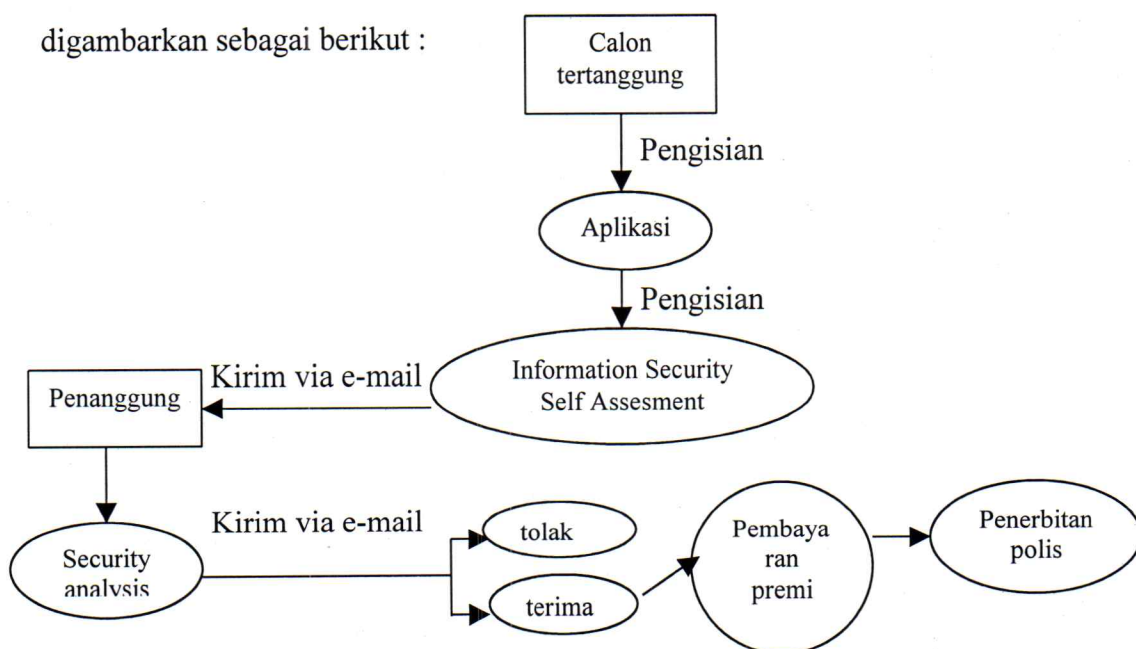
1. Terjadinya Penutupan Perjanjian *Cyber Insurance*

Pada *AIG eBusiness Risk Solution*, ada dua cara yang dapat ditempuh untuk mengadakan perjanjian *cyber insurance*, yaitu dengan cara *online* dan *offline*. Dengan cara *online*, maksudnya calon tertanggung atau pemohon dapat mengisi aplikasi permohonan yang telah disediakan oleh pihak penanggung pada situs internetnya. Setelah aplikasi tersebut selesai diisi oleh calon tertanggung atau pemohon, maka kemudian diteruskan dengan mengisi form mengenai *Information Security Self Assesment* yaitu form yang menunjukkan informasi-informasi mengenai bentuk-bentuk pertahanan yang telah digunakan oleh calon tertanggung untuk mengatasi atau paling tidak meminimalisasi serangan-serangan dari resiko digital. Setelah kedua form tersebut diisi secara lengkap oleh calon tertanggung, maka pihak penanggung mensyaratkan agar kedua form tersebut dikirimkan melalui *e-mail* ke alamat *e-mail* penanggung untuk kemudian ditinjau oleh pihak penanggung, tinjauan tersebut dinamakan dengan analisa kemanan (*Security Analysis*). Hasil dari tinjauan tersebut juga akan dikirimkan melalui *e-mail*, dimana hasil tinjauan tersebut akan dilindungi dengan menggunakan *password* yang akan diinformasikan secara terpisah.

Apabila hasil dari tinjauan tersebut menyatakan bahwa aplikasi calon tertanggung atau pemohon disetujui, maka terbentuklah perjanjian *cyber insurance*. Seperti pada perjanjian asuransi lainnya, pihak tertanggung disyaratkan untuk membayar premi asuransi yang pertama sebelum polis diterbitkan dan dikirimkan kepada pihak tertanggung.

Sedangkan pada mekanisme perjanjian *cyber insurance* secara *offline*, pada dasarnya sama dengan mekanisme perjanjian *cyber insurance* secara *online*, yang membedakan hanyalah bahwa antara calon tertanggung atau pemohon dengan penanggung saling bertemu, berhadap-hadapan (*face to face*). Sehingga wujud dari kontrak yang dihasilkan berupa kontrak yang bersifat *tangible and paper based media* (nyata dan menggunakan media kertas) seperti kontrak pada umumnya, sedangkan kontrak yang dihasilkan secara online berupa kontrak digital yang bersifat *intangible and non paper based media* (tidak nyata dan tidak menggunakan media kertas).

Mengenai mekanisme terjadinya perjanjian *cyber insurance* dapat digambarkan sebagai berikut :



Berkaitan dengan saat terjadinya perjanjian asuransi terdapat permasalahan terutama berkaitan dengan masalah polis asuransi. Jika berpegang pada pasal 225 KUHD, maka dapat ditentukan bahwa semua asuransi harus dibentuk secara tertulis dengan suatu akta yang dinamakan polis. Pasal ini menunjukkan seolah-olah suatu persetujuan asuransi ada syarat mutlak berupa tulisan yang dinamakan polis.

Kitab Undang-undang Hukum Perdata, dalam beberapa pasal mengenai suatu tulisan tertentu sebagai syarat mutlak bagi beberapa persetujuan tertentu, misalnya :

- a. Pasal 147 : perjanjian perkawinan harus diadakan dengan akta notaris.
- b. Pasal 613 : persetujuan untuk mengalihkan suatu piutang (*cessie*) harus diadakan dengan akta notaris atau akta di bawah tangan.
- c. Pasal 1171 : hipotek harus dibentuk dengan akta notaris.
- d. Pasal 1682 : penghibahan (*schenking*) harus dilakukan dengan akta notaris.
- e. Pasal 1851 : persetujuan perdamaian harus diadakan secara tertulis.

Bagi persetujuan-persetujuan tersebut diatas, adalah syarat mutlak, adanya tulisan yang berbentuk tertentu. Jika tulisan seperti itu tidak ada, maka tidak ada juga persetujuan-persetujuan tersebut. Akan tetapi tidak boleh lalu kita menarik kesimpulan bahwa polis di dalam perjanjian asuransi itu merupakan suatu syarat untuk adanya perjanjian asuransi itu. Akan tetapi janganlah keterangan itu menimbulkan suatu kesan bahwa polis itu tidak lagi perlu. Polis itu tetap mempunyai arti yang besar bagi pihak tertanggung.

Sebab polis merupakan bukti yang sempurna tentang apa yang mereka perjanjikan di dalam perjanjian asuransi itu, dan tanpa polis, pembuktian akan menjadi sulit dan terbatas.¹⁶

Pada *AIG eBusiness Risk Solution*, polis bukan merupakan suatu syarat mutlak terjadinya perjanjian *cyber insurance*. Hal ini terlihat dari pencantuman *legal notice* pada form aplikasi yang menyatakan apabila polis diterbitkan, permohonan dilampirkan dan dijadikan bagian dari polis sehingga diperlukan bahwa semua pertanyaan dijawab secara detail. Sesuai dengan penjelasan diatas, form permohonan/ aplikasi yang telah diisi lengkap, dan telah melalui proses analisis keamanan dan dinyatakan disetujui merupakan saat terjadinya perjanjian *cyber insurance* dan dengan adanya kata-kata bahwa permohonan akan dilampirkan pada polis, berarti seluruh proses pembentukan perjanjian telah selesai dilakukan baru diterbitkan polisnya.

Berkaitan dengan analisis keamanan terdapat ketentuan yang dibuat oleh pihak penanggung secara sepihak untuk calon tertanggung atau pemohon yang berupa pernyataan persetujuan dari calon tertanggung atau pemohon yang isinya bahwa pemohon memahami bahwa analisis keamanan diperlukan dalam pengambilan keputusan diterima atau tidaknya permohonan asuransi tersebut. Bahwa analisis keamanan tersebut dilakukan oleh sebuah perusahaan konsultasi keamanan yang independen yang telah disetujui oleh penanggung. Bahwa biaya atas analisis keamanan tersebut ditanggung oleh pemohon. Bahwa salinan laporan hasil analisis ini akan dikirimkan kepada

¹⁶ *Ibid*, hal 58

pihak penanggung untuk tujuan pembuatan kutipan asuransi dan bahwa salinan tersebut tidak boleh diberikan kepada pihak ketiga termasuk perusahaan asuransi yang lain kecuali atas persetujuan penanggung secara tertulis. Jika pemohon melanggar ketentuan ini maka akan dikenakan sanksi denda sebesar Lima puluh ribu dollar Amerika Serikat (US\$50.000) dan penanggung dapat mengeluarkan dengan segera sebuah keputusan yang melarang segala bentuk informasi kepada pihak ketiga dan bahwa penanggung juga mempunyai hak untuk mengejar seluruh haknya dan perbaikan secara hukum atau yang setingkat berkaitan dengan pelanggaran ini.

Ketentuan ini dicantumkan dalam form permohonan/ aplikasi yang harus diisi lengkap oleh pemohon disertai dengan tanda tangan pemohon sebagai tanda persetujuan dari pemohon. Dalam fom permohonan/ aplikasi pemohon diharuskan untuk membubuhkan tanda tangannya di dua tempat yaitu di bawah ketentuan mengenai analisis keamanan dan pada akhir lembaran permohonan/ aplikasi. Tanda tangan di bawah ketentuan mengenai analisis keamanan seperti yang telah disebutkan diatas merupakan tanda persetujuan pemohon mengenai ketentuan tersebut. Sedangkan tanda tangan di akhir lembaran permohonan/ aplikasi merupakan tanda persetujuan dari pemohon untuk keseluruhan aplikasi tersebut.

Pencantuman ketentuan mengenai analisis keamanan pada form aplikasi tersebut secara tidak langsung mengandung unsur pemaksaan pada calon tertanggung untuk menyetujui ketentuan tersebut meskipun terdapat

tempat tanda tangan yang terpisah. Jika dibaca secara teliti dan seksama, isi dari ketentuan tersebut secara tersirat menyatakan bahwa analisis keamanan tersebut harus dilakukan oleh pihak pemohon atas biaya sendiri, hal ini jelas merugikan pemohon. Jika analisis keamanan tidak dilakukan maka tidak ada jaminan bahwa permohonan tersebut akan disetujui. Ketentuan mengenai analisis keamanan ini merupakan salah satu contoh klausula baku yang dibuat secara sepihak oleh pihak penanggung yang sedikit banyak merugikan pemohon atau calon tertanggung

2. Sistem Pertanggungjawaban *Cyber Insurance*

seperti yang telah disebutkan pada bab sebelumnya bahwa *Cyber Insurance* menyangkut dua tipe asuransi yaitu asuransi kerugian dan asuransi tanggung gugat pihak ketiga (*liability insurance*). Dengan begitu bentuk pertanggungjawaban yang diberikan oleh *cyber insurance*, khususnya *AIG eBusiness Risk Solution* juga terdiri dari dua bentuk yaitu :

- a. Bentuk penggantian kerugian yang besarnya ditentukan kemudian setelah peristiwa tidak pasti terjadi. Bentuk seperti ini diberlakukan pada lingkup perlindungan *Internet Media Liability Coverage*, *Internet Professional Liability*, *Network Security Liability*, *Cyber Extortion Coverage*, *Network Business Interruption*

Sedangkan besarnya ganti kerugian yang akan dibayarkan adalah sebesar kerugian yang diderita oleh tertanggung selama tidak melebihi jumlah pertanggungan selama setahun yang telah dituangkan dalam ikhtisar polis.

Berkaitan dengan bentuk ini, bentuk pertanggungjawaban dari *AIG e Business Risk Solution* tergantung pada jenis perlindungan asuransi yang dipakai oleh tertanggung. Jika tertanggung hanya memakai satu atau dua jenis perlindungan maka pihak penanggung hanya memberikan ganti rugi terhadap kerugian yang disebabkan oleh hal-hal yang berkaitan dengan jenis perlindungan tersebut, misalnya seorang tertanggung hanya memakai jenis perlindungan *Network Security Liability*, maka penggantian kerugian oleh penanggung hanya meliputi kerugian yang berkaitan dengan sekuritas jaringan kerja tertanggung. Untuk kerugian yang disebabkan oleh hal-hal lain diluar konteks tersebut, penanggung tidak bertanggung jawab.

Jika tertanggung memakai semua jenis asuransi yang tersedia, maka segala kerugian yang timbul merupakan tanggung jawab dari pihak penanggung. Bentuk pertanggungjawaban yang seperti ini pada asuransi yang bersifat konvensional sering disebut dengan istilah "*all risk*".

- b. Bentuk yang kedua adalah bentuk ganti kerugian yang besarnya sudah ditentukan sebelum terjadi peristiwa tidak pasti. Jadi disini besarnya ganti kerugian adalah tetap dan tidak dapat berubah. Bentuk seperti ini diberlakukan terhadap dua jenis perlindungan pada *AIG eBusiness Risk Solution*, yaitu *Criminal Reward Fund Coverage* dan *Crisis Communication Management Fund*. Besarnya ganti kerugian yang diberikan pada dua jenis perlindungan adalah tetap yaitu senilai US\$50.000 (lima puluh ribu dollar Amerika).

3. Cara Pengajuan Klaim

Ketika peristiwa tidak pasti terjadi terhadap obyek perlindungan asuransi maka upaya hukum yang dapat dilakukan oleh pihak tertanggung adalah mengajukan klaim kepada pihak penanggung. Dalam pengajuan sebuah klaim terdapat proses atau mekanisme pengajuan klaim yaitu sebagai berikut :¹⁷

1. Syarat-syarat Pengajuan Klaim.

Dalam pengajuan tuntutan ganti rugi, maka syarat yang paling utama yang harus dipenuhi oleh tertanggung adalah sebagai berikut :

a. Segera, sesuai waktu yang lazim, melaporkan kejadian apapun yang akan menimbulkan tanggung gugat kepada penanggung melalui telepon, telex, facimile, atau via e-mail dengan memberikan informasi sebagai berikut :

- Waktu dan tempat kejadian.
- Obyek pertanggungan yang mengalami kerugian.
- Uraian singkat mengenai kejadian.
- Perkiraan kerugian yang diderita.

b. Apabila diperlukan, tertanggung harus mengizinkan penanggung dan/ atau Klaim Surveyor/ Adjuster yang ditunjuk untuk melihat secara langsung ke lokasi kejadian untuk melakukan penelitian.

¹⁷ *Data berasal Dari AIG eBusiness Risk Solution*

3. Cara Pengajuan Klaim

Ketika peristiwa tidak pasti terjadi terhadap obyek perlindungan asuransi maka upaya hukum yang dapat dilakukan oleh pihak tertanggung adalah mengajukan klaim kepada pihak penanggung. Dalam pengajuan sebuah klaim terdapat proses atau mekanisme pengajuan klaim yaitu sebagai berikut :¹⁷

1. Syarat-syarat Pengajuan Klaim.

Dalam pengajuan tuntutan ganti rugi, maka syarat yang paling utama yang harus dipenuhi oleh tertanggung adalah sebagai berikut :

- a. Segera, sesuai waktu yang lazim, melaporkan kejadian apapun yang akan menimbulkan tanggung gugat kepada penanggung melalui telepon, telex, facimile, atau via e-mail dengan memberikan informasi sebagai berikut :
 - Waktu dan tempat kejadian.
 - Obyek pertanggungan yang mengalami kerugian.
 - Uraian singkat mengenai kejadian.
 - Perkiraan kerugian yang diderita.
- b. Apabila diperlukan, tertanggung harus mengijinkan penanggung dan/atau Klaim Surveyor/ Adjuster yang ditunjuk untuk melihat secara langsung ke lokasi kejadian untuk melakukan penelitian.

¹⁷ *Data berasal Dari AIG eBusiness Risk Solution*

c. Melengkapi informasi dan dokumen yang diperlukan dalam rangka menentukan atau membuktikan tanggung gugat. Adapun dokumen-dokumen yang diperlukan sebagai syarat pengajuan klaim *cyber insurance* adalah :

- Polis asli
- Foto copy polis
- Surat Tuntutan Pihak Ketiga
- Laporan Kerugian Sementara

2. Penelitian Polis

Setelah menerima adanya kerugian dari tertanggung, maka penanggung melakukan penelitian mengenai validitas polis, yaitu :

- a. Ada/ tidaknya kepentingan tertanggung atas obyek yang mengalami kerugian.
- b. Apakah kerusakan yang menyebabkan kerugian terjadi dalam jangka waktu pertanggungan.
- c. Apakah premi telah dilunasi/ dibayar.

3. Penelitian Klaim

Apabila validitas polis terkonfirmasi, maka penanggung melakukan pemeriksaan/penelitian di lapangan (*survey on spot*) untuk mengetahui :

- a. Penyebab terjadinya kerugian/kerusakan
- b. Tempat terjadinya kerugian/kerusakan
- c. Jumlah kerugian yang dialami (taksiran)

- d. Usaha bertanggung untuk menyelamatkan dan menjaga obyek pertanggungan pada saat terjadi kerugian/ kerusakan.

4. Penyampaian

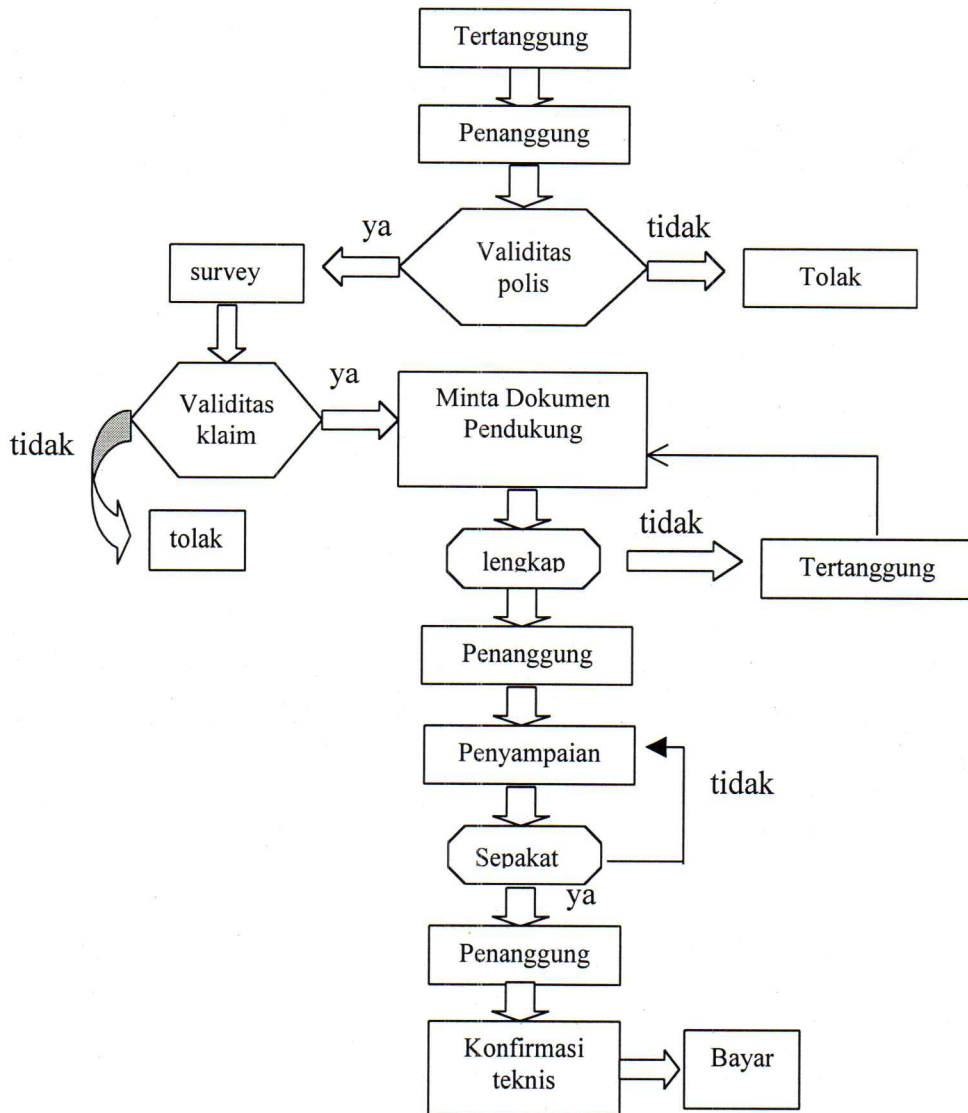
Dari proses penanganan klaim oleh penanggung sendiri ataupun Loss Adjuster, akan diketahui validitas klaim dan dalam hal klaim :

- a. Valid, maka penanggung akan memberitahukan tertanggung jumlah ganti rugi yang disetujui (menjadi tanggung jawab penanggung).
- b. Invalid, maka penanggung akan memberitahukan penolakan klaim tersebut disertai alasannya.

5. Penyelesaian

Setelah dicapai kesepakatan dengan tertanggung dalam hal pada penelitian klaim dinyatakan valid maka penanggung mempersiapkan pembayaran ganti rugi tersebut dalam waktu 4 (empat) minggu setelah tercapainya kesepakatan.

Mekanisme pengajuan klaim ini dapat digambarkan dalam bagan sebagai berikut :



BAB IV

PENUTUP

Rahayu

BAB IV

PENUTUP

1. Kesimpulan

kesimpulan yang dapat diambil dari keseluruhan isi dari skripsi ini adalah:

1. *Cyber Insurance* adalah merupakan bentuk khusus dari asuransi yang menyediakan baik layanan produk asuransi maupun manajemen resiko untuk melawan berbagai macam jenis resiko digital. *Cyber Insurance* juga merupakan suatu bentuk produk asuransi yang menutup resiko-resiko yang terkait dengan sistem keamanan jaringan komputer. *Cyber Insurance* yang mencakup lingkup komputasi dibagi menjadi dua tipe, yaitu : tipe pertama berkaitan dengan *first party* atau *cyber property* yang meliputi penutupan resiko kerugian akibat tindak kejahatan, pencurian, perusakan perangkat lunak (*software*) maupun *database*, rehabilitasi data, pemerasan (*extortion*), dan business interruption. Sedangkan tipe kedua adalah berkaitan dengan *third party* (pihak ketiga) atau sering disebut dengan *cyber liability* yang meliputi pencemaran nama baik yang terkait dengan materi suatu situs internet termasuk juga pelanggaran hak cipta.
2. Perjanjian *cyber insurance* dapat terjadi dalam dua cara yaitu dengan cara online dan dengan cara offline. Pada prinsipnya mekanisme antara kedua cara tersebut sama, yang membedakan hanyalah kontak para pihak dengan hasil dari perjanjian tersebut. Pada cara online para pihak tidak bertemu langsung

dan hasil dari perjanjiannya adalah berupa perjanjian yang berwujud *intangible and non paper based medium* (tidak nyata dan tidak menggunakan media kertas). Sedangkan pada cara *offline*, para pihak bertemu *langsung (face to face)* dan hasil dari perwujudannya adalah berwujud *tangible and paper based medium* (nyata dan menggunakan media kertas). Bentuk pertanggungjawaban dari *cyber insurance* ada dua bentuk yaitu :

- a. Bentuk penggantian kerugian yang besarnya ditentukan kemudian setelah peristiwa tidak pasti terjadi, dan
- b. Bentuk penggantian kerugian yang besarnya sudah ditentukan sebelum terjadi peristiwa tidak pasti. Pada bentuk pertanggungjawaban yang seperti ini besarnya ganti kerugian adalah tetap.

2. Saran

Saran yang dapat diberikan oleh penulis berkaitan dengan isi dari skripsi ini adalah bahwa berkaitan dengan masalah bahwa *cyber insurance* belum menjadi suatu hal yang fenomenal di Indonesia, ada baiknya apabila diberikan suatu pengetahuan mengenai *cyber insurance* sehingga kelak Indonesia dalam menghadapi perkembangan teknologi yang makin pesat dewasa ini mampu bersaing dengan negara-negara lain di dunia internasional. Karena pada perkembangannya perdagangan sudah dalam lingkup internasional yang berarti makin besar pula resiko yang mengancam. Jika negara Indonesia tidak diberikan pengetahuan mengenai *cyber insurance* yang merupakan jenis asuransi yang menutup resiko yang timbul dalam perdagangan internasional maka Indonesia

akan kalah dalam persaingan di dunia internasional. Kemudian saran lain yang dapat diberikan oleh penulis adalah perlunya suatu peraturan hukum tertulis yang mengatur khusus mengenai *cyber insurance* sebagai suatu ketentuan umum yang dapat juga sebagai standardisasi bagi perusahaan asuransi di Indonesia yang akan bergerak pada lingkup *cyber insurance* sehingga ada kepastian hukum bagi masyarakat.

DAFTAR BACAAN

Rahayu

DAFTAR BACAAN

BUKU

Djoko Prakoso, *"Hukum Asuransi Indonesia"*, PT. Rineka Cipta, Jakarta, Cetakan Keempat, Oktober 2000.

Emmy Pangaribuan Simanjuntak, *"Hukum Pertanggungan Dan Perkembangannya"*, Seksi Hukum Dagang Fakultas Hukum Universitas Gajah Mada Yogyakarta, 1990

ARTIKEL

Dian Siska Herliana, *"Peluang Baru Industri Cyber Insurance Dalam Era Teknologi Informasi"*, Lembaga kajian Hukum Dan Teknologi Fakultas Hukum Universitas Indonesia, Tayang 31 Juli 2004

<http://www.lkht.net/e-Commerce/artikel>

Sagalow, Ty, *Chief Operating Officer And Executive VP of new York City based AIG eBusiness Risk Solution*, *"Cyber Insurance Definition, Ask The Expert"*, Posted On January 27, 2003

<http://www2.cio.com/ask/expert/2003/questions/question/577.html>

Kumpulan Data-Data Dari AIG eBusiness Risk Solution.

<http://www.AIGnetAdvantageSuite.com>

MAKALAH – KARYA TULIS

Kurniawan Nugroho, *"Analisa Risiko Dan Merancang Asuransi Untuk Risiko Digital"*, Karya Tulis, Program Studi Asuransi Kerugian, Akademi Asuransi Trisakti Jakarta, 2000

Naniek Endang Wrediningsih, *"Kebebasan Berkontrak Sebagai Asas Hukum Perjanjian"*, Makalah Penelitian Hukum Kontrak Fakultas Hukum Universitas Airlangga Surabaya, 1992

PERATURAN PERUNDANG-UNDANGAN

R. Subekti dan R. Tjitrosudibio, "*Kitab Undang-Undang Hukum Perdata*", PT. Pradnya Paramita, Jakarta, Cetakan Ketigapuluhsatu, 2001.

R Subekti dan R. Tjitrosudibio, "*Kitab Undang-Undang Hukum Dagang Dan Undang-Undang Kepailitan*", PT. Pradnya Paramita, Jakarta, Cetakan Ke-27, 2002.

LAMPIRAN

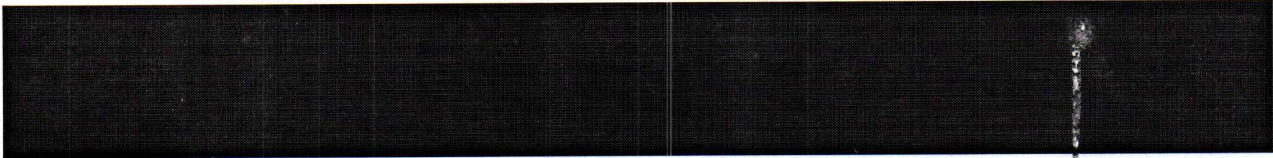
Rahayu



AMERICAN INTERNATIONAL COMPANIES®

Name of Insurance Company
To Which Application is Made:

(herein called the Company)



AIG netAdvantagesm Suite

NOTICE: THE POLICY PROVIDES THAT THE LIMITS OF LIABILITY AVAILABLE TO PAY JUDGMENTS OR SETTLEMENTS SHALL BE REDUCED BY AMOUNTS INCURRED FOR LEGAL DEFENSE. FURTHER NOTE THAT AMOUNTS INCURRED FOR LEGAL DEFENSE SHALL BE APPLIED AGAINST THE DEDUCTIBLE AMOUNT.

I. COMPANY INFORMATION & BROKER INFORMATION

COMPANY INFORMATION:

Full Name of Applicant				
Applicant Type	☐ Individual	☐ Corporation	☐ Partnership	☐ Other
(if "other")				
Address				
Address 2				
City				
State/Providence				
Zip/Postal Code				
Web site Home Page Address(es), including subsidiaries (Optional)				
Mailing Address (if different)				
Chief Information Officer (Optional)				
Date Established				
Place of Incorporation				
No. of Employees				
Descriptions of Business				
Names of Subsidiaries (or attach list) (Optional)				

II. YOUR BUSINESS ACTIVITIES ON THE INTERNET/NETWORK

- ☐ 1) **ACCESS:** Sending and receiving email, transferring files, browsing the Internet.
- ☐ 2) **PRESENCE:** Providing information or advertising over the Internet through a web server or extranet.
- ☐ 3) **PRODUCTION ACCESS:** Integration of business information or internal processes with a web site.
- ☐ 4) **ELECTRONIC COMMERCE:** The buying and selling of products, services or information over the internet between a buyer and seller. Electronic Commerce can also include three-party business transactions, typically between an internet user, a merchant, and a bank, involving buying or selling valuable goods, products, or services or the transmission of sensitive financial information to exchange. Electronic Commerce also includes your permitting of advertisements on your web site by others for a fee, regardless of any other internet activities you may conduct.
- ☐ 5) **COLLABORATION:** Virtual Private Network (VPN) or an "extranet" activities. This could also include the provision of computer system resources to a third party.
- ☐ 6) **HOSTING:** providing hosting services to third parties.
- ☐ 7) **DIGITAL CERTIFICATES:** Installation, management, or maintenance of any digital certificate
- ☐ 8) **ELECTRONIC FUNDS TRANSFER**
- ☐ 9) **OTHER:** _____
- ☐ 10) **NEXT YEAR:** The following business activities planned for next year are different than the ones checked above? _____

III. BUSINESS REVENUES

1. Please provide your total revenues:

Past Accounting Year: \$

Projected Current Year: \$

2. Please provide your total e-business revenues (if applicable):

Past Accounting Year: \$

Projected Current Year: \$

3. Please provide the number of unique visitors per day:

IV. UNDERWRITING QUESTIONS

A. Media

All applicants must complete this section.

1. Is there a review process in place to screen content (including domain names) of the web site? ☐ Yes ☐ No

 If "yes", is the content of your web site reviewed by a qualified attorney? ☐ Yes ☐ No

 Does the review include looking for any or all of the following offenses: Libel, Slander, Trademark Infringement, Copyright Infringement, Invasion of Privacy, Inaccurate Information or Trade Secrets? ☐ All ☐ Some ☐ None
2. Do you have an established procedure for deleting, editing and removing controversial, offensive (i.e. libelous) or infringing material (i.e. copyright, trademark) from your web site or Internet service? ☐ Yes ☐ No
3. Do you use material of others (such as text, videos, music, etc.) in any electronic form, including on your web site or in any electronic database? ☐ Yes ☐ No

 If "yes", in each case, have you:
 Obtained written clearance to use this material which *specifically* permits use in electronic forms including your web site? ☐ Yes ☐ No

 Scanned the material for viruses? ☐ Yes ☐ No
4. Do your agreements with the developer of your web site and any consultants providing material for your web site provide that you own the intellectual property rights to the content and business methods incorporated into the web site? ☐ Yes ☐ No

If you are applying only for media liability coverage proceed to Section V.

B. Professional Services

If you are applying for professional liability coverage, answer the following questions.

1. Please provide a division of your Firm's gross fees as follows:

Respecting clients domiciled in:	US/Canada	UK	Europe excluding UK	elsewhere
Web site design				
Web site management				
Search engines				
Software developers (pre-package)				
Internet access provider (no content)				
Web directories				
Web site hosting				
Internet access provider (with content)				
Software developers				
Encryption software				
Internet access provider (content, e-mail, BBS, Chat Room)				
Firewall software				
Security consultants				
Other (please provide details in space below)				

Please provide a listing of the Firm's business between the following markets by percentage:

Market Sectors	Current Year	Next 12 Months
Government entities	%	%
Financial Institutions	%	%
Health care/Medical	%	%
Commercial entities	%	%
Other (please specify)	%	%

2. Do you provide original content? ☐ Yes ☐ No
3. Do you have subscribers for your website? ☐ Yes ☐ No
- How many subscribers do you have capacity for?
- Do you have adequate capacity to accommodate the number of subscribers to your service? ☐ Yes ☐ No ☐ Unknown
4. Do you offer bulletin board/chat room services at your web site? ☐ Yes ☐ No
- If "yes", who manages bulletin board/chat room? ☐ We Do ☐ Subcontractor
- If a subcontractor, do you require "hold harmless" agreements for liabilities arising out of the bulletin board/chat room? ☐ Yes ☐ No
- Can you edit and remove any content or posting at your sole discretion and does the user agreement allow you to do so? ☐ Yes ☐ No
- If "yes", how often do you review the content or postings? ☐ Daily ☐ Weekly ☐ Monthly ☐
- Do you have an agreement which users of your bulletin board/chat Room must accept as a condition of using the bulletin board/chat room? ☐ Yes ☐ No
5. Do you review, edit or censor the material contained on your web site or Internet service in any way? ☐ Yes ☐ No
- If "yes", how often do you review, edit or censor your web site or Internet service? ☐ Daily ☐ Weekly ☐ Monthly ☐
6. Do you make representations that you review, edit or censor the material contained on your web site or Internet service in any way? ☐ Yes ☐ No
7. How often do you update the content of your web site or Internet service? ☐ Daily ☐ Weekly ☐ Monthly

☐]

8. Do you provide content for a web site on the behalf of a client? ☐] Yes ☐ No

If "yes", does the client approve the content before it is published on the Internet? ☐] Yes ☐ No

9. Do you limit your liability in your contracts for any breach of your professional services? ☐] Yes ☐ No

If "yes", indicate what they are:

- ☐] No liability
☐] Cap on liability as a multiple of fees
☐] Other

10. Do you make any guarantees or warranties in your contracts regarding your professional services? ☐] Yes ☐ No

If "yes", indicate what they are:

11. Does your website contain materials designed to be downloaded (such as software, plug-ins, etc.)? ☐] Yes ☐ No

If "yes", is that material scanned for viruses? ☐] Yes ☐ No

12. Does your website or internet service sell any products or services over the internet? ☐] Yes ☐ No

Are credit card transactions conducted on your website or internet service? ☐] Yes ☐ No

13. Would you like professional liability coverage to include claims arising out of failures to a network? (if yes, please complete questions #1 through #15 of Section C. below) ☐] Yes ☐ No

C. Network Security

1. Are firewalls used to prevent unauthorized access connections from external networks and computer systems to internal networks?

☐ Not Implemented ☐ Partially Implemented ☐ Fully Implemented

If implemented, what specific firewall protections do you use?

2. Are remote users authenticated before being allowed to connect to internal networks and computer systems?

☐ Not Implemented ☐ Partially Implemented ☐ Fully Implemented

If implemented, is authentication: ☐ Passwords ☐ Other:

3. Are firewall, anti-virus and intrusion detection procedures and protections used on desktops and mission critical servers?

☐ Not Implemented ☐ Partially Implemented ☐ Fully Implemented

If in place, what specific anti-virus safeguards and programs do you use?

If implemented, how often are the procedures updated?

☐ Daily ☐ Weekly ☐ Monthly ☐

4. Are backup and recovery procedures documented and implemented for:

(a) all mission critical systems? ☐ Yes ☐ No

(b) your Web site? ☐ Yes ☐ No

(c) data and information assets? ☐ Yes ☐ No

If "Yes" for each of the above, how frequently do you backup?

☐ Daily ☐ Weekly ☐ Monthly ☐

Please indicate name of the company providing backup services and provide a copy of the applicable contract/service level agreement.

5. Are special privileges restricted to primary and backup system administration personnel?

☐ Not Implemented ☐ Partially Implemented ☐ Fully Implemented

6. Are continuity plans in place for all mission critical business processes?

☐ Not Implemented ☐ Partially Implemented ☐ Fully Implemented

How often are such plans revised?

What is the maximum duration of outage anticipated based upon the business continuity plan (in hours)?

Please indicate name of the company providing business continuity services and provide a copy of the applicable contract/service level agreement.

7. Are your network and computer systems monitored?

☐ Not Implemented ☐ Partially Implemented ☐ Fully Implemented

If monitoring is handled internally, what monitoring tools do you use?

If an external vendor handles monitoring, please indicate the name of the company providing any monitoring services and provide a copy of the applicable contract/service level agreement.

8. Do you have an internal network and internet use security policy?

☐ Not Implemented ☐ Partially Implemented ☐ Fully Implemented

If so, please attach. If not in writing, check here: ☐

Do you have an Internet privacy policy?

☐ Not Implemented ☐ Partially Implemented ☐ Fully Implemented

Please attach. If not in writing, check here: ☐

9. What authentication processes or applications do you utilize with respect to your e-business?

10. Do you outsource a critical part of your Internet, network or computer system to others? ☐ Yes ☐ No

If "yes", choose all that apply, indicate the outsourced company and provide a copy of the applicable contract/service level agreements:

- ☐ Hosting Facility:
☐ Firewall Maintenance:
☐ Managed Security:
 (specify type & scope)
☐ Data Storage:

- ☐ Server Maintenance:
☐ Intrusion Detection:
☐ Applications/Software:
☐ Other:

11. Do you receive CERT or SAIC Advisories, or any similar notification? ☐ Yes ☐ No

If "yes", indicate name of the organization providing such services:

12. Do you give written warranties or indemnities regarding your Internet, network and systems operations? ☐ Yes ☐ No

If "yes", please describe such warranties or indemnities as an attachment herewith.

13. Do you receive warranties or indemnities regarding your Internet, network and computer operations? ☐ Yes ☐ No

If "yes", please describe such warranties or indemnities as an attachment herewith.

14. Has there been any change in ownership or senior management (including Chief Information Officer) in the past year? ☐ Yes ☐ No

15. Do you have a full time, dedicated Director of Information Security or its equivalent? ☐ Yes ☐ No

If you are only applying for Professional Liability coverage, STOP HERE AND PROCEED TO SECTION V. If you are applying for complete network security liability coverage CONTINUE TO END OF SECTION.

16. Do you have procedure in place to identify and detect network security weaknesses? ☐ Yes ☐ No

17. Are credit card transactions conducted on your web site or Internet service? ☐ Yes ☐ No

18. How would your revenues be impacted by a breach of security sustained by a dependent business? This would include businesses that are providing Internet, network or computer systems for your operations including hosting your Internet Web site.

☐ Substantially ☐ Moderately ☐ Minimally ☐ No Impact

19. What property of others are you responsible for that relate to your Internet or computer system?
- ☐ Money ☐ Securities ☐ Other Tangible Property ☐ Credit Card Information
☐ Information assets
20. Do you perform background checks, including credit & criminal history, on new employees, independent consultants/vendors? ☐ Yes ☐ No
21. Are all employees provided with a copy of your security policy? ☐ Yes ☐ No
- If "yes", are all employees required to provide written confirmation acknowledging they read and understood the contents of the security manual? ☐ Yes ☐ No
- If "yes", are all employees required to sign a statement confirming that failure to follow procedures set forth in your security policy manual will result in disciplinary and including termination? ☐ Yes ☐ No
22. What is the total number of independent consultant employee & contractor employee performing Internet, network and computer system services for your organization?
23. Do you require the outside consultants/contractors to maintain fidelity bond insurance? ☐ Yes ☐ No
24. With respect to the following potentially sensitive areas of the company: Finance & Accounting (such as Payables, Receivables, Collection, Payroll or Cash Management), Engineering, Research & Development, Programming, Security & Systems administration:
- How many employees (including leased workers) are employed there or otherwise have access?
- Do any non-employees (such as those identified in questions 10 and 24 above) have access? If "yes" how many? ☐ Yes ☐ No
- If "yes", is the access for these non-employees restricted in any way? ☐ Yes ☐ No
- How often are these accounts reconciled and by whom?
- ☐ Daily
☐ Weekly
☐ Monthly
☐

By:

25. Please identify your web based applications:

Application:	Vendor	Purpose
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		

Were any of the applications listed above designed by or for you?

☐ Yes ☐ No

If “yes,” have these applications been tested for security vulnerabilities?

☐ Yes ☐ No

If “yes,” was any vulnerability uncovered?

☐ Yes ☐ No

If “yes,” please describe the vulnerability and actions taken:

26.

Have you implemented any of the following security solutions?

Data Integrity Programs	☐ Yes ☐ No	Product:
Access Control	☐ Yes ☐ No	Product:
Virtual Private Networking	☐ Yes ☐ No	Product:
File Encryption Software	☐ Yes ☐ No	Product:
Security Management Software	☐ Yes ☐ No	Product:
Public Key Infrastructure	☐ Yes ☐ No	Product:
Automated Content Inspection Software	☐ Yes ☐ No	Product:
Vulnerability Assessment Software	☐ Yes ☐ No	Product:
Other:	☐ Yes ☐ No	Product:

27.

With respect to electronic funds transfer (if applicable):

What is the average/maximum number of transfers made daily?

What is the average/maximum dollar value of the transfers made daily?

Do you maintain a current manual covering procedures for the funds transfer function? ☐ Yes ☐ No

Is written verification of the transfer made by the financial institution within 24 hours of the transfer? ☐ Yes ☐ No

Is the verification sent to a department and person other than the department executed the transfer? ☐ Yes ☐ No

Is reconciliation of the account from which the transfer was made completed on the same day the transfer confirmation is received? ☐ Yes ☐ No

V. OTHER INSURANCE

Have you purchased any of the following insurance policies? If yes, provide insurer, limits, retentions or deductibles, and policy period:

Coverage	Insurer	Expiration Date	Limits	Deductible
(a) General Liability WITH Advertising Injury/Personal Injury				
(b) General Liability WITHOUT Advertising Injury/Personal Injury for Internet Activities				
(c) Errors & Omissions				
(d) Property & Business Interruption (with EDP Coverage)				
(e) Property & Business Interruption (without EDP Coverage)				
(f) Employee Dishonesty/ Crime (with Computer Fraud Extension)				
(g) Employee Dishonesty/ Crime (without Computer Fraud Extension)				
(h) Directors & Officers				
(i) Other				

Do you wish to apply for Excess/Difference-in-Conditions coverage for any of the above?
If yes, state which coverages (A-I):

☐ A ☐ B ☐ C ☐ D ☐ E ☐ F ☐ G ☐ H ☐ I

VI. DESIRED COVERAGES

AIG netAdvantage Applicants:	Complete Section (a) only
AIG netAdvantage Professional Applicants:	Complete Sections (a) & (b) only
AIG netAdvantage Liability Applicants:	Complete Sections (a), (b), (c) & (d) only
AIG netAdvantage Security Applicants:	Complete Sections (a), (c), (d) & (e) only
AIG netAdvantage Complete Applicants:	Complete Sections (a), (b), (c), (d) & (e)

Coverage	Limits of Liability (\$)	Retentions
(a) Media Liability	\$_____ per claim \$_____ aggregate	\$_____ per claim
(b) Professional Services Liability	\$_____ per claim \$_____ aggregate	\$_____ per claim
(c) Security Liability	\$_____ per claim \$_____ aggregate	\$_____ per claim
(d) Cyber-Extortion	\$_____ per occurrence \$_____ aggregate	\$_____ per extortion claim
(e) Asset & Income Protection	\$_____ per occurrence \$_____ aggregate	\$_____ per occurrence _____ waiting period (hrs) (12, 24, 36, 48)

Policy Aggregate (for all coverage under the policy):

\$

Proposed Effective Date

Proposed Retroactive Date (Coverage B & C)

VII. CLAIMS/INCIDENTS/LOSS HISTORY

1. Has any insurance similar to the kind found under this policy, or your property GL D&O policy, ever been declined or cancelled during the past three years? (not applicable in MO)

☐ Yes ☐ No

If "yes":

Name of Policy:	
Insurer:	
Date Declined or Cancelled:	

2. Are you aware of any pending or prior incident, circumstance, event or litigation during the last three years concerning the content of your web site relevant to intellectual property content or advertising offenses that may be reasonably expected to give rise to a claim or would have given rise to a claim if similar insurance was in force for coverage or benefits provided by this insurance?

☐ Yes ☐ No

If "yes":

Loss doesn't exceed:	
Date:	
Litigation involved?	☐ Yes ☐ No
This has been the only incident?	☐ Yes ☐ No
Have steps been taken to prevent this type of incident from occurring again?	☐ Yes ☐ No

3. During the past 3 years, have you ever received a complaint concerning:

Professional liability:	☐ Yes ☐ No
If "yes", loss doesn't exceed:	
Date:	
Litigation involved?	☐ Yes ☐ No
This has been the only incident?	☐ Yes ☐ No
Have steps been taken to prevent this type of incident from occurring again?	☐ Yes ☐ No
Security of network/website:	☐ Yes ☐ No
If "yes", loss doesn't exceed:	
Date:	
Litigation involved?	☐ Yes ☐ No
This has been the only incident?	☐ Yes ☐ No
Have steps been taken to prevent this type of incident from occurring again?	☐ Yes ☐ No

During the past three years, have you suffered any loss under a Commercial Crime or Dishonesty bond/policy or computer crime policy? ☐ Yes ☐ No

If "yes",

Loss doesn't exceed:	
Date:	
Litigation involved?	☐ Yes ☐ No
This has been the only incident?	☐ Yes ☐ No
Have steps been taken to prevent this type of incident from occurring again?	☐ Yes ☐ No

4. During the past three years, have you experienced an incident involving loss of service except for planned maintenance of computer systems, exceeding four hours? ☐ Yes ☐ No

If "yes",

Cost to restore service (USD):	
Amount of lost revenue (USD):	
Theft/damage to info. assets (USD):	
Date:	
Length of time out of service:	
Litigation involved:	☐ Yes ☐ No
Has this been the only incident?	☐ Yes ☐ No
Have steps been taken to prevent this type of incident from occurring again?	☐ Yes ☐ No

5. During the past 3 years, have you had any other breaches of security causing damage to your existing security systems in excess of \$25,000? ☐ Yes ☐ No

If "yes",

Loss doesn't exceed:	
Date:	
Litigation:	☐ Yes ☐ No
This has been the only incident?	☐ Yes ☐ No
Have steps been taken to prevent this type of incident from occurring again?	☐ Yes ☐ No

6. Is a security incident log kept and reviewed? ☐ Yes ☐ No

VIII. AUTHORIZATION FOR SECURITY ANALYSIS, PAYMENT AND RELEASE OF LIABILITY

I, the applicant, understand that a security analysis may be required to quote this insurance. An independent security consulting firm approved by the insurer will perform this security risk survey or electronic remote security scan. If such is required, either the consulting firm or the insurer will advise the cost for such security analysis. SUBMISSION OF THIS APPLICATION IS NOT AUTHORIZATION TO PERFORM THE SECURITY ANALYSIS. HOWEVER, I UNDERSTAND THAT UPON BEING ADVISED OF THE COST OF THE SECURITY ANALYSIS, IF I AUTHORIZE THE CONDUCTING OF THE ANALYSIS, THAT A COPY OF THE REPORT WILL BE SENT TO THE INSURER FOR THE PURPOSE OF DEVELOPING AN INSURANCE QUOTATION.

Further, I understand and agree that in consideration for the insurer providing access to the consulting firm for the purposes of the security analysis, the applicant shall not provide a copy of the analysis to any other person or entity, including specifically other insurance entities, without the insurer's prior written consent. Applicant further acknowledges that unauthorized disclosure or use of such information to third parties (including but not limited to other insurance entities) would cause irreparable harm and significant injury to the Insurer, the degree of which may be difficult to ascertain and accordingly the Applicant has agreed to an liquidated damage amount in cases of intentional violations of this agreement of Fifty thousand United States dollars (\$50,000). Accordingly, Applicant agrees that the Insurer will have the right to obtain an immediate injunction enjoining any such disclosure and that the Insurer also has the right to pursue any and all other rights and remedies available at law or in equity for such a breach. A confidentiality

agreement can be executed between the insurer and the applicant upon request. I also understand and acknowledge that the applicant is financially responsible to pay, and hereby agrees to pay, for the security analysis. Execution of this application together with any subsequent authorization constitutes an agreement between the applicant and the security consulting firm to pay the security consulting firm for the analysis. A list of approved independent security consulting firms can be obtained from the insurer.

I, the applicant, agree that the insurer is not responsible for any loss or damage howsoever caused whether direct or indirect which may arise as a result of the provision of services to the applicant or to any of the applicant's related entities by such independent security consulting firm or any representative, agent, employee or contractor of such independent security consulting firm, including the performance of any electronic remote security scan, risk assessment survey, security workshop or related service, and you agree to indemnify and hold the insurer harmless in respect of any such loss or damage. Further, the insurer does not warrant the effectiveness or accuracy of any such security analysis.

APPLICANT'S SIGNATURE: _____

In order for us to efficiently process your application, please attach the following to the signed application:

- | | | |
|--|-----------------------------------|---------------------------------------|
| • Most recent audited financial statement | ☐ Attached | ☐ Not Attached |
| • Descriptive advertising materials regarding your business | ☐ Attached | ☐ Not Attached |
| • A copy of a standard service contract or a recent contract issued | ☐ Attached | ☐ Not Attached |
| • If the company has been established for three years or less, please provide resumes of senior professional staff | ☐ Attached | ☐ Not Attached |

IX. LEGAL NOTICES AND SIGNATURE

IF A POLICY IS ISSUED, THE APPLICATION IS ATTACHED TO AND MADE PART OF THE POLICY SO IT IS NECESSARY THAT ALL QUESTIONS BE ANSWERED IN DETAIL.

PLEASE READ THE FOLLOWING STATEMENT CAREFULLY AND SIGN BELOW WHERE INDICATED. IF A POLICY IS ISSUED, THIS SIGNED STATEMENT WILL BE ATTACHED TO THE POLICY.

The insured hereby acknowledges that he/she/it is aware that the limit of liability contained in this policy shall be reduced, and may be completely exhausted, by the costs of legal defense and, in such event, the Company shall not be liable for the costs of legal defense or for the amount of any judgment or settlement to the extent that such exceeds the limit of liability of this policy.

The insured hereby further acknowledges that he/she/it is aware that legal defense costs that are incurred shall be applied against the deductible amount.

THE UNDERSIGNED DECLARES THAT THE STATEMENTS SET FORTH HEREIN ARE TRUE. THE UNDERSIGNED AGREES THAT IF THE INFORMATION SUPPLIED ON THIS APPLICATION CHANGES BETWEEN THE DATE OF THIS APPLICATION AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE (UNDERSIGNED) WILL IMMEDIATELY NOTIFY THE INSURANCE COMPANY OF SUCH CHANGES, AND THE COMPANY MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS AND/OR AUTHORIZATION OR AGREEMENT TO BIND INSURANCE.

NOTICE: IN SOME STATES, ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY MATERIALLY FALSE INFORMATION, OR CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME.

NOTICE TO ARKANSAS APPLICANTS: "ANY PERSON WHO KNOWINGLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT, OR KNOWINGLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO FINES AND CONFINEMENT IN PRISON."

NOTICE TO COLORADO APPLICANTS: "IT IS UNLAWFUL TO KNOWINGLY PROVIDE FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO AN INSURANCE COMPANY FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES, DENIAL OF INSURANCE, AND CIVIL DAMAGES. ANY INSURANCE COMPANY OR AGENT OF AN INSURANCE COMPANY WHO KNOWINGLY PROVIDES FALSE, INCOMPLETE, OR MISLEADING FACTS OR INFORMATION TO A POLICYHOLDER OR CLAIMANT FOR THE PURPOSE OF DEFRAUDING OR ATTEMPTING TO DEFRAUD THE POLICYHOLDER OR CLAIMANT WITH REGARD TO A SETTLEMENT OR AWARD PAYABLE FROM INSURANCE PROCEEDS SHALL BE REPORTED TO THE COLORADO DIVISION OF INSURANCE WITHIN THE DEPARTMENT OF REGULATORY AUTHORITIES."

NOTICE TO FLORIDA APPLICANTS: "ANY PERSON WHO KNOWINGLY AND WITH INTENT TO INJURE, DEFRAUD, OR DECEIVE ANY INSURER FILES A STATEMENT OF CLAIM OR AN APPLICATION CONTAINING ANY FALSE, INCOMPLETE OR MISLEADING INFORMATION IS GUILTY OF A FELONY IN THE THIRD DEGREE."

NOTICE TO KENTUCKY APPLICANTS: "ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY MATERIALLY FALSE INFORMATION, OR CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME."

NOTICE TO MAINE APPLICANTS: "IT IS A CRIME TO KNOWINGLY PROVIDE FALSE, INCOMPLETE OR MISLEADING INFORMATION TO AN INSURANCE COMPANY FOR

THE PURPOSE OF DEFRAUDING THE COMPANY. PENALTIES MAY INCLUDE IMPRISONMENT, FINES OR A DENIAL OF INSURANCE BENEFITS.”

NOTICE TO NEW JERSEY APPLICANTS: “ANY PERSON WHO INCLUDES ANY FALSE OR MISLEADING INFORMATION ON AN APPLICATION FOR AN INSURANCE POLICY IS SUBJECT TO CRIMINAL AND CIVIL PENALTIES.”

NOTICE TO NEW MEXICO APPLICANTS: “ANY PERSON WHO KNOWINGLY PRESENTS A FALSE OR FRAUDULENT CLAIM FOR PAYMENT OF A LOSS OR BENEFIT OR KNOWINGLY PRESENTS FALSE INFORMATION IN AN APPLICATION FOR INSURANCE IS GUILTY OF A CRIME AND MAY BE SUBJECT TO CIVIL FINES AND CRIMINAL PENALTIES.”

NOTICE TO NEW YORK APPLICANTS: “ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE OR STATEMENT OF CLAIM CONTAINING ANY MATERIALLY FALSE INFORMATION, CONCEALS FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME, AND SHALL ALSO BE SUBJECT TO A CIVIL PENALTY NOT TO EXCEED FIVE THOUSAND DOLLARS AND THE STATED VALUE OF THE CLAIM FOR EACH SUCH VIOLATION.”

NOTICE TO OHIO APPLICANTS: “ANY PERSON WHO, WITH INTENT TO DEFRAUD OR KNOWING THAT HE IS FACILITATING A FRAUD AGAINST AN INSURER, SUBMITS AN APPLICATION OR FILES A CLAIM CONTAINING A FALSE OR DECEPTIVE STATEMENT IS GUILTY OF INSURANCE FRAUD.”

NOTICE TO PENNSYLVANIA APPLICANTS: “ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION OR CLAIM CONTAINING ANY FALSE INCOMPLETE OR MISLEADING INFORMATION SHALL UPON CONVICTION BE SUBJECT TO IMPRISONMENT FOR UP TO SEVEN YEARS AND PAYMENT OF A FINE OF UP TO \$15,000.”

APPLICANT’S SIGNATURE: _____

TITLE: _____

DATE: _____

BROKER: _____

ADDRESS: _____

Information Security Self Assessment

Please complete the following informational questions before filling out the assessment. Please note that all fields are required. When you have completed the assessment, please save as a Microsoft Word file and e-mail to: netAdvantageAssessment@aig.com Your assessment will be reviewed by an AIG IT-Security analyst, and you will receive the results of your assessment via return e-mail. The results will be password protected and the password will be communicated separately via email.

Primary Contact Information	
Primary Contact First Name	
Primary Contact Last Name	
Email Address	
Job Function	Other (If "Other" please fill in:)
Company	
Industry	Other (If "Other" please fill in:)
Address	
Address 2	
City	
State/Province	
Zip Code	
Country	
Name of Broker (if applicable)	
How many employees does your company have?	1 - 50 employees

Please answer all of the following questions to the best of your knowledge. You may need to refer certain sections of this questionnaire to other managers in your company for completion. For your convenience, next to each section heading we have noted the job function(s) that may be best equipped to answer the questions within that section

For each question, choose an answer of either 'Yes' or 'No'. If 'Yes' is selected, please check all of the additional sub points that apply to your company. Please provide any relevant additional information in the space provided.

If there are any questions that you feel are not applicable to your company, please check 'No' and explain in the 'Additional Information' section at the end of each question. If the topic of any section pertains to a service that your company outsources, please answer the questions to the best of your knowledge and/or fill out the additional information section of the question. Please also enter details on the outsourcer that you use in the vendor management section of this questionnaire.

When you have completed the assessment, please save as a Microsoft Word file and e-mail to: netAdvantageAssessment@aig.com. Your assessment will be reviewed by an AIG IT-Security analyst, and you will receive the results of your assessment via return e-mail. The results will be password protected and the password will be communicated separately via email.

Security Organization – (Suggested respondent: CIO, CSO, CTO, Information Security Manager)	
1. What percentage of your total global IT budget is allocated to security?	Please Choose Additional Information:
2. Does your company have an information security infrastructure and organization?	☐ There is an IT security strategy document that details the company's security vision, mission statement, and security management structure. ☐ The board of directors or audit committee provides oversight for the security function. ☐ Information security roles and responsibilities are defined, documented, and address separation of duties (e.g. information security steering committee, security administrators, information owners, etc.). ☐ A security contact has been designated at each company site or facility. ☐ The name and contact information for the security contact has been

security training on an ongoing basis.

The following areas are addressed in documented security policies:

- ☐ Business Continuity Management
- ☐ Change Control
- ☐ Security Assessment and Compliance
- ☐ Computer & Network Management
- ☐ Electronic Access Control
- ☐ Email Usage and Protection
- ☐ Encryption
- ☐ Incident Response
- ☐ Information Asset Classification and Data Protection
- ☐ Internet Usage
- ☐ Password Management
- ☐ Personnel Security and Hiring Standards
- ☐ Physical Access
- ☐ Privacy & Confidentiality
- ☐ Remote Access
- ☐ Security Awareness
- ☐ Systems Development & Maintenance
- ☐ Vendor/Third Party Management
- ☐ Web Application Security
- ☐ Virus Protection

Additional Information:

Physical and Environmental Security – (Suggested respondent: Facilities manager, CSO, CIO)

5. Does your company have physical security controls in place? ☐ Yes ☐ No
- ☐ A security perimeter has been identified and documented, which includes computer rooms, media storage rooms, data centers, etc.
- ☐ Biometric access controls are used to access company data center(s).
- ☐ Computers are physically secured with lock devices.
- ☐ Surveillance cameras and guards are in place to monitor premises.
- ☐ Departments and work areas that deal with sensitive information or systems are limited to authorized personnel.
- ☐ ID badges are required for employee, visitor and vendor access.
- ☐ ID badges are electronically verified for access.
- ☐ Computer, media storage and telecom room access is secured and restricted to authorized personnel.
- ☐ Cables and network ports are protected from unauthorized access.
- ☐ Disposal of computer systems and media storage devices (hard drives, tapes, floppies, CDs, etc) is handled in a secure fashion (i.e. de-magnetization).
- ☐ Remote locations have physical security similar to the main location.

Additional Information:

Computer and Network Management – (Suggested respondent: CTO, CIO, CSO, Information Security Manager)

6. Does your company enforce a patch management process? ☐ Yes ☐ No
- ☐ Vulnerabilities and exploits are monitored and prioritized on a daily basis (i.e. subscriptions to security sites, vendor sites etc.)
- ☐ Security patches or workarounds are identified and prioritized on a daily basis.

Highest priority security patches or workarounds are implemented within the following timeframe of identification: Please Choose

Other security patches or workarounds are implemented within the following timeframe of identification: Please Choose ☐ Patches are tested on non-production systems before they are implemented. ☐ Implementation of patches is formally documented. Please summarize your patch implementation process: Additional information:	
7. Does your company have a virus protection program in place? ☐ Yes ☐ No	☐ Virus protection/detection software is installed and enabled on servers, workstations and laptops. ☐ Virus definition files are updated on servers, workstations and laptops at least weekly and immediately in the event of an outbreak. ☐ In the event of an outbreak, the user community is alerted with actions to be taken. ☐ Email attachments, downloads and other potentially malicious extensions are pre-screened for viruses by network filtering devices Additional information:
8. Are systems in your Internet/DMZ environment secured? ☐ Yes ☐ No	☐ Internet accessible systems are tested for vulnerabilities prior to being placed in production. ☐ Only services that are required by a specific business need and that have been assessed for their impact on security are enabled. ☐ All essential protocols (i.e. DNS, LDAP, SMTP, FTP, etc) are securely configured. ☐ Firewall(s) are configured to ensure source(s), destination(s) and

protocol(s) are as specific as possible. ☐ The DMZ architecture is multi-tiered. ☐ External networks and DMZ servers are monitored 24 x 7 for security violations. Additional information:	
9. Are internal systems secured?	☐ Yes ☐ No ☐ Applications on internal web servers run in non-privileged mode. ☐ Host based firewalls are implemented between segregated networks. ☐ Server performance metrics (CPU, disk, memory, hardware, etc.) are monitored. ☐ Critical applications residing within the internal networks (and behind the firewall) are monitored 24 x 7 for security violations. ☐ Systems are scanned for unauthorized software installations. ☐ Desktop machines, laptops and servers are configured according to your company's technical security configuration standards. ☐ Password protected screensavers automatically activate after a predetermined period of inactivity. Additional information:
10. Do critical systems receive full security testing before deployment?	☐ Yes ☐ No ☐ Security vulnerability testing is performed according to a defined and documented methodology. ☐ Attack and penetration testing is performed by an independent third party. ☐ Testing for web applications includes checking for session management weaknesses and cross-site scripting vulnerabilities. ☐ Availability testing is conducted on redundant systems. ☐ Written results are produced and retained for a minimum of 1 year. Additional information:

Access Control - (Suggested respondent: CIO, CSO, CTO, Information Security Manager)

11. Do your company's access control procedures address access to sensitive systems, files and directories?
- ☐ Yes ☐ No
- ☐ Procedures for access to mission critical systems and sensitive data (e.g. company financial data, customer data, etc.) include user authorization and authentication.
- ☐ Files stored on servers are protected from unauthorized access or use.
- ☐ Access to system files and directories is explicitly restricted to authorized IT personnel.

Additional information:

12. Does your company enforce a password management process?
- ☐ Yes ☐ No
- ☐ Unique username and password for user authentication is required.
- ☐ Password complexity scheme is in place and is technically enforced where feasible or testing is performed to ensure compliance.
- ☐ Technology is configured to require users to change passwords at least every 180 days.
- ☐ Technology is configured to require privileged users to change passwords at least every 90 days.
- ☐ Passwords cannot be reused for at least 4 changes.

Additional information:

13. Are controls in place to secure network access? ☐ Yes ☐ No	☐ There is a documented process in place to activate new network connections. ☐ Extranet connections are limited and secured (e.g. via firewall rules established as required by a documented business need). ☐ Connections to legacy systems are secured. Additional information:
14. Are connections from laptops, mobile devices, and remote users into the company's network secured? ☐ Yes ☐ No	☐ Advanced authentication controls are in place for remote access. ☐ VPN software is configured to prohibit broad-band users from accessing the corporate network while also accessing the Internet (i.e. split tunnel) ☐ Remote user access is limited to only those applications needed. ☐ Remote users are required to have a personal firewall installed if using a VPN connection to the network. Additional information:
15. Does your company have a process for managing user accounts? ☐ Yes ☐ No	☐ There is a documented process to approve new accounts and modify user privileges. ☐ User privileges are based upon job function. ☐ User privileges are changed within one week for internal transfers. ☐ User privileges are revoked for terminated users within 2 business days of the termination. ☐ Users are required to verify their identity prior to a password reset. ☐ User privileges are reviewed at least annually. Additional information:

16. Is encryption used to protect sensitive information when it is transmitted over external networks? ☐ Yes ☐ No	☐ Public/private keys are used for the encryption of sensitive information. ☐ 128-bit encryption products (e.g. SSL, RSA) and/or algorithms (e.g. Triple DES) are used. ☐ Database encryption is used for sensitive information (e.g. credit card numbers, social security numbers, etc.). ☐ Passwords are encrypted. ☐ File encryption is used for locally stored materials (e.g. on laptops, etc.) Additional information:
17. Do your company's policies address access to data based on a data classification scheme? ☐ Yes ☐ No	☐ Data classification policies are based on risk assessments. ☐ Data protection requirements are defined and documented. ☐ Information owners are responsible for the protection of the data they own. Additional information:

System Development and Maintenance – (Suggested respondent: Development Manager, CIO, CSO, CTO, Information Security Manager)	
18. When a new system is developed or purchased, are security considerations taken into account? ☐ Yes ☐ No	☐ Security requirements are an integral part of new project plans. ☐ Security is defined within the system architecture. ☐ Security coding standards for your company are defined (e.g. global variables are not used). ☐ A security expert is involved in new projects. Additional information:

19. Are staging, test, and development systems kept separate from production systems? ☐ Yes ☐ No	☐ There is no sharing of databases and configuration files. ☐ There is no sharing of accounts. ☐ Developers do not have access to production. ☐ Staging, test and development systems are in separate environments (i.e. separate segments, separate servers) ☐ Development tools, including compilers and linkers, are not installed on production systems. Additional information:
20. Does your company perform configuration management? ☐ Yes ☐ No	☐ Software products are used to maintain version control and restrict access to programming libraries. ☐ There is a documented process to review and approve changes to code. ☐ Modifications made by individuals to code are tracked. ☐ The development system has the ability to back out changes. ☐ The development system is protected by appropriate security measures. ☐ Developers do not have the ability to migrate code to production. ☐ Change control procedures are documented. ☐ Management reviews documentation of emergency changes. Additional information:
21. Are new applications and non-cosmetic changes reviewed for security vulnerabilities prior to migration to production? ☐ Yes ☐ No	☐ Code reviews are performed by an independent individual or third party. ☐ The impact of changes to security is documented. ☐ Assessments of applications are performed according to a defined procedure, which includes security guidelines. ☐ Security assessments of applications are performed with automated scanning tools and manual techniques as appropriate. ☐ A report documents assessment findings. ☐ Data input testing standards are defined (e.g. buffer overflow check).

Additional information:

Compliance – (Suggested respondent: Compliance Officer, CIO, CSO, Information Security

22. Does your company have a program in place to periodically test security controls? ☐ Security assessments are based on a risk evaluation and are performed at least once a year. ☐ Security assessment processes and methodologies are documented. ☐ Access to security assessment tools and utilities and the directories where they are stored are restricted to authorized personnel

(NOTE: This can include internal audits, external audits or security consulting engagements.)

☐ Yes ☐ No

Security assessments include the use of :

- ☐ Outside security specialists to perform penetration testing
- ☐ Automated vulnerability scanners
- ☐ Policy compliance checking tools (e.g. eTrust)
- ☐ Secure configuration checkers
- ☐ Performance tools
- ☐ Modem Sweeps
- ☐ Source code comparison tools.
- ☐ Security policies and controls are subject to independent reviews and audits.

- ☐ All high risk vulnerabilities are remediated within 1 month.
- ☐ All medium risk vulnerabilities are remediated within 3 months.

Additional information:

23. Do you maintain system logs?

☐ Yes ☐ No

System logs are maintained for the following:

- ☐ Internet connections
- ☐ Access attempts
- ☐ Critical Applications
- ☐ Internal network devices (e.g., firewalls, routers, IDS, etc.)

- ☐ Logs are stored securely in a central location.
- ☐ A copy of the logs is stored off site for at least 90 days.

Additional information:

24. Are system logs reviewed for security related events?

☐ Yes ☐ No

System log reviews:

- ☐ Occur at least daily
- ☐ Use automated tools
- ☐ Are performed by trained personnel

- ☐ System clocks are synchronized with a trusted time server.

Additional information:

Vendor Management – (Suggested respondent: General Counsel, CIO, CTO, Contracts Manager)

25. Does your company enforce security standards for third parties that connect to your network?

☐ Yes ☐ No

- ☐ Requests for third party connectivity must be reviewed and approved by your management.

- ☐ Technical risk assessments are performed on third parties that request access.

- ☐ Third party connections are monitored for security events.

Additional information:	
26. Do third party contracts include security provisions? ☐ Yes ☐ No	Third party contracts include: ☐ A service level agreement that specifies security requirements and responsibilities ☐ Provisions for compliance with applicable regulations (e.g., GLBA, HIPAA, Basel II, etc.) ☐ A right to audit clause ☐ Procedures for escalating security related events Additional information:
27. Does your company outsource any portion of your information security? ☐ Yes ☐ No	Please provide the name(s) of outsourced security vendor in each area: Access Control: Business Continuity: Computer and Network Management: Compliance: Physical and Environmental Security: Systems Development and Maintenance: Security Organization: Security Policy and Standards: Additional information:

Business Continuity – (Suggested respondent: CIO, CTO, CSO, Information Security Manager)

28. Does your company have backup and restore procedures in place?

☐ Yes ☐ No

Backup and restore procedures are:

- ☐ Documented
- ☐ Tested annually to ensure their effectiveness
- ☐ Performed by trained personnel

Backup tapes/disks are:

- ☐ Made at least once a week
- ☐ Kept for a minimum of 90 days
- ☐ Stored in fire proof safes
- ☐ Rotated off site for storage
- ☐ Retired once their lifespan has been reached

Additional information:

29. Does your company have a Business Continuity Plan (BCP)?

☐ Yes ☐ No

The Business Continuity Plan:

- ☐ Is managed by a dedicated group
- ☐ Is formally documented
- ☐ Is tested on an annual basis
- ☐ Addresses every department

- ☐ Users are trained on their BCP responsibilities.
- ☐ A “hot site” is in place.
- ☐ Redundant systems are in place.
- ☐ Hardware vendors are contracted to provide replacement systems.

Additional information:

Financial Management of Network Security Losses -- (Suggested respondent: CFO, CIO)

30. Security breaches cause unexpected financial losses. Has your company planned for the funding of such expenses?

☐ Yes ☐ No

Funding is available via:

- ☐ Cash on hand
☐ A loss reserve
☐ Available credit
☐ Network Security Insurance
☐ Other Insurance

Additional information:

31. Does your company require all vendors to maintain liability insurance?

☐ Yes ☐ No

Liability insurance includes the following:

- ☐ Limits of at least \$1,000,000.
☐ Loss arising from vendor negligence.
☐ Loss arising from a breach of security (including data corruption, business interruption, etc.)

Additional information:

When you have completed the assessment, please save as a Microsoft Word file and e-mail to: netAdvantageAssessment@aig.com

Your assessment will be reviewed by an AIG IT-Security analyst, and you will receive the results of your assessment via return e-mail. The results will be password protected and the password will be communicated separately via email.