Model Pendekatan Manajemen Resiko Keamanan Dalam e – *Commerce*

Yohan Wismantoro

ABSTRACT: *E-commerce security is a complex issue; it is concerned with a number of security risks that can appear at either a technical level or organisational level. This paper uses a systemic framework, the viable system model (VSM) to determine the high level security risks and then uses baseline security methods to determine the lower level security risks.*
Keywords: *Electronic commerce, Risk analysis, Information systems*

1. Pendahuluan

Pesatnya perkembangan bisnis *Internet Banking* di Indonesia seakan tidak mencerminkan pertumbuhan ekonomi Indonesia yang sebenarnya. Kalau berbicara tentang teknologi, apa yang ramai di luar negeri, Indonesia pun dengan cepat mengadopsi dan mengikutinya. Ada kesan, apa yang dapat dilakukan sebuah bank, dengan sangat mudah diikuti oleh bank lain, bagaimanapun kondisinya. Aplikasi teknologi tinggal disesuaikan dengan fondasi yang ada dan besarnya potensi market masing-masing bank.

Internet Banking untuk kasus Indonesia perlahan tapi pasti tampaknya mulai menggeser gaya perbankan yang konvensional yang melibatkan puluhan juta nasabah bank di negara ini. Bukan suatu yang mudah menggeser pola kebiasaan lama - *cash and carry banking* - atau *old banking style* ini ke *new banking*. Tapi kenyataannya, perkembangan Internet Banking ini tidak perlu menunggu kesiapan nasabahnya. Siap tidak siap, industri perbankan terus maju. Padahal, kalau kita kembali ke teori ekonomi klasik, sebuah produsen (bank dalam hal ini) harus menciptakan produk yang sesuai dengan profil market. Kesiapan *market* menyerap produk atau fasilitas tersebut selalu menjadi *critical point*.

Dari fenomena di atas, meningkatnya persaingan diantara para penyedia jasa keuangan, berkenaan dengan semakin meningkatnya jumlah pelaku pasar yang baru, berkurangnya biaya peralihan nasabah dan retensi nasabah sebagai akibatnya, telah meningkatkan tekanan pada *profit margin*. Meskipun banyak

Yohan Wismantoro *adalah Staf Pengajar dan Ketua Program Magister Manajemen Udinus*

organisasi jasa keuangan telah menekankan perubahan ke diferensiasi sebagai suatu strategi bersaing (Ennew *et al*, 1990), penekanan yang utama untuk pengurangan rasio biaya-pendapatan telah mengemuka di dalam industri ini. Tekanan-tekanan persaingan disertai dengan perkembangan teknologi baru sekarang telah menekankan peran "strategik" dari teknologi sebagai sumber diferensiasi dan pengurangan biaya yang potensial.

Dalam lingkungan dimana barang dan jasa tersedia dalam bentuk informasi digital, pelanggan bisa melayani dirinya sendiri tanpa harus melakukan tatap muka (*Internet Self Service Tecnology*). Agar penggunaan secara kontinyu bisa terlaksana, persepsi pelanggan mengenai atribut-atribut yang berkaitan dengan teknologi melayani sendiri (*Internet Self Service Tecnology*) menjadi sangat penting. Oleh sebab itu, semua organisasi yang ada menggunakan dan sangat mengandalkan sistem-sistem informasi sehingga mustahil bagi mereka untuk mengelola organisasinya tanpa sistem informasi tersebut. Hal ini dibuktikan dengan adanya perkembangan terbaru dari *e-commerce* dalam lingkungan konsumen dan perusahaan. Situasi yang berkembang akhir-akhir ini menunjukkan bahwa sistem informasi yang ada terancam oleh berbagai macam resiko keamanan dan yang diperlukan adalah sebuah metode keamanan yang dapat mengevaluasi resiko-resiko tersebut serta memastikan bahwa pertahanan keamanan yang tepat telah diterapkan. Dengan demikian, konsumen akan merasakan tingkat keamanan dan kenyamanan ketika menggunakan atau melakukan transaksi secara *online*.

2. Metode-metode Keamanan

Tujuan dari tulisan ini adalah mencoba memberikan gambaran tentang penggabungan sebuah metode *modeling* sebuah sistem informasi dengan sebuah metode keamanan *baseline* schingga akan terbentuk sebuah metode keamanan gabungan. Metode ini dapat digunakan untuk mengevaluasi tinggi-rendahnya tingkat resiko keamanan yang terkait dengan *e- commerce*. Metode yang digunakan dalam model ini adalah V*iable System Model* (VSM) dan pendekatan keamanan *baseline (*Warren dan Hutchinson (2003). VSM digunakan untuk membentuk fungsi-fungsi dasar organisasi dan aliran – aliran terkait, sedangkan pendekatan keamanan *baseline* digunakan untuk menerapkan pertahanan keamanan yang tepat.

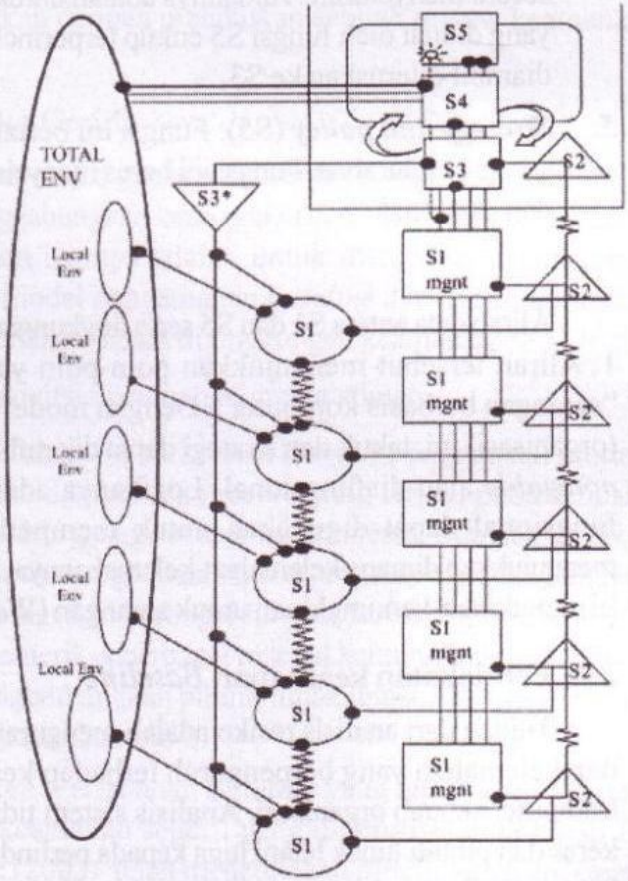
2.1 Viable System Model (VSM)

Viable System Model (VSM) dikembangkan oleh Stafford Beer (Beer, 1985) dengan menggunakan prinsip-prinsip *cybernetic*. Model ini berhasil digunakan untuk mendiagnosa struktur-struktur o rganisasi yang ada dan

membentuk struktur yang baru. Sifat-sifat utama dari VSM memungkinkannya untuk digunakan dalam berbagai macam situasi. Dari sudut pandang tulisan ini, model tersebut akan digunakan untuk menganalisa bagian-bagian tertentu dari sistem informasi sebuah organisasi yang rentan terhadap gangguan. (Hutchman dan Warren, 2000).

Sebelum menggunakan VSM, sangatlah penting bagi organisasi untuk memahami dinamika penerapan model ini, dan penggambaran diagramiknya terdapat dalam Gambar 1. VSM terdiri dari lima fungsi atau sub sistem. Fungsi itu meliputi:

1. ***Implementation*** (S1): Fungsi ini terdiri dari unit-unit semi otonom yang menjalankan tugas operasional dalam sisitem. Fungsi-fungsi ini merupakan dasar dari tujuan sistem-sistem tersebut. Mereka berinteraksi dengan lingkungan lokalnya dan mereka juga saling berinteraksi satu sama lain. Tiap-tiap unit memiliki manajemen lokal tersendiri yang terhubung dengan manejemen yang lebih besar melalui aliran-aliran informasi vertikal. Fungsi inilah yang merupakan "tindakan" dari sebuah organisasi. VSM memiliki sebuah elemen pengulangan, dan setiap S1 yang ditambahkan pun akan memiliki VSM yang ditambahkan kedalamnya.



Gambar 2. ***The Viable System Model***
Sumber : Warren dan Hutchinson (2003)

2. ***Co-ordination*** (S2): Fungsi ini mengkoordinasikan unit-unit S1 untuk memastikan bahwa masing – masing unit S1 bertindak dengan memperhatikan kepentingan seluruh sistem dan tidak terfokus ke sistemnya sendiri. Hal ini dapat dicontohkan dengan sesuatu yang sederhana seperti jadwal atau moril karyawan.
3. ***Internal control*** (S3): Fungsi ini menerjemahkan informasi kebijakan dari fungsi "yang lebih tinggi" (S4), dan fungsi "yang lebih rendah". Fungsi ini tidak bertugas membuat kebijakan, melainkan hanya melaksanakan kebijakan itu. Informasi yang diterima dari S1 harus diaudit kualitas dan kebenarannya secara berkala. Fungsi S3 ini merupakan fungsi audit.
4. ***Intelligence and development*** (S4): Fungsi ini bertindak sebagai penyaring informasi yang datang dari fungsi S3 dan dari lingkungan luarnya secara menyeluruh. Tujuannya adalah untuk memastikan bahwa kebijakan yang dibuat oleh fungsi S5 cukup terperinci dan keptusan-keputusan yang diambil diteruskan ke S3.
5. ***Strategy and policy*** (S5): Fungsi ini bertanggung jawab atas laju sistem secara keseluruhan. Fungsi ini harus menyeimbangkan antara faktor internal dan eksternal.

Aliran data antara S1 dan S5 serta lingkungannya dapat dilihat pada Gambar 1. Aliran tersebut menunjukkan poin-poin yang memiliki potensi terkena "serangan berbasis komputer". Dengan model konseptual dari sistem *viable* (organisasi) ini, taktik dan strategi dapat dikembangkan untuk membuat sistem *nonviable* atau disfungsional. Logikanya adalah penyelidikan kekurangan fungsional dapat digunakan untuk memperbaiki sebuah organisasi dan menunjukkan dimana kelemahan-kelemahannya, tetapi juga, untuk menunjukkan kemungkinan-kemungkinan untuk serangan (Warren dan Hutchinson, 2003)

2.2. Pendekatan keamanan *Baseline*

Tujuan dari analisis resiko adalah mengurangi atau menghilangkan resiko dan kelemahan yang berpengaruh terhadap keseluruhan operasi dari sistem komputer sebuah organisasi. Analisis sistem tidak hanya terfokus pada piranti keras dan piranti lunak tetapi juga kepada perlindungan area-area lainnya seperti keamanan fisik, keamanan personil, perusahaan dan perlindingan dari bencana. Dalam prakteknya, terdapat beberapa masalah utama dalam penggunaan analisis resiko; waktu yang diperlukan untuk melakukan review; biaya sewa konsultan

dan staff training. Untuk menanggulangi aspek - aspek negatif tersebut, pendekatan keamanan *baseline* dikembangkan. Pengamanan *baseline* menawarkan sebuah alternatif dari metode-metode resiko konvensional ketika metode-metode tersebut menunjukkan pertahanan keamanan yang dapat diterima secara minimal sehingga harus dilaksanakan oleh sebuah organisasi. Pertahanan ini diterapkan secara umum, sebagai contoh, setiap organisasi harus mempunyai pelaksanaan pertahanan keamanan *baseline* yang sama.

Keuntungan dari penggunaan metode *baseline* (Warren dan Hutchinson, 2000) adalah:

- Murah,
- Sederhana,
- Tidak memerlukan pelatihan khusus dalam penggunaannya,
- Lebih cepat dibandingkan dengan melakukan sebuah review keamanan menyeluruh.

3. Model analisis Resiko Ganda

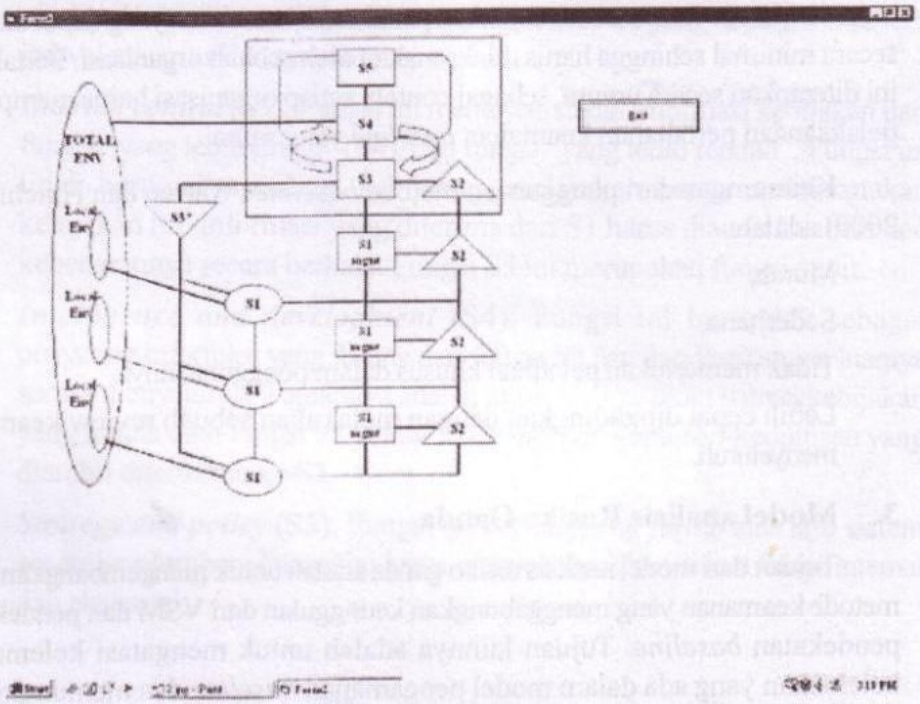
Tujuan dari model analisis resiko ganda adalah untuk mengembangkan suatu metode keamanan yang menggabungkan keunggulan dari VSM dan pendekatan-pendekatan *baseline*. Tujuan lainnya adalah untuk mengatasi kelemahan-kelemahan yang ada dalam model pengamanan *baseline* dan memungkinkan pendekatan VMS untuk digunakan dalam di lingkungan keamanan.

Tahap-tahap dalam model analisis keamanan ganda adalah:

- *Tahap1 – tahap VMS.* Tahap ini berkenaan dengan penggunaan model VMS untuk menentukan dampak dan resiko yang terjadi pada sebuah organisasi apabila mengalami gangguan keamanan tertentu. Dampak tersebut dapat ditaksir dari keseluruhan organisasi seperti yang tertera dalam Gambar 1. Kelemahan – kelemahan dari berbagai fungsi (dari S1 sampai dengan S5) digunakan untuk memeriksa berbagai macam kemungkinan serangan. Beberapa ahli telah mengembangkan piranti lunak untuk membantu tugas ini seperti yang tertera pada Gambar 2.
- *Tahap 2 – tahap baseline.* Pertahanan *baseline* yang tepat dipilih untuk mengurangi ancaman keamanan seperti yang didefinisikan di tahap 1. Warren dan Hutchinson (2003) telah menciptakan piranti lunak *advisory* khusus yang menentukan pertahanan yang tepat. Contohnya garis – garis pedoman BS7799 yang berhubungan dengan virus komputer.

Gambar 2. *Model VSM situations*

Sumber : Warren dan Hutchinson (2003)



- *Tahap 3 – evaluasi dampak.* Proses dari tahap 1 diulangi, namun kali ini dampak dari pertahanan keamanan dievalusi. Proses ini akan memberikan evaluasi terhadap pertahanan keamanan dan menunjukkan efektifitasnya bagi organisasi secara menyeluruh. Informasi yang diperoleh dari proses ini akan memungkinkan pihak manajemen untuk menentukan efektifitas dari pertahanan keamanan yang ada.

Pendekatan ini dapat digunakan untuk mengevaluasi resiko-resiko keamanan yang terkait dengan *e-commerce.* Tipe pendekatan ini akan memungkinkan suatu organisasi untuk memperkirakan resiko keamanan dan bagaimana menghubungkan resiko tersebut kepada organisasi itu.

4. Keabsahan Penelitian

Lebih lanjut Warren dan Hutchinson (2003) mengatakan, untuk mensahkan sebuah model, perlu memperhatikan beberapa resiko keamanan yang dapat memberi dampak negatif bagi organisasi dalam kaitannya dengan *e-commerce.*

Dalam bagian ini akan dilihat juga dampak yang ditimbulkan oleh virus. Tipe serangan virus yang digunakan sebagai model adalah virus "*Word Macro*" yang infeksinya sama dengan virus "*Love Bug*".

Tingkat 1 – tahap VMS

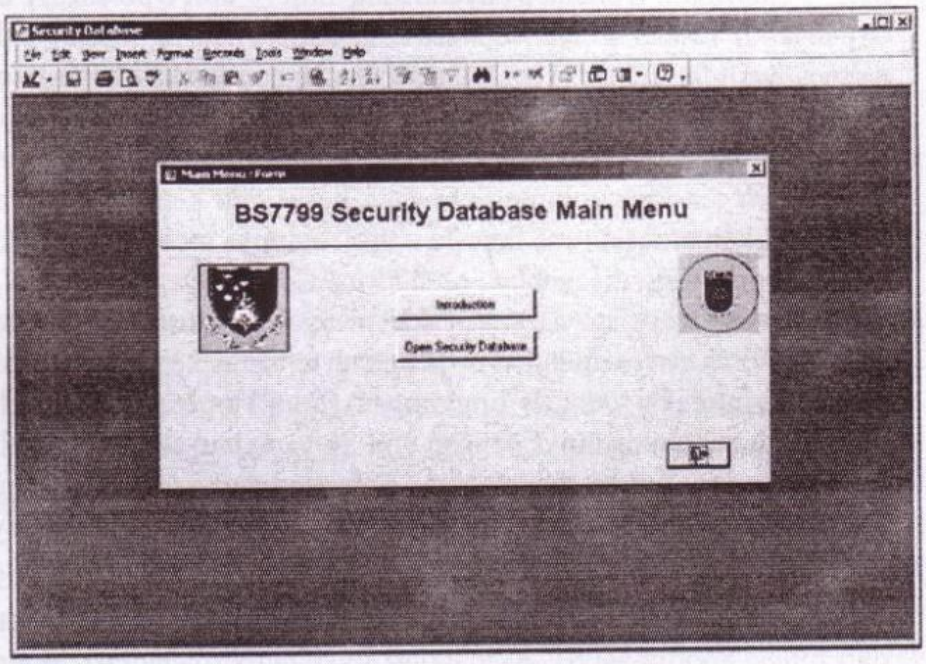
Gambar 1 memberikan ilustrasi tentang tingkatan-tingkatan yang berbeda dari sebuah organisasi sampel. Dampak yang timbul dari serangan virus terhadap organisasi sampel tersebut adalah:

- *S1 – Penerapan.* S elama p enyerangan, unit – unit o perasi S1 a kan terpengaruh. Dalam sebuah organisasi, sebaiknya masing-masing unit S1 mempunyai infrastruktur TI tersendiri sebagai bagian dari keseluruhan sistem organisasi. Serangan virus akan trpusat pada infrastruktur komunikasi dari unit S1. Dampaknya yang ditimbulkan oleh serangan ini adalah *e-mail server* akan *crash* diantara volume data yang besar dan kemungkinan akan menyebabkan efek domino kepada unit S1 lainnya melalui peningkatan *traffic e-mail* yang disebabkan oleh virus. Contohnya, jika *e-mail* dari server *crash*, hal apalagi yang akan akan mengalami *crash*? Dengan begitu serangan virus *macro* mungkin berpengaruh terhadap kemampuan unit S1 untuk berinteraksi dengan lingkungan (lokal) operasinya sekaligus memutuskan hubungannya dengan unit S1 yang lain serta memisahkan fungsinya dari fungsi manajemen. Serangan terhadap unit S1 akan mengurangi efisiensi seluruh sistem yang disebabkan oleh ganguan yang ditimbulkan oleh serangan tersebut pada aspek operasional.
- *S2 – Koordinasi.* Akan terjadi dampak yang datang secara mendadak dari fungsi koordinasi S1. Akibat dari serangan virus *macro,* fungsi S2 tidak dapat berjalan karena terisolasinya unit-unit S1. Terdapat juga kemungkinan terinfeksinya unit-unit S2 oleh virus yang menyebar dari unit S1 dan oleh karenanya unit-unit S2 akan terisolasi dan berakibat pada kegagalan fungsi koordinasi.
- *S3 – Kontrol internal.* Kontrol internal sistem informasi akan terganggu dengan adanya kekacauan yang terjadi di tingkatan bawanya. Karenanya akan sulit untuk menerapkan suatu kebijakan apabila struktur dari sistem informasi dimatikan.
- *S4 – Intelejen dan pengembangan / S5 – Strategi dan kebijakan.* Virus tidak memiliki dampak langsung terhadap S4 dan S5, kecuali apabila efek-efek domino dari kegagalan sangatlah besar sehingga mempengaruhi sistem

dari tingkat yang lebih tinggi atau ketika fungsi S4 dan S5 memang menjadi sasaran serangan yang mengakibatkan fungsi-fungsi ini terisolasi dan terpisah dari fungsi organisasi lainnya.

Tingkat 2 – tingkat keamanan *baseline*

Piranti lunak keamanan yang mampu mendukung pembuatan keputusan akan digunakan untuk memilih pertahanan keamanan *baseline* yang tepat. Gambar 3 memperlihatkan sebuah *screenshot* dari sebuah *tool* keamanan *baseline*.



Gambar 3. *Security Baseline Tools*

Sumber : Warren dan Hutchinson (2003)

Piranti lunak ini akan bekerja dengan *user* yang memilih pertahanan keamanan *baseline* yang tepat untuk diterapkan. *User* tersebut akan menggunakan piranti lunak keamanan *baseline* (seperti yang diperlihatkan pada Gambar 3) dan menemukan langkah pertahanan keamanan yang tepat yang berkaitan dengan virus yang ada. Piranti lunak itu kemudian akan menunjukkan pertahanan keamanan *baseline* yang tepat seperti: *Implement appropriate virus protection strategy.* Sang *user* dapat memilih hal ini sebagai pertahanan keamanan yang ingin mereka taksir.

Tingkat 3 re-evaluasi dampak

Pengguna/user me-*review* situasi dimana pertahanan yang baru berada dengan menggunakan pendekatan VMS (Warren dan Hutchinson, 2003)

- *S1 – Penerapan.* Strategi perlindungan terhadap virus melokalisasi kerusakan yang ditimbulkan menjadi hanya beberapa unit S1 saja, dengan menganggap bahwa beberapa unit S1 tidak menerapkan sebuah sistem perlindungan terhadap virus dengan tepat, contohnya ketika *virus checker* yang ada sudah kadaluarsa.
- *S2 – Kordinasi.* Akan terdapat beberapa gangguan unit S1 yang terlokalisasi. Fungsi koordinasi yang ada dapat disesuaikan untuk mengatasi kesulitan yang terlokalisasi sampai terdapat pemecahan terhadap masalh yang terjadi.
- *S3 – Kontrol internal.* Tidak terdapat dampak langsung.
- *S4 – Intelejen dan pengembangan / S5 – Strategi dan kebijakan.* Tidak terdapat dampak langsung.

Tingkat 2 dan tingkat 3 untuk selanjutnya dapat diulangi apabila pertahanan keamanan tidak mencukupi dalam mengurangi resiko keamanan sampai ke tingkat tertentu.

1. Kesimpulan

Dari pembahasan diatas, dapat disimpulkan bahwa keamanan dalam suatu sistem online, khususnya penyedia jasa online adalah merupakan hal sangat penting, karena *security risks* dapat muncul baik ditingkat teknis maupun tingkat organisasional. Tulisan ini diharapkan dapat menunjukkan bahwa model-model analisis resiko keamanan gabungan dapat digunakan untuk menghasilkan solusi-solusi keamanan yang kompleks dalam kaitannya dengan *e- commerce*. Penelitian ini tidak bertujuan untuk mengganti secara utuh metode analisa resiko keamanan yang mendetil melainkan untuk menawarkan solusi alternatif yand dapat digunakan untuk memodelkan resiko keamanan *e-commerce* yang berbeda-beda dan untuk menentukan dampak dari pertahanan keamanan yang tepat.

REFERENSI

Australian and New Zealand Standard Committee (1998), *AS/NZS 4444.1 Information Security Management*.

Beer, S. (1985), *Diagnosing the System forOrganisations*, John Wiley & Sons, Chichester.

British Standards Institute (1995), *BS7799 ± Code of Practice for Information Security Management*, BSI, London.

British Standards Institute (1998), *BS7799-2, Information security management, Specification for Information Security Management Systems*, BSI, London.

BSI (1994), *Information Technology Baseline Protection Manual*, Bundesamt fur Sicherheit in der Informationstechnik, available at: www.bsi.bund.de

Hutchinson, W. and Warren, M. (2000), "Using the viable systems model to develop an understanding information system security threats to an organisation", *Proceeding of the 1st Australian Information Security Management Workshop, Deakin University, Geelong, Australia*, November.

Warren, M. and Hutchinson, W. (2000), "The Australian and New Zealand Security Standard AS/NZS 4444", *New Zealand Journal of Computing*, Vol. 8 No. 1/2, pp 37-43.

Warren, M. and Hutchinson, W. (2003), A security risk management approach for e-commerce, *Information Management and Computer Security*, p 238-242