MODEL IDENTIFIKASI PERENCANAAN KEAMANAN PADA E-BUSINESS

Roland Tumbelaka Palar[1], Bentar Priyopradono[2], Theopillus J. H. Wellem[3]
Jurusan Magister Sistem Informasi, Fakultas Teknologi Informasi,Universitas Kristen Satya Wacana
Jl. Diponegoro No. 52 - 60, Salatiga 50711
Telp. (0298) 321212 ext. 274, Faks. (0298) 321433
E-mail: roland.palar@gmail.com,bentarpriyopradono@yahoo.com,ermanwellem@gmail.com

ABSTRAK
E-Business sebagai salah satu entitas yang mampu menghasilkan keuntungan bagi organisasi / perusahaan maupun individu adalah aset yang berharga yang harus dijaga dan dilindungi. Dalam proses menjaga tersebut, tidaklah mudah dikarenakan banyak rintangan dan masalah yang harus dihadapi. Berbagai masalah yang mengancam keamanan e-Business perlu di lakukan identifikasi agar kedepannya sistem dapat menangkal ancaman-ancaman tersebut. Proses identifikasi sebagai lapisan pertama atau tahap awal dari tahapan-tahapan manajemen keamanan dalam e-Business, adalah sangat penting dilakukan karena tahapan selanjutnya yaitu proses evaluasi resiko, hasilnya bergantung pada temuan yang berhasil diidentifikasi dari tahap ini. Pendekatan yang dilakukan dalam merancang model identifikasi perencanaan keamanan yaitu melalui studi literatur yang berhubungan dengan proses manajemen keamanan e-Business. Hasil yang diharapkan dari perumusan adalah berupa rekomendasi proses-proses apa saja yang perlu dilakukan dalam melakukan identifikasi perencanaan keamanan pada e-Business.

Kata kunci: e-business, securiy plan

1. PENDAHULUAN

Dalam proses manajemen keamanan e-Business, dibutuhkan strategi pelaksanaan yang tepat. Tahap identifikasi rencana keamanan e-Business adalah penting artinya dikarenakan tahap tersebut merupakan tahapan awal yang menjadi dasar dari segala tahapan dalam menajemen keamanan e-Business (Vasilyevna, 2008). Dalam melakukan identifikasi perlu dipikirkan apa saja yang menjadi tujuan dari manajemen keamanan e-Business. Tujuan yang dimaksud antara lain adalah kerahasiaan (confidentiality), integritas (integrity) dan ketersediaan (availability) (Tyagi dan Srinivasan, 2011). Mengacu pada tujuan manajemen keamanan e-Business tersebut, maka dalam penelitian ini, penulis mengajukan model identifikasi dalam perencanaan manajemen keamanan e-Business dengan melakukan modifikasi pada pendekatan arsitektur perencanaan sebagai penjabaran dari model identifikasi tersebut. Pemodifikasian model ini bertujuan memberikan pendekatan yang lebih optimal melalui penambahan cakupan proses identifikasi dalam mengindentifikasi rencana keamanan dalam arsitektur keamanan e-Business.

2. E-BUSINESS

2.1 Definisi E-Business

E-Business dapat di definisikan sebagai penggunaan media jaringan internet dengan harapan dapat meningkatkan proses bisnis, perdagangan elektronik, komunikasi organisasi dan mengkolaborasikan perusahaan dengan pelanggan, pemasok dan stakeholder lainya, e-Business menggunakan internet, intranet, extranet dan menggunakan jaringan lain untuk mendukung proses bisnisnya (Combe, 2006).

E-Business bertujuan untuk meningkatkan daya saing organisasi / perusahaan dengan menyebar luaskan informasi yang inovatif dan teknologi komunikasi di seluruh organisasi melalui link kepada mitra dan pelanggan, tidak sebatas pada penggunaan teknologi untuk melakukan otomasi proses bisnis suatu organisasi/perusahaan tetapi harus juga mencapai proses transformasi dengan menerapkan teknologi untuk mengubah proses bisnis yang telah ada (Chaffey, 2009). Dari definisi di atas dapat di tarik kesimpulan bahwa e-Business melibatkan atau mengguanakan teknologi sebagai pendukung dalam meningkatkan semua aspek yang di miliki organisasi / perusahaan sebagai salah satu usaha mengoptimalkan value chain organisasi.

2.2 Electronic Data Interchange (EDI)

EDI (Electronic Data Intercange) merupakan standar dalam melakukan pertukaran data / dokumen dalam organisasi dalam bentuk elektronik antar aplikasi komputer, banyak prosedural yang dilakukan dalam e-Business dalam melakukan pertukaran data yang melibatkan EDI sebagai salah satu standar seperti pesanan pembelian dan faktur. Ada beberapa fitur utama dalam EDI (Minoli, 1998) diantaranya :

a. Penggunaan media transmisi elektronik.
b. Penggunaan pesan diformat berdasarkan standar yang disepakati.
c. Pengiriman dokumen elektronik dapat dilakukan dengan cepat dari pengirim ke penerima
d. Komunikasi langsung antara aplikasi dan sistem.

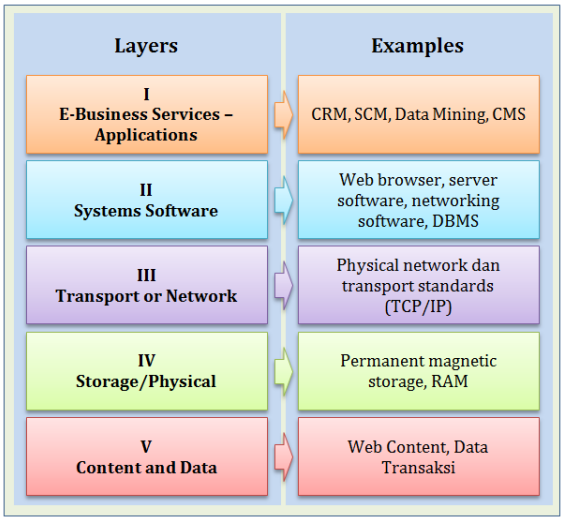
 ISSN: 1907-5022

Manfaat yang terkait dengan penggunaan EDI diantaranya :

a. Menurunkan biaya administrasi dan pengolahan data.
b. Biaya lebih rendah dalam posting dan penyusunan transaksi.
c. Peningkatan efisiensi dalam proses transaksi.
d. Mengurangi kesalahan.
e. Peningkatan layanan pelanggan.

2.3 Infrastruktur E-Business

Infrastruktur e-Business secara langsung mempengaruhi kualitas layanan bagi para pengguna sistem baik organisasi/perusahaan dalam hal kecepatan dan responsif. Infrastruktur e-Business mengkombinasikan perangkat keras (*hardware*) dan perangkat lunak (*software*) dalam organisasi / perusahaan bertujuan memberikan pelayanan kepada para pekerja, mitra dan pelanggan mereka. Terlihat pada gambar 1 beberapa komponen arsitektur e-busines yang saling berhubungan dan perlu dikelola dengan baik, beberapa lapisan dalam komponen tersebut dapat dipahami sebagai tugas yang perlu di pahami oleh setip pengguna e-Business baik organisasi / perusahaan (Chaffey, 2009).



Gambar 1. Model *5-layer E-Business Infrastructure*

2.4 Infrastruktur Kemanan E-Business

Keamanan merupakan isu yang paling mendasar yang mempengaruhi dalam pengelolaan e-Business oleh suatu organisasi / perusahaan, transaksi yang aman menjadi tolah ukur dalam memberi nilai lebih (*high value*) kepada pelanggan dan keamanan juga menjadi dasar kepercayaan dalam bertransaksi dalam lingkungan e-Business (Karmakar, 2003).

Infrastruktur kemanan e-Business di rancang sebagai model desain kemanan dalam e-Business agar dapat membantu organisasi/ perusahaan untuk membangun, memelihara keamanan dalam mengoperasikan e-Business secara aman dalam menjalankan aplikasi di dalam e-busines (Vasilyevna, 2008). Gambar 2 desain infrastruktur kemanan e-Business yang terdiri dari 4-layer *physical access, network communication, operating systems dan application*.

Gambar 2. Desain Infrastruktur keamanan E-Business

2.5 Bentuk Pelanggaran Keamanan pada E-Business

Banyak cara dimana kemanan sistem dapat di langgar atau di serang mulai dari kegiatan kriminal serius, suatu organisasi / perusahaan harus mulai menentukan arah kebijakan mereka dalam menyiasati pemasalahan kemanan yang muncul dan seiring perkembangan nya yang mulai serius mengancam, perusahaan harus siap dalam membangun langkah-langka pencegahan serangan keamanan untuk dapat melindungi data internal perusahaan seperi data transaksi, konsumen dan aset komersial lainya dari beberapa serangan berikut seperti hacking, spam, fraud dan kekeliruan dalam mengidentifikasi (*misrepresentation of identity*) ini merupakan beberapa serangan yang umum dilakukan (Combe, 2006) :

a. Hacking
   Haking merupakan kegiatan dimana sesorang dengan sengaja dan secara ilegal melakukan akses ke suatu sistem jaringan bertujuan untuk mendapatkan informasi berharga seperti kartu kredit dan melakukan penipuan dengan cara menggunakan informasi yang telah di dapat. Ada beberapa jenis kegiatan dalam heking diantaranya pemantauan informasi, mengakses database dan *Denial Of Service*.
b. Spam
   Spam merupakan e-mail yang dikirim ke alamat secara acak dan disebut sebagai 'e-mail sampah', spam telah menjadi masalah yang signifikan untuk organisasi / perusahaan dan individu untuk menangani permasalahannya, motivasi pengiriman spam e-mail bermacam-macam seperti berbentuk iklan dan lainya.
c. Fraud
   Fraud atau sering di sebut penipuan merupakan salah satu hambatan terbesar untuk pertumbuhan internet untuk bisnis dan perdagangan. Skala

sebenarnya dari aktivitas penipuan di internet tidak pernah diketahui karena banyak korban memilih untuk tidak melaporkan kejahatan dan perusahaan memilih untuk menghindari publikasi akibat penipuan ini dengan tujuan menjaga kenyamanan dari konsumen mereka.

3. TUJUAN DAN MANFAAT PENELITIAN

Adapun tujuan dari penelitian ini adalah untuk memodelkan dan menjabarkan proses identifikasi perencanaan keamanan dalam manajemen keamanan e-Business. Pada proses penjabaran ini, kami memodifikasi rumusan *Three-Layer* Vasilyena dengan menambahkan layer *Tool Identification*. Dari penelitian ini, diharapkan dapat bermanfaat bagi perancangan infrastruktur e-Business kedepannya terutama pada perancangan komponen keamanan.

4. RELATED WORK

4.1 Nadejda Belbus Vasilyevna

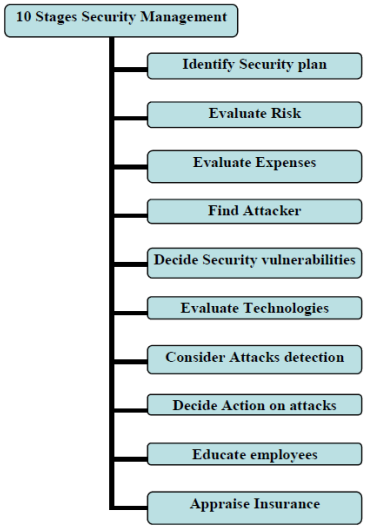
Dalam tulisannya Vasilyevna melakukan pendekatan dalam mendesain kemanan di lingkungan e-busines dengan menggunakan arsitektur *Three-Layer* dengan melibatkan berbagai tahapan proses manajemen seperti *planning*, *administration*, *deployment*, *adminisration*, *auditing* dengan kontrol keamanan yang terdiri dari beberapa layer seperti sistem operasi, *physical access*, *network communication* dan *aplication*.

Gambar 3 menjelaskan tahapan dalam perencanaan dalam manajemen kemanan dengan melibatkan tiga proses yaitu *asset identification*, *risk identification* dan *action planning* (Vasilyevna, 2008).

Gambar 3. Tahapan perencanaan dalam manajemen keamanan e-Business

4.2 Tyagi dan Srinivasan

dalam tulisannya Tyagi dan Srinivansa memberikan gambaran keamanan tingkat tinggi pada e-Business, mereka merumuskan model strategi keamanan yang dapat dilihat pada gambar 4 yang menjelaskan 10 tahapan manajemen keamanan dalam e-Business (Tyagi dan Srinivasan, 2011).



Gambar 4. Model 10 Tahapan Strategi Manajemen Kemanan E-Business

5. METODE PENELITIAN

Pendekatan yang dilakukan dalam merancang model identifikasi perencanaan keamanan adalah melalui studi literatur yang berhubungan dengan proses manajemen keamanan e-Business. Hasil yang diharapkan dari perumusan ini berupa rekomendasi proses-proses apa saja yang perlu dilakukan dalam melakukan identifikasi perencanaan keamanan pada e-Business.

6. HASIL

Proses identifikasi ini dirasa sangat penting dikarenakan proses ini adalah proses awal dan sebagai dasar untuk melakukan proses-proses selanjutnya. Dalam paper penelitian ini, rumusan Vasilyevna di modifikasi dengan penambahan 1 layer management untuk melengkapi arsitektur *three layer* yang disebutkan sebelumnya. Layer tersebut adalah *Tool Identification*.

Adapun 4 (empat) layer pendekatan yang digunakan untuk menjabarkan proses perencanaan sebagai bagian dari 10 tahapan manajemen keamanan pada e-Busines yakni *aset identification*, *risk identification*, *action planning* dan *tool identification*, lebih detailnya akan dijelaskan sebagai berikut.

6.1 Pendekatan *Aset Identification*

Dalam proses identifikasi keamanan, perlu didefinisikan aset berharga yang akan diamankan. Pada e-Business aset yang dimaksud adalah data atau informasi yang tersimpan dalam database, infrastruktur hardware (server, router, dsb) pada pusat layanan e-Business dan perangkat lunak (software) sebagai antarmuka dalam mengakses layanan e-Business.

 ISSN: 1907-5022

6.2 Pendekatan *Risk Identification*

Untuk mempermudah mengidentifikasi resiko yang mungkin terjadi, pertama dapat kita lihat, dari aset berharga yang telah kita definisikan, maka kita dapat menentukan resiko yang mungkin terjadi. Bila aset berupa data dan informasi, resiko yang mungkin terjadi adalah data rusak, data hilang, data dimodifikasi oleh pihak yang tidak berwenang dan sejenisnya.

Bila aset berupa perangkat keras, maka resiko yang akan terjadi kemungkinan besar adalah perangkat hilang dicuri, perangkat mengalami kerusakan pada komponen elektronik dan salah konfigurasi pada perangkat yang mengakibatkan perangkat beroperasi tidak sebagaimana mestinnya.

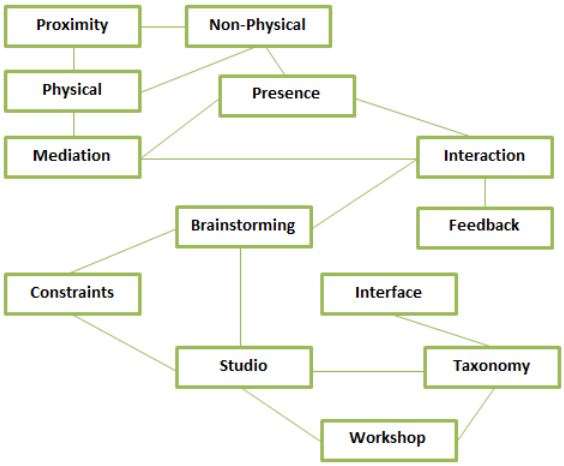
Bila aset adalah perangkat lunak (software) berupa halaman web, *web service*, *driver* dan sistem operasi, maka kemungkinan resiko yang terjadi adalah apikasi dalam e-Business mudah di eksploitasi oleh pihak yang tidak kita inginkan akibat kesalahan konfigurasi, celah keamanan dan bug yang belum di patch dan sejenisnya. Dalam *risk identification*, tidak sebatas aset saja yang di nilai akan resiko yang berpeluang muncul. Resiko lain adalah misalnya penggunaan hak akses yang tidak sesuai, pengaksesan resource oleh tanpa ijin yang jelas dan sebagainya.

6.3 Pendekatan *Tool Identification*

Pendekatan yang ditawarkan sebelumnya akan lebih optimal lagi bila *tool identification* disertakan kedalamnya. *Tool* atau alat, disadari sebagai bagian yang perlu di identifikasi. Alat yang dimaksud ini bukan termasuk aset yang perlu diamankan, melainkan "alat" ini yang akan digunakan untuk mengamankan aset. Dalam pendekatan *tool identification* ini, dikelompokkan 4 (empat) *tool* yang perlu di identifikasi antara lain sebagai berikut.

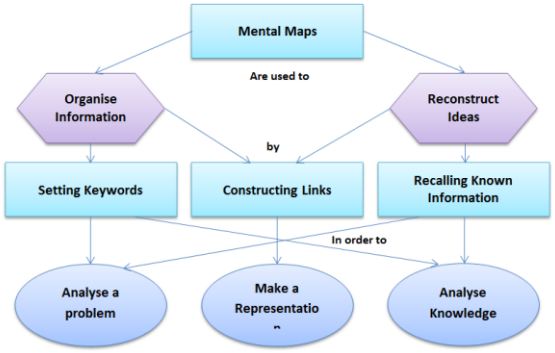
a) Konsep atau teori

Konsep atau teori merupakan *tools* atau alat yang harus di identifikasi. Identifikasi atau pemetaan konsep merupakan alat yang dapat digunakan untuk proses pembelajaran (Cicognani, 2000). Dalam aplikasinya pada arsitektur keamanan e-Business, pemetaan konsep diarahkan pada pembelajaran terhadap ancaman keamanan yang timbul di masa lalu, masa kini dan untuk memprediksikan ancaman di masa mendatang. Selain itu pemetaan konsep juga telah lama diaplikasikan sebagai tool untuk bidang lainnya misalkan pemetaan konsep untuk pengajaran guru-guru dalam peningkatan kewaspadaan mereka pada murid yang diajarnya (Hedberg dan Harper, 1998) dan sebagainya. Sebagai contoh pemetaan konsep divisualisasikan dalam gambar 4 berikut ini (Cicognani, 2000).



Gambar 4. Contoh visualisasi pemetaan konsep.

Didalam pemetaan konsep, tidak hanya berbentuk kata-kata yang terhubung dengan garis/link melainkan dapat juga berbentuk flowchart dimana setiap konsep disusun dalam tingkatan hierarki (Kelly dan Odom, 1997), seperti pada gambar 5 berikut ini (Cicognani, 2000).



Gambar 5. Pemetaan konsep digambarkan dalam bentuk flow chart.

Cicognoni juga berpendapat bahwa dibalik pemetaan konsep ini, dapat diperoleh representasi visual dari informasi yang telah berhasil dirangkum.

b) Perangkat Lunak

Perangkat lunak sebagai tool dalam memberikan pertahanan keamanan pada sistem komputer adalah bukan merupakan issue yang baru di masa ini. Berbagai aplikasi perangkat lunak seperti antivirus, firewall, anti spam dan sebagainya telah banyak beredar di dunia maya.

Tujuan dari melakukan identifikasi atas perangkat lunak pada layer *tool identification* ini adalah untuk menemukan perangkat lunak yang dianggap sesuai sebagai solusi berbentuk tool yang kedepannya akan dimanfaatkan untuk menangkal dan menganalisa ancaman-ancaman keamanan yang timbul mengancam infrastruktur e-Business yang tidak dapat diperkirakan kapan munculnya, bagaimana cara menyerangannya dan komponen atau bagian apa yang akan diserang.

c) Perangkat Keras

Selain tool perangkat lunak, ada pula tool yang berwujud perangkat keras (*hardware*). Khusus untuk tool seperti ini, biasanya memiliki harga yang tidak murah. Pemilik sistem kadang mengabaikan pengadaan perangkat ini dikarenakan perangkat lunak untuk keamanan sistem telah dirasa cukup. Alasan lain yang sering dikemukakan adalah karena demi mendapatkan keuntungan, pengeluaran berlebih atas pembelian perangkat keras yang mungkin beberapa fungsinya telah cukup digantikan oleh perangkat lunak yang lebih murah menjadi dibatasi atau ditiadakan.

Perlu disadari, pc atau perangkat yang di pasang piranti lunak keamanan kadang kala kurang optimal dalam menjalankan fungsinya. Karena sering pula, pc tersebut dipakai bersama / dioperasikan dengan piranti lunak lainnya. Penurunan performa dapat terjadi oleh karena penyebab yang telah disebutkan diatas. Melalui perangkat keras yang secara khusus didekasikan untuk menjaga keamanan sistem, hal ini dapat menjadi solusi yang lebih baik. Untuk menghindari pengeluaran yang tidak perlu atau tidak sesuai dengan tujuan keamanan sistem komputasi e-Business, maka diperlukan identifikasi perangkat keras apa yang sesuai untuk menangkal dari ancaman keamanan yang diperkirakan mungkin akan muncul.

d) Prosedur dan Aturan

Prosedur atau aturan atau *policy* merupakan satu hal yang pada hakekatnya adalah sama. Aturan-aturan yang berlaku perlu di identifikasi untuk melihat aturan mana yang lemah yang dapat membuka celah keamanan sehingga perlu diperbaiki dan bahkan bila perlu dihilangkan, atau aturan mana yang mendukung proses pengamanan e-Business. Contoh dari prosedur atau aturan, misalnya penggunaan gabungan angka, huruf dan karakter khusus dalam membuat password, ukuran password yang harus lebih dari 8 karakter dan sebagainya.

Melalui penambahan *tool identification* ini kedalam 3 (tiga) layer pendekatan penjabaran perencanaan identifikasi keamanan, diharapkan langkah perencanaan menjadi lebih siap dengan cakupan yang luas dan lebih tepat sasaran.

6.4 Pendekatan *Action Planning*

Selanjutnya dalam pendekatan ketiga yakni melalui proses *action planning.* Berkaca pada resiko yang telah diidentifikasi, dapat ditentukan rencana tindakan yang akan dilakukan. Masing-masing resiko dianalisa dan direncanakan tindakan pencegahannya. Sebagai contoh, untuk mencegah resiko akses yang tidak sesuai terhadap resource atau aset e-Business, dapat dilakukan proses autentikasi jati diri pengakses dan sebagainya. Selanjutnya, setiap tindakan yang direncanakan untuk dijalankan, haruslah melalui tahap pengujian terlebih dahulu sehingga rencana yang disusun menjadi lebih matang untuk dilaksanakan dan peluang terjadinya kesalahan dalam penerapan rencana menjadi lebih sedikit karena kerena tiap rencana tindakan yang akan dilakukan telah dibuktikan hasilnya.

7. KESIMPULAN

Penjabaran proses perencanaan identifikasi keamanan melalui pendekatan 4 (empat) layer identifikasi yakni layer *tool identification* yang digabungkan bersama *aset identification*, *risk identification*, *tool identification* dan *action planning*, membuat cakupan proses identifikasi menjadi lebih luas, lengkap dan lebih detail. Proses identifikasi pun lebih terarah dan tepat sasaran. Output dari proses identifikasi yang dilakukan dengan empat pendekatan tersebut menjadi lebih siap untuk masuk ke tahap selanjutnya yaitu dalam tahap *evaluate risk* sebagai bagian dari 10 tahapan strategi manajemen keamanan e-Business.

PUSTAKA

Combe, C. (2006). *Introduction to E-Business Management and Strategy*. Butterworth-Heinemann is an imprint of Elsevier.

Chaffey, D. (2009). *E-Business and E-Commerce Management Strategy Implemetation and Practice*. Pretince Hall.

Cicognani, A. (2000). *Concept Mapping as a Collaborative Tool for Enhanced Online Learning.* Educational Technology & Society 3(3) 2000, ISSN 1436-4522.

Hedberg, F. B., Harper, B. (1998). *How do preservice teachers use concept maps to organize their curriculum content knowledge?*. Working Document.

Kelly, P., Odom, L. (1997). *The union of concept mapping and the learning cycle for meaningful learning: Diffusion and osmosis*. National Science Teachers Association – National Convention Converence Proceedings, New Orleans, Louisiana

Karmakar, N. (2003). *Digital Security, Privacy and Law in Cyberspace: A Global Overview. In Proceedings of the International Association for the Development of Information Systems (IADIS)*, Lisbon, Portugal, 3–6 June, pp. 528–36.

Minoli, D. and Minoli, E. (1998). Web Commerce Technology Handbook. McGraw-Hill: Maidenhead.

Vasilyevna, B. N. (2008). *Security Design for E-Business Applications*. International Symposium on Ubiquitous Multimedia Computing.

Tyagi, N.K., Srinivasan, S. (2011). *Ten-Stage Security Management Strategy Model for The Impacts of Security Threat on e-Business.* International Journal of Computer Application (0975-8887), Vol 21 – No.5.