1. O PROBLEMA

A consolidação da internet como canal de comunicação, trabalho e entretenimento trouxe à tona um problema que vinha sendo posto como de baixa prioridade por empresas e indivíduos. Quanto mais as empresas se expõem à internet, tornando o acesso às informações disponível 24 horas por dia, 7 dias por semana, mais vulneráveis podem se tornar, correndo o risco de que dados confidenciais venham a ser obtidos, alterados ou excluídos por pessoas não autorizadas.

O crescente uso da internet como canal de negócios no mercado brasileiro pode ser avaliado por meio de uma pesquisa divulgada pela FGV (IDG, 2003). A pesquisa mostra que o comércio eletrônico entre empresas (B2B) e para consumidores finais (B2C) cresceu, no cenário mais conservador, 105% de 2001 para 2002. As transações B2B atingiram algo entre 5,6 e 5,8 bilhões de dólares em 2002 contra algo entre 2,6 e 2,8 bilhões de dólares em 2001. Já as transações B2C atingiram valores entre 1,8 e 2,0 bilhões de dólares em 2002 contra 800 milhões de dólares em 2001. Somando-se os valores apresentados, o comércio eletrônico brasileiro atingiu cifras entre 7,4 bilhões e 7,8 bilhões de dólares em 2002.

É importante ressaltar que a mesma tecnologia que revolucionou as comunicações - estreitando laços entre empresas e aproximando pessoas em todo o mundo - também pode ser utilizada para fins pouco éticos. Apesar de todo o avanço tecnológico, o ser humano ainda desempenha papel fundamental na determinação do uso da tecnologia para gerar bem-estar social.

Também vale assinalar, conforme Neto (2002) apontou, que a informação não passa somente pela internet, mas pode estar presente impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de outros meios de comunicação, mostrada em filmes e falada em conversas. Seja qual for a forma apresentada, ela deve contar com a proteção necessária.

1.1. Introdução

A segurança da informação (SI) é uma área nova dentro do ainda jovem setor da tecnologia da informação. Todos os dias, diversos sistemas são invadidos, muitas pessoas são vítimas de vírus, os mais variados dados são obtidos ilegalmente e muitas empresas ficam de uma hora para outra sem poder operar normalmente. A SI se ocupa exatamente da proteção dos recursos de informação de empresas e indivíduos.

Uma pesquisa do CERT (2002) ilustra a crescente preocupação com as invasões digitais. Segundo o estudo, de janeiro a setembro de 2002 foram registrados cerca de 70 mil ataques no mundo[1]. Em 2001, o total de ataques ficou em cerca de 53 mil.

Nos Estados Unidos, onde as empresas em geral possuem maior preocupação com questões relativas à SI, uma pesquisa recente do Forester Research (IBM, 2002) revelou que 91% das organizações americanas detectaram brechas na segurança de suas empresas nos últimos 12 meses.

Devido aos sérios danos causados pelo descuido na proteção de dados confidenciais, a segurança da informação tem também recebido crescente atenção dos governos no mundo inteiro[2]. O governo americano gastou cerca de US$ 1,2 bilhão com a proteção de seus dados em 2002. A previsão para 2003 é que sejam gastos cerca de US$ 1,7 bilhão. Já a União Européia oficializou a criação da Agência Européia de Segurança da Informação e Redes que começará suas atividades em janeiro de 2004 com orçamento inicial de aproximadamente US$ 125 milhões.

Todos esses dados demonstram um mercado enorme a ser explorado. Segundo informa a International Data Corp. (IDG, 2003), o mercado de segurança da informação terá vendas de US$ 45 bilhões em 2006 contra US$ 17 bilhões em 2001, sendo que o segmento de serviços deve crescer anualmente 24%, enquanto a venda de software terá expansão de 16%, entre 2001 e 2006.

[1] O CERT define "ataques" como tentativas (frustradas ou não) de entrar em locais não autorizados.

[2] Para referências sobre decretos emitidos pelo governo brasileiro sobre o assunto, ver Federal (2000, 2001 e 2002).

Esse crescimento tem aumentado consideravelmente a demanda por profissionais especializados, justificando, inclusive, o surgimento de uma nova posição em diversas empresas, o CSO (*chief security officer*), responsável pela gerência da área de SI.

Dentre os diversos assuntos abrangidos pela segurança da informação, o plano de continuidade de negócios (PCN), que descreve os procedimentos que visam a assegurar a continuidade das atividades em caso de incidentes, é o objeto de estudo deste trabalho. Antes confinado à literatura especializada, o PCN ganhou projeção na mídia a partir de setembro de 2001, quando o mundo assistiu perplexo a queda das torres do World Trade Center.

No dia seguinte a esse trágico evento, milhares de funcionários não tinham a onde ir trabalhar e dezenas de empresas ficaram sem seus sistemas e dados mais importantes. Ao prejuízo financeiro vem se somar a perda de vidas, processos, procedimentos, informações e tudo mais que estava em formato digital. Apenas quem investiu na continuidade de seus negócios, como o Deutsch Bank (Pritchard, 2003), pôde restabelecer suas operações em pouco tempo.

Embora eventos dessa natureza sejam raros, pequenos incidentes podem trazer grandes transtornos para as empresas. Um banco, por exemplo, depende inteiramente de seus sistemas de informação. Se algum acontecimento interrompe o funcionamento de um dos sistemas, seja um defeito de programação, uma queda de luz ou uma sobrecarga do servidor, a instituição pode perder informações sobre as movimentações financeiras realizadas pelos seus clientes naquele período de tempo. Assim, pequenos incidentes podem ocasionar sérias conseqüências. Portanto, os PCNs não se aplicam somente a eventos catastróficos, mas também a situações comuns do dia-a-dia.

O plano de continuidade de negócios tem como objetivo principal evitar, ou reduzir sensivelmente, as perdas das empresas em casos de incidentes que afetem suas operações, além de restaurar suas atividades no espaço de tempo mais breve possível.

Ao longo desse estudo, propõe-se responder às seguintes perguntas:

a. As empresas brasileiras estão elaborando planos eficazes de continuidade de negócios?

b. Como estes planos podem ser aprimorados para tornar as empresas menos vulneráveis a novas e potenciais ameaças?

1.2. Objetivo final

O objetivo final do projeto é estabelecer o retrato atual dos planos de continuidade de negócios das empresas brasileiras e propor sugestões para torná-las menos vulneráveis às ameaças internas e externas, sejam novas, antigas ou potenciais.

1.2.1. Objetivos intermediários

Os objetivos intermediários são formulados pelas seguintes perguntas:

a. Qual é a importância do tema continuidade de negócios para as empresas brasileiras?

b. Qual é o investimento realizado pelas empresas na continuidade de seus negócios?

c. Qual é a tendência de variação dos orçamentos das empresas reservados para a continuidade do negócio?

d. Como as empresas que elaboram o PCN mantêm o plano atualizado?

e. Qual é a abrangência do PCN, considerando a equipe de TI, demais funcionários, fornecedores, clientes, terceiros e serviços públicos?

f. Como é o treinamento dos funcionários dentro das diretrizes do PCN?

1.3. Delimitação do estudo

O estudo em questão tem como foco identificar a observância de um plano de continuidade de negócios em diversas empresas operando no Brasil e reportar falhas em sua utilização, de modo a servir de alerta para um problema crucial que não tem recebido a devida prioridade.

O período escolhido para análise dos dados de investimentos e dos incidentes de segurança ficou limitado ao triênio 2001-2003.

O estudo foi realizado com mais de 100 empresas representativas de diferentes indústrias, que demonstraram interesse em participar da pesquisa, escolhidas conforme critérios explicados no Capítulo 3.

1.4. Relevância do estudo

Hoje em dia, os sistemas, as pessoas e as empresas estão interconectados como nunca antes estiveram, revolucionando a forma como os governos provêem serviços, como as empresas fazem negócios e como as pessoas se comunicam (OECD, 2002).

A integração da economia por meio de processos eletrônicos desencadeou uma intensa troca de informações sem barreiras que ultrapassa fronteiras nacionais, disponibilizando um volume imenso de dados e expandindo conhecimentos através de uma complexa teia de redes de computador.

O grande problema que a interconectividade traz é a exposição ao mundo exterior de dados internos sensíveis. A informação é um ativo valioso para as organizações, necessitando ser adequadamente protegida (Neto, 2002).

Dentro desse contexto, a SI surgiu para proteger os recursos de informação de organizações e pessoas, minimizando possíveis danos aos negócios. É importante frisar que os recursos não podem ser simplesmente ocultos, porque, conforme Schneier (1996) observou, obscuridade não é segurança.[3]

Entre os assuntos estudados pela segurança da informação, a disponibilidade dos serviços prestados por sistemas e empresas é um dos mais importantes.

[3] Ocultar uma senha dentro de um cofre que, por sua vez, é deixado em algum apartamento na cidade do Rio de Janeiro não significa que a senha esteja em segurança. Ela está apenas oculta. Para maior aprofundamento no assunto, ver referência Schneier (1996).

Garantir a disponibilidade de serviços e a retomada de atividades em caso de interrupção é o escopo dos planos de continuidade de negócios.

A relevância do estudo em questão pode ser determinada, examinando-se as possíveis conseqüências de eventos que interrompem as atividades de empresas que não possuem um PCN: perdas tangíveis e intangíveis enormes ou mesmo a falência da empresa. Dentre as prováveis perdas, podem ser citadas: de mercado, de imagem, de competitividade, de faturamento, de credibilidade e de funcionários.

Segundo Goldani (2001), problemas de pequeno porte, causadores de paralisações, refletem os prejuízos menos importantes, e, por isso, são perceptíveis quase que imediatamente. Outros, normalmente os de grande proporção, somente são passíveis de serem mensurados posteriormente à ocorrência, quando já se apresentam difíceis, ou mesmo impossíveis, de serem eficazmente reparados.

Apesar de possíveis conseqüências de grande impacto nos negócios, uma pesquisa divulgada pelo Gartner Group (IDG, 2002) revela que 80% das corporações em todo o mundo não possuem planos de continuidade de negócios. Somando-se a isso, de acordo com Greg Valdez, Vice-Presidente da Veritas, empresa especializada em prevenção de desastres em TI, 40% das empresas que passaram por desastres tiveram que fechar as portas em menos de cinco anos (IDG, 2002).

Um levantamento (Galvão, 2002) conduzido em 2002 pelo FBI, baseado nas respostas de 503 profissionais que atuam em segurança da informação em grandes corporações americanas, agências do governo, instituições financeiras e universidades, traz alguns dados importantes:

a. 90% dos que responderam ao questionário detectaram incidentes de segurança nos últimos 12 meses.

b. 80% reconheceram perdas financeiras como conseqüência destes incidentes.

c. 42% (223 entrevistados) foram capazes de quantificar estas perdas financeiras, tendo reportado perdas superiores a U$ 455.848.000.

d. 34% denunciaram as tentativas de ataque sofridas para as agências legais (na primeira pesquisa realizada em 1996, apenas 16% reconheceram ter divulgado as tentativas de ataque sofridas).

e. 85% tiveram problemas com infecções de seus sistemas por vírus de computador.

As estatísticas apresentadas demonstram o despreparo das organizações em garantir a continuidade de seus negócios, bem como a dificuldade em se apurar incidentes não divulgados.

A cultura característica do nosso país também não ajuda. Lopes (2000) cita a cultura cordial e hospitaleira dos brasileiros como um agravante no que diz respeito à segurança das informações nas empresas operando no país. O pensamento "isso nunca vai acontecer com a gente" é, por si só, uma ameaça à sobrevivência das empresas.

Procurando atacar esse problema de frente, a OECD (2002) sugere o desenvolvimento de uma cultura de segurança que seja assimilada por todos os funcionários. A nova cultura de segurança não pode ser somente meros sistemas de controle de acesso (McLean 1994; Coltro, 2000), mas deve, sim, promover a adoção de uma nova forma de usar e interagir com os sistemas de informação.

Mesmo utilizando todos os recursos tecnológicos, humanos e financeiros disponíveis, conforme a norma N3017 (ISO, 2002) esclarece, nenhum tipo de equipamento ou medida de segurança é capaz de oferecer proteção total contra todos os incidentes. Riscos residuais sempre vão existir. Portanto, qualquer empresa que esteja seriamente preocupada com segurança deve possuir um planejamento de SI adequado.

Para encerrar essa sessão, vamos recorrer a Porter (1992) que afirma que a estratégia de tecnologia é essencial para a estratégia competitiva geral das empresas. A segurança da informação, como parte integrante da tecnologia da informação, deve ser também encarada como estratégica para empresas de todos os setores e portes.