5. DISCUSSÃO

Neste capítulo, são discutidos os resultados apresentados no capítulo anterior, bem como são resgatados os objetivos traçados para este estudo, de forma a se poder avaliar se foram adequadamente atingidos. Além disso, serão fornecidas contribuições, a fim de que as empresas possam melhorar a prevenção à continuidade de seus negócios.

Relevância

Há uma tendência, por certo natural, dos executivos afirmarem que a continuidade de seus negócios é assunto primordial para suas respectivas empresas. Isso se reflete nos resultados obtidos para as afirmações de que SI e PCN são importantes para a diretoria da empresa. O estudo fornece assim subsídios para atingir o primeiro objetivo intermediário, **a** - Qual é a importância do tema continuidade de negócios para as empresas brasileiras?

No caso da segurança da informação, devido a uma maior maturidade do tema – principalmente por causa das intensas atividades de vírus eletrônico e de roubos de números de cartões de crédito por hackers nos últimos tempos – já existe uma maior conscientização de sua importância. Por isso, o número de 66% dos respondentes, que concordam ou concordam totalmente com a afirmação, já era esperado. Outro fato positivo é que nenhum discordou. Não obstante, 34% das empresas ainda não se convenceram da relevância da SI, o que é preocupante.

Já no caso do plano de continuidade de negócios, por ser um tema muito recente, ainda há falta de informação sobre o assunto. Já era esperado que o número de empresas que consideram PCN importante seria menor do que as que consideram SI importante. De fato, apenas 41% dos respondentes assinalaram que concordam ou concordam totalmente com a afirmação.

Pelo mesmo motivo, não é uma grande surpresa que somente 21% das empresas possuam um plano de continuidade de negócios. Como já assinalado no capítulo anterior, existe uma discrepância nesses números, uma vez que das empresas que afirmam ser a continuidade dos negócios importante, apenas a metade possui efetivamente um PCN. Ou seja, o apoio teórico não está se refletindo na prática.

A conscientização é a chave para reverter esse quadro. O apoio pela priorização do tema deve começar pela direção da empresa e ser disseminada por todos os funcionários. Isso, porque pode acontecer que a alta direção apóie firmemente a continuidade dos negócios, mas os funcionários apresentem reações adversas, quando da implantação dos procedimentos contidos no PCN. Infelizmente, esse processo de conscientização é lento e gradual, mas deve ser com urgência acelerado.

Não é possível fazer comparações temporais, já que este tipo de estudo ainda é incipiente. Contudo, espera-se que ao longo dos próximos anos, os percentuais de empresas que consideram SI e PCN temas de crucial relevância aumentem consideravelmente.

Investimento

É recorrente a reclamação de que os custos de segurança da informação são muito elevados, mas também é possível observar que o orçamento reservado para SI é baixo. Este resultado contribui para atingir os objetivos **b** e **c**, ou seja, respondendo às perguntas: Qual é o investimento realizado pelas empresas na continuidade de seus negócios? Qual é a tendência de variação dos orçamentos das empresas reservados para a continuidade do negócio?

Conforme obtido na pesquisa, dois terços das empresas reservam menos de 1% de seu orçamento para SI e quase nove em 10 reservam menos de 1% para PCN. Isso sugere que os recursos destinados especificamente para a prevenção de incidentes de segurança são ainda muito tímidos.

De fato, uma empresa que queira montar um segundo escritório que sirva de contingência para o caso do primeiro ficar interditado, gastará uma grande quantia. Entretanto, o PCN não envolve apenas grandes gastos, mas, principalmente, contém uma série de procedimentos que visam a oferecer melhor prevenção contra interrupções nas atividades operacionais.

É verdade que existe uma grande dificuldade de se medir o retorno sobre o investimento realizado em segurança. Reforça-se que a segurança da informação não pode ser vista simplesmente como um investimento que deve dar retorno

financeiro, mas, sim, como um seguro que a empresa deve arcar para garantir sua própria sobrevivência.

Em relação à tendência de variação do orçamento, é grave apurar que quase três quartos vão manter os recursos atuais em SI e quase 9 em 10 manterão, em PCN. Ou seja, não estão previstos maiores aportes de recursos para 2004. Vale notar que, como já citado anteriormente, dois terços das empresas consideram segurança da informação muito importante para seus negócios, porém são poucas as que vão aumentar os recursos financeiros destinados a SI.

Atualização

A atualização do plano de continuidade de negócios é essencial para preservar a eficácia do mesmo. O dinamismo verificado nos negócios, hoje em dia, propicia o aparecimento contínuo de novos riscos, os quais devem ser devidamente contemplados no plano. Estes resultados fornecem subsídios para responder as perguntas, referentes aos objetivos **d** e **e** – Como as empresas que elaboram o PCN mantêm o plano atualizado? Qual é a abrangência do PCN, considerando a equipe de TI, demais funcionários, fornecedores, clientes, terceiros e serviços públicos?

Aqui aparece o primeiro resultado positivo da pesquisa. 83% das empresas que possuem PCN revisam o plano uma ou mais vezes por ano. Isso demonstra uma grande conscientização dessas empresas em se manterem precavidas contra os incidentes que possam vir a acontecer.

O mesmo percentual se obteve para a freqüência de simulação maior ou igual a um dos procedimentos contidos no PCN. Ou seja, as empresas estão corretamente realizando simulações, testando os resultados obtidos e revendo os procedimentos que necessitam serem alterados.

Apesar disso, dois resultados obtidos preocupam. As revisões e simulações são ótimas para testar os procedimentos do plano e verificar se continuam eficazes. Contudo, não são suficientes para detectar novos riscos. Para isso, é imprescindível realizar periodicamente uma análise de riscos e uma análise de impacto nos negócios. Nesse ponto é que as empresas ainda estão aquém do ideal. Apenas 13% delas realizaram uma AR nos últimos 12 meses e 12%, uma análise de impacto nos negócios nesse mesmo período.

Outro resultado que traz apreensão é que a abrangência dos envolvidos nas simulações dos procedimentos está muita restrita. Por exemplo, somente 38% das empresas envolveram todos os funcionários e apenas 5% envolveram os serviços públicos. Restrições orçamentárias e o desconhecimento da importância da abrangência das simulações são as causas mais prováveis dessa situação. Contudo, as empresas devem se conscientizar que, como não vivem isoladas, os incidentes que as afetam podem se disseminar para seus fornecedores, parceiros e clientes, e vice-versa. Portanto, as simulações devem passar a envolver todos os elos da cadeia.

Treinamento

É necessário que as empresas ofereçam treinamento direcionado para segurança da informação e continuidade de negócios. O treinamento pode ser em forma de simulações, como já explorado previamente, de palestras, seminários, por meio de textos enviados para os funcionários, entre outras. Ele deve ser mais específico para a área da empresa que cuida de segurança e mais genérico para o resto dos funcionários. Estes resultados contribuem para atingir o último objetivo intermediário da pesquisa, **f** – Como é o treinamento dos funcionários dentro das diretrizes do PCN?

Três quartos das empresas disseram que treinam sua equipe de TI em segurança da informação com freqüência igual ou maior do que um. Não entrando no mérito da qualidade desse treinamento – que não estava no escopo do estudo –, o percentual é surpreendentemente grande. Infelizmente, o quadro não é tão favorável em relação ao treinamento para todos os outros funcionários. Apenas um terço treina seus funcionários das outras áreas em segurança da informação uma ou mais vezes por ano. Novamente, restrições orçamentárias e a falta de conhecimento da importância do treinamento de todos os funcionários são as causas mais prováveis de terem gerado essa situação.

O mesmo fenômeno ocorre em relação ao treinamento em PCN. Das empresas que possuem PCN, a grande maioria (83%) treina sua equipe de TI com freqüência igual ou maior do que um. Esse é mais um percentual alto obtido na pesquisa. Esse dado reforça a tese de que as empresas que investem em continuidade de negócios estão muito conscientes da importância do tema e da

responsabilidade da equipe de TI em prevenir os incidentes de segurança. No entanto, o treinamento dos funcionários de outras áreas novamente deixa a desejar, pois somente pouco mais de um terço das empresas treinam todos os seus funcionários uma ou mais vezes por ano.

Apesar do grande número de empresas que realizam treinamentos em SI e PCN, elas ainda não estão totalmente satisfeitas com os resultados obtidos. Um pouco mais da metade das empresas não acreditam que a equipe de TI não está bem preparada para agir em casos de incidentes e quase três quartos delas não acreditam que todos seus funcionários estejam bem preparados. Se por um lado os percentuais preocupam por serem altos, por outro eles demonstram que as empresas estão conscientes das limitações de seus funcionários para prevenir e atuar em eventos de interrupção de atividades.

Uma alternativa que algumas empresas têm empregado para contornar esse problema é a criação de comitês especializados em continuidade de negócios, envolvendo membros de diversas áreas. Esses comitês são responsáveis por manter o PCN, disseminar conhecimentos de segurança para todos os funcionários e assegurar o cumprimento das diretrizes da diretoria em relação à prevenção de incidentes.