SEGURANÇA DA INFORMAÇÃO – CUSTO OU INVESTIMENTO?

Ao participar de congressos, palestras e eventos relacionados à Tecnologia da Informação, é muito comum participantes mencionarem a seguinte questão: "tratando-se de segurança da informação, estamos sempre a um passo atrás...". À primeira vista, tal afirmação conduz profissionais a acreditarem que não há como resolver o impasse. Talvez seja difícil, mas há maneiras de minimizá-lo.

Pensando nisso, este artigo tem como função elencar alguns pontos que podem transformar ideias em iniciativas. Primeiramente, é imprescindível que o leitor entenda que a sociedade contemporânea apresenta um perfil diferenciado, o qual reflete na economia, na política, no direito e nas demais áreas.

É fato que, nos dias atuais, a tecnologia está intrínseca às relações pessoais e comerciais, influenciando diretamente na atividade de profissionais, consumidores e investidores. O dinamismo trazido pela internet norteia o estilo de negócio e a forma de escolha de produtos e serviços.

Partindo dessa premissa, cabe a reflexão: qual o poder da internet sobre a atividade de uma empresa, bem como o relacionamento com o cliente? Qual a ligação com a segurança da informação (SI)? Por que investir em SI? Quais as consequências de um incidente envolvendo ataques cibernéticos e vazamento de dados para a marca de uma empresa? Por fim, como prevenir tais infortúnios?

I – O Poder Influenciador da Internet

A internet exerce um papel influenciador sobre o consumidor, modificando, por conseguinte, o modelo de negócio de diversas empresas. Por exemplo, cita-se o caso da Casa Berti, fundada em 1976, empresa do setor atacadista, que se iniciou com um estabelecimento físico, o qual deu origem à Distribuidora de Bebidas Berti Ltda., devido à grande demanda. Em 2007, lançou sua loja virtual, passando do marketing "boca a boca" para o alcance expressivo da internet.[1] Adicionou-se um toque de tecnologia no seu perfil de negócio e obteve um resultado gratificante.

Conforme pesquisa realizada pela Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (Fecomércio), em parceria com a e-bit, o comércio eletrônico no Brasil faturou aproximadamente

---

Turchi, Sandra R. Estratégias de Marketing Digital e E-commerce – São Paulo : Atlas, 2012 - p. 50/51

R$ 15 bilhões, no período de janeiro a julho de 2010, superando o total de vendas dos shopping centers da Grande São Paulo, o qual apresentou o montante de R$ 7,2 bilhões no mesmo período.[2]

Destaca-se que o consumidor está conectado a todo o momento, seja através do computador, notebook, *tablet* ou celular. O que antes era feito pessoalmente, pode ser realizado pela internet, como pagamento de contas, compra de produtos, contratar serviços, etc.

Por consequência, a quantidade de informações indexadas na rede mundial é imensurável. Maior número de pessoas se adequando a essa nova realidade e diversas empresas modificando seus negócios a fim de atingir esse novo perfil de consumidor. Portanto, neste vasto mundo da internet, pode-se encontrar todo e qualquer tipo de informação, tanto de pessoas físicas quanto de jurídicas.

O fato central é que, com o desenvolver das tecnologias, as pessoas passaram a buscar informações; procuram críticas (positivas ou negativas) antes de comprar algum produto ou serviço. Para tanto, utilizam-se de buscadores, nos quais 75% da população creditam confiança nos resultados obtidos nas primeiras páginas de busca.[3]

Esta credibilidade nos sites de busca é tão expressiva que empresas têm investido milhões em marketing digital, com o objetivo de fortalecer sua marca e seu relacionamento com o cliente, de modo a aparecer na primeira página do buscador com notícias e críticas positivas.

Não obstante, já existem profissionais especializados em tentar recuperar a boa reputação de pessoas físicas ou jurídicas, tendo em vista a influência que a internet exerce sobre os consumidores. Cita-se como exemplo dessas empresas, a "*Reputation Defender*". Sendo assim, claro está o poder influenciador da internet sobre as relações pessoais e comerciais.

II – Segurança da Informação nas Empresas

Partindo dessa breve explanação sobre o poder influenciador da internet sobre as relações comerciais, é de suma importância que diretores e gestores comecem a entender a dinâmica instaurada por essa nova era.

Turchi, Sandra R. Estratégias de Marketing Digital e E-commerce – São Paulo : Atlas, 2012 - p. 50

Turchi, Sandra R. Estratégias de Marketing Digital e E-commerce – São Paulo : Atlas, 2012 - p. 72

Primeiramente, deve-se refletir sobre a estrutura atual da empresa: quais as ferramentas utilizadas pelos funcionários e colaboradores: computadores, notebooks, tablets, smartphones? Essas ferramentas são disponibilizadas pela empresa ou são dos próprios usuários? Há uma tendência para o trabalho *home-office* ou externo, por exemplo, em clientes? Onde são armazenadas as informações: servidores, *cloud computing*? As áreas de Tecnologia da Informação, Jurídico, Recursos Humanos e Administrativo/Financeiro estão interligadas? Como é o processo de desligamento de funcionários? Houve um projeto de gestão da informação, ou seja, ao implementar algum sistema de informação, foi realizado um projeto com pesquisas de softwares, licenças, treinamentos de usuários? Há políticas e normas internas sobre uso de redes sociais, acesso a diversos sites, uso de e-mail pessoal, dispositivos móveis, aparelhos pessoais, bem como termo de confidencialidade? Há treinamentos e programas de conscientização de funcionários e colaboradores para o uso ético e legal das ferramentas disponibilizadas e sigilo das informações?

A princípio, parecem questões que não se interligam. Contudo, é essencial que a diretoria esteja atenta a esses pontos, pois podem afetar diretamente na parte financeira, jurídica e de marketing da empresa. Faz-se necessário uma avaliação fria do mecanismo que os departamentos adotam: como os procedimentos são realizados no dia a dia, na prática, e não na teoria?

A segurança deve ser de toda a informação da empresa, desde dados constitutivos, balancetes, relatórios, vendas, orçamentos, propriedade intelectual, tecnologia, lançamento de produtos, até registros e dados pessoais de funcionários, colaboradores e terceirizados; bem como, eventuais dados de clientes, fornecedores e parceiros.

Conjuntamente com os bens corpóreos ou materiais de um estabelecimento comercial (mercadorias, máquinas, veículos, etc.), os bens incorpóreos ou imateriais (marca, patente, nome empresarial, desenho industrial, dentre outros) formam o ativo de uma empresa. Contudo, estes últimos têm obtido maior relevância no cenário atual, pois estes bens individualizam e identificam a pessoa jurídica junto ao mercado e, principalmente, perante o consumidor, somando valores inestimáveis.

Desta feita, a segurança da informação deve ser implementada por toda a empresa. É um processo que se inicia dentro dos diversos departamentos, atingindo, consequentemente, o consumidor e, inclusive, investidores, que verão a empresa com bons olhos.

III – Por que investir em Segurança da Informação?

Investir em segurança da informação é investir na marca, no diferencial que a empresa representa para o mercado, na credibilidade e segurança para outros investidores, clientes e parceiros.

De acordo com um estudo realizado pela HBGary, divulgado em março deste ano, no qual participaram 405 investidores, verificou-se que 69% dificilmente investiriam em uma empresa com histórico de um ou mais casos envolvendo violação de dados.[4]

Trata-se, pois, de uma questão de credibilidade e segurança que a empresa passará para aqueles que investirão. Qual a garantia de que os dados não serão violados a ponto de causar um desastre financeiro para a empresa, considerando os diversos casos de ciberataques? E se ocorrer um incidente, a empresa possui profissionais qualificados para identificar, cessar e impedir que o dano ocorra novamente?

Investir em segurança da informação vai além de criar um departamento de Tecnologia da Informação (TI). Para grandes corporações, é preciso criar uma equipe específica e responsável pelo departamento de Segurança da Informação, que por sua vez, difere da equipe de TI. É estruturar um ambiente e um grupo hábil para agir a qualquer momento. São pessoas especializadas que saberão erradicar o problema ou, no mínimo, amenizar os prejuízos.

Além disso, é instaurar políticas que designem métodos e procedimentos em casos de incidentes. É conscientizar funcionários e colaboradores de que todo e qualquer tipo de informação é importante, independentemente da função que exerça, de modo a ser imperioso que se atentem às normas internas.

É o conjunto de ações que se torna essencial para que a empresa funcione. Todos trabalham direta ou indiretamente com conteúdos confidenciais.

Investir em segurança da informação é assegurar aos seus clientes, parceiros e investidores que a empresa se preocupa com os dados aos quais tem acesso, seja de sua propriedade ou de terceiros em sua custódia, e que agirá da melhor forma possível para que incidentes não ocorram. Sobretudo, caso venham a ocorrer, assegurar que haverá uma equipe pronta e séria para erradicar o problema.

IV – Como prevenir?

Diante do cenário exposto, ideias podem já ter surgido. Sendo assim, é hora de colocá-las em prática! Vejamos algumas:

a. Analise como a empresa funciona diariamente. Desapegue-se da teoria, observe atentamente o que ocorre na prática: o que os funcionários e colaboradores usam? Os dispositivos utilizados são fornecidos pela empresa?

   Acredite, sempre terá alguém que levará trabalho para casa, utilizando-se, assim, dispositivos pessoais! Não obstante, com a "consumerização" da tecnologia, a sociedade como um todo vive

---

Notícia: "Histórico de ciberataques e violações de dados afasta investidores" veiculada em 11/03/2012, na página da Revista CIO – Disponível em: - Acessado em: 16/04/2013

em função de seus dispositivos. Estão sempre conectadas. Ao proibir acessos a sites, redes sociais, e-mails pessoais, lembre-se: podem acessar de seus próprios meios tecnológicos. Portanto, cuidado com as redes sem fio abertas!

b. Como são tratadas as informações confidenciais? Todos possuem acesso? Qual o procedimento de segurança desses conteúdos? Há um sistema de gestão da informação implementado? Gestores, funcionários e colaboradores sabem lidar com o mesmo?

   Quando da implementação de um sistema, imperioso elaborar um plano estratégico bem definido, ou seja, que haja uma gestão da informação com respaldo jurídico. Profissionais capacitados que percebam as necessidades da empresa e das equipes; licenças; contratos de serviços; manutenção e treinamento de funcionários e colaboradores para que o sistema seja devidamente implementado sem perda de informações e uso incorreto.

c. Há um departamento de TI e SI segmentados? Há profissionais qualificados e cursos de capacitação? A área é integrada com as demais? Há respaldo técnico-jurídico especializado para TI e SI?

   Em um mundo em que se exija tecnologia, o departamento de TI é fundamental e muitas empresas delegam a eles a responsabilidade de SI. Porém, a função da equipe de TI vai além de "apagar incêndios" ou auxiliar em uma manutenção de máquina, pode-se dizer que tem um papel estratégico e essencial seja qual for o ramo de negócio.

   Os profissionais desta área devem ser treinados e conscientizados sobre a importância de sua atividade dentro da empresa. São eles que serão responsáveis por identificar, conter e erradicar incidentes, bem como por recuperar o sistema e colocá-lo em funcionamento, quando não houver uma equipe de resposta a incidentes.

   Sobretudo, são essas equipes, seja de TI, SI ou Resposta a Incidentes, que geralmente têm acesso às diversas informações, inclusive as confidenciais. Sendo assim, os contratos de trabalho devem ser específicos e minuciosos, acrescentando cláusula de confidencialidade, horas, e recursos de trabalho, incluindo atenção à legislação que preceitua sobre trabalho remoto, vez que é comum o acesso remoto por tais equipes.

   Ademais, esta área deve estar integrada com as demais. Por exemplo, quando da demissão de um funcionário, o setor de Recursos Humanos (RH) deve avisar imediatamente a área de TI, com o intuito de limitarem e/ou extinguirem o acesso deste com o sistema da empresa.

Alerta: Symantec divulga pesquisa informando que 62% dos funcionários que deixaram ou foram demitidos nos últimos 12 meses ainda possuem informações confidenciais da empresa;

56% destes afirmam que pretendem utilizar esses dados em seus novos empregos; 44% dos entrevistados brasileiros entendem que esta ação não constitui crime.[5]

Por fim, é de suma importância que participem das decisões da empresa, pois é esta área que implementará, de uma forma ou de outra, aquilo que foi decidido. Portanto, a eles cabem opinar o que seria ou não viável e quais as dificuldades que a empresa enfrenta e/ou enfrentará diante das circunstâncias determinadas.

d. Diante do fenômeno do **BYOD – Bring Your Own Device** cujos funcionários levam seus próprios dispositivos para a empresa, também é preciso muita cautela e ações de prevenção conforme a seguir:

- Revisão dos contratos: como e quando foram elaborados os contratos de trabalho? Há cláusulas referentes às ferramentas tecnológicas e respectivas responsabilidades? Há cláusulas que envolvam propriedade intelectual e confidencialidade?

- Normas e políticas internas são imprescindíveis! Devem ser claras e objetivas. Todos os funcionários e colaboradores devem ter fácil acesso. É um meio de demonstrar boa-fé e, sobretudo, de obter alguma garantia para a empresa. É limitar as funções e poderes de todos os usuários de sistemas. O que pode e o que não pode ser acessado; redes sociais; regras sobre o uso de dispositivos móveis pessoais; informações confidenciais e responsabilizações.

Alerta: muitas vezes, em questões concernentes a processos trabalhistas, concorrência desleal e indenizações, podem servir como prova!

e. **Treinamento e conscientização**: tudo o que foi mencionado somente funcionará se houver um ambiente de colaboração. Todas as equipes devem estar cientes da importância de suas funções! Palestras e cursos dinâmicos devem ser realizados constantemente, a fim de alertar aos novos funcionários e, relembrar aos antigos, a relevância de seus atos e o motivo pelo qual deve se trabalhar preventivamente, ou seja, justificar a real necessidade da segurança da informação.

Manter um ambiente colaborativo não é fácil. Contudo, é possível, é preciso que os gestores estejam interessados em saber quais são as dificuldades enfrentadas, o que os funcionários acham sobre determinada decisão da empresa e, acima de tudo, deixar claro que as regras

Notícia "Maioria dos ex-funcionários leva dados da antiga empresa, diz pesquisa" veiculada no portal O Globo, em 19/03/2013 – Disponível em: – Acessado em: 16/04/2013

existem não apenas para proteger a pessoa jurídica, mas inclusive o próprio colaborador; demonstrar interesse por aqueles que estão ali diariamente cumprindo suas funções também é benéfico. Consequentemente, verificar-se-á que a empresa estará integrada e estimulada a cumprir seus deveres e obrigações.

V – Conclusão

É fato que o momento atual exige uma atenção especial às tecnologias. Modelos e procedimentos diários de negócios são modificados para expandir e fornecer produtos e serviços que atendam às necessidades dos consumidores.

Como toda boa inovação, há seus aspectos negativos, no caso, *malwares*, ataques cibernéticos, violação de dados confidenciais, dentre outros, os quais precisam ser ultrapassados para garantir aos usuários finais, investidores e parceiros certa estabilidade e credibilidade.

Implementar um projeto de segurança da informação é essencial para aqueles que visam expansão e reconhecimento de mercado. Para alguns, é um custo adicional. Para outros, investimento.

Para os que acreditam apenas em custos, cabe a reflexão sobre o que se pretende, qual a meta, sobretudo, entender que a empresa não está blindada para eventuais ataques. Esses podem acontecer com pequenas, médias e grandes empresas! Recentemente, grandes potências foram atacadas como New York Times, Twitter, Facebook, inclusive, a Apple. Outras, foram indiretamente, como a Netflix, que devido ao "maior ataque da história" teve seus serviços prejudicados.[6]

Por outro lado, para os que acreditam em investimento... Invistam! Não será a total certeza de que nunca serão atacados. Contudo, é a segurança de que haverá pessoas capacitadas para, no mínimo, amenizar os prejuízos. É investir na marca, na credibilidade perante o mercado. É comprometimento com consumidores, fornecedores, parceiros, empregados e investidores.

Este processo é longo e não acontecerá de um dia para o outro, mas é preciso ter um início, tudo tem seu começo.

Andréia Cristina dos Santos é advogada, formada pela Universidade Presbiteriana Mackenzie, finalizando curso de Pós-graduação em Direito Digital e das Telecomunicações junto à mesma instituição. Associada do escritório Cristina Sleiman Sociedade de Advogados.

Notícia "Maior ataque cibernético da história atinge internet em todo o mundo" veiculada no portal Uol Notícias, em 27/03/2013 – Disponível em: – Acessado em: 16/04/2013