RISCO CIBERNÉTICO

EM ALERTA MÁXIMO!

Como a sua empresa lida com a segurança da informação?

A ameaça cibernética é uma realidade no mercado e coloca em risco o que as instituições têm de mais valioso: a **informação**. A segurança da informação tornou-se um ponto crucial para a sobrevivência das instituições e esse assunto não deve ser tratado apenas do âmbito da Tecnologia da Informação (TI), mas através de uma governança corporativa consciente e responsável. Essa consciência tem que começar de cima, e o Conselho de Administração tem um papel importantíssimo a desempenhar neste combate, que deve ser atacado de forma sistêmica. É um trabalho educativo, de informação, conscientização e capacitação, que envolve mudar a cultura e a forma que a gestão é feita.

por **MONIQUE AZEREDO**

"Toda empresa é vulnerável, principalmente quando há dados digitais. Tem sempre alguém querendo entrar no seu sistema", ressalta **Jeffry Powell**, vice-presidente executivo da Diligent Boardbooks, empresa americana que oferece soluções de segurança na informação para Conselhos de Administração. Durante evento promovido pela Revista RI em parceria com a Diligent, Powell citou pesquisas que apontam que no ano passado 43% das empresas nos Estados Unidos tiveram os seus dados violados, e que a maior parte das violações é resultado de erro humano.

Ele destaca que apesar das empresas terem alguma tecnologia de proteção ou sistema antivírus, a maior parte delas não treina os seus funcionários quando o assunto é segurança da informação. "Tecnologia é importante, mas quem controla são as pessoas, e se elas não estiverem bem treinadas e conscientes do risco, fica uma porta aberta para a ação do hacker", afirma.

Powell cita várias técnicas, como o wi fi de um restaurante ser substituído pelo wi fi hackeado, possibilitando ao criminoso entrar no seu sistema. Outra maneira é o que ele chama de "fishing" que ocorre quando o usuário

JEFFRY POWELL, DILIGENT

PATRICIA PECK PINHEIRO,
PPP ADVOGADOS

> **Ao capacitar os seus colaboradores quanto a esses riscos, a empresa se blinda em eventuais incidentes porque pode comprovar que fez a sua parte nesse processo de educação.**

recebe um email do seu banco, por exemplo, solicitando digitar a sua senha. "Na verdade você nunca sabe o que o hacker vai fazer e a grande preocupação é que algumas empresas demoram meses até descobrirem que tiveram os seus dados violados", conta.

O vice-presidente da Diligent ainda revela que 27% das empresas americanas não contam com um plano de resposta à violação de dados. Quando perguntadas se estão confiantes de que o Conselho da sua instituição adota medidas preventivas contra o risco cibernético, 63% responderam "um pouco", 23% disseram "não estar confiantes" e apenas 15% que "sim".

Para Powell, é fundamental que a empresa adote um plano que identifique quando há algum tipo de violação de dados e estabeleça medidas para conseguir deter. "A instituição deve ter um plano de contenção, saber como reagir e como responder ao mercado. Não adianta esconder, porque isso só vai prejudicar. Precisamos ter políticas adequadas para tratar esse assunto, e se uma empresa não possui, pode ser fatal ao negócio. É importante ter uma cultura de gestão de mudança, e o Conselho tem que entender isso e saber como as outras pessoas estão agindo nessas situações. A responsabilidade é de todos!", alerta.

Muitas empresas preferem apenas reconhecer os danos decorrentes de ataques cibernéticos como "perda", a fim de proteger a confiança em seus sistemas e em suas marcas e evitar impactos negativos à instituição. Especialistas afirmam que é preferível combater o incidente com uma resposta rápida, um posicionamento oficial sobre o fato, a fim de evitar as especulações na internet, que são um risco ainda maior para a marca, de crise de imagem digital.

Patricia Peck Pinheiro, advogada especialista em Direito Digital e Segurança Cibernética da PPP Advogados, acrescenta que não implementar boas práticas para prevenir risco de vazamento de informação é vista por especialistas como uma atitude negligente. Patricia alerta para a importância de investir na capacitação de colaboradores e parceiros sobre a proteção da privacidade digital, tanto de dados pessoais quanto corporativos, a fim de se proteger contra violação de dados confidenciais ou essenciais ao sucesso do negócio. "Ao capacitar os seus colaboradores quanto a esses riscos, a empresa se blinda em eventuais incidentes porque pode comprovar que fez a sua parte nesse processo de educação", diz.

A advogada diz que a cultura no Brasil sobre riscos digitais ainda é bastante incipiente. Durante o evento, Patricia questionou aos participantes se as empresas adotam por exemplo alguma regra de conduta sobre o CEO ou CFO baixar qualquer aplicativo gratuito em seu smartphone pessoal. Indagou ainda quantos dos presentes possuíam algum sistema antivírus nos seus celulares e se algum assunto confidencial da Companhia é discutido via WhatsApp. "A possibilidade de vazar uma informação no WhatsApp é grande porque muitos não usam antivírus e adotam sistema de segurança no celular. É como deixar uma informação aberta na sua mesa", alerta.

Ela explica que o trabalho de conscientização em segurança da informação necessita de um plano de educação contínua, que vai além do ambiente corporativo, e pode ser iniciado até antes da pessoa integrar a empresa, como em escolas, universidades, em campanhas públicas para o cidadão. Ela acrescenta que esse treinamento deve alcançar inclusive o cuidado que um colaborador tem que ter com comentários e publicações em perfis pessoais de mídias sociais.

"A blindagem precisa ser completa, pessoal e profissional, para aí sim, criar o hábito da segurança digital. O estagiário que se comunica através do twitter pode ser o CEO no futuro, e pequenas informações que geram vulnerabilidade estão no dia a dia das pessoas, mas só temos o "start" no momento do incidente", alerta.

No entanto essa é ainda uma discussão recente, na qual muitas empresas sequer incluíram este tema em suas pautas. "Lidar com a segurança da informação requer investimento e dedicação de uma boa parcela de tempo, e um dos maiores desafios que vejo hoje nas empresas é como destinar horas das equipes e dos altos executivos em treinamentos preventivos para aumentar a segurança empresarial, que abrange desde a patrimonial à digital. Precisamos rever a agenda obrigatória dos executivos, e esta pauta tem que estar mais presente", destaca.

Patricia conta que muitas empresas realizam um evento anual, ou uma palestra, de presença não obrigatória, e os chefes normalmente não comparecem, o que está muito aquém do que é necessário para gerar uma mudança de cultura.

Peck ressalta que quanto mais alto o cargo do executivo, maior o nível de conhecimento de informações relevantes da empresa, e portanto mais intenso deve ser o seu treinamento em segurança, pois 20% dos executivos de "alto escalão" detêm 80% das informações confidenciais de uma companhia. "Eles precisam ser os primeiros a serem conscientizados - tem que ser de cima para baixo - e alcançar inclusive a camada de profissionais ao redor deles, como motoristas, secretárias, equipe de limpeza e de vigilância. Esta é a linha de frente, principalmente do executivo que viaja muito, está sempre em mobilidade e tem que saber proteger os dados da empresa onde quer que vá, e não somente dentro da empresa", diz.

Em uma sociedade digital, sem muros, um dos grandes desafios é blindar o conselho contra vazamento de informações. Alguém pode estar de olho em você e qualquer um de qualquer lugar pode atacar. Vivemos na era dos ativos intangíveis e isso pode afetar o valor de ação.

Patricia revela que estudos demonstram que companhias com forte proteção de seus ativos intangíveis possuem resultados financeiros mais estáveis. Ela explica que a segurança da informação já está presente em mais de 1/3 dos relatórios anuais das Companhias com capital aberto, o que reflete a importância deste tema, que ultrapassa a área de TI e alcança o alto escalão das Companhias. Envolve um compromisso do Conselho em adotar medidas que buscam mitigar riscos e reduzir incidentes. "A necessidade da empresa adotar uma postura proativa já é cobrada pela SEC (Securities and Exchange Commission) e segue como tendência global", ressalta.

No entanto, quanto ao combate às ameaças e ao terrorismo cibernético, ela diz que ainda estamos longe de sermos eficientes, pois em uma sociedade global, sem fronteiras físicas, a atuação da autoridade ainda está muito restrita a um território geográfico, e as questões envolvendo legitimidade para agir e a soberania dos países geram uma barreira na perseguição destes grupos criminosos, que acabam agindo de forma quase intocável.

"Precisamos aprimorar muito o diálogo internacional e a capacidade de atuação conjunta das polícias, e a burocracia é um grande limitador para aumentarmos nossa proteção. Não é tarefa fácil, pois vivemos o paradoxo entre a privacidade do indivíduo e a segurança pública digital da coletividade. Há que se chegar a um consenso mais amplo, se não toda forma de vigilância acaba sendo interpretada como espionagem ou invasão de privacidade", diz.

PAULO CONTE VASCONCELLOS,
PROXYCON

> **A internet trouxe um mundo sem fronteiras e não há nenhum computador que não possa ser hackeado. Quem está conectado está vulnerável, e um ataque cibernético contra uma empresa não é uma questão de "se", mas de "quando.**

Paulo Conte Vasconcellos, conselheiro profissional e sócio da ProxyCon, empresa de assessoria em Governança Corporativa, alerta para o fato do governo e das empresas não estarem dedicando atenção e recursos para combater os riscos cibernéticos. "A internet trouxe um mundo sem fronteiras e não há nenhum computador que não possa ser hackeado. Quem está conectado está vulnerável, e um ataque cibernético contra uma empresa não é uma questão de "se", mas de "quando"."

Os criminosos atualizam constantemente as suas técnicas e *modus operandi*. Em 2013 a Kaspersky, empresa produtora de softwares de segurança para a Internet, identificou a existência de cerca de 200.000 novos malwares diariamente (softwares indesejados que causam alguns danos, alterações ou roubo de informações). Já a Verizon, uma das maiores empresas de telecomunicações no mundo, aponta que 62% dos ataques levam no mínimo dois meses para serem detectados, e 75% dos hackers são bem sucedidos ao penetrarem nas empresas em questão de minutos. A Gartner empresa americana de pesquisa e consultoria tecnológica, estima que em 2017 o investimento em software de segurança alcance o montante de US$ 94 bilhões. Em 2012 esse valor foi de US$ 20 bilhões.

"A reputação de uma empresa é vital para o negócio, e neste sentido não tem preço que pague o investimento que se fizer necessário para protegê-la e não ter a sua imagem destruída diante de um ataque. Não imaginamos a dimensão do risco que envolve esse assunto", destaca.

Trata-se de um tema ainda desconhecido, mas que requer a atenção das empresas. De acordo com Paulo Vasconcellos, o Conselho precisa criar políticas e diretrizes relacionadas ao tema e estabelecer uma série de ações, como estimular a conscientização de executivos e colaboradores; assegurar-se da existência de programas educacionais e de comunicação; exercer constante vigilância sobre como o tema está sendo tratado pelos executivos; interagir com auditores e área de gestão de riscos e garantir a existência de respostas aos incidentes.

Sandra Guerra, presidente do IBGC - Instituto Brasileiro de Governança Corporativa - e da Better Governance -, diz que o nível de consciência do conselho em relação à segurança cibernética é naturalmente maior em empresas que estão mais expostas pelas atividades que exercem, e/ou que estão inseridas em um ambiente regulado, e os seus profissionais buscam melhores práticas e referências de mercado nacio-

nais e internacionais nesse assunto. Mas no geral, a executiva diz que a adoção de um conjunto de práticas robustas para o conselho monitorar os riscos cibernéticos ainda é pouco disseminado, e no âmbito da gestão ainda é um assunto emergente.

"Quando sabemos de casos de empresas que tiveram seus dados violados é que a dimensão foi tão grande que é impossível omitir tamanha magnitude. E os casos menores acabam sendo objetos de estudo, e o mundo inteiro está aprendendo com esses casos públicos. O que a gente conhece é a ponta do iceberg, pois a maior parte dos casos é mantida em sigilo", diz.

Sandra reforça que o risco cibernético precisa ser entendido como risco corporativo, e não está restrito apenas à área e ao conhecimento tecnológico, mas que envolve um entendimento do modelo de negócio da empresa e a sua estratégica, para poder entender o risco que pode sofrer. "Quando a empresa está montando a sua estratégia, ou lançando o seu produto, ela deve desde já incluir aspectos de vulnerabilidade e modelos de gerenciamento de risco. Isso já deve estar embutido desde o seu nascimento, mas ainda é uma recomendação inovadora."

A executiva recentemente esteve nos Estados Unidos participando de dois eventos sobre segurança cibernética e diz que essa discussão é tão recente, mesmo em mercados onde há mais consciência sobre esse risco, que ainda envolve como devemos desenvolver práticas para que o Conselho lide melhor com esse risco, se esse assunto deveria ser alocado em comitês, e de que forma deve haver uma comunicação entre gestão e conselho sobre os riscos cibernéticos.

"O conselheiro de alguma forma tem que saber como lidar bem com todos os riscos, inclusive o cibernético, se capacitar aprender e entender os pontos centrais e não apenas o detalhamento da tecnologia. Ao mesmo tempo o conselho sempre pode utilizar "experts" para ver se o modelo de gestão de risco que está sendo usado está sendo robusto", diz.

O IBGC entende que a gestão de risco deve ser tratada como elemento fundamental e que requer a atenção dos conselheiros, para que saibam lidar com esse tema de forma efetiva. "O IBGC vai contribuir desenvolvendo competências para ajudar o mercado a se proteger de possíveis ataques", finaliza Sandra. **RI**

SANDRA GUERRA,
IBGC E BETTER GOVERNANCE

> **O conselheiro de alguma forma tem que saber como lidar bem com todos os riscos, inclusive o cibernético, se capacitar aprender e entender os pontos centrais e não apenas o detalhamento da tecnologia.**