Como evitar a espionagem corporativa

*__Laurent Serafini__
sócio-diretor da Velours International no Brasil

A espionagem corporativa existe praticamente desde que existe economia. No entanto, com o advento da internet, essa prática se potencializou trazendo sérios perigos às empresas. A atividade consiste em colher dados empresariais sigilosos de maneira ilícita e usá-los ou até mesmo vendê-los de modo a prejudicar a empresa que, com segurança e atenção às minúcias pouco valorizadas, pode reduzir este sério risco.

Se pegarmos o caso de uma startup - ou seja, uma empresa que está nascendo e, portanto, lutando para conquistar seu espaço e crescimento - ou de uma empresa de médio porte que esteja lançando um serviço ou produto inédito, um roubo de informações pode custar sua consolidação ou até seu futuro. Na França, uma pesquisa revelou que metade das pequenas e médias empresas vítimas de roubo de informações pediu falência dois ou três anos depois do ocorrido.

Porém, como o roubo de dados está diretamente ligado ao nome e à imagem das empresas, dificilmente é admitido, dificultando a mensuração dos dados e o possível melhoramento do setor. As empresas envolvidas preferem não externar o ocorrido para preservarem sua imagem e evitar que se tornem ainda mais vulneráveis.

Para que a companhia possa se proteger da espionagem corporativa, o primeiro passo é admitir o risco e ter consciência de que todas as empresas estão suscetíveis a isso, indiferente do ramo de atividade ou do porte. O pensamento não deve ser de "se a crise acontecer", mas sim "quando a crise acontecer", ou seja, é reconhecer a fragilidade e antever as ações a serem tomadas na crise.

Efetuar uma auditoria, mapeando os riscos (operacionais, financeiros, sociais, jurídicos, ambientais, de fraude e de imagem) e identificando as vulnerabilidades, é crucial para que se iniciem os planos gerais de segurança, com as ações cabíveis, além da conscientização, capacitação e treinamento dos colaboradores.

Implantar uma rotina de trabalho e um comportamento seguro dos colaboradores pode evitar que informações sigilosas sejam disseminadas para fora da empresa. Afinal, tão importante quanto possuir um sistema de segurança adaptado contra os ataques de hackers ou crackers, é o fato das empresas estarem atentas para minúcias como a falta de preparo ou de atenção de seus colaboradores, que podem transmitir as informações, mesmo que involuntariamente, por meio de um simples telefonema.

Por fim, criar programas de motivação e identificação do funcionário com a empresa também é uma medida preventiva contra a espionagem. Na pior das hipóteses, um trabalhador descontente pode até vir a praticar, ele mesmo, a espionagem, copiando e enviando por e-mail um arquivo, salvando em pen-drives ou FTP (Protocolo de Transferência de Arquivos) e, posteriormente, vendendo a informação ou a usando em proveito próprio em ato de revanchismo contra a companhia.

Em uma época em que os cargos estão cada vez mais flexíveis e a permanência em uma mesma empresa cada vez menor, o colaborador costuma ser menos comprometido e, assim, dá menos valor e importância ao sigilo. Portanto, compete aos líderes estarem atentos às atividades mais corriqueiras para que não possam se tornar uma arma contra a própria empresa.

> "Na França, uma pesquisa revelou que metade das pequenas e médias empresas vítimas de roubo de informações pediu falência dois ou três anos depois do ocorrido."