BAPTISTA LUZ ADVOGADOS
R. Ramos Batista . 444 . Vila Olímpia
04552-020 . São Paulo – SP
baptistaluz.com.br

Checklist de *Data Breach*

Primeiro, é preciso compreender que incidentes de segurança da informação podem acontecer mesmo em empresas que tomam todas as precauções razoáveis. Nesse contexto, estar verdadeiramente preparado para lidar com um incidente de segurança da informação pode ser o grande diferencial para que a resposta ao incidente seja bem-sucedida e que danos aos titulares dos dados e à própria empresa sejam mitigados.

Tendo isso em mente, criamos um "checklist" com algumas medidas que podem ser adotadas internamente pelas empresas antes que um incidente ocorra. Essas medidas exprimem tanto obrigações legais quanto recomendações de boas práticas.

- **Designar um Comitê de Segurança da Informação ("CSI")**: o comitê é o órgão da empresa que tem a função de discutir e deliberar sobre assuntos relacionados à segurança da informação. O CSI é responsável, por exemplo, pela elaboração da PSI;
- **Implementar uma Política de Segurança da Informação ("PSI")**: documento que estabelece diretrizes sobre padrões e medidas técnicas internas de segurança da informação, devendo ser seguidos por todos aqueles que mantêm um relacionamento com a empresa e que, no âmbito dessa relação, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados da empresa;
- **Elaborar um plano de resposta à incidentes de segurança da informação**: este plano deve endereçar os seguintes pontos: (i) a natureza do incidente (se a motivação foi interna ou externa); (ii) as áreas da empresa afetadas pelo incidente; (iii) a categoria dos dados e a quantidade de titulares dos dados afetados; (iv) a execução do plano de notificação. Para a GDPR, o plano de resposta deve respeitar o prazo de 72 horas, enquanto a LGPD determina que a resposta seja em um tempo razoável;

- **Elaborar um DPIA**: o DPIA aliado a um plano de resposta para incidentes de segurança da informação, em conjunto com outras medidas técnicas e administrativas, são efetivamente levados em consideração no momento em que a Autoridade for avaliar quais foram as medidas que a Empresa tomou ou fez a título de prevenção em um eventual incidente de segurança da informação. Portanto, recomendamos fortemente que as medidas acima destacadas sejam providenciadas;
- **Elaborar um plano de notificação do incidente de segurança da informação**: uma equipe efetiva inclui o chefe do departamento de privacidade ou diretor de segurança (ou seus equivalentes), um representante da unidade de negócios da qual os dados foram acessados, advogados (internos ou externos) e um coordenador de relações públicas. É importante incluir no plano de avaliação inicial um protocolo de comunicação para notificar a equipe quando ocorrer um incidente e estabelecer um cronograma e uma lista de itens de ação para uma avaliação inicial e etapas subsequentes, conforme necessário; elaboração de notificação à Autoridade;(v) comunicado para veiculação aos titulares dos dados afetados pelo incidente; e (vi) canal de comunicação para com os titulares dos dados afetados;
- **Elaborar um plano de comunicação interna e externa sobre o incidente de segurança da informação**: o plano deve identificar os membros da equipe de resposta, que também devem estar envolvidos no desenvolvimento do plano; e
- **Contratar um seguro com cobertura específica para incidentes de segurança da informação.**

É preciso ressaltar que toda a empresa deve estar alinhada com essas medidas e todos devem seguir o procedimento do plano de resposta para incidentes, com padrões de respostas que possam vir a orientar o *board* da Empresa, a área de comunicação, área de segurança da informação, o jurídico e os acionistas, uma vez que todas as áreas precisam colaborar internamente para mapear os danos e estar ao mesmo tempo preparada para implementar o plano de resposta ao incidente.

REFERÊNCIAS:

BRASIL. Lei nº 13.709, de 14 de agosto de 2018.

RAETHER, Ronald I. "Security before and after a Data Breach." *Business Law Today*, vol. 16, no. 2, 2006, pp. 56–62. *JSTOR*, JSTOR, www.jstor.org/stable/23296723.