CIBERSEGURANÇA UM TEMA DE GOVERNANÇA CORPORATIVA

Por: **WILSON LAURIA**

O INCIDENTE CDK: O DESPERTAR

Em junho de 2024, a norte-americana CDK Global — uma das maiores provedoras de Dealer Management Systems (DMS) — foi alvo de um ataque de Ransomware que paralisou a operação de mais de 15 mil concessionárias. O episódio expôs, de forma contundente, a dependência digital e a fragilidade cibernética do setor automotivo de varejo, trazendo à tona um alerta global: cibersegurança é, hoje, um fator de continuidade e sustentabilidade do negócio.

Este artigo, busca responder a uma questão central e cada vez mais urgente: O que os administradores precisam saber sobre cibersegurança?

GOVERNANÇA: O PAPEL DA LIDERANÇA E O DEVER DE DILIGÊNCIA

O primeiro e talvez mais importante entendimento é que cibersegurança deixou de ser um tema técnico. Hoje, ela está no núcleo das decisões estratégicas e na pauta dos Conselhos de Administração e Diretorias Executivas. Seu impacto sobre a sustentabilidade e a reputação das empresas a posiciona no mesmo patamar de temas como conformidade regulatória e gestão financeira.

A relação entre cibersegurança e sustentabilidade é clara: diversas pesquisas indicam que a maioria das pequenas e médias empresas (PMEs) vítimas de incidentes cibernéticos encerram suas atividades em até seis meses após o ataque.

Nesse contexto, conhecer os ativos digitais críticos — sistemas, aplicações e bases de dados — não é uma questão técnica, mas parte do dever de diligência do administrador. O gestor precisa saber o que é essencial para o negócio e quais as consequências de seu comprometimento. A alegação de que “esse é um tema muito técnico” já não encontra amparo na boa governança.

PARTES RELACIONADAS: OS RISCOS NÃO PERCEBIDOS

Entre as percepções mais perigosas está a ideia de que “negócios pequenos não atraem criminosos”. Na prática, o oposto tem ocorrido. As PMEs tornaram-se alvos preferenciais porque, em geral, dispõem de defesas mais frágeis e estão digitalmente conectadas a grandes organizações.

Em um mundo interconectado, cada empresa faz parte de um ecossistema digital. Essa conexão, se mal protegida, funciona como uma via expressa para que agentes maliciosos acessem toda a cadeia produtiva. Assim, o comprometimento de um elo menor pode abrir uma porta para atingir empresas de maior porte e valor.

Sob essa ótica, a segurança de uma empresa depende também da segurança de suas parceiras. Por isso, conhecer e mitigar o risco cibernético das partes relacionadas deixou de ser uma boa prática e passou a ser um requisito estratégico de gestão.

PLANO DE RESPOSTA A INCIDENTES: UM DIFERENCIAL COMPETITIVO

Não existe sistema infalível. Toda organização — independentemente de porte ou segmento — está sujeita a incidentes cibernéticos. Essa é uma realidade inescapável, e ignorá-la pode amplificar seus efeitos.

Nesse cenário, possuir um Plano de Resposta a Incidentes (PRI) é uma vantagem competitiva. O plano deve definir papéis, responsabilidades e ações objetivas, ser conhecido e testado periodicamente. Nas primeiras 24 horas após um ataque, a clareza e a prontidão na resposta podem representar a diferença entre a recuperação e o colapso operacional.

É dever da liderança assegurar que o PRI esteja operacional, atualizado e integrado às rotinas de gestão de crises, garantindo que a resposta ocorra com fluidez e precisão quando mais se precisa dela.

INSIGHTS PARA O GESTOR AUTOMOTIVO

Como resposta à questão central que orientou este artigo, seguem quatro reflexões essenciais para os líderes do setor de distribuição automotiva:

- cibersegurança é um tema estratégico, pois um incidente pode comprometer a continuidade do negócio;
- conhecer os ativos digitais críticos faz parte do dever de diligência do gestor;
- gerenciar o risco das partes relacionadas é essencial para proteger o ecossistema da cadeia produtiva;
- treinar e validar o Plano de Resposta a Incidentes é a garantia de uma atuação eficaz diante da crise.

Wilson Laria é CEO da GRCIBER Soluções. Especialista em Cyber Security and Executive Strategy pela Stanford University (EUA). Professor Convidado na Escola Superior de Defesa e na Fundação Getúlio Vargas. Membro da Comissão de Gestão de Riscos Corporativos do IBGC.