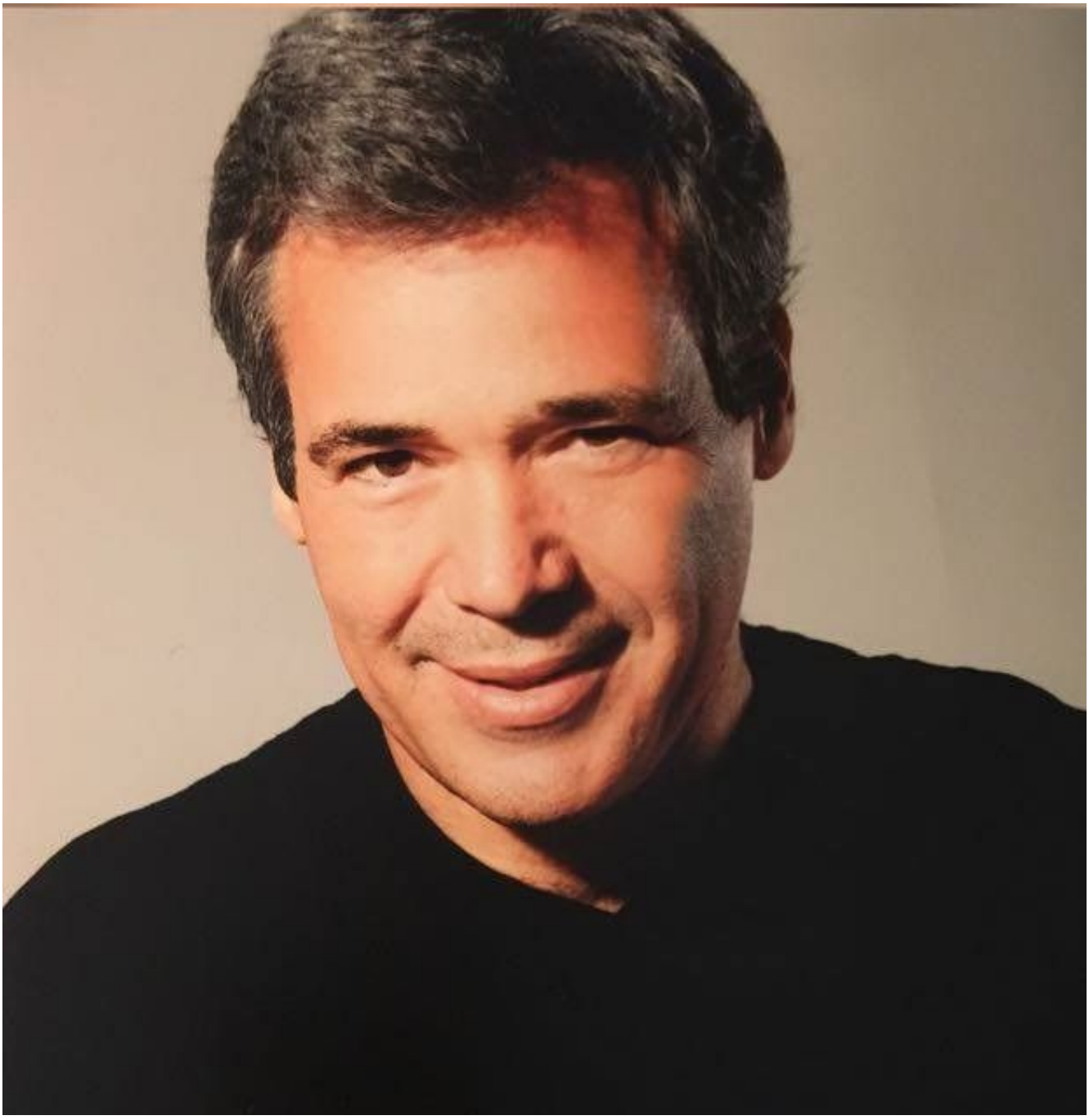
Por Augusto Schmoisman (*)



O número crescente e a complexidade dos incidentes de segurança cibernética levaram muitas organizações a desenvolverem procedimentos e habilidades para gerenciá-los. Isso inclui recursos de resposta em tempo real, capacidade tecnológica e a formação de equipes encarregadas da manutenção dos sistemas de informação. Esses esforços, no entanto, são insuficientes quando os aspectos gerenciais, as habilidades e ferramentas exigidas não são considerados, gerando uma situação fora do controle em que a crise se torna grave, afetando outas áreas da companhia como a financeira, jurídica, além de interferir na reputação da empresa.

A maioria dos incidentes cibernéticos é gerenciada por processos de rotina como, por exemplo, lidar com infecções de malware. Ataques graves, no entanto, podem causar danos duradouros à capacidade de funcionamento e à prestação de serviços aos clientes. Esses casos requerem, de

fato, atenção especial. Um modelo eficaz que analisa o processo de gestão de uma crise posiciona o incidente no centro e identifica as defesas e controles projetados para evitá-lo. Algumas fases do processo são: detecção do incidente, análise dos fatos, contenção e erradicação. A recuperação pós-crise deve incluir uma investigação do ocorrido, avaliação das conclusões e o aprendizado.

Para gerir com eficiência uma crise é necessário ter a definição do que ela é e criar uma linguagem comum e clara, estabelecendo regras para gerenciá-la. É muito importante determinar quem serão os responsáveis dentro da organização por essas situações, criando um comitê de gestão. Esse grupo deve ser composto por funcionários que conheçam o negócio e suas atividades, os sistemas tecnológicos e gerenciais e ter habilidades como boa comunicação interpessoal, capacidade para ouvir os outros, inteligência emocional, saber trabalhar em equipe e proatividade na tomada de decisões. Todos os participantes devem passar por um treinamento com exercícios rotineiros para identificar incidentes em condições tão reais quanto possível. Afinal, lidar de forma eficaz com uma crise cibernética pode reduzir os danos e levar a organização à rápida recuperação.

Além dessas ações, outras grandes aliadas no gerenciamento de crises são as ferramentas tecnológicas que auxiliam na interpretação e análise dos fatos relevantes para compreender como a situação pode se desenvolver, além de examinar suas ramificações de acordo as ações que foram tomadas. Durante a crise, o foco deve estar na erradicação do incidente e na rápida recuperação dos sistemas para volta ao funcionamento pré-crise. A análise do motivo deve ser feita posteriormente.

É fundamental que as corporações formulem um plano para desenvolver ferramentas e habilidades e configurem um programa ordenado de sistemas, treinamentos, simulações e exercícios. Ações bem arquitetadas serão de extrema importância para enfrentar uma crise cibernética e sair dela com danos mínimos.

(*) **Augusto Schmoisman** é especialista em defesa cibernética corporativa, militar, aeroespacial e CEO da Citadel Brasil.