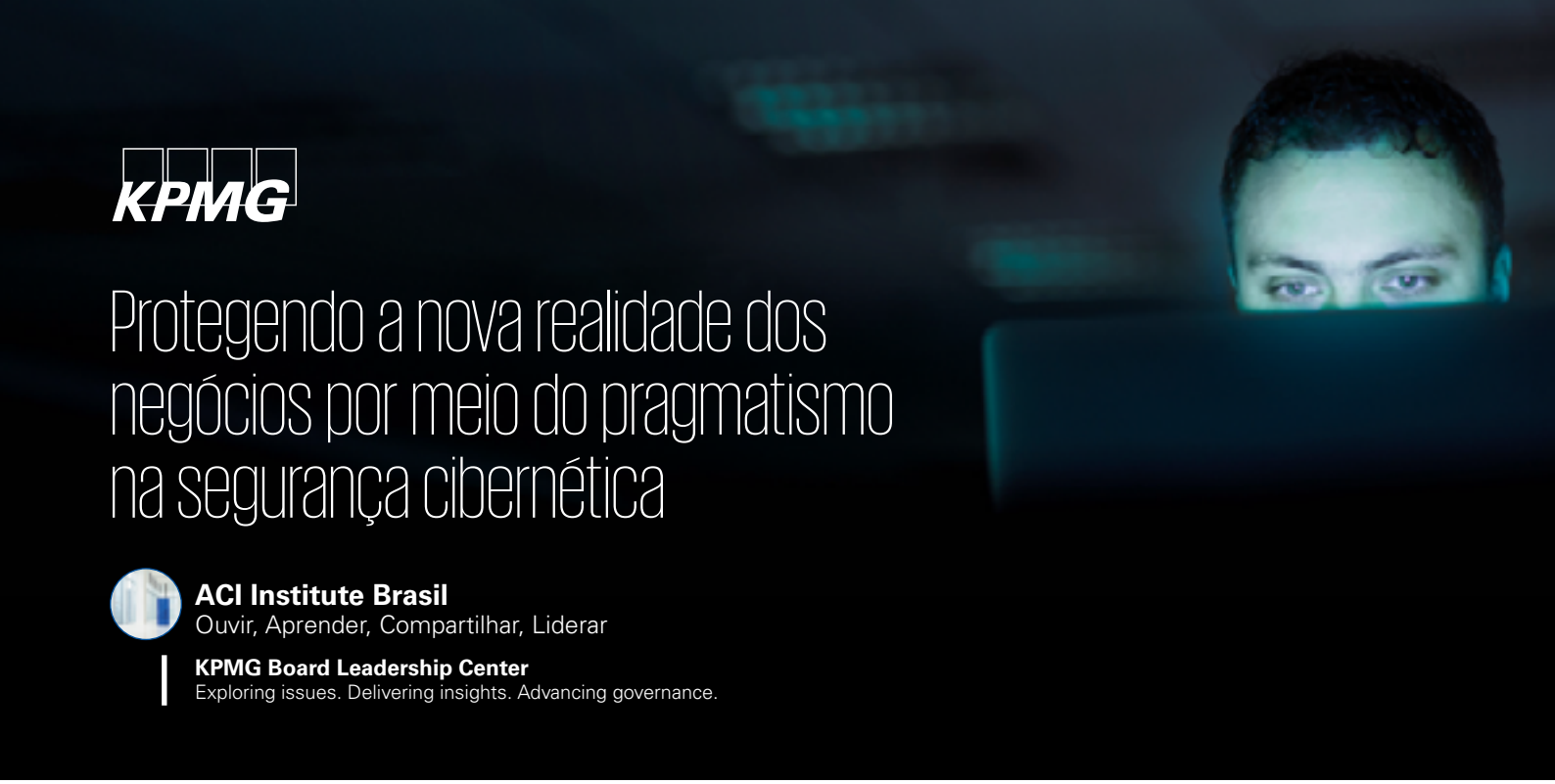

Protegendo a nova realidade dos negócios por meio do pragmatismo na segurança cibernética

ACI Institute Brasil
Ouvir, Aprender, Compartilhar, Liderar

KPMG Board Leadership Center
Exploring issues. Delivering insights. Advancing governance.

As rápidas transformações pelas quais as empresas passaram para assegurar a continuidade das operações durante a pandemia da Covid-19, representam uma oportunidade tanto para quadrilhas de crime organizado mais sofisticadas como para hackers que atuam de forma solitária.

Como consequência, os ataques cibernéticos aumentaram consideravelmente desde março de 2020, com golpes que variam desde e-mails de *phishing*[1] , passando por vendas de *kits* falsos de testes de Covid, portais enganosos que se passam por sites oficiais do governo, até ataques *ransomware*[2] a hospitais para extorquir dinheiro. Modelos operacionais provisórios e as implicações de longo prazo de um ambiente de negócios com distanciamento social — influenciados em grande medida pela tecnologia da informação (TI) — requerem cautela e foco especial na segurança cibernética.

Como resposta imediata à Covid-19, muitas empresas flexibilizaram os controles internos para garantir mais facilidade na adaptação digital e aumentaram a presença *online*. Agora, precisam ajustar seus processos de segurança e fraudes para garantir e manter os benefícios a longo prazo dessas transformações digitais.

Por exemplo: em situações em que a empresa dependia de instalações físicas de segurança, supervisão *online* da gestão dos funcionários ou da utilização da TI corporativa, talvez seja preciso repensar a abordagem de segurança cibernética para incorporar um mix diferente de controles de detecção e prevenção para suportar o uso extensivo de dispositivos pessoais e redes de conexão não confiáveis, incluindo plataformas de reuniões remotas. Outro aspecto que precisa ser considerado é que os controles de segurança nas redes residenciais dos funcionários são, frequentemente, mais fracos do que aqueles adotados em ambientes corporativos. Nesses casos, embora permitir a utilização de dispositivos pessoais possa ser conveniente e eficiente, existem novos riscos que precisam ser ativamente monitorados e mitigados.

Paralelamente, a migração para os canais digitais — com o aumento de recursos alocados na economia digital — está atraindo a atenção de criminosos cibernéticos. A segurança em torno das plataformas digitais de pagamento, bem como dos dados do cliente e da propriedade intelectual, é essencial.

Conforme as empresas mudam o foco de reação e resiliência para a recuperação e a adaptação à nova realidade, os debates dos Conselhos de Administração precisarão se concentrar principalmente nas seguintes questões:

— **Oferecer aos funcionários ferramentas, tecnologias e treinamentos necessários para que atuem em um ambiente de negócios remoto**. Sobre esse tópico, os conselheiros devem se perguntar: como será o futuro do ambiente de trabalho? Já existe uma estratégia em vigor para identificar os modelos de trabalho remoto e híbrido? De quais tecnologias a empresa depende para prosperar na nova realidade, incluindo treinamentos em cibersegurança e campanhas de conscientização dos colaboradores?

— **Incorporar a segurança cibernética e a governança de dados nas estratégias de transformação digital.** Por exemplo: a migração para ambientes em nuvem (*cloud*) é uma oportunidade para incorporar controles de segurança com grau de consistência difícil de se alcançar em sistemas operacionais mais antigos. A segurança deve ser parte integral do desenvolvimento de novos aplicativos e sistemas. Não deve ser vista como um potencial obstáculo para estratégias de transformação digital mais agressivas nem ser adotada tardiamente, quando uma crise se instala.

[1] Fraude eletrônica para adquirir informações sigilosas, tais como: senha, números de cartão de crédito e outros dados confidenciais. O método mais comum é enviar um e-mail para a vítima solicitando a confirmação de dados pessoais.

[2] Tipo de software malicioso (malware) que bloqueia o acesso a um sistema de computador ou criptografa dados de um sistema, até que seja pago um valor de resgate em dinheiro.

— **Manter expertise em TI, recursos e investimentos necessários para acompanhar os desafios da segurança cibernética.** Em diferentes setores, a área de segurança permanecerá sob pressão de redução de custos, assim como outras esferas dos negócios. A companhia tem considerado oportunidades para automatizar os processos? Qual o modelo orçamentário mais adequado para a área de segurança daqui em diante?

— **Reforçar os protocolos de cibersegurança do Conselho de Administração**. Além da maior supervisão da segurança das reuniões e dos canais de comunicação do Conselho, a utilização de e-mails e dispositivos pessoais ou softwares não autorizados por conselheiros para conduzir as operações pode apresentar sérios riscos cibernéticos. A diretoria de segurança da informação informou ao Conselho sobre os protocolos de segurança cibernética da empresa no contexto do novo ambiente operacional? Nesse ambiente de negócios emergente, sairão na frente as companhias com modelos digitais robustos, que impulsionam os canais de relacionamento com o cliente e a cadeia de suprimentos; a conectividade dos funcionários e as operações orientadas a dados (*data-driven*). Essa vantagem competitiva, daqui em diante, dependerá da segurança e do enfoque digital abrangente da organização.

Material originalmente produzido por John Rodi e Tony Buffomante, da KPMG nos Estados Unidos, e publicado na Revista Directorship da National Association of Corporate Directors (NACD).

O ACI Institute Brasil

Criado em 1999 pela KPMG International, nos Estados Unidos, o ACI Institute tem o propósito de disseminar a importância das boas práticas de governança e de estimular a discussão sobre esse tema tão relevante para o desenvolvimento da economia e dos negócios. Presente em mais de 30 países, o ACI chegou ao Brasil em 2004 e, nesses 17 anos de existência, tornou-se um importante fórum de discussão para membros de Conselhos de Administração, Conselhos Fiscais e Comitês de Auditoria. O ACI Brasil já promoveu mais de 70 Mesas de Debate. Os mais de 600 membros do ACI recebem, mensalmente e em primeira mão, informações relacionadas a governança corporativa, gerenciamento de riscos, Compliance, auditoria, ESG e outros assuntos. Ao incentivar a troca de experiências entre seus membros e propiciar um espaço para interlocução de alta qualidade, o ACI Institute Brasil e a KPMG contribuem para fortalecer as boas práticas de governança corporativa no Brasil.

Saiba mais em https://home.kpmg/br/pt/home/services/aci-institute-brasil.html

Fale com o nosso time

Leandro Augusto M Antonio
Sócio-líder de Cyber Security e Privacy da KPMG no Brasil
lantonio@kpmg.com.br

Fernanda Allegretti
Sócia-diretora do ACI Institute, do Board Leadership Center Brasil e de Markets da KPMG no Brasil
fallegretti@kpmg.com.br

Ser criativo transforma negócios.

#KPMGTransforma

Baixe o nosso APP

kpmg.com.br /kpmgbrasil

Projeto gráfico e diagramação: Gaudí Creative Thinking