Auditoria interna e cibersegurança

Como melhorar a transparência e a qualidade das informações sobre segurança cibernética em um ambiente regulatório cada vez mais exigente

PwC Brasil
2022

pwc

Os reguladores estão exigindo cada vez mais responsabilidade das empresas por suas práticas cibernéticas. Para enfrentar essa realidade, os líderes precisam **aprimorar os relatórios corporativos** externos e compartilhar **mais informações sobre o tema** para ajudar os investidores a tomar suas decisões. Em paralelo, isso os ajuda a fortalecer as defesas da organização contra um dos riscos mais ameaçadores da atualidade.

Seguindo a tendência de exigir das organizações mais transparência e consistência nas informações sobre o tema, a Comissão de Valores Mobiliários dos Estados Unidos (SEC, na sigla em inglês) propôs às empresas de capital aberto novas regras de gestão de riscos, estratégia, governança e divulgação de incidentes de segurança cibernética.

Os novos requisitos, anunciados em 9 de março de 2022, ajudarão os *stakeholders* a entender melhor como uma empresa gerencia suas exposições a riscos cibernéticos. O caminho para a adequação às novas exigências passa pela auditoria interna, especialmente em relação aos controles de segurança aplicados nas operações com terceiros.

Cibersegurança no radar: o argumento em favor de mais transparência

49%
dos CEOs em todo o mundo estão preocupados em algum nível com os riscos cibernéticos, o que faz do tema a principal ameaça ao crescimento das receitas.

Apenas

33%
dos conselheiros dizem entender as vulnerabilidades cibernéticas de sua empresa.

62%
dos consumidores e empregados concordam que a proteção de dados e a cibersegurança são fundamentais para a confiança.

Fontes: PwC. *25ª CEO Survey, 2021 Annual Corporate Directors Survey e Trust in Business Survey 2021*.

Principais mudanças propostas pela SEC

Relatórios de incidentes cibernéticos

- Inclusão de incidente(s) “relevante(s)” de segurança cibernética no relatório.
- Atualização sobre incidentes de segurança cibernética relatados anteriormente.
- Divulgação de incidentes de segurança cibernética individualmente irrelevantes não divulgados anteriormente, mas que se tornaram relevantes de forma agregada.

Estratégia e gestão de riscos cibernéticos

- Necessidade de descrever políticas e procedimentos da empresa – se houver – para identificar e gerenciar riscos de segurança cibernética. É preciso relatar também se a segurança cibernética está inserida na estratégia e governança corporativa, no planejamento financeiro e na projeção de investimentos.

Outras medidas de governança

- Maior divulgação e formalização sobre:
  - a supervisão exercida pelo conselho e alta administração em relação a riscos de segurança cibernética.
  - o papel e a experiência do conselho e alta administração na avaliação e gestão de riscos de segurança cibernética e na implementação de políticas, procedimentos e estratégias de segurança cibernética.
  - a experiência em segurança cibernética dos membros do conselho e alta administração.

Três lacunas nas divulgações atuais

1

Relatórios de incidentes cibernéticos

Apesar de novos e importantes tipos de ataques cibernéticos relatados por pesquisadores em 2020 e 2021, o número de divulgações de incidentes cibernéticos em formulários 8-K ou 10-K diminuiu em relação a 2019. Em 2020, foram relatadas 117 violações, em comparação com 144 em 2019, segundo relatórios "Trends in Cybersecurity Breaches", da Audit Analytics.

2

Estratégia e gestão de riscos cibernéticos

Muitas empresas fornecem informações limitadas sobre os programas de gestão de riscos em suas comunicações. Em geral, elas não informam sobre políticas e procedimentos, como as práticas de gestão de riscos de terceiros ou o uso de consultores ou outro tipo de terceiros para avaliar seus programas de segurança cibernética ou planos de recuperação e continuidade de negócios.

3

Governança cibernética

Embora muitas empresas divulguem informações sobre sua estrutura de governança, como os responsáveis por lidar com os riscos cibernéticos no nível gerencial e se há supervisão do conselho sobre a segurança cibernética, outras informações a respeito da frequência de relatórios para o conselho e detalhes específicos da experiência dos conselheiros sobre questões cibernéticas são limitadas e inconsistentes.

Riscos provenientes de terceiros

A gestão de riscos e controles de segurança de terceiros é um dos principais pontos abordados na proposta da SEC. A pandemia de covid-19 evidenciou como a falha em gerenciar adequadamente o risco nas relações com terceiros pode impactar a marca, as operações, os clientes e os resultados.

Riscos

Disrupção
Um terceiro (ou fornecedor dele) passa por uma crise causada por um evento ou por insolvência e torna-se incapaz de fornecer produtos essenciais ou serviços de que a empresa precisa ou de executar um serviço no nível esperado.

Risco para a marca por associação
A associação de um terceiro a comportamentos antiéticos, como suborno, envolvimento com corrupção ou outras práticas comerciais questionáveis, traz impacto para a marca por associação ou aumento da vigilância regulatória.

Aumento da fiscalização
As regulamentações anticorrupção e de proteção de dados e privacidade continuam a se multiplicar, com forte atenção em terceiros. Aumenta também a ênfase dos governos na necessidade de conhecer, avaliar e gerenciar terceiros de forma eficaz.

Conectividade, vulnerabilidades e incidentes
A conectividade e a vulnerabilidade de terceiros são usadas por agentes maliciosos para penetrar no ambiente da empresa contratante. Violações de dados em um terceiro importante também podem revelar informações confidenciais sobre a empresa, seus clientes ou empregados e gerar impactos negativos para a própria empresa.

Potenciais impactos

Perda financeira

Danos à marca

Desvantagem competitiva

Sanções regulatórias

Perda de participação no mercado

Incidentes graves

Papel da auditoria interna na gestão de riscos de cibersegurança e de terceiros

Principais questões de auditoria que organizações de todos os setores devem considerar:

Como os CISOs e os conselhos devem começar a se preparar

A nova era de transparência cibernética exige que diretores de segurança da informação (CISOs, na sigla em inglês) desenvolvam a capacidade de divulgar informações para que o conselho, a alta administração e os investidores possam entendê-las e agir.

Isso requer uma estratégia de comunicação diferente da usada no cotidiano da segurança cibernética. Os CISOs precisam também pensar na frequência e no conteúdo das informações transmitidas aos conselhos e CEOs, a fim de garantir que os principais riscos de segurança cibernética sejam abordados.

O conselho, por sua vez, deve avaliar se precisa dispor de maior conhecimento cibernético para supervisionar efetivamente a evolução dos riscos nessa área. A questão passa até mesmo pela composição do órgão. Treinamento adicional e sessões educacionais com conselheiros também podem se mostrar valiosos.

Como podemos ajudar

- Analisamos as práticas de gestão de riscos cibernéticos, suficiência de controles de defesa e de comunicação de sua empresa para avaliar o grau de alinhamento às regras da SEC e elaboramos um plano para eliminar possíveis lacunas e indicar mudanças.
- Avaliamos a conexão entre a área de segurança cibernética e as equipes responsáveis por relatar informações para o público externo, visando melhor eficácia da comunicação.
- Avaliamos a prontidão da empresa para divulgar diferentes tipos de informações e antecipamos possíveis impactos da comunicação.

Uma rede global à sua disposição

Brasil

3.600 profissionais

137 sócios

15 escritórios

321 clientes* entre as 500 maiores empresas**

43* dos 50 maiores bancos**

31* das 50 maiores seguradoras**

Global

295 mil profissionais

11 mil sócios

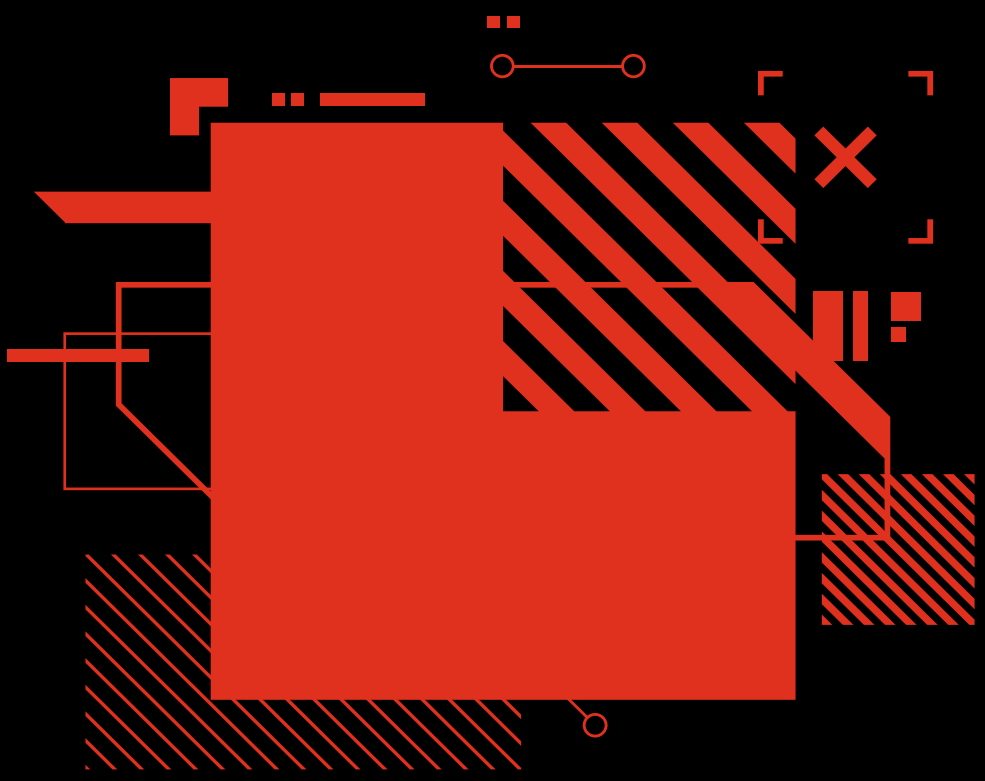
732 escritórios

420 clientes entre as Fortune 500

155 territórios

US$ 45 bi de receita global

*Considerando FY21 (acumulado do ano)
**Ranking Valor 1000 (Valor Econômico – edição 2021)



Contatos

André Medeiros
Sócio de GRC e Auditoria Interna
andre.medeiros@pwc.com

Rosana Napoli
Sócia de GRC e Auditoria Interna
rosana.napoli@pwc.com

André Pannunzio
Sócio e líder de GRC e Auditoria Interna
andre.pannunzio@pwc.com

pwc

www.pwc.com.br

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil

(DC0) Informação Pública
Versão: Agosto 2022 | [F309]