TONE at the TOP®

Trazendo à alta administração, conselhos de administração e comitês de auditoria informações concisas sobre tópicos relacionados a governança.

Edição 113 | Outubro de 2022

Mitigando as Ameaças Cibernéticas

A cibersegurança tornou-se um elemento permanente no cenário moderno de riscos e os conselhos enfrentam uma pressão crescente para fazer a supervisão adequada de uma ameaça multifacetada e em constante evolução. Um total de 70% dos diretores do conselho chamou a cibersegurança de "um risco empresarial estratégico" em uma pesquisa *NACD Board Survey*.[1] Uma ampla gama de questões faz parte do âmbito da cibersegurança — todas são preocupações críticas, alguns exemplos que podemos citar incluem proteção de privacidade; *ransomware*, *malware* e ataques de negação de serviço ou de *phishing*; políticas de cibersegurança inadequadas; e planos de resposta a incidentes e de recuperação.

As organizações também estão enfrentando novos regulamentos que exigem que elas reportem as violações que sofreram. A lei *Cyber Incident Reporting for Critical Infrastructure Act*[2], por exemplo, exige um reporte que permitiria à *Federal Cybersecurity and Infrastructure Security Agency* prestar assistência às vítimas durante ciberataques, identificar tendências e compartilhar informações com outras vítimas em potencial. A *Securities and Exchange Commission* (SEC) também propôs regulamentos[3] que padronizariam as divulgações relacionadas ao gerenciamento de riscos de cibersegurança, estratégia, governança e reporte de incidentes de empresas públicas.

A auditoria interna, que fornece às organizações avaliação e assessoria independentes e objetivas, pode ser um recurso poderoso para os conselhos de administração lidarem com os riscos cibernéticos. De acordo com um relatório da PwC[4], "muitas empresas alavancam a auditoria interna para revisar processos e controles cibernéticos, incluindo a resiliência cibernética e o processo de resposta".

Passos para uma Segurança Aprimorada

Conforme os conselhos ponderam sobre as ameaças que enfrentam à cibersegurança, há várias áreas em que a auditoria interna pode fazer a diferença.

Reconhecer o risco. As ameaças cibernéticas passaram para o topo das classificações de risco das empresas. "A crescente sofisticação e variedade dos ciberataques continuam causando estragos nas marcas e reputações das organizações, muitas vezes resultando em impactos financeiros desastrosos", de acordo com *OnRisk 2022*[5] do The Institute of Internal Auditors (IIA). O relatório, baseado em entrevistas com membros do conselho, executivos da alta administração e chefes executivos de auditoria (CAEs), identificou a cibersegurança como o principal risco deste ano.

Infelizmente, alguns líderes da empresa podem não reconhecer totalmente a ameaça. No relatório *OnRisk*, uma preocupação específica foi a lacuna entre as classificações de relevância do risco de cibersegurança atribuídas pelos CAEs, membros do conselho e gestão executiva. Enquanto 97% dos CAEs classificaram a cibersegurança como um risco altamente relevante para sua organização (6 ou 7, em uma escala de 7 pontos), apenas 87% dos membros do conselho e 77% dos executivos da alta administração deram essa classificação.

A forte classificação de relevância entre os CAEs sugere seu alto nível de conscientização sobre as questões de cibersegurança. Não é de surpreender, dado o conhecimento holístico da auditoria interna sobre a organização. Conforme os conselhos buscam alavancar e melhorar a avaliação de riscos, indo além dos riscos financeiros e de conformidade, podem recorrer à auditoria interna para ajudar a descrever as preocupações de cibersegurança e quantificar seu impacto potencial. Isso pode incluir destacar falhas na cobertura de riscos, monitorar riscos emergentes e fazer o melhor uso das ferramentas de tecnologia nos esforços de cibersegurança.

Aproveitar o valor do Modelo das Três Linhas. O Modelo das Três Linhas do The IIA[6] permite que as organizações identifiquem estruturas e processos que melhor auxiliem na realização dos objetivos e que viabilizem uma forte governança e gerenciamento de riscos, inclusive referentes à cibersegurança. O Modelo das Três Linhas identifica os principais papéis desempenhados por:

Sobre o The IIA

The Institute of Internal Auditors Inc. (The IIA) é uma associação profissional internacional com mais de 218.000 membros em mais de 170 países e territórios. O The IIA atua como principal defensor da profissão de auditoria interna, criador global de normas e maior pesquisador e educador.

The IIA

1035 Greenwood Blvd.
Suíte 401
Lake Mary, FL 32746 EUA

Assinaturas Gratuitas

Visite www.theiia.org/Tone para se cadastrar para uma assinatura gratuita.

Feedback do Leitor

Envie perguntas/comentários para Tone@theiia.org

- O corpo administrativo, que é responsável perante os stakeholders pela supervisão organizacional.
- A gestão, que atua para atingir os objetivos organizacionais.
- A auditoria interna, que presta avaliação independente e objetiva sobre o atingimento desses objetivos.

Pesquisas já mostraram que a cooperação entre as três linhas tem um impacto positivo na eficácia do gerenciamento de riscos de cibersegurança. De acordo com um artigo do *ISACA Journal*[7], a auditoria interna pode oferecer avaliações valiosas e identificar ameaças e vulnerabilidades. Isso pode incluir identificar tendências de cibersegurança e expectativas dos stakeholders, fazer uma avaliação preliminar dos riscos cibernéticos e definir critérios de auditoria eficazes. Ao reportar e assessorar sobre suas descobertas, "os auditores podem ajudar significativamente [o conselho de administração] a exercer sua supervisão", afirma o artigo.

Garantir que a contribuição da auditoria interna seja otimizada. Em muitas organizações, os comitês de auditoria são responsáveis por abordar todos os tipos de riscos, incluindo ameaças cibernéticas.[8] No entanto, por vários motivos, algumas organizações atribuem preocupações cibernéticas a outros comitês. Dependendo do tamanho e da indústria da organização, e das ameaças que ela enfrenta, o comitê encarregado de supervisionar questões cibernéticas pode ser um comitê separado de cibersegurança, de riscos, de tecnologia, de nomeação e governança ou outro comitê. Os conselhos podem determinar que o comitê de auditoria já tem responsabilidades demais ou que não tem a expertise necessária para supervisionar as preocupações cibernéticas, entre outros motivos.

A auditoria interna normalmente reporta ao comitê de auditoria, mas a organização pode perder valiosas recomendações e avaliações de riscos cibernéticos, se a auditoria interna não oferecer relatórios também a algum comitê responsável separadamente pela cibersegurança. Ter esse relacionamento com qualquer comitê que supervisione as questões cibernéticas garante que os insights da auditoria interna sejam compreendidos e aplicados com eficácia.

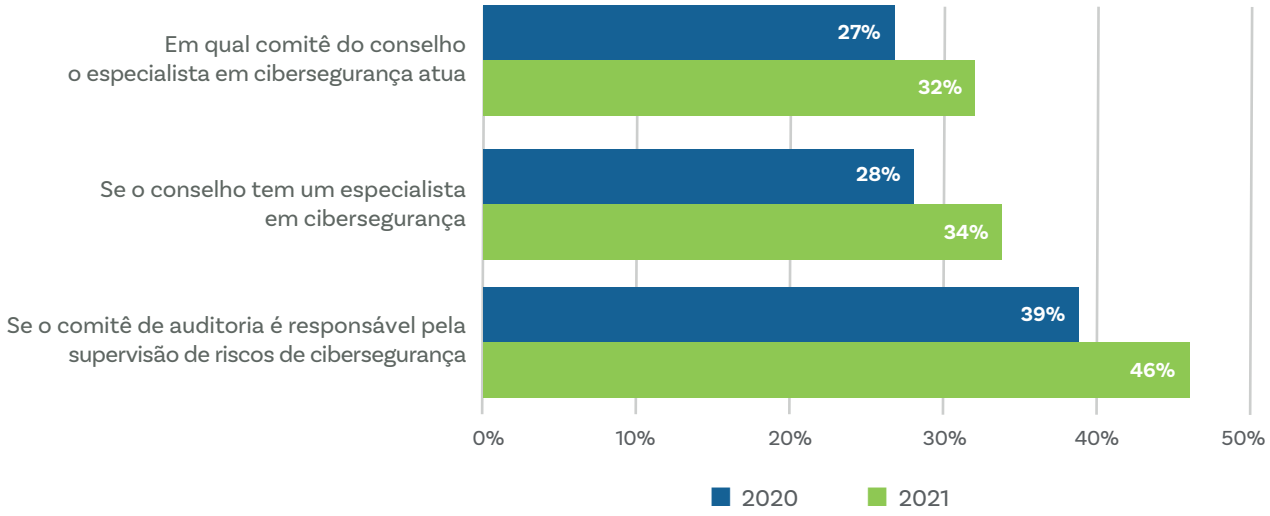
Identificar ameaças ocultas. Os conselhos podem se surpreender com o número de descuidos aparentemente pequenos que podem prejudicar os esforços de cibersegurança e potencialmente levar ao desastre. A auditoria interna pode oferecer insights para ajudar os conselhos a determinar quão bem o plano de auditoria de sua organização é capaz de identificar ameaças negligenciadas e encontrar riscos emergentes. De acordo com um relatório da Deloitte[9], apenas algumas das ameaças cibernéticas que a gestão normalmente subestima incluem:

- A quantidade de ex-funcionários que ainda podem fazer login no sistema e o número de fornecedores terceirizados que têm acesso aos sistemas corporativos. Em ambos os casos, as empresas podem não ter total ciência de quantos usuários externos não identificados e não autorizados podem entrar nos seus sistemas.

PERGUNTAS PARA MEMBROS DO CONSELHO

- Estamos fazendo o melhor uso da assessoria e dos insights da auditoria interna em nosso planejamento estratégico relacionado à cibersegurança?
- Temos a equipe e o financiamento devidos para os esforços de cibersegurança?
- A organização definiu sua tolerância aos riscos, em termos financeiros, quando se trata da cibersegurança?
- Um comitê específico está encarregado de supervisionar a cibersegurança?
- Os diretores entendem os procedimentos da empresa em caso de violação cibernética e, se isso acontecer, eles sabem os seus próprios papéis?

Quantas Empresas do S&P 500 Divulgam:



Fonte: 2021 Audit Committee Transparency Barometer, Center for Audit Quality, novembro de 2021.

- O número de contas na nuvem que a empresa usa. Uma maior movimentação na nuvem pode deixar mais aberturas para ataques cibernéticos. O relatório da Deloitte recomenda que as organizações perguntem aos provedores da nuvem sobre a resiliência da infraestrutura, tempo de inatividade do serviço, desempenho e outras métricas, bem como sobre conformidade regulatória e avaliações independentes dos controles.

- O número total real de violações cibernéticas que a organização vivenciou. Contraintuitivamente, se a empresa sofreu poucos ataques cibernéticos, isso pode ser um sinal de alerta de que os incidentes simplesmente não estão sendo detectados. A equipe de auditoria interna pode ajudar a garantir que esses tipos de sinais de alerta estejam sendo monitorados.

Abordar as preocupações nas relações com parceiros de negócios. A Gartner prevê[10] que, até 2025, 60% das organizações considerarão o risco de cibersegurança ao se envolver em transações com terceiros e em trabalhos comerciais. Atualmente, apenas 23% dos líderes de segurança e gerenciamento de riscos monitoram a exposição da cibersegurança de terceiros em tempo real e podem limitar esse monitoramento a vendedores e fornecedores mais próximos, em vez de toda a cadeia de suprimentos.

Novamente, os líderes de auditoria, os executivos da alta administração e os membros do conselho não estão em sincronia com suas opiniões, de acordo com o *OnRisk 2022*. Enquanto os CAEs classificaram a capacidade organizacional nessa área em 37%, os executivos acreditam que ficou em 53% e os diretores em 57%. A menor confiança dos CAEs nessa área, provavelmente em parte, decorre da classificação de relevância mais alta que atribuem a esse risco, que foi 17 pontos superior à classificação dos diretores (77% *versus* 60%).

De qualquer forma, os conselhos devem garantir que obtenham todo o valor das contribuições e experiências da auditoria interna nessa área. Como a auditoria interna trabalha com equipes por toda a organização, ela pode alertar o conselho sobre riscos cibernéticos associados ou identificados em um determinado fornecedor, ou em toda a cadeia de suprimentos. Quando os parceiros de negócios da organização desejam reavaliações sobre a confiabilidade de suas proteções de cibersegurança, a auditoria interna pode fornecer os tipos de dados e a avaliação que eles buscam.

Otimizando Recursos

Conforme as organizações lutam com preocupações aterradoras de cibersegurança, precisarão otimizar todos os seus recursos existentes. Os conselhos podem melhorar a segurança de sua empresa, entendendo e aproveitando o valor que os auditores internos podem trazer para toda a organização, ao identificar oportunidades para aumentar a eficiência e a eficácia.

Referências

1 Principles for Board Governance of Cyber Risk, National Association of Corporate Directors, Internet Security Alliance e Fórum Econômico Mundial, em colaboração com PwC, março de 2021.

2 https://www.cisa.gov/circia

3 https://www.sec.gov/rules/proposed/2022/33-11038.pdf

4 Overseeing Cyber Risk: The Board's Role, PwC, janeiro de 2022.

5 OnRisk 2022: A Guide to Understanding, Aligning, and Optimizing Risk, The Institute of Internal Auditors, 2021.

6 The IIA's Three Lines Model: An Update of the Three Lines of Defense, The Institute of Internal Auditors, julho de 2020.

7 "How Effective Is Your Cybersecurity Audit?," Matej Drašček, et al., ISACA Journal, 1º de junho de 2022.

8 "Cybersecurity: An Evolving Governance Challenge," Harvard Law School Forum on Corporate Governance, Phyllis Sumner, et al., 15 de março de 2020.

9 Internal Audit: Risks and Opportunities for 2022 , Deloitte, 2021.

10 Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem, Sam Olyaei, et al., Gartner, 24 de janeiro de 2022.

Pesquisa Rápida

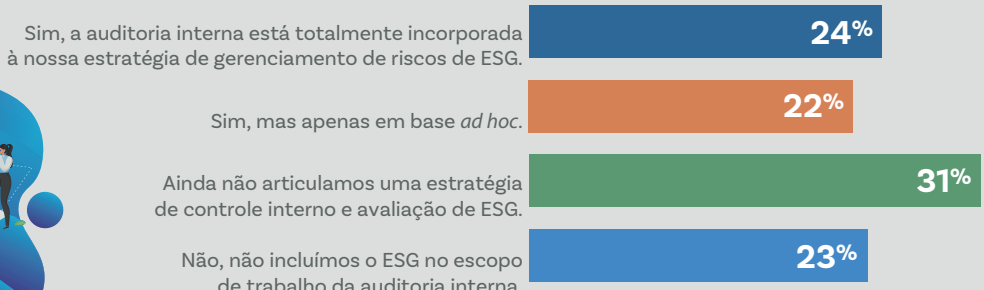
Qual comitê é responsável por supervisionar o gerenciamento de riscos de cibersegurança em sua organização?

- ◯ Comitê de Auditoria
- ◯ Comitê de Cibersegurança
- ◯ Comitê de Tecnologia
- ◯ Comitê de Nomeação e Governança
- ◯ Outro

Visite www.theiia.org/Tone para responder à pergunta e ver como outros estão respondendo.

RESULTADOS DA PESQUISA RÁPIDA

Sua organização alavanca a auditoria interna para avaliação de ESG?



Fonte: Pesquisa do Tone at the Top de junho de 2022.