TONE at the TOP®

TRADUZIDO POR • INSTITUTO DOS AUDITORES INTERNOS DO BRASIL • IIA Brasil

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

Edição 137 | Outubro de 2026



Da Violação à Sala do Conselho:

Fortalecendo a Supervisão da Cibersegurança

Em fevereiro de 2024, um ataque de *ransomware* à Change Healthcare, subsidiária da UnitedHealth Group, paralisou o processamento de pedidos de reembolso e de pagamentos em grande parte do sistema de saúde dos EUA. Os danos: US$ 2,2 bilhões em custos de resposta direta, outros US$ 867 milhões em disrupção dos negócios e cerca de 190 milhões de pessoas afetadas.

O ponto de entrada foi um portal sem autenticação multifator — um controle de segurança básico, como o CEO Andrew Witty reconheceu perante o *Senate Finance Committee*. O então presidente do comitê, Ron Wyden, atribuiu a culpa ao topo, argumentando em sua declaração de abertura que a empresa precisava de um verdadeiro especialista em cibersegurança no conselho.

Isso deixou de ser mera retórica. Em uma série de decisões de 2025, o *Delaware Court of Chancery* decidiu que a cibersegurança é um risco "crítico à missão", que os conselhos não podem simplesmente delegar à gestão. Agora se espera que os conselheiros recebam informes regulares e a falta de atas sobre essas discussões pode, por si só, sugerir uma falha de supervisão.

Esse não é um risco que vai desaparecer tão cedo. No relatório *Risk in Focus* de 2026/2027 do The IIA, 80% dos líderes de auditoria interna escolheram a cibersegurança como um dos cinco principais riscos enfrentados por sua organização, um aumento de 7% em relação a 2025 e 22% acima do segundo risco mais escolhido, a disrupção digital (incluindo IA).

Claramente, a cibersegurança é uma área crítica que exige a máxima atenção do próprio topo da organização. Os membros do conselho têm a obrigação de tratar a supervisão dos riscos cibernéticos como parte de seus deveres e desenvolver conhecimento especializado adequado para cumpri-los.

Esta edição examina possíveis lacunas nos esforços de cibersegurança das organizações, a gama crescente de divulgações sobre governança de cibersegurança e como os auditores internos podem ajudar os conselhos a abordar suas responsabilidades de governança nessa área.

Um Trabalho em Andamento

A cibersegurança evoluiu de uma preocupação estritamente técnica para um dos riscos de negócios centrais enfrentados pelas empresas modernas. Como observa a CrowdStrike em seu relatório, "*Cybersecurity Risk Oversight: A Governance Guide for Board Directors*", os conselhos de hoje viram a cibersegurança passar "de um exercício de conformidade para um mandato central de governança".

A forma como as organizações estão tratando as divulgações de cibersegurança é um exemplo claro dessa mudança. A *U.S. Securities and Exchange Commission* estabeleceu regras sobre divulgações de cibersegurança em 2023, mas muitas organizações vão além, oferecendo voluntariamente detalhes sobre a supervisão da cibersegurança e o conhecimento especializado do conselho.

De fato, conforme investidores e stakeholders continuam exigindo mais informações sobre a supervisão da cibersegurança, uma análise de empresas de grande capitalização feita pela EY constatou aumentos significativos nas divulgações em muitas áreas nos últimos anos. As principais constatações da pesquisa da EY incluem:

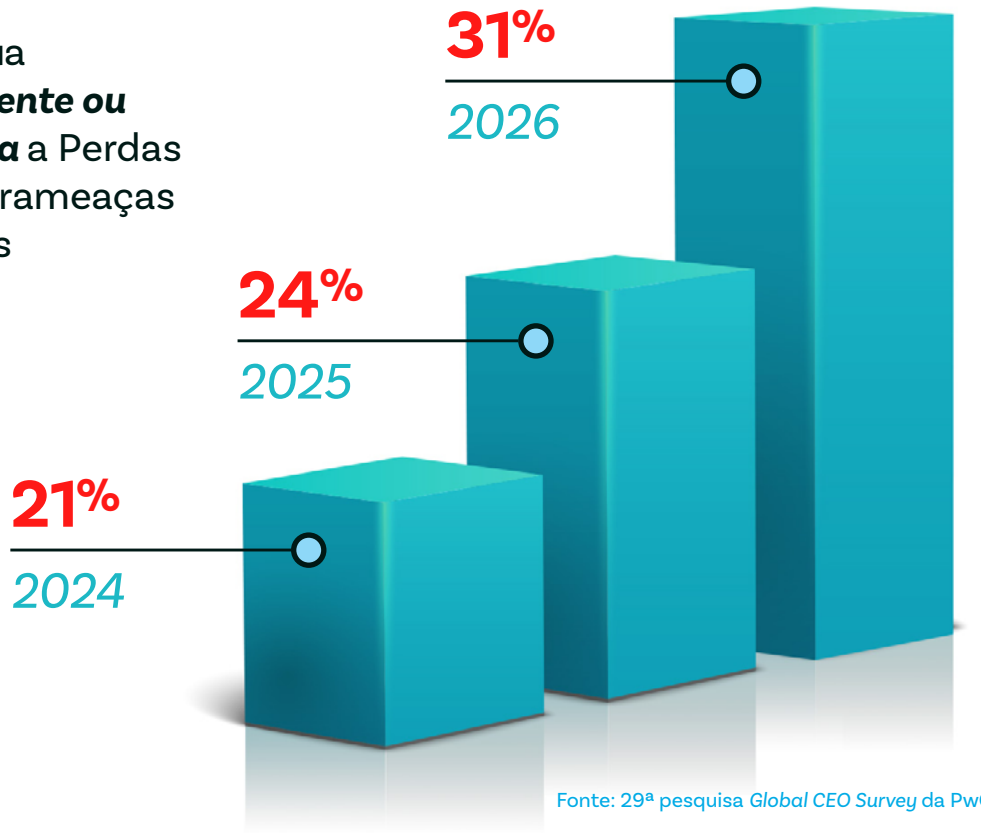
- Setenta e oito por cento das empresas dizem que os comitês de auditoria são responsáveis pela supervisão da cibersegurança.
- Oitenta e seis por cento afirmam divulgar a cibersegurança como uma área de conhecimento especializado que um conselheiro possui ou que o conselho busca — um aumento em relação aos 53% de 2019.
- Setenta e três por cento estão alinhando seus esforços de cibersegurança a um framework externo, como o NIST CSF 2.0 ou a ISO 27001.
- Cinquenta e oito por cento estão realizando atividades de preparação em cibersegurança, incluindo simulações, simulados de mesa ou testes de prontidão de resposta — um aumento em relação aos 3% de 2019.

Embora as organizações estejam claramente levando os riscos cibernéticos a sério, há lacunas significantes em sua capacidade de acompanhar a velocidade do risco. Isso pode ser visto, por exemplo, em seu uso e compreensão da IA, que, na melhor das hipóteses, continua sendo um trabalho em andamento.

De acordo com a pesquisa da Workiva *MidYear Executive Benchmark Survey* de 2026, 84% dos executivos dizem estar pelo menos um pouco confiantes na precisão dos resultados da IA, mesmo sem qualquer revisão humana. Ao mesmo tempo, 26% afirmam que auditorias internas detectaram erros de IA que chegaram a públicos externos ou a membros do conselho. Esses resultados indicam uma possível desconexão entre as suposições dos executivos sobre a IA e a realidade de como ela está funcionando em suas próprias organizações.

"Conforme a IA remodela a empresa em uma velocidade sem precedentes, um novo risco está surgindo", diz a Workiva. "[A] transformação poderia estar superando os instintos dos líderes encarregados de supervisioná-la."

CEOs que Dizem que Sua Empresa ***Estará Altamente ou Extremamente Exposta*** a Perdas Significativas por Ciberameaças nos Próximos 12 Meses



Fonte: 29ª pesquisa *Global CEO Survey* da PwC

Sobre o The IIA

O Institute of Internal Auditors (IIA) é uma associação profissional internacional sem fins lucrativos, que atende a mais de 265.000 membros e concedeu mais de 200.000 certificações *Certified Internal Auditor* (CIA) no mundo todo. Criado em 1941, o The IIA é reconhecido em todo o mundo como o líder da profissão de auditoria interna em normas, certificações, educação, pesquisa e orientação técnica. Para mais informações, visite theiia.org.

The IIA

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

Assinaturas Gratuitas

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

Feedback do Leitor

Envie perguntas/comentários para Tone@theiia.org.



O Lugar dos Auditores Internos na Discussão Cibernética

A função de auditoria interna é uma parceira valiosa nos esforços das organizações para mitigar riscos de cibersegurança. O Requisito Temático de Cibersegurança do The IIA e seu Guia do Usuário ilustram claramente o papel da auditoria interna no plano de gerenciamento de riscos de cibersegurança e o que ela deve fazer para estar em conformidade com as Normas Globais de Auditoria Interna™.

O requisito foi criado para fornecer "uma abordagem consistente e abrangente para avaliar a criação e implementação dos processos de governança, gerenciamento de riscos e controle de cibersegurança". Para isso, a auditoria interna tem o dever de avaliar três áreas principais:

- Governança: Objetivos e estratégias básicos de cibersegurança claramente definidos, que apoiam as metas, políticas e procedimentos organizacionais;
- Gerenciamento de Riscos: Processos para identificar, analisar, gerenciar e monitorar ciberameaças, incluindo um processo para escalar prontamente os riscos cibernéticos;
- Controles: Processos de controle criados pela gestão e avaliados periodicamente para mitigar riscos cibernéticos.

Em relação à governança de cibersegurança, o Requisito Temático mapeia os requisitos de governança em relação aos frameworks apropriados. A compreensão desses frameworks deveria ser um componente crítico da base de conhecimento do comitê de auditoria e do conselho sobre o plano de gerenciamento de riscos cibernéticos da organização. Além disso, o requisito exige que a auditoria interna revise como os processos de governança são aplicados aos objetivos de cibersegurança, incluindo a existência de:

- Planos e objetivos formalizados;
- Políticas, procedimentos e outros documentos relevantes usados para gerenciar processos de cibersegurança;
- Papéis e responsabilidades que apoiam o atingimento dos objetivos de cibersegurança e se a função de cibersegurança reporta a um nível suficientemente alto na organização para obter apoio e visibilidade suficientes;
- Evidências de envolvimento com stakeholders relevantes dentro e fora da organização.

Em conjunto, esses requisitos deveriam dar aos conselhos e comitês de auditoria uma visão clara do que esperar da auditoria interna em relação à cibersegurança. Além disso, como esses requisitos são obrigatórios para a conformidade com as Normas Globais de Auditoria Interna™, os membros do conselho podem confiar que uma função de auditoria interna em conformidade está maximizando o valor que pode entregar.

Atenção Crescente às Preocupações Cibernéticas

A indústria de telecomunicações é um dos muitos setores que lidam com o risco de cibersegurança e os avanços recentes de *Advocacy* nessa área oferecem um estudo de caso útil para ajudar os conselhos a entender quão valiosa a auditoria interna pode ser nesse campo.

Os perigos na indústria de telecomunicações incluem "ciberataques em velocidade de máquina", bem como respostas geralmente lentas das operações de segurança a ameaças emergentes, de acordo com a EY em *"How Telecoms Can Dial Up Cybersecurity in the Age of AI Attacks".*

A legislação recentemente promulgada no Canadá aprimora a capacidade do governo de proteger o sistema de telecomunicações do país contra tais perigos. Ela exige que operadores de sistemas cibernéticos críticos em setores regulados pelo governo federal tomem as medidas necessárias para proteger sua infraestrutura cibernética.

Em seus comentários sobre o que viria a ser a lei *Critical Cyber Systems Protection Act* do Canadá, o The IIA observa a necessidade de desenvolver processos eficazes para identificar e mitigar possíveis riscos cibernéticos para as organizações, bem como garantir a presença de controles internos apropriados e procedimentos independentes de avaliação. A lei prevê "uma auditoria interna em um operador designado regulado nos termos desta legislação".

Os regulamentos cibernéticos em outras jurisdições incluem:

- Estados Unidos: *Cyber Incident Reporting for Critical Infrastructure Act of 2022;*
- União Europeia: *NIS2 Directive;*
- Reino Unido: *Network and Information Systems Regulations 2018.*

Os Conselhos Precisam da Perspectiva da Auditoria Interna

A cibersegurança é um tema vasto e, por vezes, avassalador para qualquer organização considerar. Com todas as variáveis técnicas e em evolução em jogo, os conselhos precisarão contar com estruturas sólidas de governança e de reporte para garantir que recebam as informações mais claras, precisas e relevantes possíveis. Para isso, não há função mais bem posicionada do que a auditoria interna para contribuir de forma eficaz com a discussão.

