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 125 | Outubro de 2024

O Papel do Conselho na Resiliência Cibernética

Sua empresa está preparada para o próximo ciberataque? A maioria das organizações espera sofrer um ciberataque no futuro, com 73% dos líderes de negócios e de cibersegurança prevendo que um incidente cibernético irá prejudicar seus negócios nos próximos 12 a 24 meses, de acordo com o **2024 Cisco Cybersecurity Readiness Index.**

Há muitas consequências potenciais de um ciberataque, incluindo o comprometimento de dados confidenciais, a disrupção das operações e danos a relacionamentos com terceiros e à reputação da empresa. De acordo com o relatório **Risk in Focus de 2025** do The IIA, os líderes de auditoria interna atribuem à cibersegurança as classificações de risco mais altas por uma ampla margem. Eles também a citam como a área na qual a auditoria interna dedica mais tempo e esforço.

De acordo com o relatório, a cibersegurança continua sendo o principal risco que os líderes esperam que suas organizações enfrentem daqui a três anos, com a disrupção digital (incluindo a inteligência artificial (IA)) crescendo rapidamente em relação às pesquisas anteriores e assumindo o segundo lugar. "A IA está aumentando os riscos de cibersegurança e fraude em todo o mundo", diz o relatório. A cibersegurança foi classificada como a principal área em que a IA teria o impacto mais negativo.

Em um ambiente em que a questão não é se, mas quando ocorrerá um ataque, a resiliência cibernética é fundamental para ajudar as empresas a enfrentar um incidente. As empresas podem fazer grandes esforços para se proteger contra ciberataques, mas também devem estar preparadas para responder e se recuperar de tais ataques.

Resiliência cibernética é "a capacidade de prever, resistir, recuperar-se e adaptar-se a condições adversas, estresses, ataques ou problemas em sistemas que usam ou são habilitados por recursos cibernéticos. A resiliência cibernética destina-se a permitir que os objetivos de missão ou de negócios que dependem de recursos cibernéticos sejam alcançados em um ambiente cibernético conturbado." — National Institute of Standards and Technology.

Novas Expectativas para os Conselhos

Os órgãos reguladores e os acionistas estão examinando a responsabilidade do conselho em relação à cibersegurança e desenvolvendo novas expectativas para a supervisão pelos membros do conselho sobre as vulnerabilidades de suas organizações. De acordo com uma norma finalizada, **Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure**, a Comissão de Valores Mobiliários dos EUA estabelece as divulgações necessárias para as empresas públicas, abordando especificamente a divulgação sobre incidentes materiais de cibersegurança e divulgações periódicas sobre como os registrantes avaliam, identificam e gerenciam esses riscos, bem como a função da gestão na avaliação e no gerenciamento desses riscos. A norma final também exige divulgações sobre a supervisão dos riscos de cibersegurança pelos conselhos.

Como parte de sua função de supervisão, os conselhos deveriam garantir que os executivos e suas equipes estabelecessem um alto padrão de cibersegurança, de acordo com um artigo da McKinsey, **"Boards of Directors: The Final Cybersecurity Defense for Industrials."** Em seguida, deveriam monitorar os esforços de cibersegurança, determinando se as metas foram alcançadas e se as equipes estão assumindo a responsabilidade pela cibersegurança. "O conselho é a última linha de defesa para garantir que essas iniciativas sejam planejadas e financiadas", observa o artigo.

Um ciberataque é projetado para dificultar que as organizações continuem fazendo negócios normalmente. A resiliência cibernética consiste em estar informado e preparado, para que as opções e prioridades estejam claras quando ocorrer uma crise. Para garantir que suas organizações estejam bem preparadas, os conselhos deveriam determinar se há planos documentados de gestão de crises, resposta a incidentes e recuperação de desastres, que a gestão testa periodicamente em simulados de mesa, de acordo com o relatório da PwC **Overseeing Cyber Risk: The Board's Role**. Os exercícios deveriam se concentrar no estabelecimento de papéis e responsabilidades claros, para esclarecer a tomada de decisões da gestão durante uma crise.

Muitos conselhos recebem da gestão um scorecard ou dashboard cibernético que destaca os riscos atuais e o progresso das metas de cibersegurança. A PwC aponta diversas áreas que podem fazer parte de um relatório para o conselho:

- *Plano estratégico plurianual e plano de negócios para o ano corrente.*
- *Detalhes sobre a alocação de recursos de cibersegurança divididos por financiamento e equipe.*
- *Uma avaliação de maturidade mensurada em relação a um framework reconhecido, como o* **NIST Cybersecurity Framework.**
- *Um inventário atualizado regularmente dos sistemas críticos.*
- *Um resumo dos principais riscos cibernéticos para a organização.*
- *Uma análise dos incidentes de segurança significativos que a organização sofreu.*
- *Dados sobre esforços de treinamento e conscientização da equipe.*
- *Detalhes sobre os frameworks de prontidão para incidentes da organização, incluindo dados da apólice de seguro cibernético.*
- *Destalhes sobre a estratégia de risco cibernético de terceiros.*
- *Informações que comparem os esforços da organização com os de seus pares.*
- *Detalhes sobre os principais avanços legais e regulatórios relacionados.*
- *Lições a serem aprendidas com ciberataques recentes.*

Embora seja fundamental proteger a organização contra ataques, os conselhos deveriam lembrar que a proteção, por si só, só pode resolver questões que a organização já conhece. Infelizmente, armados com ferramentas tecnológicas emergentes que usam IA, os inovadores cibercriminosos desenvolvem continuamente novas formas de causar danos. Como resultado, "para mitigar adequadamente o risco cibernético, os líderes da empresa devem ter planos sólidos para responder e se recuperar rapidamente, para que a empresa possa continuar em operação", reporta o artigo do MIT News, "**Now Corporate Boards Have Responsibility for Cybersecurity, Too."**

Sobre o The IIA

O Institute of Internal Auditors (IIA) é uma associação profissional internacional sem fins lucrativos, que atende a mais de 245.000 membros e concedeu mais de 195.000 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.

Auditoria Interna: Uma Parceira Confiável de Cibersegurança

Os conselhos deveriam estar cientes do valor que as funções de auditoria interna podem agregar aos esforços de cibersegurança. A auditoria interna presta serviços de avaliação e consultoria exclusivos, objetivos e independentes sobre estratégia, governança e controles de cibersegurança. "Muitas empresas alavancam os auditores internos para revisar os processos e controles cibernéticos, incluindo a resiliência e a resposta", observa o artigo da PwC.

As funções de auditoria interna podem contribuir para os esforços de resiliência cibernética de diversas formas, inclusive por meio de uma auditoria de recuperação e resposta a incidentes cibernéticos. O relatório Risk in Focus do ano passado apresenta parte do valor que os auditores internos podem agregar, e a lista permanece válida até hoje:

- Avaliar o nível de conscientização, conhecimento e habilidades nas principais partes da empresa, incluindo o conselho, para garantir que as respostas de defesa cibernética sejam relevantes e atualizadas.
- Avaliar as linhas de reporte entre o diretor de segurança da informação, o diretor de informação e o conselho, para garantir uma comunicação clara dos riscos e recomendações e que eles possam ser escalados para o nível mais alto, quando necessário.
- Avaliar a frequência, a pontualidade e a eficácia das campanhas de phishing de teste simuladas e outras atividades de conscientização e os níveis de envolvimento da equipe, bem como o grau de integração da equipe com os processos de treinamento e acompanhamento.
- Usar cenários para educar o conselho sobre suas responsabilidades de governança e para testar se os processos de mitigação estão completos e com eficácia.
- Avaliar a eficácia do ambiente de controle interno e quão bem os controles estão incorporados na primeira e na segunda linhas de acordo com o **Modelo das Três Linhas** do The IIA, prestando atenção especialmente às práticas que a equipe considera disruptivas ou intrusivas e que provavelmente ignorará, esquecerá ou contornará.
- Avaliar até que ponto a estrutura de governança da organização permite a colaboração entre as três linhas.
- Determinar até que ponto a organização monitora os avanços globais nas regulamentações de cibersegurança e tecnologia e até que ponto os controles internos podem ser prontamente alterados para atender aos requisitos futuros.

Um Risco em Expansão e Evolução

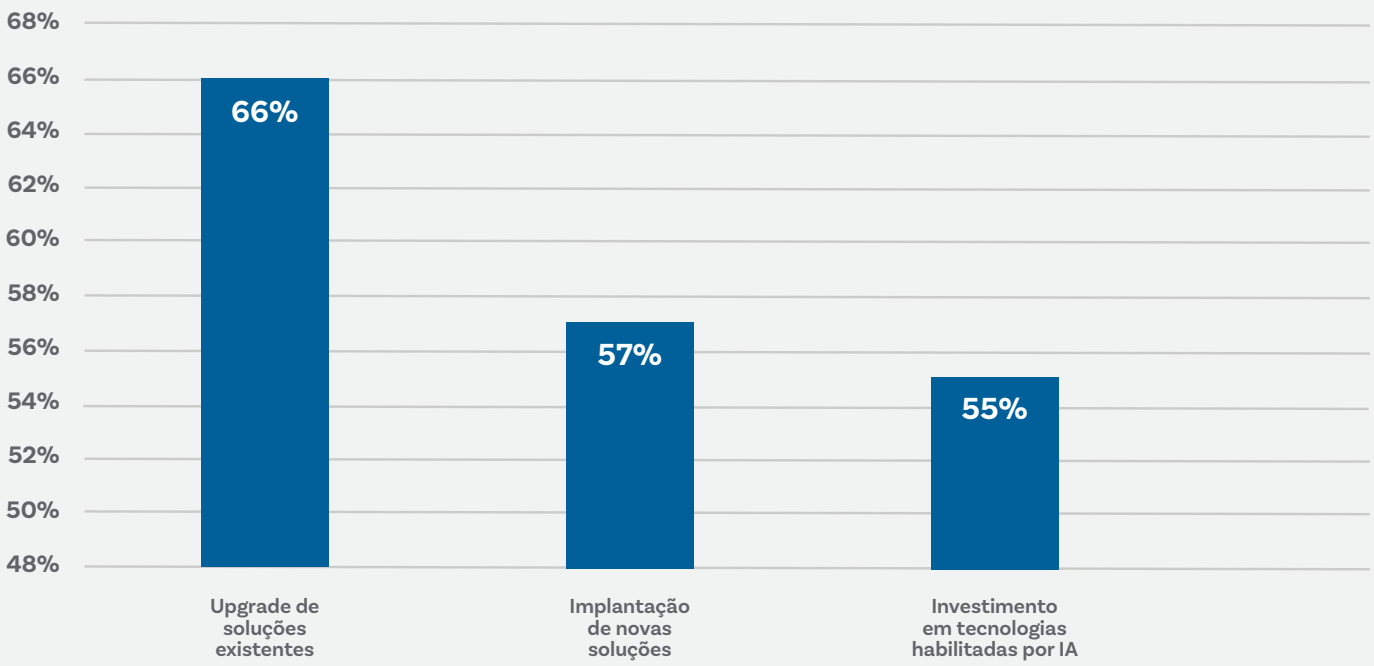
Conforme as novas tecnologias evoluem, muitas ferramentas emergentes estão tornando os ciberataques ainda mais fáceis de executar. Embora a IA e ferramentas semelhantes possam aprimorar os esforços de cibersegurança, também podem simplificar o phishing e o spam, a chantagem e o terrorismo, a desinformação e a interferência eleitoral, de acordo com Jen Easterly, chefe da Agência de Cibersegurança e Segurança de Infraestrutura do governo federal dos EUA. Ela também **destaca** que a IA generativa está gerando novas oportunidades para os cibercriminosos, inclusive os menos sofisticados.

Os membros do conselho deveriam recorrer às suas equipes de auditoria interna para obter informações e conselhos cruciais sobre a melhor forma de evitar ciberataques e avaliar a agilidade de suas respostas depois que eles ocorrerem. Os auditores internos podem oferecer avaliações independentes do ambiente de controle e de quaisquer riscos identificados que possam ajudar a permitir que a organização se recupere melhor de um ataque.

PERGUNTAS PARA OS MEMBROS DO CONSELHO

- Como monitoramos as novas ciberameaças, inclusive como outras organizações reagiram a elas?
- Como a organização mensura e avalia sua própria resiliência cibernética?
- Como usamos essas informações para adaptar nossa preparação para um ataque e nossas possíveis respostas?
- Quais são os nossos planos de recuperação de desastres? Até que ponto eles funcionaram bem no passado? O que aprendemos com essas experiências?
- Quais funções têm responsabilidade direta pelas estratégias de resiliência cibernética?
- Todos os funcionários entendem a necessidade da resiliência cibernética e o papel que podem desempenhar nela?

Como as empresas estão aprimorando sua cibersegurança?



Fonte: 2024 Cisco Cybersecurity Readiness Index.