Guardians of digital trust
Cybersecurity Awareness Month

Como os Conselhos de Administração poderão aprofundar os seus conhecimentos sobre Cibersegurança

Seis estratégias para proteger a sua organização contra ciberameaças

BDO

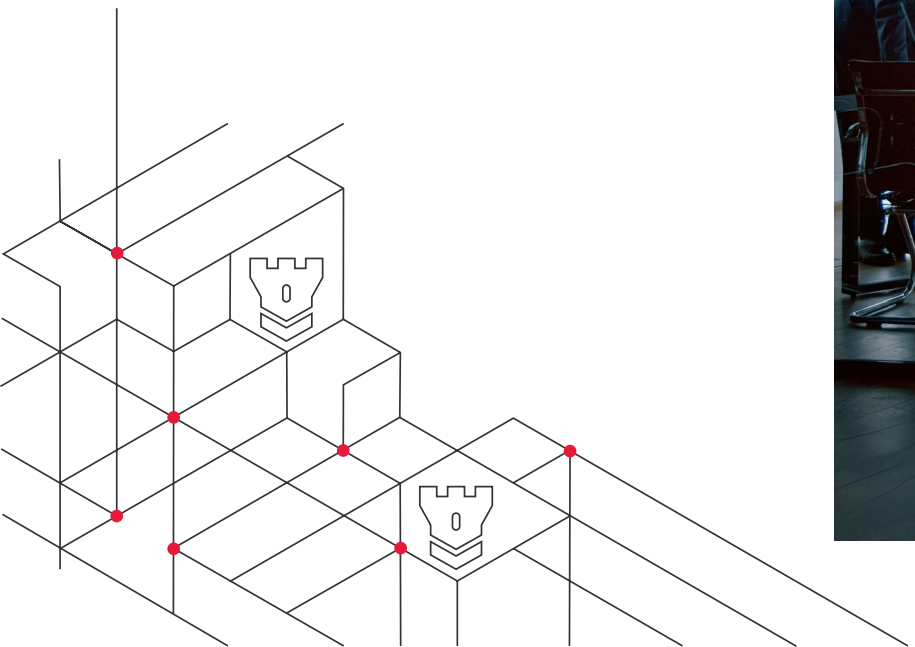
Como os Conselhos de Administração poderão aprofundar os seus conhecimentos sobre cibersegurança: seis estratégias para proteger a sua organização contra ciberameaças.

Os incidentes de cibersegurança estão a aumentar não só em frequência, mas também em custo.

De facto, o custo médio global de uma violação de dados em 2024 é de 4,88 milhões de dólares, o que representa um aumento de 10% em relação a 2023. Este é também o custo mais elevado até à data. Naturalmente, as repercussões financeiras não são o único custo que as organizações enfrentam ao lidarem com um incidente de cibersegurança, uma vez que os danos reputacionais e operacionais podem igualmente comprometer o negócio.

Os membros do conselho devem desempenhar um papel ativo na mitigação e prevenção de ciberataques. No entanto, apenas 12% das empresas do S&P 500 têm um membro do conselho, atual ou anterior, que seja especialista em cibersegurança. Esta lacuna de conhecimento pode estar a prejudicar a sua organização, tanto agora como no futuro.

Como pode garantir que a sua organização não se torne uma notícia sobre a mais recente violação de cibersegurança? Começa por fazer as perguntas certas.



Navegando no atual panorama da cibersegurança: Áreas de foco para o conselho

As capacidades tecnológicas cresceram significativamente ao longo dos anos, permitindo que as organizações operem de forma mais eficiente e acelerem resultados. À medida que a tecnologia se torna cada vez mais interligada com os objetivos empresariais, os membros do conselho precisam avaliar as decisões tecnológicas da mesma forma que avaliam as decisões estratégicas de negócio. Assim como o conselho orienta a direção do negócio da organização, também é agora responsável por garantir que os elementos tecnológicos adequados estão ativados para apoiar a estratégia empresarial e que o nível apropriado de tolerância ao risco cibernético é alcançado e gerido.

Para garantir uma supervisão responsável, o conselho deve focar nas seguintes áreas:

01

Alinhamento estratégico

Assegure que as iniciativas de cibersegurança estão alinhadas com os objetivos empresariais e tecnológicos da organização. Para ser proativo, os conselhos devem também garantir que os riscos e tendências futuras são considerados.

02

Conformidade regulamentar

Proporcionar supervisão sobre a conformidade da organização com as regulamentações e leis relevantes. Isto inclui assegurar que as auditorias e avaliações necessárias são realizadas e que o conselho tem conhecimento e uma compreensão clara dos resultados.

03

Governança e supervisão

Supervisionar as políticas, estratégias e alinhamento relacionadas com a cibersegurança da organização, bem como a sua conformidade com o quadro geral de gestão de riscos. O conselho deve compreender os riscos cibernéticos relevantes para a organização e garantir que as políticas estabelecidas apoiam a mitigação.

04

Monitorização e reporte

Como membro do conselho, é importante garantir que recebe atualizações regulares sobre a saúde cibernética da organização, incluindo o progresso em iniciativas-chave de cibersegurança, métricas essenciais e indicadores de desempenho.

05

Envolvimento de especialistas

Envolva-se com especialistas em cibersegurança, seja através da nomeação de um especialista em cibersegurança para o conselho, aproveitando um CISO na equipa de gestão ou consultando um CISO Virtual (vCISO) externo. Isso garantirá que o conselho está bem informado sobre ameaças e tendências emergentes.

06

Resposta a incidentes cibernéticos

Assegure que a organização possui um programa definido de resposta a incidentes e que revê regularmente as atualizações sobre os resultados dos testes de resposta a incidentes. No caso de um incidente cibernético, o conselho deve desempenhar um papel na supervisão de como a organização comunica com o público e as partes interessadas.

Seis estratégias para aumentar o seu conhecimento em cibersegurança

Para que os conselhos supervisionem com sucesso o programa de cibersegurança da sua organização, é essencial preencher a lacuna de conhecimento atual. Isso ajudará a garantir que a cibersegurança seja devidamente abordada nas reuniões regulares do conselho e permitirá que os conselhos cumpram as suas funções com confiança no que diz respeito à cibersegurança.

Aqui estão seis estratégias que pode utilizar para aprofundar o seu conhecimento e estar mais preparado para integrar o risco tecnológico nos processos de tomada de decisão:

01

Estabeleça sessões regulares de educação em cibersegurança.

Assegure-se de que recebe atualizações regulares sobre cibersegurança. Durante estas sessões, reserve tempo para discutir os principais riscos na sua indústria e as experiências relevantes de organizações similares, e faça perguntas sobre o que a sua empresa está a fazer para mitigar, prevenir ou responder ao risco de que esses tipos de incidentes ocorram na sua organização. As respostas que receber podem ser fundamentais para fortalecer a estrutura de defesa da sua organização.

02

Redirecione as métricas e utilize benchmarks da indústria.

É importante mudar o foco de métricas técnicas para métricas de bom senso que destaquem o risco e o valor. Por exemplo, identificar o número de sistemas obsoletos com vulnerabilidades e os controlos implementados para mitigar os seus riscos, ou discutir os custos totais das violações cibernéticas, que incluem a equipa de resposta real, apoio jurídico, assim como os impactos nos prémios de seguros e na receita da organização. Utilize benchmarks da indústria para comparar a sua organização com outras no seu setor, ajudando a entender onde a organização se posiciona e quais melhorias são necessárias.

03

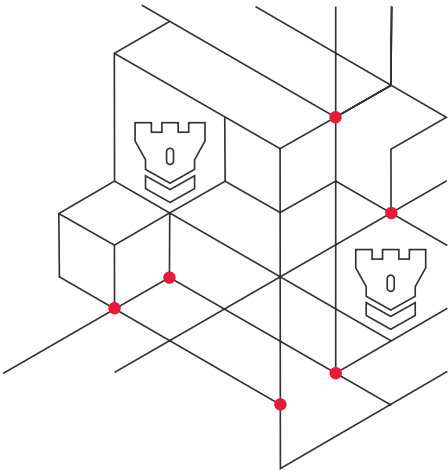
Traga especialistas em cibersegurança externos.

Ao trazer especialistas em cibersegurança externos, os membros do conselho podem não só aprimorar o seu conhecimento em cibersegurança, mas também obter apoio para "traduzir" informações focadas na tecnologia em percepções e estratégias centradas no risco. No final, adicionar um assento dedicado à cibersegurança no conselho oferecerá acesso regular à expertise necessária que complementa a gestão de riscos, segurança e equipas tecnológicas da sua organização.

04

Realize simulações cibernéticas.

Para obter uma compreensão mais profunda das ameaças cibernéticas reais e como responder a estas, considere realizar simulações de incidentes. Estes exercícios ajudarão a entender o seu papel como membro do conselho durante um evento cibernético, os impactos potenciais, áreas para melhoria contínua nos fluxos de processo e a desenvolver memória muscular.



05

Proporcionar supervisão durante um incidente.

No caso de um ciberataque, os membros do conselho devem envolver-se ativamente e receber atualizações dos especialistas em segurança e das equipas de resposta a incidentes. Ao manter-se atualizado sobre o progresso e os resultados do incidente, poderão oferecer supervisão independente e fazer perguntas para descobrir riscos persistentes. É também importante que os conselhos compreendam como a organização planeia responder a futuros ciberataques.

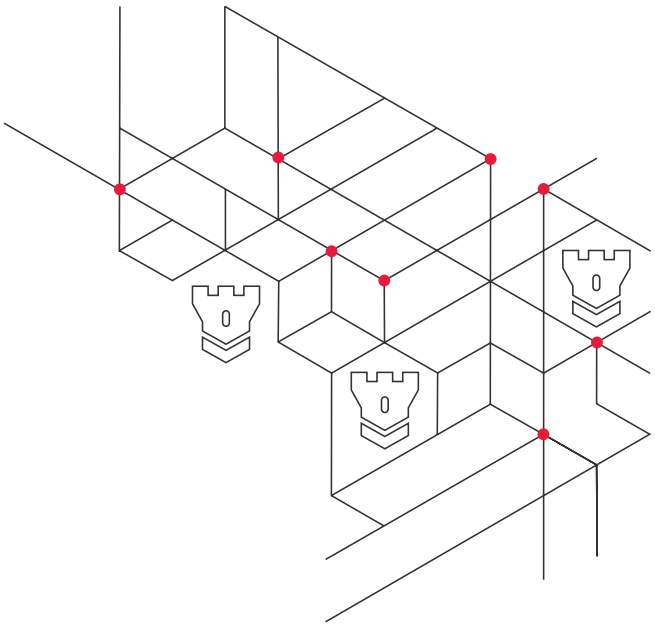
06

Olhe para trás com perspicácia.

O que pode aprender com situações limites ou mesmo um incidente cibernético anterior pode ser o que impede que ocorra novamente, especialmente uma vez que 83% das organizações já tiveram mais de uma violação de cibersegurança. Pergunte quantas vezes estas situações limites ou incidentes reais ocorreram e o que a organização aprendeu para identificar lacunas e desenvolver medidas adequadas.

O que mudou nos últimos anos é o nível de escrutínio em torno do conselho de administração. Afinal, os conselhos estão lá para ajudar a organização a gerir riscos — e isso inclui riscos de incidentes de cibersegurança.

Num estudo recente da Gartner, 88% dos conselhos de administração afirmaram ver a cibersegurança como um risco empresarial, o que destaca a mudança para priorizar a cibersegurança como um foco do conselho. É seu dever fiduciário não apenas fornecer supervisão independente para gerir a postura de cibersegurança da empresa, mas também desafiar a sua organização de diferentes maneiras para elevar o padrão da sua estrutura de defesa.



Na BDO, a nossa abordagem à cibersegurança inclui uma abordagem focada no negócio para gerir o risco cibernético. Oferecemos sessões de educação para o conselho para ajudar a preencher a lacuna de conhecimento e permitir que os membros do conselho se mantenham à frente do panorama tecnológico em rápida evolução. Nessas sessões, mostramos aos membros do conselho como redirecionar uma conversa centrada na tecnologia para uma sobre risco empresarial, de modo que os conselhos possam oferecer efetivamente um nível responsável de supervisão e fazer as perguntas certas às suas equipas. As nossas sessões de educação para o conselho também abordam os mais recentes riscos cibernéticos que as organizações estão a enfrentar atualmente e o que as organizações estão a fazer para mitigar essas ameaças.

CONTACTE A NOSSA EQUIPA DE LIDERANÇA EM CIBERSEGURANÇA HOJE

Aumente o seu conhecimento sobre cibersegurança e esteja preparado para o que o panorama de ameaças traz a seguir.