Relatório CISO

O caminho para a resiliência digital começa com seu conselho de administração

splunk>
a CISCO company

Os CISOs vivem em meio a riscos todos os dias. Combatemos malware, impedimos pessoas mal-intencionadas e aplicamos conformidade.

Mas estar em descompasso com seu conselho de administração apresenta outro tipo de risco. Se não conseguirmos articular o impacto potencial das questões de segurança, elas provavelmente continuarão a representar uma ameaça.

Esse é o desafio por excelência para os CISOs e seus conselhos de administração: contar a história de segurança na altitude certa para pessoas que possam apoiar a nossa visão. No Relatório CISO deste ano, colocamos esse relacionamento sob um microscópio para descobrir o que cada um pensa da outra parte. A pesquisa confirmou uma tendência que temos observado nos últimos anos: os CISOs estão interagindo mais com os conselhos.

No entanto, ainda existem muitas áreas de desalinhamento, incluindo quais as competências mais importantes para os CISOs desenvolverem, como os CISOs passam o tempo e quais as estratégias eficazes para persuadir os conselhos de administração para orçamento adicional.

Para preencher essas lacunas, os CISOs terão de falar a mesma língua que os conselhos de administração. Na minha experiência, isso significa passar muito mais tempo cara a cara com eles e outros líderes da empresa para entender melhor os negócios e tornar a segurança um facilitador empresarial. Os CISOs que conseguem atribuir segurança às receitas e sabem o que causa preocupação ao conselho de administração demonstram que estão envolvidos no jogo e podem oferecer soluções – não apenas problemas que precisam que o conselho de administração resolva.

Esperamos que o Relatório CISO seja um recurso para você contar sua história, preencher lacunas de comunicação e obter o apoio do conselho para seu programa de segurança.

Michael Fanning

CISO, Splunk

Conteúdo

O início de uma bela amizade?

Óleo e água. Marte e Vênus. Seja qual for a metáfora, os CISOs e os conselhos de administração são inerentemente diferentes, com origens que podem parecer mundos separados.

As preocupações financeiras dos líderes empresariais, muitas vezes, entram em conflito com a insistência dos CISOs em investimentos vitais em cibersegurança. Mesmo um ligeiro mal-entendido sobre as prioridades pode causar divisões consideráveis no futuro, e os CISOs e os conselhos de administração podem não chegar ao ponto desejado.

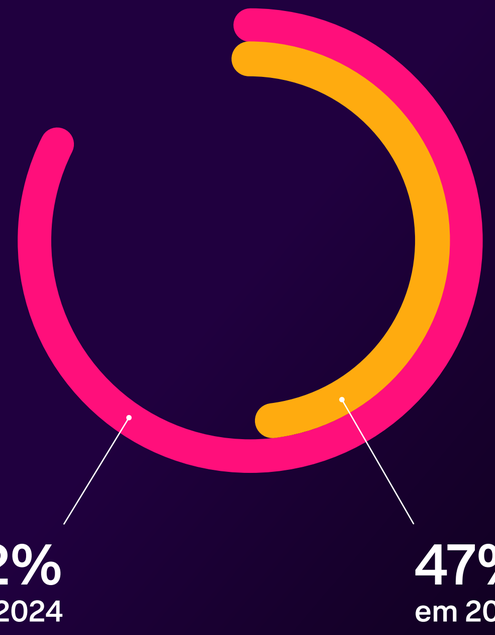
O relacionamento entre o CISO e o conselho está se aprofundando, pois eles têm mais oportunidades de se envolver em questões de cibersegurança e risco empresarial. A maioria dos CISOs (82%) reportam agora diretamente ao CEO, um aumento significativo em relação aos 47% em 2023. Os dois são como vizinhos que evoluem de conhecidos para amigos próximos, descobrindo interesses em comum ao longo do tempo, enquanto conversam.

Apesar das lacunas, eles compartilham o dever de proteger a empresa. Os conselhos protegem a rentabilidade e o preço das ações; Os CISOs protegem dados e sistemas. Isso é algo importante. Mas será preciso comunicação, compreensão e uma dose generosa de paciência para que tudo aconteça.

Para ter sucesso, cada parte terá de sair da zona de conforto e aprender a linguagem da outra parte. Para os CISOs, isso significa compreender o negócio além da superfície e encontrar novas maneiras de transmitir o ROI das iniciativas de segurança aos seus conselhos de administração. Para os membros do conselho, isso significa comprometer-se com uma cultura de segurança em primeiro lugar e considerar o CISO como a principal parte interessada nas decisões que afetam o risco e a governança empresarial.

Quando os CISOs e os conselhos de administração realizam a sua missão conjunta, tornam-se aliados imparáveis que podem impulsionar a organização no caminho para a resiliência digital.

Mais CISOs estão se reportando ao CEO



Os CISOs atuam na gerência executiva

À medida que mais CISOs se reportam diretamente ao CEO, eles consolidam seu lugar na diretoria e nas salas de reunião, influenciando decisões estratégicas de negócios. O status elevado, no entanto, teve sua cota de dificuldades crescentes. Assim como acontece em muitos relacionamentos, um dos parceiros pensa que tem um relacionamento um pouco melhor do que o outro.

Analisando de forma ampla o desempenho dos CISOs, 84% dos entrevistados do conselho afirmam que os CISOs atendem às suas expectativas. Em um primeiro momento, isso parece positivo. Dados os desafios complexos dos chefes de segurança, será suficiente cumprir os rigorosos padrões de excelência dos conselhos? Presumivelmente, os CISOs que vão além gerariam mais confiança, mas apenas 8% dos entrevistados do conselho disseram que os CISOs superam as expectativas.

Quando analisamos os detalhes do relacionamento, os dados da pesquisa mostram que os CISOs consistentemente acham que estão melhor posicionados com o conselho de administração nas responsabilidades principais. Em comparação com os entrevistados do conselho, os CISOs sentem que estão em terreno mais firme em tudo, incluindo a contratação e a formação da organização de segurança, a orçamentação adequada e o alinhamento com os objetivos estratégicos de cibersegurança.

Os CISOs superestimam seus relacionamentos com os conselhos em áreas-chave

Entrevistados que disseram que o relacionamento era *muito bom* ou *excelente*

Os conselhos são líderes empresariais muito bons no gerenciamento de negócios e resultados financeiros. Mas eles não entendem materialmente que sua dependência está na tecnologia e nas ramificações de segurança de como eles gerenciam a tecnologia.

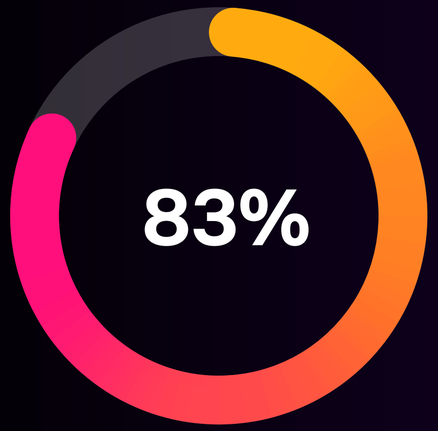
Christopher Kennedy, CISO, Group 1001

Mas a situação não é muito diferente do outro lado. Os CISOs não estão exatamente confiantes nas medidas do conselho de administração com relação à cibersegurança. Embora 60% reconheça que os membros do conselho com experiência em cibersegurança influenciam mais fortemente as decisões de segurança, nem todos os conselhos têm uma autoridade como essa. Apenas 29% dos CISOs afirmaram que o seu conselho inclui pelo menos um membro com experiência em cibersegurança.

É nessas relações fundamentais do conselho que começa grande parte da futura divisão. Uma pequena desconexão nesse sentido pode ter reflexos em áreas críticas, como resposta a incidentes e crescimento dos negócios.

No entanto, algumas dessas percepções podem mudar, dado que 83% dos CISOs participam atualmente em reuniões do conselho de administração com *alguma frequência* ou a *maior parte do tempo*. É concebível que essa evolução molde a forma como os conselhos abordam a política de cibersegurança e a cultura organizacional.

Felizmente, as atuais lacunas não são intransponíveis. A presença regular dos CISOs na sala de reuniões e seus conselhos sobre riscos empresariais fortalecerão a confiança e o alinhamento do conselho.



dos CISOs agora participam de reuniões do conselho *com certa frequência* ou *na maior parte do tempo*

Quando comecei como CISO, o importante era conseguir um lugar à mesa do conselho. Isso mudou. Agora, não há discussão ou debate sobre se a função do CISO deveria fornecer relatórios diretamente ao conselho.

Bruce Foreman, CISO, UMass Memorial Health

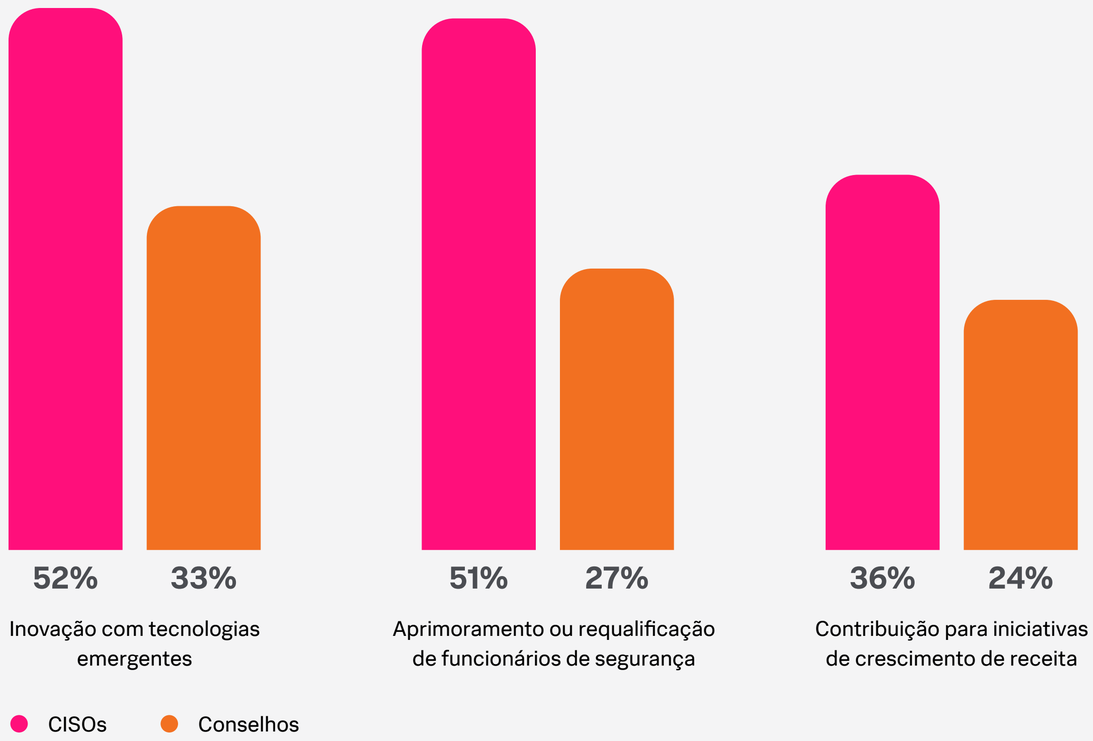
Os CISOs e os conselhos cuidam das lacunas

Nossa pesquisa indica que a lacuna pode estar diminuindo entre os conselhos e os CISOs em determinadas prioridades de segurança. Por exemplo, eles estão fortemente alinhados na proteção de informações confidenciais da empresa — 70% dos conselhos e 68% dos CISOs dizem que isso é *muito importante* ou *de máxima importância*.

No entanto, ainda há lacunas críticas. As prioridades dos CISOs correspondem aos seus conhecimentos técnicos, moldando a forma como executam essas prioridades e, em última análise, eles alcançam os objetivos de longo e curto prazo.

Maiores lacunas nas prioridades entre CISOs e conselhos

Respostas classificadas como *muito importantes* ou *de extrema importância*



Os conselhos de administração querem saber: como otimizar o tempo?

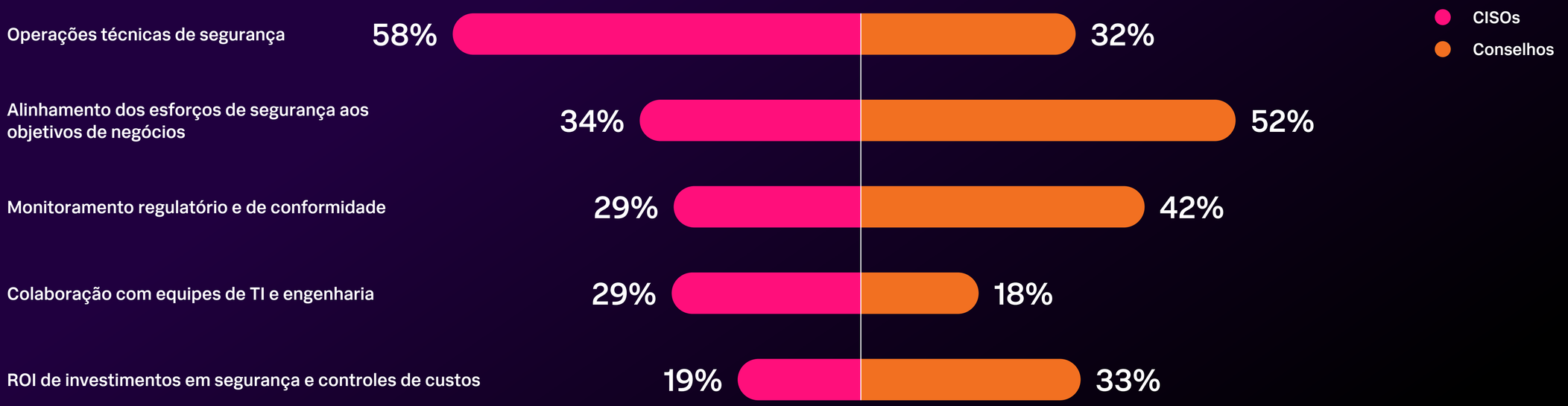
Com algumas das prioridades mais significativas em conflito, os CISOs e os conselhos de administração também divergem sobre como os CISOs e as equipes de segurança devem utilizar o seu tempo e energia para tornar os seus objetivos viáveis.

Então, o que exatamente os CISOs fazem o dia todo? Embora 63% dos CISOs e dos conselhos estejam alinhados, dizendo que os CISOs dedicam a maior parte do seu tempo à postura de segurança e à mitigação de riscos, as suas percepções divergem depois disso. 52% dos entrevistados do conselho acreditam que os CISOs passam a maior parte do tempo capacitando os negócios – alinhando os esforços de segurança aos objetivos de negócios — em comparação com apenas 34% dos CISOs. Na realidade, os aspectos técnicos da cibersegurança ocupam muito mais tempo do CISO do que o conselho imagina. De acordo com 58% dos CISOs, a maior parte do tempo deles e de sua equipe é gasta na escolha, instalação e operação de tecnologia.

> **Se uma empresa não está acostumada com o alto custo da cibersegurança, então um CISO precisa explicar ao conselho todas as funções da equipe de segurança e mapear como as responsabilidades de segurança estão interligadas em toda a estrutura do negócio.**
>
> Christopher Kennedy, CISO, Group 1001

Percepção x realidade

Como os CISOs e suas equipes passam a maior parte do tempo



Habilidades de negócios ajudam os CISOs a diversificar

Os conselhos têm grandes esperanças nos CISOs, sendo a maior delas que eles se tornem melhores líderes empresariais. No entanto, os CISOs podem ver essa ambição de forma diferente ou seguir caminhos alternativos para chegar lá.

Mais do que os CISOs, os entrevistados do conselho enfatizaram a perspicácia empresarial e as competências interpessoais, como empatia e comunicação, como as principais competências a desenvolver. Para os CISOs, a colaboração com as equipes de TI e engenharia e o conhecimento de conformidade são as áreas de desenvolvimento mais importantes.

"Adicionar novos conjuntos de habilidades para aprender e aprofundar torna o trabalho do CISO mais complexo e possivelmente mais desafiador", disse Marcus LaFerrera, diretor da equipe de pesquisa de segurança da SURGe.

Pode ser por isso que 53% dos CISOs afirmam que as suas responsabilidades e expectativas se tornaram mais difíceis desde que assumiram o cargo.

Apesar da importância dos CISOs nas fileiras executivas e do desejo dos conselhos de que eles desenvolvam conhecimentos de negócios, talvez os conselhos ainda não enxerguem além das suas credenciais técnicas. No entanto, os CISOs podem mudar essa percepção. "A menos que o CISO tenha a sabedoria e os recursos para defender um lugar mais apropriado na hierarquia, acho que os CISOs ainda são considerados uma função específica para resolver problemas com a tecnologia, em vez de entender materialmente como a tecnologia impulsiona nossos negócios", disse Christopher Kennedy, CISO, Group 1001.

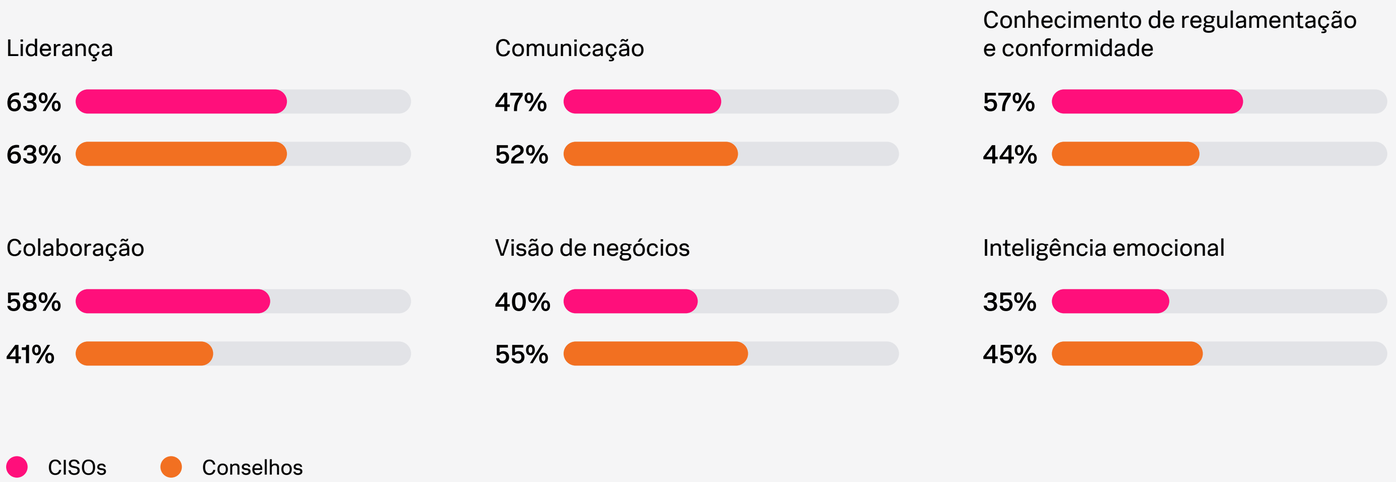
Caberá aos CISOs aumentar a consciência sobre as prioridades dos negócios e do conselho e como elas se relacionam com os objetivos de receita e crescimento. Eles podem preencher lacunas através de uma comunicação ascendente proativa e eficaz e do cultivo de uma compreensão mais profunda da estratégia da organização. Depois de terem uma visão geral, eles podem determinar como uma estratégia de segurança deve se encaixar nisso.

"O CISO precisa colaborar e fazer parceria com outras funções da empresa. A segurança não deve ser um departamento isolado. Precisamos trabalhar em conjunto com o jurídico, com os riscos e com os chefes de negócios. Portanto, o CISO tem que ser um bom comunicador", disse Chenxi Wang, sócio geral da Rain Capital e membro do conselho da MDU Resources.

53%

dos CISOs afirmam que as suas responsabilidades e expectativas se tornaram mais difíceis

As habilidades mais importantes para os CISOs desenvolverem



O sucesso é diferente para CISOs e conselhos

Em geral, os conselhos de administração e os CISOs concordam que os principais KPIs de cibersegurança, como o número de incidentes materiais de segurança e a oportunidade da gestão de vulnerabilidades, são importantes. No entanto, a maior parte dos conselhos e CISOs (79%) afirmam que os KPIs para as equipes de segurança mudaram substancialmente nos últimos anos.

"Os negócios estão mudando. Temos aspirações de entrar em novos modelos comerciais e em novas áreas de negócios, e depois vamos lidar com dados de consumidores e dados pessoais. A minha postura mudou porque agora vejo a segurança como um risco maior do que há dois anos", disse Prasanna Ramakrishnan, CISO global da Clarios.

Os conselhos também têm padrões específicos para avaliar o desempenho de um CISO, como o ROI dos investimentos em segurança. Essa é provavelmente uma das razões pelas quais os conselhos esperam que os CISOs sejam estratégicos e não táticos, comunicando de forma mais holística sobre como as suas iniciativas impactam os negócios.

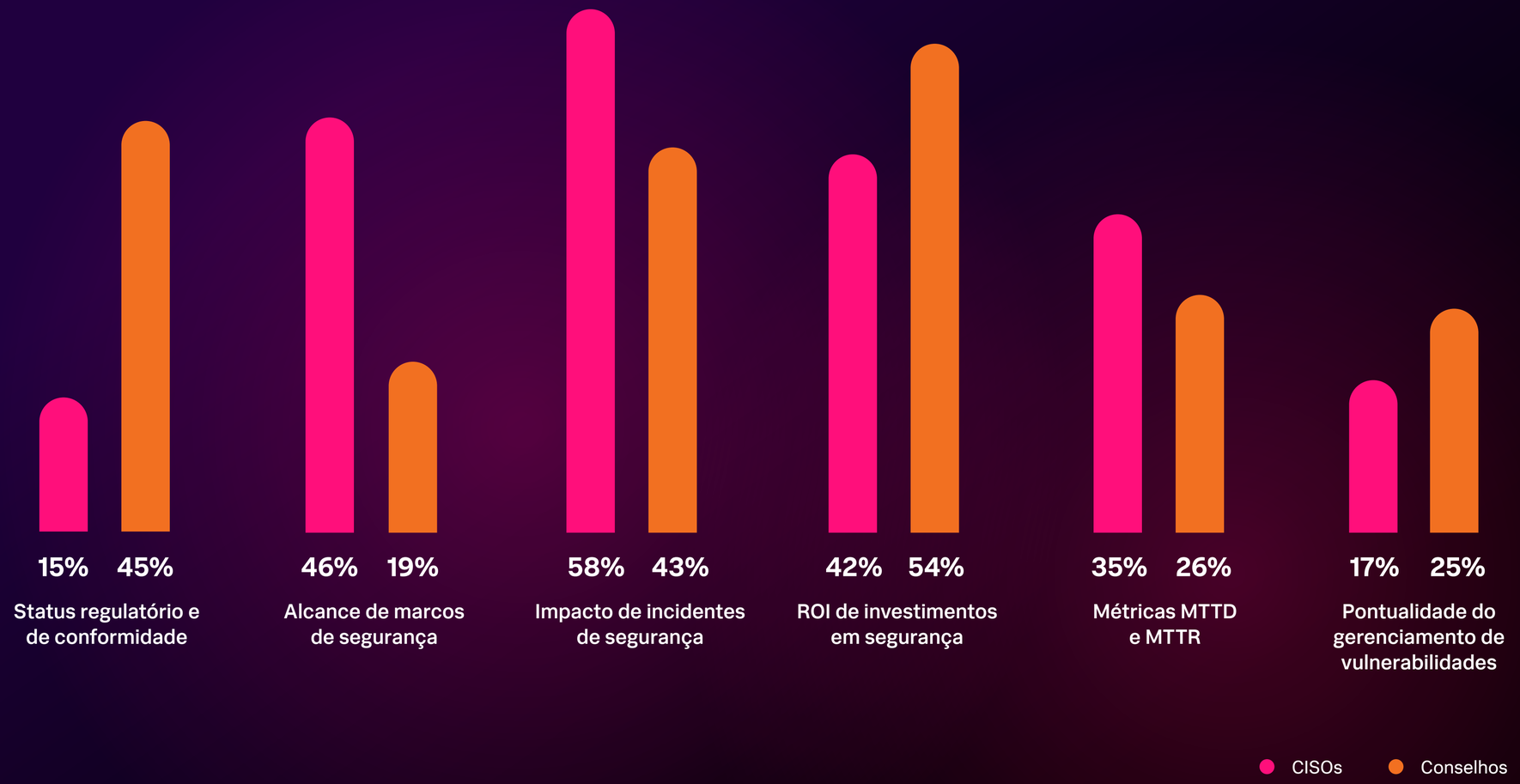
"Não consideraremos avançar com um investimento em segurança, a menos que tenha um ROI mínimo de 15%. Caso contrário, será difícil justificar", disse um membro do conselho de um grupo bancário multinacional com sede no Reino Unido.

O resultado disso? Por um lado, os conselhos não querem heroísmo no combate a incêndios por parte dos CISOs. Eles buscam liderança madura, estratégica e proativa e capacitação de negócios, e não apenas controle de danos quando um incidente ocorre inevitavelmente. Os CISOs que conseguem educar o conselho sobre como seus KPIs de segurança podem beneficiar os negócios terão mais sucesso.

Ao apresentar estimativas para iniciativas futuras, os CISOs podem persuadir os conselhos de administração, enfatizando que as despesas incorridas com a perda de receitas e danos à reputação serão provavelmente inferiores ao custo do tempo de inatividade devido a um incidente de segurança.

> **Os CISOs também precisam mudar as suas tácticas para serem melhor ouvidos, utilizando o precioso tempo no conselho de administração para justificar o ROI dos seus investimentos em segurança e elevar a segurança a um facilitador de negócios, e não apenas a um centro de custos.**
>
> Kirsty Paine, CTO de campo e consultora estratégica, Splunk

CISOs e conselhos medem o sucesso de forma diferente

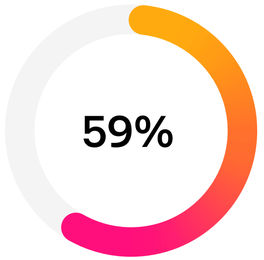


A conformidade está se tornando pessoal para os CISOs

Os ambientes regulatórios tornaram-se mais complexos, expansivos e punitivos, exigindo relatórios de incidentes mais rápidos e colocando mais responsabilidades diretamente sobre os ombros dos CISOs. Como resultado, eles estão adotando uma abordagem mais rigorosa e pessoal em relação à conformidade.

Uma questão importante: o atrito de relatar a não conformidade

Não é de surpreender que os CISOs levem a sério a postura de conformidade de suas organizações – muito depende de suas decisões. Afinal, os CISOs, e não os conselhos, serão os maiores responsáveis pelos incidentes de segurança. Os CISOs enfrentam mais escrutínio regulatório, responsabilidade legal, pesadas penalidades financeiras e a possibilidade de perderem seus empregos se forem encontrados em violação.



dos CISOs relatariam se sua organização ignorasse os requisitos de conformidade

Talvez ainda mais chocante, 21% dos CISOs revelaram que foram pressionados a não reportar um problema de conformidade. Felizmente, a maioria dos CISOs entrevistados está disposta a avançar e fazer a coisa certa – 59% disseram que se tornariam denunciantes se a sua organização ignorasse os requisitos de conformidade.

"Pressionar os CISOs para não reportarem problemas, em vez de serem abertos e transparentes sobre quaisquer falhas e lições a aprender, significa que não podem ser tomadas decisões baseadas no risco — as pessoas certas não têm a informação real. Isso pode ser muito perigoso", disse Kirsty Paine, CTO de campo e consultora estratégica do Splunk, uma empresa da Cisco.

É claro que, quando um incidente é considerado "material" (e a definição é superficial), as empresas devem comunicá-lo às autoridades dentro de horas ou dias, dependendo do local do mundo em que operam. Mandatos recentes, incluindo a decisão sobre cibersegurança da SEC dos EUA, o NIS2 da Europa e a DORA, impõem janelas de comunicação muito mais estreitas – tão curtas quanto 24 horas no NIS2 – para a divulgação de incidentes de cibersegurança. Da mesma forma, a Lei de Segurança de Infraestruturas Críticas (SOCI) da Austrália exige relatórios obrigatórios dentro de 12 horas após a descoberta de um incidente.

Ao reportar incidentes e outros protocolos de conformidade, os CISOs devem trabalhar na gestão de crises muito antes de qualquer crise ocorrer. Um plano proativo ajudará a alinhar as expectativas com o conselho e a ter uma resposta definida para a empresa em geral.

“Acho que todos os que atuam como chefes de segurança ou na diretoria de empresas públicas deveriam se preocupar com a responsabilidade pessoal caso não estejam fazendo as coisas certas.

Chenxi Wang, sócio geral da Rain Capital e membro do conselho da MDU Resources

21%

dos CISOs foram pressionados a não relatar um problema de conformidade

Os CISOs se inclinam para a conformidade... até certo ponto

No rigoroso ambiente regulatório atual, a conformidade está se tornando uma parte descomunal do trabalho de um CISO. Isso poderia explicar por que 57% classificaram "profundidade de conhecimento relacionado a regulamentações e conformidade" como uma habilidade importante a ser desenvolvida.

E embora manter a conformidade seja vital para os negócios, os CISOs não acham necessariamente que seja a melhor maneira de medir o seu sucesso na supervisão da segurança. Apenas 15% dos CISOs classificaram o estado de conformidade como uma métrica de desempenho superior, uma diferença significativa em comparação com 45% dos conselhos. Historicamente, os CISOs não a viam como uma atividade de segurança estratégica.

Essa desconexão pode significar que os conselhos e os CISOs conversam entre si sobre conformidade. "Embora os conselhos saibam que a conformidade é importante, muitos podem não perceber ou compreender totalmente o trabalho necessário para alcançar isso. Com a falta de visão do dia a dia, não é surpreendente que os membros do conselho pensem que deveria ser 'fácil' ou fiquem confusos quando os CISOs e suas equipes gastam muito tempo para alcançar e manter uma forte postura de conformidade", disse Kirsty Paine, CTO de campo e consultor estratégico do Splunk, uma empresa da Cisco.

> **HIPAA e qualquer outra conformidade são cruciais. "Ao fazer isso, você está em conformidade." Mas isso não significa que você esteja em segurança. É uma linha de base, mas acho que isso é pouco.**
>
> Bruce Foreman, CISO, UMass Memorial Health

CAPÍTULO 4

Trazer melhores evidências para o debate orçamentário

Os orçamentos cibernéticos refletem apoio inconsistente e desalinhamento, diminuindo as expectativas dos CISOs, frustrando os conselhos de administração e ampliando o abismo entre eles.

Apenas 29% dos CISOs afirmam receber o orçamento adequado para iniciativas de cibersegurança e para atingir os seus objetivos de segurança, em comparação com 41% dos membros do conselho que consideram que os orçamentos de cibersegurança são adequados. Justificavelmente, os CISOs estão preocupados com a forma como essa falta de apoio afetará a postura de segurança da sua organização, e 64% revelam que a ameaça atual e o ambiente regulamentar os deixam preocupados por não estarem fazendo o suficiente.

Quando você vai ao conselho dizer que temos uma potencial ameaça cibernética, é difícil justificar o investimento. O problema habitual que enfrento é a certeza de um investimento versus a probabilidade de uma ameaça que pode não acontecer.

Membro do conselho de um grupo bancário multinacional com sede no Reino Unido

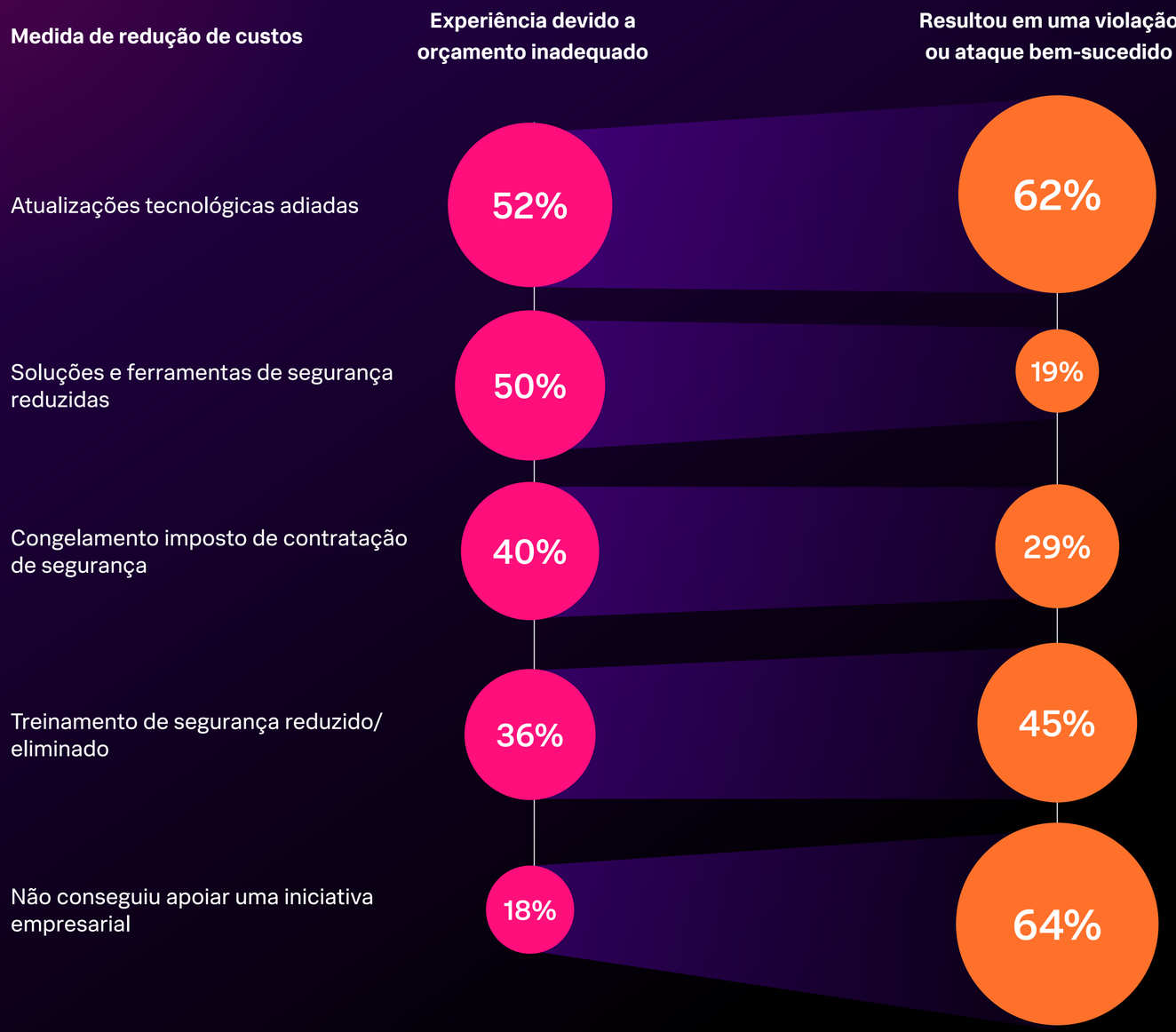
Pequenos cortes, consequências graves

Muitos CISOs adotaram medidas de redução de custos devido a orçamentos inadequados. Alguns dos cortes mais substanciais incluíram o adiamento de uma atualização de segurança, a redução do número de soluções para reduzir custos de licença e o congelamento de promoções, aumentos e contratações. Mas esses cortes de segurança não passam simplesmente despercebidos – eles geralmente trazem consequências graves, como ataques de segurança bem-sucedidos ou violações de dados.

Enquanto isso, os ataques cibernéticos não mostram sinais de desaceleração. Impressionantes 94% dos CISOs relatam ter sido vítimas de um ataque cibernético disruptivo. A maioria, 55%, relata tê-los experimentado pelo menos *algumas vezes* e outros 27% disseram que foram vítimas *muitas vezes*.

O financiamento adequado será crucial para garantir defesas cibernéticas adequadas, com os CISO a afirmarem que a área mais significativa de investimento futuro será na gestão de riscos cibernéticos (64%). Esses e outros novos investimentos em infraestruturas, ferramentas, soluções e serviços serão fundamentais para ajudar os CISOs e as suas equipes a proteger os dados e sistemas das suas organizações.

Orçamentos de segurança inadequados trazem consequências



Os CISOs defendem a segurança falando a linguagem do conselho

Então, o que realmente convence os conselhos a abrirem suas carteiras? Muitos conselhos afirmam que dão prioridade ao crescimento dos negócios (44%) em detrimento do reforço do programa de cibersegurança (24%), o que significa que estão inclinados a apoiar iniciativas de cibersegurança que proporcionem maior valor aos acionistas e à organização. Apresentar a segurança como um facilitador de negócios é, de longe, o argumento mais poderoso, com 64% dos conselhos. Mas apenas 43% dos CISOs afirmam envolver-se nesta prática.

Para conseguirem o que desejam, os CISOs terão de aprender como defender o que precisam de uma forma que seja convincente para o conselho. Resumindo, eles precisam aprender a falar fluentemente a linguagem do conselho.

Os CISOs podem fazer com que os conselhos ouçam e respondam às solicitações de orçamento, apresentando-lhes cálculos concretos sobre os custos diretos e secundários do tempo de inatividade, incluindo perda de receita, multas de SLA e fatores que afetarão os acionistas. O tempo de inatividade custa anualmente 400 bilhões de dólares às empresas da Global 2000, com uma média de 200 milhões de dólares por empresa, ou cerca de 9% dos lucros.

46% dos conselhos afirmam que estes tipos de custos são convincentes nas discussões orçamentais. Embora 39% dos CISOs já façam isso, ainda existem amplas oportunidades para refinarem os seus poderes de persuasão, como apresentar métricas e recomendações de risco cibernético que orientem as decisões de gestão e educar o conselho sobre o impacto dos ataques cibernéticos.

A questão financeira é crucial. E, com a alocação correta, isso pode evitar violações dispendiosas e violações de conformidade, salvando a reputação da sua organização e economizando milhões de dólares no futuro.
A estratégia de comunicação vencedora é explicar como a segurança impulsiona o ROI, ajuda o negócio a crescer e protege os preços das ações. Isso sempre chamará a atenção do seu conselho.

As abordagens que os conselhos consideram mais convincentes quando solicitadas a aumentar os orçamentos de cibersegurança

34%
Enfatiza os requisitos de conformidade regulatória

49%
Fornece métricas e recomendações de risco cibernético

46%
Apresenta cálculos sobre o custo do tempo de inatividade

37%
Explica o impacto comercial dos ataques à segurança

64%
Posiciona a segurança como um facilitador de negócios

CAPÍTULO 5

A IA capacita defensores e adversários

Tanto para os CISOs como para os conselhos de administração, a IA está repleta de incertezas e de potencial. Eles concordam que ela é digna de investimento atual e futuro. Ainda assim, uma parte significativa dos CISOs sente que não está avançando suficientemente rápido na IA para se manterem competitivos ou acompanharem o ritmo da inovação.

A IA pode ser um multiplicador de força de segurança para análise de malware, detecção de ameaças, padrões de configuração e outras funções – mas apenas se os CISOs ajudarem os seus conselhos a ver as possibilidades e motivá-los a investir mais em infraestruturas, formação e governança.

A IA dá vantagem aos adversários cibernéticos

A IA ainda representa uma ameaça na fronteira cibernética, com 53% dos CISOs acreditando que ela dará aos invasores uma vantagem ligeira ou significativa. No entanto, esse grupo está diminuindo visivelmente de 70% em 2023.

As ameaças de IA percebidas mais preocupantes são ataques de phishing mais realistas e deep fakes (57%), seguidos por novas variedades de malware (44%), ataques adaptativos de engenharia social (40%) e exploração de soluções generativas existentes (40%). E o medo, especialmente em relação à ameaça dos deepfakes, não é infundado. A engenharia social já é o vetor de ataque mais comum vivenciado no ano passado, com 67%. É concebível que esse tipo de ataque cresça à medida que a IA continua a emular o comportamento e a fala de humanos de forma mais convincente.

As ameaças generativas de IA mais preocupantes para CISOs

57% E-mails de phishing altamente realistas

44% Novo malware que pode escapar da cibersegurança

40% Táticas adaptativas de engenharia social

40% Exploração de ferramentas de geração de IA usadas pela empresa

38% Ataques mais automatizados e eficientes

33% Ataques de força bruta mais rápidos

30% Deep fakes de voz e imagem realistas

As infinitas possibilidades da IA

Apesar das suas preocupações sobre a IA nas mãos de agentes de ameaças, a maioria dos CISOs reconhece a promessa que ela representa, considerando a IA *apropriadamente significativa* (70%) ou mesmo*subestimada* (21%).

Os CISOs e suas equipes muitas vezes ficam tão envolvidos se escondendo, em um jogo defensivo com invasores cibernéticos, que sonhar acordado com investimentos futuros, às vezes, pode parecer uma indulgência. Por sorte, a ascensão da IA como ferramenta de defesa cibernética permitirá que eles sejam mais inovadores.

22% dos CISOs afirmam que a IA dará aos defensores cibernéticos uma ligeira vantagem sobre os invasores. A maioria dos CISOs (53%) também acredita que estão adotando a IA ao ritmo certo, embora mais de um terço (38%) acredite que não estão avançando suficientemente rápido. Os conselhos também afirmam que as suas organizações utilizam atualmente IA para cibersegurança (24%), têm planos imediatos de utilizá-la no próximo ano (41%) ou têm interesse em fazer isso (33%).

Muitos CISOs estão lançando as bases para novas defesas cibernéticas baseadas em IA. Quase dois terços (65%) dos CISOs estão treinando ativamente equipes de segurança em engenharia de prompts. Além disso, mais de metade (56%) estão estabelecendo protocolos para determinar quais tarefas são apropriadas para a IA e quais são mais adequadas para humanos.

Olhando para o futuro nos casos de uso, a IA será uma área importante de investimento para CISOs e seus conselhos. Assim, os CISOs têm muitas chances de destacar o ROI desta ferramenta como um facilitador de negócios. Mostrar que a IA aumentará a competitividade e o tempo de colocação no mercado contribuirá muito para conseguir a adesão do conselho. Isso poderá até aumentar a alocação orçamental.

Principais casos de uso de segurança para IA generativa, de acordo com CISOs

47%
Análise de malware, detecção de ameaças e enriquecimento de alertas

39%
Criação de padrões de configuração de software de segurança

32%
Criação de regras de detecção de ameaças

30%
Análise de fontes de dados para reduzir o ruído de alerta

30%
Caça proativa a ameaças

28%
Criação de relatórios de segurança para comunicação interna

25%
Desenvolvimento de políticas de cibersegurança

CAPÍTULO 6

É mágico quando CISOs e conselhos se alinham

À medida que a cibersegurança se torna um componente padrão das decisões de negócios, ter um membro no conselho com experiência em segurança é cada vez mais vantajoso. Em virtude da proximidade, ter um CISO no conselho ou alguém com experiência em cibersegurança tende a fortalecer o relacionamento entre o CISO e o conselho. Devido ao seu profundo conhecimento de segurança, os membros do conselho com experiência em CISO podem se sentir mais confiantes sobre a postura de segurança da organização – eles são muito menos propensos do que outros membros do conselho a expressar preocupação por não estarem fazendo o suficiente para proteger a organização (37% contra 62% média da pesquisa).

Estar em ambos os mundos permite traçar um quadro preciso da postura de segurança da organização, apresentar melhores argumentos para investimentos futuros e ilustrar como a cibersegurança impulsiona os negócios.

No entanto, simplesmente colocar um CISO no conselho não será a solução única para as deficiências de segurança. É provável que uma empresa que leva a segurança a sério também tenha um CISO ou alguém com experiência em segurança no conselho, o que reflete uma dedicação à melhoria da cultura de segurança e uma vontade de adotar iniciativas relacionadas.

Mas, quer façam parte de um conselho ou não, os CISOs em situação regular com o conselho aproveitam visivelmente mais seus relacionamentos.

Ter membros do conselho com experiência em CISO é uma vantagem de relacionamento

Áreas em que os relacionamentos foram classificados como *muito bom* ou *excelente*

A comunicação aumenta a colaboração... e o orçamento

Não são apenas as relações com o conselho que funcionam melhor quando os CISOs interagem regularmente com o conselho, embora essas relações beneficiem claramente ambas as partes. Os CISOs com relacionamentos saudáveis com o conselho se beneficiam de uma melhor colaboração em toda a organização, reportando parcerias particularmente fortes com operações de TI (82% versus 69% de outros CISOs) e engenharia (74% versus 63% de outros CISOs). Isso pode ocorrer porque eles conseguem comunicar com eficácia as necessidades e estratégias de negócios do conselho aos departamentos mais técnicos, de uma forma que os conecta ao restante da organização.

Os CISOs com bons relacionamentos com o conselho também recebem maior confiança para testar e explorar novos investimentos em tecnologia. É mais provável que eles tenham a capacidade de buscar casos de uso para IA generativa, como criação de regras de detecção de ameaças (43% versus 31% de outros CISOs), análise de fontes de dados (45% versus 28% de outros CISOs), resposta a incidentes e investigações forenses (42% versus 29% de outros CISOs) e caça proativa a ameaças (46% versus 28% de outros CISOs).

Os CISOs são ligações críticas, traduzindo a linguagem dos departamentos orientados para a tecnologia e defendendo a segurança de uma forma que os conselhos possam compreender e vice-versa. No futuro, eles terão ainda mais oportunidades para desenvolver e fortalecer esses relacionamentos. Os conselhos demonstraram que estão dispostos a aprender simplesmente porque isso faz sentido para a sua estratégia, práticas e investimentos empresariais. Isso significa que os CISOs podem contribuir ainda mais para moldar o negócio através da cibersegurança.

CAPÍTULO 7

Abra o caminho para a parceria com seu conselho

A jornada continua para CISOs e conselhos. Eles fizeram grandes avanços para harmonizar metas, prioridades e estratégias de negócios. No entanto, ainda há a oportunidade de reduzir lacunas.

Aqui estão algumas etapas fundamentais que os CISOs podem seguir para ajudar a impulsionar o alinhamento e garantir relacionamentos com o conselho mais fortes, saudáveis e produtivos.

1

Explique ao seu conselho o que você está fazendo (e por quê)

Sempre há espaço para que os conselhos aprimorem seus conhecimentos em segurança. Isso é especialmente verdadeiro quando se discute a estratégia em torno da resposta a incidentes, o que não só lhes dará uma janela para os procedimentos padrão em qualquer momento, mas também iluminará o valor desses procedimentos quando enfrentam auditores ou durante uma crise.

Portanto, crie exercícios práticos para torná-los reais. Use recursos visuais e narrativa para transmitir sua mensagem. Em seguida, desenvolva uma estratégia e cadência e siga seu plano com sessões iterativas.

2

Aumente a confiança (e o orçamento)

É importante aprender a falar a língua do conselho. Embora os conselhos se beneficiem de sua experiência em cibersegurança, cabe a você fazê-los compreender suas necessidades e prioridades. Enfatize o ROI em vez do MTTD e aprenda como comunicar o valor dos seus investimentos e a importância da alocação de recursos de forma eficaz. (Talvez seja mais difícil de fazer, mas quando a segurança foi fácil?)

Também é importante se aprofundar em tópicos como proteção de receita e valor para os acionistas, minimização de interrupções nos negócios, melhoria da confiança na marca e fornecimento de experiências seguras e integradas ao cliente. Os conselhos se preocupam com o crescimento da empresa, então fale com os KPIs.

3

Assuma a conformidade e conheça sua responsabilidade pessoal

Os CISOs enfrentam um ambiente regulatório mais rigoroso e punitivo, por isso é aconselhável estar preparado. Isso significa conhecer a sua responsabilidade pessoal, potencialmente contratar um advogado em caso de incidente e adotar uma abordagem estratégica e bem documentada. Articule os riscos ao conselho e explique por que eventos relevantes exigem relatórios em primeiro lugar.

Você também deve saber o que os conselhos esperam em uma crise, codificar essas expectativas por escrito e certificar-se de que todas as partes concordam antes que ocorra um incidente, e não durante. Releia o seu contrato de trabalho e, se houver alguma lacuna, preencha.

4

Expanda seu escopo para incluir estratégia de negócios

Sabemos que sair da zona de conforto não é fácil. No entanto, ao assumir o papel de estrategista de negócios, você descobrirá como equilibrar as necessidades de negócios e, ao mesmo tempo, proteger sua organização. Porque se você quiser aumentar a segurança, deverá mostrar como a segurança faz a empresa crescer.

E não se trata apenas de desenvolver visão de negócios, embora você precise disso em abundância. Desenvolva suas habilidades interpessoais. Isso inclui aprimorar meios de comunicação mais eficazes e compreender como seu conselho prefere receber informações. Refinar a inteligência emocional também será um grande avanço.

5

Desenvolva liderança em toda a empresa, não apenas na segurança

Os CISOs e os conselhos concordam sobre a importância das habilidades de liderança. Isso significa gerenciar compreendendo o que é importante para o conselho e por quê. Isso também envolve uma comunicação eficaz com o RH, o jurídico e a gerência executiva, que são cruciais para avançar nas suas prioridades e garantir maiores investimentos em tecnologia.

Construa relacionamentos sólidos, mapeie as partes interessadas, passe tempo com elas e mostre interesse genuíno em seu trabalho e desafios. Colabore em iniciativas importantes para que, quando surgir uma crise, seus colegas já o vejam como um membro da equipe e estejam ansiosos para apoiar seus esforços.

Torne-se um líder de segurança com o Splunk

Perspectivas do Splunk — de líderes, para líderes

Procurando mais liderança inovadora e insights dos CISOs? Saiba como os líderes de segurança enfrentam os desafios mais críticos da atualidade, incluindo conformidade regulatória, IA e o cenário de ameaças em evolução.

Obter insights executivos

Estado de segurança 2024: A corrida para uso da IA

Descubra como os líderes e profissionais de segurança navegam por oportunidades e obstáculos, como exigências de conformidade, escassez de talentos e a ascensão da IA generativa.

Leia o relatório

Apêndice de setor

Produção

Em comparação com os equivalentes do setor, os CISOs de produção sentem-se menos apoiados pela gerência executiva, geralmente expressando menos otimismo sobre os seus orçamentos de colaboração e cibersegurança. Esta falta de apoio pode ser um fator que explica por que esse setor sofre mais ataques cibernéticos do que outras indústrias.

É menos provável que os CISOs digam que a gerência executiva apoia a estratégia da equipe cibernética e defende as suas políticas (41% contra 57% dos CISOs em todos os setores). Eles também são menos propensos (52%) a sentir que os KPIs das suas equipes cibernéticas são importantes para os conselhos, contra 64% em todos os setores.

Quanto ao financiamento da cibersegurança, apenas 20% dos entrevistados do setor dizem que as suas organizações fornecem orçamentos de cibersegurança adequados, e apenas 50% sentem que podem convencer os seus conselhos de administração a aumentar os orçamentos das equipes quando necessário. Os gastos do setor de produção estão aquém da média global, com 65 milhões de dólares em gastos anuais esperados contra 75 milhões de dólares.

Com apoio limitado e menos adesão estratégica à cibersegurança, as organizações de produção podem estar cada vez mais propensas a vulnerabilidades, como credenciais roubadas (relatadas por 58% dos seus CISOs) e processos de resposta a incidentes indefinidos (44%), que levaram a ataques bem-sucedidos. 95% do setor relata ter sido atingido por ataques cibernéticos diversas vezes nos últimos 12 meses (em comparação com 82% das organizações em todos os setores). Apesar desses ataques, apenas 9% dos conselhos de administração do setor citam o reforço do seu programa cibernético como o investimento futuro mais significativo.

Pode ser que os conselhos de produção estejam mais preocupados com o cenário geopolítico. 36% deles (em comparação com 25% em todos os setores) consideram a instabilidade geopolítica como o maior risco para a organização, possivelmente porque a produção é distribuída globalmente e afetada por perturbações na cadeia de abastecimento.

Para estarem em sintonia com seus conselhos, os CISOs de produção têm oportunidades de aumentar o foco na conformidade regulatória. 64% dos conselhos citam a conformidade como uma métrica principal para o sucesso dos CISOs, mas apenas 26% dos CISOs relatam que a equipe gasta muito tempo e esforço em questões legais e regulamentares.

Serviços financeiros

Os CISOs de serviços financeiros tendem a ter relacionamentos mais bem-sucedidos com seus conselhos do que outros setores. Eles entendem que o ROI dos investimentos em segurança indica seu sucesso (60% concordam) — uma métrica essencial usada pelos conselhos para avaliar o desempenho do CISO (64%).

Mas o setor não está isento de dificuldades. Os serviços financeiros têm maior probabilidade do que qualquer outro setor de serem vítimas de ataques de ransomware, com 65% enfrentando pelo menos um no ano passado, em comparação com 48% das organizações em todos os setores. À medida que os invasores de ransomware procuram prêmios lucrativos, os conselhos desse setor dão prioridade ao fortalecimento dos seus programas cibernéticos. 55% se concentrarão na cibersegurança como sua prioridade número um de investimento, em comparação com 24% dos conselhos de todos os setores – com algumas das lacunas mais amplas, incluindo segurança de terceiros e da cadeia de suprimentos (68%) e infraestrutura em nuvem (56%).

Os CISOs muitas vezes têm um lugar à mesa, já que 42% participam das reuniões do conselho na maior parte do tempo (em comparação com 20% dos CISOs de todos os setores). E quando colaboram no orçamento de cibersegurança, é mais provável que os seus conselhos avaliem positivamente esse aspecto da sua relação de trabalho. 73% acham que a parceria conselho-CISO é eficaz, em comparação com apenas 32% dos conselhos de todos os setores. A saúde dessa parceria pode influenciar o maior nível de investimento do setor na cibersegurança. As organizações de serviços financeiros têm em média 105 milhões de dólares em gastos anuais com cibersegurança, bem acima da média de 75 milhões de dólares para todos os setores.

Outra área em que os serviços financeiros lideram é a IA generativa. Os entrevistados do FSI foram mais propensos a acreditar que os defensores cibernéticos ganhariam uma vantagem sobre os adversários ao usarem a nova tecnologia (44% contra 25% dos entrevistados de todos os setores). Esse otimismo se traduz em uma maior adoção da IA generativa, já que 46% dos conselhos de administração de serviços financeiros afirmam que as suas equipes de cibersegurança estão usando IA generativa, em comparação com apenas 24% em todos os setores.

Comunicações e mídia

A relação entre CISOs e o conselho no setor de comunicações e mídia é complexa. Embora os CISOs tenham algum contato direto, eles não participam frequentemente das reuniões do conselho. E, embora as equipes de cibersegurança pareçam obter financiamento adequado, muitas organizações do setor não fizeram investimentos em medidas adequadas de cibersegurança que impediriam ataques bem-sucedidos.

Embora a maioria dos CISOs do setor de comunicações e mídia esteja atendendo às expectativas dos seus conselhos, preocupantes 9% apresentam "desempenho significativamente inferior" (em comparação com 1% dos CISOs em todos os setores). Isso pode ser motivado pela forma como os CISOs de comunicação e mídia são menos propensos a alinhar as prioridades da sua equipe com as prioridades de segurança do conselho (51% fazem isso contra 62% dos CISOs em todos os setores).

Os CISOs também lutam para comunicar o progresso em relação às suas metas de segurança aos conselhos. 35% dos CISOs afirmam que essa área da sua relação de trabalho é muito boa ou excelente, enquanto apenas 27% dos seus conselhos dizem o mesmo. Esse desalinhamento poderia ser corrigido se os CISOs tivessem mais tempo de fala durante as reuniões do conselho para proporcionar maior transparência às iniciativas cibernéticas e garantir que essas se alinham com as prioridades do conselho. Embora 78% dos CISOs tenham "pelo menos algum contato direto" com seus conselhos, apenas 7% dos CISOs de comunicações e mídia participam a maior parte ou todo o tempo nas reuniões do conselho.

Apesar dos desafios entre os CISOs e o conselho, os conselhos de comunicação e mídia estão dispostos a aumentar o investimento em cibersegurança, com 100% afirmando que provavelmente aumentarão o financiamento para cibersegurança nos próximos três anos (contra 89% em todos os setores).

No futuro, o apoio financeiro constante do conselho será fundamental. Nos últimos 12 meses, 49% das organizações de comunicação e mídia sofreram ataques cibernéticos disruptivos muitas vezes, contra 27% em todos os setores. Os tipos de ataque mais comuns incluem engenharia social (69%), DDoS (44%) e invasão de contas (40%). Para enfrentar essas ameaças, os CISOs e os conselhos de administração se beneficiariam de dar prioridade a uma melhor formação em segurança, destinada a melhorar a higiene das senhas e a ajudar os funcionários a reconhecer esquemas de phishing e outros ataques de engenharia social.

Setor público

Em muitas áreas, os CISOs do setor público e os seus conselhos não estão em sintonia quando se trata de cibersegurança. Embora 80% dos conselhos pensem que os seus CISOs dedicam muito tempo à capacitação dos negócios, apenas 26% fazem isso. E embora 51% dos CISOs pensem que são capazes de criar com sucesso um plano de registo com os seus conselhos de administração, apenas 20% dos seus conselhos concordam.

Para melhorar o consenso e o alinhamento, os CISOs do setor público precisam de compreender até que ponto os seus conselhos valorizam a eficiência operacional. 80% dos conselhos do setor público classificam isso como *muito importante* ou de *extrema importância*, em comparação com 29% de todos os conselhos que afirmam o mesmo. Priorizar a eficiência operacional faz sentido, considerando que o setor enfrenta muitas vezes dificuldades com orçamentos e pessoal limitados. Os gastos com cibersegurança do setor público foram, em média, de US$ 55 milhões em 2024, em comparação com US$ 75 milhões em todos os setores.

Ao avaliar o desempenho dos CISOs, os conselhos enfatizam o ROI dos investimentos em segurança como uma métrica-chave (80% dos conselhos do setor público versus 54% nos conselhos de todos os setores). Olhando para o futuro, os CISOs precisarão comunicar melhor o valor dos seus investimentos em segurança, uma mudança que os preparará para o sucesso com os seus conselhos de administração à medida que apresentam KPIs, defendem investimentos futuros e criam roteiros de segurança. O alinhamento sobre como defender o orçamento também ajudará os CISOs e as suas equipes a enfrentar o dilúvio de ataques de engenharia social, o tipo de ataque mais comum que afeta 72% das organizações do setor público.

As futuras estratégias de defesa cibernética também poderiam incluir IA. Os CISOs e os conselhos de administração do setor público concordam sobre o investimento nessa tecnologia e a aceleração da adoção. Embora ninguém esteja atualmente utilizando IA generativa para casos de uso de cibersegurança, 100% dos conselhos do setor público afirmam que planejam ou têm interesse em fazer isso nos próximos doze meses.

Apêndice de região

América do Norte

Os CISOs na América do Norte normalmente têm fortes relações de trabalho com seus conselhos. Com um maior alinhamento nas prioridades e no orçamento em comparação com outras regiões, 71% dos CISOs norte-americanos relatam estar diretamente alinhados com as prioridades do seu conselho, em comparação com 62% globalmente. Os conselhos norte-americanos também são mais solidários com os desafios do trabalho dos seus CISOs do que os seus equivalentes globais, com 67% observando que as responsabilidades e expectativas dos CISOs se tornaram mais complexas.

Quando o conselho compreende o papel do CISO, e quando o CISO, por sua vez, compreende as prioridades do conselho, a sua relação de trabalho melhora – e o mesmo acontece com o orçamento. As organizações norte-americanas afirmaram que os seus orçamentos para a cibersegurança são adequados (44% versus 31% a nível global). Os CISOs também afirmam que podem convencer os conselhos de administração a aumentar o orçamento, se necessário (68% versus 59% dos CISOs a nível mundial). As organizações norte-americanas têm orçamentos mais cheios, com gastos anuais esperados em cibersegurança em média de 110 milhões de dólares, em comparação com 75 milhões de dólares a nível mundial.

Como os CISOs na América do Norte parecem entender o que os conselhos valorizam, eles podem entregar e atender melhor às expectativas dos seus conselhos. 15% dos conselhos de administração na América do Norte afirmam que os seus CISOs têm um desempenho superior, em comparação com 8% a nível global. É claro que há oportunidades para progresso. Os CISOs na América do Norte podem ter melhor sucesso enfatizando o ROI dos seus investimentos em segurança durante conversas com os membros do conselho. Embora 55% dos conselhos citem isso como uma métrica para avaliar o sucesso do CISO, apenas 35% dos CISOs classificam como um indicador de desempenho superior.

Para se manterem competitivas no cenário global, as organizações norte-americanas precisarão aumentar a adoção da IA generativa. Apenas 15% dos membros do conselho da região utilizam a tecnologia para cibersegurança, em comparação com 24% em todo o mundo. Essa descoberta contrasta com a forma como mais de metade (54%) dos entrevistados na região acreditam que a IA generativa dará uma vantagem aos adversários cibernéticos. Olhando para o futuro, os CISOs norte-americanos podem precisar priorizar a adoção de IA para acompanhar o ritmo dos concorrentes e superar os ciberataques.

Europa

Em comparação com os CISOs a nível mundial, os CISOs europeus podem defender melhor as respectivas organizações de cibersegurança e investir em tecnologias avançadas como a IA generativa. É mais provável que os conselhos europeus tenham um subcomitê centrado na segurança cibernética (55%) do que seus equivalentes globais. Os CISOs na Europa também são mais propensos a participar em reuniões do conselho com alguma frequência (87%) do que os seus equivalentes de outras regiões.

Apesar dessas tendências positivas, os CISOs na Europa têm espaço para melhorias quando defendem iniciativas de cibersegurança e aumentos de financiamento. 49% têm menos probabilidades de reportar que a sua relação de trabalho com o conselho de administração está correndo bem, um valor inferior à média global. A maioria acredita que a melhor maneira de defender os investimentos é discutir métricas e recomendações de risco cibernético (55%) e requisitos de conformidade (49%). No entanto, é mais provável que os seus conselhos aprovem aumentos orçamentais quando os CISOs demonstram a segurança como um facilitador de negócios (58%) e descrevem os custos do tempo de inatividade (56%).

Alguns desses aumentos orçamentais poderão ser direcionados para a adoção de IA generativa para a cibersegurança, uma área em que a Europa está à frente. 39% das organizações na Europa implementaram IA para iniciativas de cibersegurança, em comparação com 24% a nível global. Os CISOs europeus também estão à frente no estabelecimento de protocolos para determinar as tarefas mais bem executadas pela IA e aquelas que são mais bem executadas pelos membros da equipe de segurança.

Quando se trata de ataques de ransomware, as organizações europeias também são diferenciadas. Apenas 3% daqueles que sofreram um ataque de ransomware pagam o resgate diretamente (inferior à média global) e 23% afirmam que o seguro cibernético os cobre em caso de ataque (mais do que os entrevistados de todas as outras regiões).

APAC

Os CISOs da APAC tendem a ter relações mais fracas com os seus conselhos de administração do que os seus equivalentes globais, tendo menos sucesso quando defendem a cibersegurança e aumentos orçamentais. Poucos dizem que é muito provável que os seus conselhos apoiem o aumento do investimento da organização em cibersegurança nos próximos três anos (18% dos CISOs da APAC versus 27% globalmente).

Entretanto, os conselhos de administração da APAC são menos propensos a classificar o reforço do seu programa cibernético como uma alta prioridade de investimento para os próximos 12 meses (9% deles versus 24% dos conselhos a nível mundial). Em vez disso, a gerência executiva na APAC está mais focada no crescimento dos negócios, com 38% citando isso como a prioridade principal.

Uma vantagem dos CISOs da APAC é que eles participam com mais frequência nas reuniões do conselho, já que 22% indicam que estão presentes na maioria ou em todas as reuniões do conselho. Se reorientarem as suas conversas para explicar aos conselhos sobre ameaças cibernéticas, os seus conselhos poderão ter maior probabilidade de apoiar aumentos orçamentais ou apoiar uma nova iniciativa de cibersegurança.

Outro desafio que as organizações da APAC enfrentam é a conformidade. 28% dos CISOs nesta região dizem que foram pressionados a não relatar um incidente ou problema de conformidade, o número mais elevado de qualquer região. Isto pode ser, em parte, devido ao atraso da APAC no estabelecimento de uma governação clara para a comunicação de incidentes de cibersegurança; 40% das organizações na região definiram protocolos claros de notificação de incidentes, o que fica atrás das outras regiões.

Quando questionados sobre até que ponto a sua organização utiliza IA generativa para a cibersegurança atualmente, 18% dos conselhos da APAC reportam que a utilizam de alguma forma, ficando atrás da média global. Mas isso pode mudar em breve. 44% dos conselhos planejam aplicar IA generativa para fins de defesa cibernética nos próximos 12 meses, e outros 35% manifestaram interesse na ideia.

Metodologia

Os pesquisadores da Oxford Economics entrevistaram 600 pessoas (500 CISOs, CSOs ou líderes de segurança equivalentes e 100 membros do conselho) em junho e julho de 2024. As categorias de entrevistados incluíram CISOs que se identificaram como membros do conselho. Os entrevistados estavam na Alemanha, na Austrália, nos Estados Unidos, na França, na Índia, na Itália, no Japão, na Nova Zelândia, no Reino Unido e em Singapura. Eles representaram também 16 setores: agricultura, serviços empresariais, construção/engenharia, educação, energia e serviços públicos, serviços financeiros, governo, saúde, ciências biológicas, serviços de informação, tecnologia, manufatura, varejo, bens de consumo, telecomunicações e mídia e comunicações. A Oxford Economics também conduziu oito entrevistas aprofundadas com CISOs e membros do conselho para obter informações qualitativas.

Sobre o Splunk

O Splunk, uma empresa da Cisco, ajuda a tornar as organizações mais resilientes digitalmente. As organizações líderes usam nossa plataforma unificada de segurança e observabilidade para manter os sistemas digitais seguros e confiáveis. As organizações confiam no Splunk para evitar que incidentes de infraestrutura, aplicações e segurança se tornem grandes problemas, recuperação mais rápida de choques em sistemas digitais e adaptação ágil a novas oportunidades.

Com o Splunk, a conversa não para.

splunk> a CISCO company

25_CMP_report_CISO-report-2025_v13