KPMG

KPMG Cyber Trust Insights 2022

A construção da confiança por meio da segurança cibernética e da privacidade

Janeiro de 2023 | kpmg.com.br

Conteúdo

Visão geral

Cinco passos cruciais para construir a confiança por meio da segurança cibernética e da privacidade

Cada vez mais, as empresas reconhecem o valor da confiança. Em um ambiente incerto e em constante mudança, os clientes, os funcionários e os investidores valorizam aquelas organizações nas quais eles sabem que podem confiar! Para construir, fortalecer e manter esse sentimento, é essencial que as diversas áreas atuem em harmonia, entregando ao cliente a consistência e a imagem unificada que ele tanto valoriza.

Agora que vivemos em um mundo digitalizado, no qual os dados são o ponto de partida para muitas decisões e estratégias, é essencial que estes sejam colhidos e tratados de maneira ética, íntegra e transparente; , também é fundamental que os sistemas sejam resilientes, confiáveis e aptos a responder rapidamente aos desafios que surgem diuturnamente. O cliente quer sentir-se seguro ao fazer transações, bem como, para integrar o ecossistema mais amplo de parceiros, investidores, órgãos reguladores e sociedade. Em suma: confiança digital importa. E muito!

A segurança cibernética e a privacidade desempenham papel-chave na construção e na manutenção dessa confiança. As empresas estão aumentando a coleta de dados, expandindo o uso de tecnologias como a inteligência artificial (IA) e o *machine learning*, (ML) e adotando a pauta ambiental, social e de governança (ESG), ao mesmo tempo em que precisam se adequar a normas regulatórias extremamente complexas.

Neste documento, intitulado ***KPMG Cyber Trust Insights 2022***, abordamos a confiança cibernética em 2022. O estudo se baseia em opiniões fornecidas por 1.881 executivos e em uma série de discussões com líderes e profissionais corporativos de todo o mundo, realizadas com o objetivo de entender como os executivos enxergam o desafio da confiança e quais serão seus próximos passos nessa jornada. Também exploramos o papel-chave que os diretores de segurança da informação (CISOs) podem desempenhar nessa caminha.

Como resultado, foram identificados cinco passos cruciais para a construção da confiança por meio da segurança cibernética: **tratar a privacidade e a segurança cibernética como assunto da máxima importância; construir alianças internas; reimaginar o papel do CISO; garantir o apoio da liderança; e atuar em sinergia com o ecossistema.**

Principais constatações

Tempestade de dados

As empresas estão minerando dados em escala. Isso levanta preocupações em relação a como esses dados estão sendo protegidos, usados e compartilhados.

A maioria dos respondentes participou de uma coleta ou análise mais abrangente dos dados dos clientes no último ano.

O investimento em atividades impulsionadas por dados tem se tornado prioritária nas organizações.

Desafios de *Inteligência Artificial* e *Machine Learning*

Há crescentes preocupações comerciais e sociais em relação à ética, à segurança e às implicações de privacidade na adoção de soluções de IA e ML para análise de *big data*.

78% concordam que IA e ML trazem desafios únicos para a segurança cibernética.

3 em cada 4 afirmam que AI e ML intensificam questões éticas fundamentais

Valor e confiança

A confiança nunca foi tão importante como agora! E não se trata apenas de manter uma boa reputação: o incremento da confiança cria vantagem competitiva e gera resultados.

Mais de 1/3

das organizações reconhecem que o aumento da confiança incrementa os lucros.

Mas 65% relatam que as informações de segurança requeridas são definidas de acordo com os requisitos de conformidade do momento, em vez de serem estabelecidas com visão de longo prazo e ambições estratégicas.

Regulação crescente

Os reguladores estão mais atentos a questões de segurança cibernética e as organizações estão preocupadas em transitar por um cenário global cada vez mais complexo do ponto de vista regulatório.

36% dos respondentes estão preocupados com sua capacidade de atender às regulamentações de segurança cibernética – tanto as já existentes quanto aquelas que vierem a ser criadas – nos casos de terceirização de atividades para provedores de serviços digitais.

34% preocupam-se com os relatórios corporativos de divulgações relacionadas à segurança cibernética.

Comunidades e confiança

As parcerias externas tendem a desempenhar papel cada vez mais vital para o sucesso em ecossistemas hiperconectados; porém, barreiras de ordem prática podem atravancar essa colaboração.

79% afirmam que a colaboração construtiva com fornecedores e clientes é vital, mas apenas 42% relatam viver isso na prática.

60% admitem que sua cadeia de suprimentos os deixa vulneráveis a ataques.

CISO em evolução

As organizações reconhecem o papel que o CISO pode desempenhar na incorporação de uma abordagem de confiança digital por toda a organização?

Metade dos executivos tem dúvidas de que o relacionamento entre o CISO e o board se caracterize pela mais alta confiança.

13% dizem que o CISO não é visto como um executivo fundamental; por isso, ele tem menos influência do que seria necessário para efetivamente proteger a organização e seus dados.

Propósito de confiança

As empresas reconhecem o vínculo entre confiança digital e a agenda ambiental, social e de governança (ESG)?

Menos de 1 em cada 5

disse que o time do CISO integra a equipe de ESG.

50% reportam que o time do CISO desempenha um papel muito limitado no âmbito do ESG.

1

Transformação digital

Business case: para investir em confiança

O que entendemos como confiança?

Uma definição clara de confiança pode ajudar as empresas a assumir um papel ativo em mensurá-la, incrementá-la e, desse modo, aproveitar uma ampla gama de benefícios potenciais tangíveis.

A confiança digital é a confiança que os *stakeholders* depositam na capacidade de uma organização de aproveitar a tecnologia digital para proteger seus interesses e defender as expectativas e os valores da sociedade.

Embora seja provável que cada organização tenha prioridades diferentes e possa usar linguagens diversas para descrever aspectos da confiança digital, o conceito geralmente abrange:

Segurança e confiabilidade

Neste aspecto, a prioridade é garantir que a tecnologia e os dados de uma organização estejam bem protegidos, enquanto operam conforme projetado.

Uso inclusivo, ético e responsável

Dessa forma, garante-se que uma organização projete, construa e opere suas ferramentas tecnológicas e utilize dados com total responsabilidade em relação aos indivíduos, à sociedade em geral, ao meio em que esteja inserida e a todos os seus *stakeholders*.

Responsabilidade e fiscalização

A organização deve definir claramente suas responsabilidades no que tange à confiança e observá-las e cumpri-las rigorosamente.

Por que isso importa: o aumento da confiança pode aumentar os lucros e fidelizar clientes

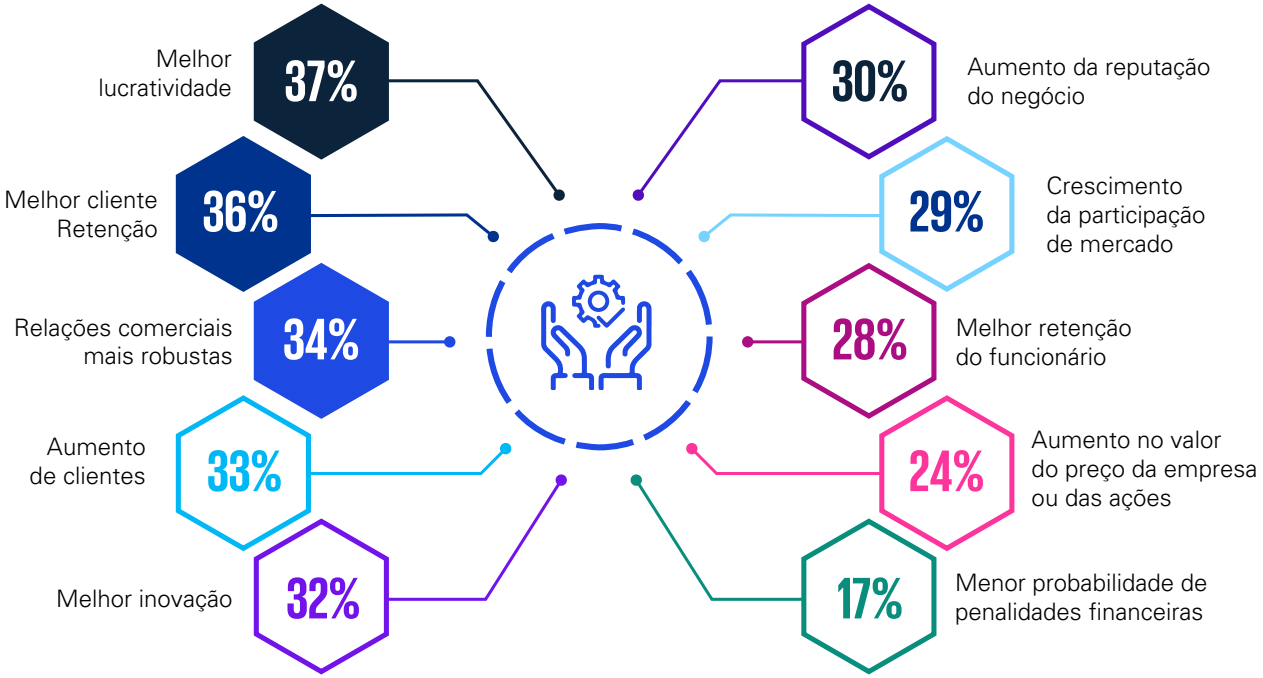
De acordo com nossos respondentes, os três principais benefícios esperados do aumento da confiança são:

1. Melhor lucratividade
2. Melhor retenção de clientes
3. Relações comerciais mais fortes

Outros ganhos potenciais incluem inovação aprimorada, maior retenção de funcionários e uma maior participação de mercado.

Os principais benefícios do aumento da confiança

A tabela mostra a porcentagem de respondentes que selecionaram cada opção entre os três primeiros.



As empresas estão investindo em dados e dando enfoque na experiência do cliente

A transformação digital está em andamento: em todos os setores, as empresas estão analisando a tecnologia e colocando dados avançados e análises sofisticadas no centro das operações. Nos próximos três anos, as organizações planejam fazer uma série de investimentos

em ferramentas digitais para impulsionar o crescimento, otimizar as interações com o cliente, incrementar as operações comerciais e gerar valor nos dados. Porém, cada nova atividade de dados expõe as empresas a potenciais vulnerabilidades e riscos à reputação.

De acordo com o *Global Tech Report da KPMG*, **61% das empresas esperam adotar novas plataformas tecnológicas revolucionárias no prazo de dois anos; em até três anos**, elas podem aumentar o investimento em Internet das Coisas (IoT, do inglês *internet of things*), computação de ponta e 5G. Em menor medida, também podem investir em realidade virtual e realidade aumentada.

No mesmo relatório da KPMG, **a digitalização dos canais de clientes é citada como o segundo desafio mais grave de segurança cibernética enfrentado pelas organizações**, logo atrás da adoção de ambientes de trabalho híbridos.

O uso de dados sobre experiências para customizar interações digitais em tempo real recebe investimentos de 37% dos respondentes, ao passo que 36% estão investindo na integração em vários canais para aprimorar a experiência do cliente.

À medida que essas tendências se consolidam e disseminam, as expectativas de privacidade dos clientes também mudam. Cada vez mais, os usuários esperam ser capazes de customizar controles de privacidade em todos os seus dispositivos e canais, exigindo que as organizações ofereçam controles flexíveis em seus produtos e serviços futuros.

As principais áreas de investimento em experiência digital

A tabela mostra a porcentagem de respondentes que selecionaram cada opção entre os três primeiros.

> *Investir em segurança cibernética e proteção da privacidade é necessário para manter a confiança"*
>
> **Bashar Abouseido**
> **Vice-presidente sênior e CISO da Charles Schwab**

A segurança cibernética está mudando e os dados importam mais do que nunca

As empresas precisam reforçar suas salvaguardas em áreas cruciais para garantir a confiança de seus *stakeholders*. Mais de 80% dos respondentes reconheceram a importância de melhorar a segurança cibernética e a proteção de dados, incluindo um aumento na transparência a respeito do uso dos dados. Mais da metade (51%) dos respondentes consideram extremamente importante proteger de ataques os ativos de TI.

À medida que as organizações impulsionam a transformação digital, os investimentos em segurança cibernética e privacidade devem constar em orçamento e ser cumprido à risca, como parte integral das iniciativas estratégicas. "*O sucesso dos serviços digitais transformadores provavelmente dependerá de as organizações incorporarem a segurança e a privacidade à sua elaboração e implementação*" afirma Allan Cocksaur, CISO da Shell.

" Estamos priorizando aquilo que chamamos de 'segurança por normas de elaboração' na maneira pela qual construímos tecnologia. Queremos que essas normas sejam transparentes para os clientes porque nossa obrigação é manter e aumentar a confiança", declara.

"*A proteção da confiança do cliente é o que impulsiona nossos investimentos em segurança cibernética e privacidade*" comenta Bashar Abouseido, vice-presidente sênior e CISO da Charles Schwab. "*Para manter a confiança dos clientes, estamos dispostos a ir além, por meio de melhorias proativas e contínuas dos controles de privacidade e na transparência sobre nossas medidas de proteção desses dados.*"

Perspectiva da KPMG: A confiança está se tornando fundamental para o sucesso das tecnologias emergentes

Tecnologias emergentes como a distribuída tecnologia de razão contábil (DLT), computação quântica, redes 5G, IA/ML, realidade aumentada e virtual estão se desenvolvendo rapidamente e prometem transformar a maneira pela qual as empresas operam.

No entanto, o lançamento bem-sucedido de aplicativos futuros (economia conectada, sistemas inteligentes, NFT, metaverso, etc.) que dependem dessas tecnologias provavelmente será regido pela capacidade da organização de incutir confiança em várias dimensões. Isso significa incorporar controles de segurança e privacidade com transparência, confiabilidade e integridade.

Atul Gupta
Sócio-líder de Digital Trust e Cyber Security Services da KPMG na Índia

2

Tendências da confiança digital

Entendimento dos fatores que impulsionam a confiança

Como enfrentar os desafios éticos da IA

O uso crescente das tecnologias de IA está impondo novas questões de confiança que ainda não são plenamente compreendidas. Pesquisa da KPMG mostra que as empresas estão determinadas a adotar ferramentas de IA, com expectativas de benefícios que abrangem desde o aumento da eficiência e produtividade até a ampliação da capacidade de gerar *insights* preditivos sobre os clientes e mercados.

O perigo é que essas tecnologias, se não receberem a abordagem correta, podem acarretar riscos à segurança cibernética e à privacidade, com potencial de danos à reputação e sanções regulatórias.

As organizações estão começando a reconhecer esses riscos. Mais de três quartos dos respondentes (78%) concordam que a inteligência artificial traz desafios únicos de segurança cibernética.

Os respondentes também apontaram a existência de questões éticas fundamentais que precisam ser resolvidas à medida que essas tecnologias forem adotadas, e dizem que as organizações precisarão comunicar-se de maneira mais aberta sobre como estão gerenciando essas questões.

Tudo isso enfatiza o importante papel das equipes de segurança cibernética e privacidade para moldar o debate ético e o gerenciamento dos riscos.

"*Estamos trabalhando muito na IA adversária — coisas como envenenamento por ataques de IA , porque acreditamos que essa será a próxima onda de ataques*" afirma Ann Johnson, vice-presidente corporativa da Microsoft Security Business Development.

A IA e a inteligência artificial criam novos desafios para a equipe de segurança das informações

A tabela mostra a porcentagem de respondentes que concordam ou concordam plenamente.

78%	76%	76%	76%	75%
A adoção da IA/Inteligência Artificial levanta desafios únicos de segurança cibernética que exigem atenção especial	A adoção da IA/ML exige que coloquemos em prática salvaguardas adicionais sobre como treinamos os sistemas de IA/Inteligência Artificial e monitoramos seu desempenho	A adoção da IA/ML exige que sejamos mais transparentes na maneira pela qual comunicamos como utilizamos as técnicas de IA/Inteligência Artificial	A adoção da IA/ML levanta questões éticas fundamentais para nós que exigem governança e supervisão cuidadosas	A adoção da inteligência artificial/inteligência artificial levanta preocupações-chave sobre a privacidade sobre a maneira pela qual agregamos e analisamos dados de clientes e colaboradores comerciais

Perspectiva da KPMG: IA ética

As organizações sabem que precisam tornar-se baseadas em dados. Muitos estão expandindo a IA para automatizar a tomada de decisões impulsionada pelos dados, mas a IA traz novos riscos à marca e à lucratividade. A tecnologia tem o potencial de estimular a desigualdade e violar a privacidade, bem como. de limitar a capacidade de tomada de decisões autônoma e individual.

Você não pode simplesmente culpar o próprio sistema de IA por resultados indesejados. A IA ética e confiável não é um luxo, mas uma necessidade do negócio. Um número cada vez maior de líderes empresariais reconhece isso — mas a confiança não é assegurada sem esforços ou desafios.

Não menos importante, o que é considerado ético e idôneo em um setor ou região pode não ser visto da mesma forma em outros contextos. Não há uma solução única. Por isso, simplesmente copiar as soluções existentes não é eficaz. A IA digna de confiança requer uma abordagem holística, agnóstica e amplamente endossada para a conscientização, a governança da IA e o gerenciamento de riscos

Por exemplo: as avaliações do impacto da IA devem envolver os *stakeholders* certos para identificar os riscos. Além disso, as organizações devem avaliar de maneira cuidadosa o cumprimento das leis e regulamentos e mensurar o retorno sobre o investimento da IA. As decisões precisam ser rastreáveis e auditáveis e todas essas proteções devem ser colocadas em prática sem se tornarem um impeditivo para a inovação.

Sander Klous
Sócio de Desenvolvimento de Negócios de D&A da KPMG na Holanda

> **"Estamos realizando uma reformulação no trabalho, porque a web acredita que ele não vai mais atacar."**
>
> **Ann Johnson**
> Vice-presidente corporativa da Microsoft Security Business Development.

As perspectivas regulatórias

À medida que crescem as preocupações sociais sobre a confiança digital, legisladores e órgãos reguladores, tendem a impor mais demandas por transparência e supervisão. A pesquisa de 2022 da KPMG sobre a confiança cibernética traz os seguintes destaques:

36%

dos respondentes preocupam-se com sua capacidade de atender à regulamentação (existente ou nova) de segurança cibernética quando as atividades são terceirizadas para prestadores de serviços digitais.

34%

preocupam-se com divulgações sobre a preparação e divulgação de informações corporativas relacionadas à segurança cibernética.

31%

preocupam-se com as crescentes demandas em torno da infraestrutura crítica, que é objeto de um aumento da regulamentação no Reino Unido, na União Europeia e nos Estados Unidos.

Para aumentar o ônus, as organizações internacionais devem lidar com regulamentações extraterritoriais cada vez mais complexas e até constraditórias. "*Um desafio para os diretores de TI é que os stakeholders de diferentes regiões têm interpretações diferentes dos mesmos regulamentos*", afirma Ulrich Baisch, CIO da Bechtle, uma das maiores prestadoras de serviços de TI da Europa. "*Você precisa ter um conceito claro daquilo que pode ou não fazer.*"

Perspectiva da KPMG: fatores que influenciam os órgãos reguladores

Globalmente, observa-se um crescimento acelerado da regulamentação sobre segurança cibernética e privacidade. Quase 140 países têm algum tipo de regime de proteção de dados, frequentemente reivindicando jurisdição extraterritorial sobre os serviços oferecidos no país que utilizem dados dos cidadãos. Regimes mais maduros de privacidade estão ingressando na segunda geração de regulamentações e enfrentando novos desafios, que são impulsionados pela adoção da tecnologia. Por exemplo, discussões sobre a regulamentação da IA estão agora sendo formalizadas em uma minuta de legislação.

Além disso, à medida que crescem as preocupações a respeito de ataques a sistemas de controle industrial, os países implementam regulamentações de segurança cibernética de infraestrutura cada vez mais estritas. Essas regulamentações estão passando da autoavaliação para estruturas de controle mais diretivas, incluindo a preparação e divulgação obrigatória de informações sobre incidentes e auditoria externa.

Os órgãos reguladores também estão sendo mais prescritivos em suas estruturas de controle, ao mesmo tempo em que procuram reforçar a independência do CISO e seu papel na definição de normas de controle. Requisitos mais holísticos de resiliência, com foco na recuperação dos negócios em cenários extremos, mas plausíveis, também estão surgindo em setores como o financeiro. Requisitos corporativos de transparência sobre os riscos cibernéticos estão em debate com requisitos crescentes para a divulgação de incidentes de *ransomware*. As empresas devem investir para automatizar o monitoramento de *compliance* e a preparação e divulgação de informações; manter um relógio regulatório. Devem, ainda, considerar as tendências regulatórias de privacidade e segurança ao elaborar novos serviços e produtos.

David Ferbrache
Sócio-líder global de cyber futures da KPMG no Reino Unido

Olhando além da regulamentação

A confiança digital, que envolve segurança cibernética e proteção da privacidade, deve fazer parte da pauta ESG das empresas. "As questões de ESG são parte integral da empresa como um todo, mas naturalmente o CISO desempenha um papel-chave, particularmente quando se trata de questões sociais e relacionadas à governança," afirma Ulrich Baisch, de Bechtle.

Porém, menos de uma em cada cinco organizações descreve a segurança como um dos focos de ESG. Em sua maioria, os respondentes afirmam que essa questão ainda desempenha um papel muito limitado. As organizações também precisam reconhecer os imperativos sociais e as expectativas crescentes em torno desses tópicos.

Nas organizações, os indivíduos responsáveis pelas questões de ESG devem trabalhar em colaboração com os responsáveis pela segurança cibernética (frequentemente, o CISO) e pela privacidade de dados (frequentemente, o DPO).

> ***"ESG é parte integrante do negócio como um todo; mas, naturalmente, o CISO tem um papel fundamental quando se trata de questões relacionadas à governança"***
>
> **Ulrich Baisch**
> CIO da Bechtel

Perspectiva da KPMG: ESG e responsabilidade social

As organizações que realmente adotam a pauta de ESG podem ganhar a confiança dos clientes e reforçar a força das marcas. No mundo digital de hoje, os conselhos de administração, os investidores, os órgãos reguladores, os clientes e o público em geral esperam uma preparação e divulgação transparente de informações sobre a postura de segurança cibernética e privacidade da organização.

As partes interessadas querem sentir-se confiantes de que os conselhos e os executivos apreciam as implicações sociais da luta para assegurar a resiliência e a integridade dos serviços críticos, ao mesmo tempo que protege as informações em que confiam.

Considerações-chave para essas partes interessadas incluem:

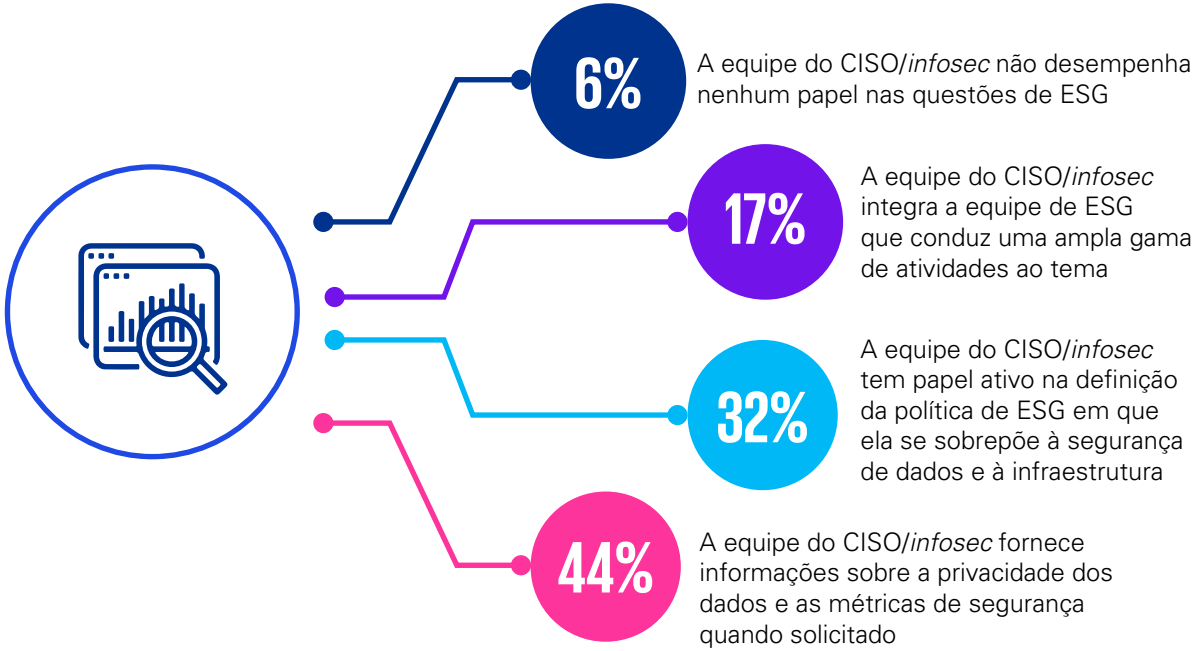
- Monitoramento proativo dos ativos digitais para ajudar a assegurar o acesso a conteúdos seguros e confiáveis em um momento de maior exploração *on-line* e armamento das informações por meio de "falsas notícias" e "*fakes* profundas".
- Ajudando a proteger os clientes, particularmente aqueles que estão abaixo da linha da pobreza cibernética, contra fraudes digitais e roubo de identidade.
- Com o objetivo de assegurar a adoção ética de tecnologias como a IA e a inteligência artificial, que coletam e analisam os dados dos clientes.
- A manutenção da confiabilidade, integridade e disponibilidade dos serviços digitais nos quais nós, como sociedade, nos baseamos.
- Demonstração de um comprometimento mais amplo com a capacitação e habilidades cibernéticas no ecossistema de fornecedores.

Srinivas Potharaju
Sócio de digital trust da KPMG na Índia

Siddharth Durbha
Diretor de digital trust da KPMG na Índia

A maioria dos diretores de TI tem envolvimento passivo nas políticas e atividades de ESG

A tabela mostra a porcentagem de respondentes que selecionaram a opção que consideraram melhor.



Perspectiva da KPMG: como estimular a confiança indo além do mínimo regulatório

As organizações com visão de futuro estão incorporando as métricas de privacidade de dados às estruturas de preparação e divulgação de informações de ESG.

Dessa forma, elas ganham confiança garantem que os requisitos regulatórios estejam sendo minimamente atendidos. É como que as organizações busquem, de maneira proativa, extrapolar as normas regulatórias mínimas, de forma que os *stakeholders* sintam-se mais confiantes de que suas informações pessoais estão sendo coletadas, utilizadas ou divulgadas de maneira apropriada — não somente do ponto de vista jurídico, mas de uma perspectiva que se encaixa na narrativa articulada de ESG da organização.

Sylvia Klasovec Kingsmill
Sócia-líder global de privacidade da KPMG no Canadá

3

Construção de uma comunidade de confiança

O poder da colaboração

As empresas digitalizadas de hoje não operam no vácuo; são cada vez mais ativas na parceria, demonstrando colaboração abrangente. Isso aumenta o desafio enfrentado pelas equipes de segurança cibernética: elas devem construir ecossistemas confiáveis para suas organizações, em sintonia com aliados que ajudem a garantir segurança mútua e sustentar a confiança no ecossistema como um todo.

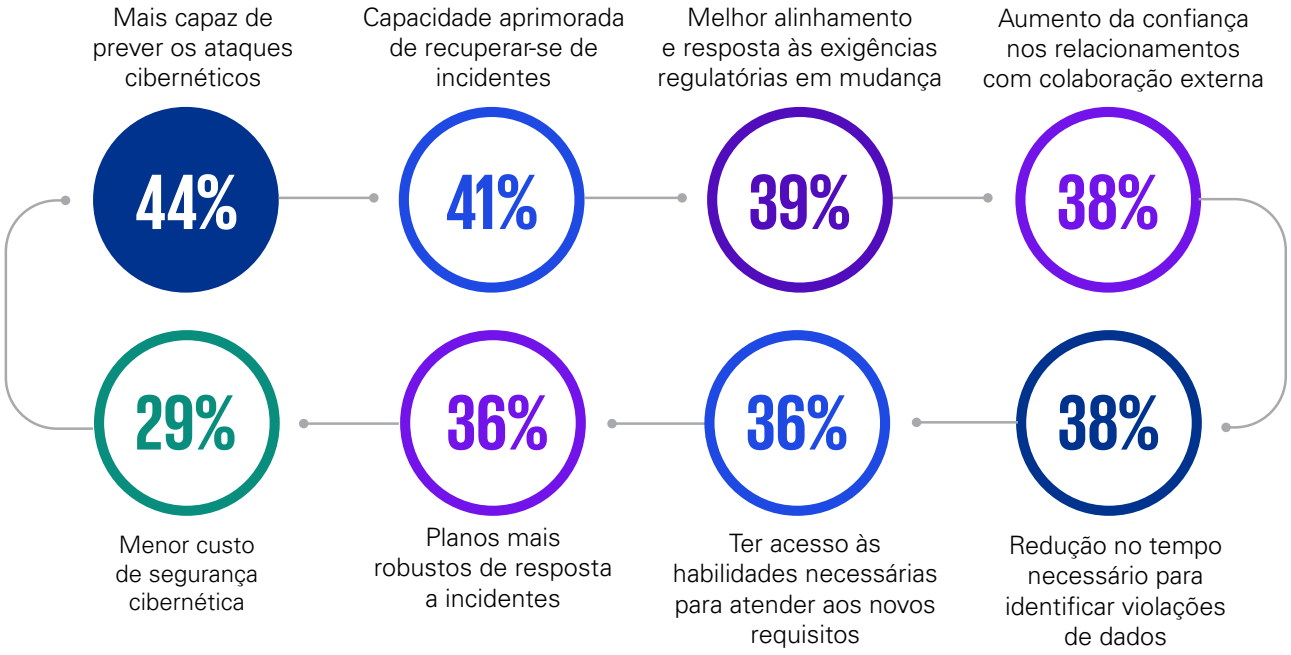
A união faz a força. Neste estudo, quase metade dos respondentes (44%) afirma que a colaboração em relação à segurança cibernética em todo o ecossistema mais amplo os ajudará a prever os ataques, por exemplo.

Em que pese a colaboração ser desejável, nem sempre é direta. Mais de um terço dos respondentes (38%) diz que as preocupações com privacidade estão no caminho das parcerias externas de segurança cibernética e 36% preocupam-se com o risco de "revelar demais" a respeito de seus próprios esquemas de segurança. Outros problemas incluem restrições regulatórias, falta de apoio dos diretores-executivos e falta de recursos.

> ***A norma é reconhecida de maneira anárquica e não é reconhecida como padrão."***
>
> **Mark Thompson**
> CSO da Associação Internacional dos Profissionais de Privacidade (IAPP)

A colaboração em relação à segurança cibernética em todo o ecossistema pode ajudar as organizações a antecipar-se e recuperar-se de ataques

A tabela mostra a porcentagem de respondentes que selecionaram cada vantagem entre as três primeiras.



Há soluções práticas, de acordo com Mark Thompson, CSO da Associação Internacional dos Profissionais de Privacidade (IAPP). "Se eu lhe der os parâmetros do firewall, há o risco de você ver uma vulnerabilidade ou uma lacuna", ele explica. "Mas ter um padrão e dizer que as regras do *firewall* atendem a esses requisitos é algo que pode ser feito, porque não entrega detalhes intrincados e ajuda a viabilizar a confiança."

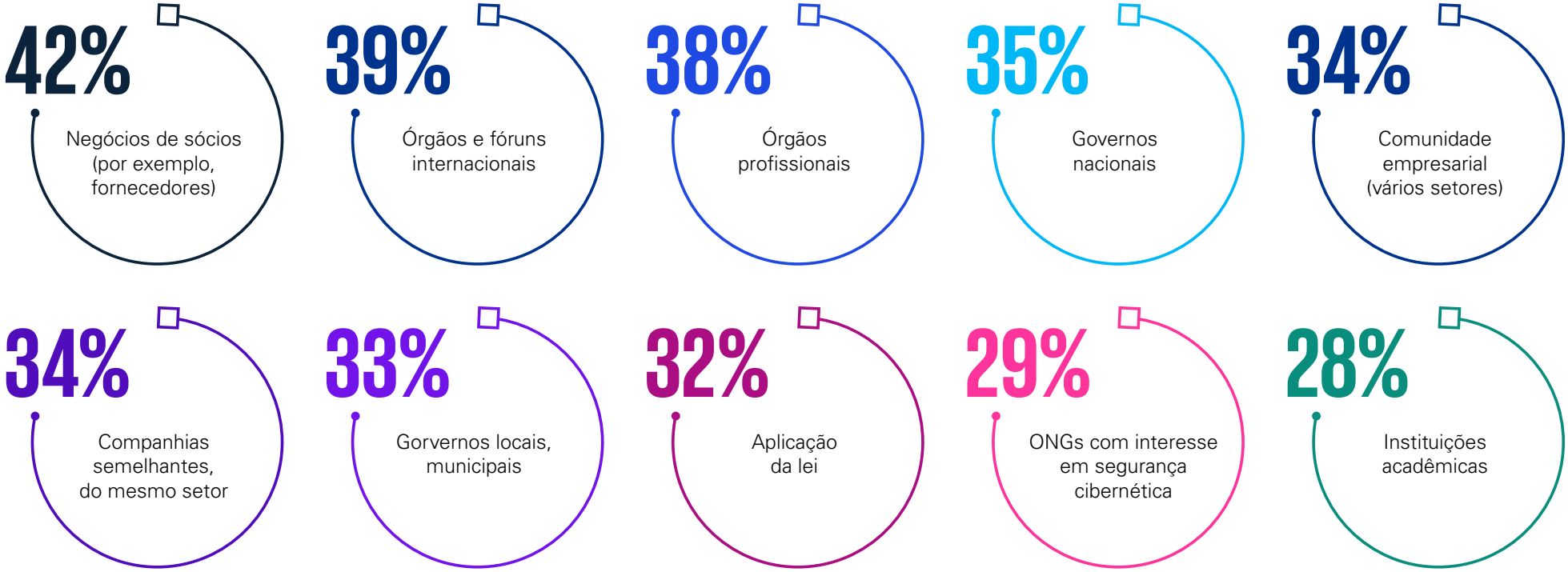
A imaturidade das normas e das melhores práticas de compartilhamento de informações pode ajudar a explicar por que menos da metade das empresas está colaborando ou trocando informações com parceiros-chave. Embora 79% digam que o engajamento construtivo dos fornecedores é crucial para uma segurança cibernética eficaz, somente 42% dos respondentes disseram estar realmente trabalhando juntos para alcançá-la.

Mas essa relutância pode causar danos graves. Mais da metade das empresas admite que não sabe se suas defesas são fortes o suficiente para impedir que *cyber* criminosos ataquem as vulnerabilidades da cadeia de suprimentos e da contratação de bens e serviços.

Essa abordagem mais limitada de colaboração não pode continuar, porque ela impede que seja oferecida proteção suficiente para as organizações individuais ou os ecossistemas, diminuindo a confiança em ambas. Não por acaso, 53% dos respondentes temem que suas respectivas organizações não sejam proativas o suficiente em suas colaborações em segurança cibernética.

Mais colaborações de segurança cibernética são necessárias em todo o ecossistema

O gráfico mostra a porcentagem de respondentes que selecionaram todas as opções que se aplicavam a seus respectivos casos.



Perspectiva da KPMG: o valor da unidade

A construção eficaz da comunidade é crucial para lidar com os desafios da segurança cibernética: as organizações individuais devem trabalhar juntas. No entanto, questões relacionadas ao gerenciamento de riscos, à reputação, à lei e à estratégia ainda podem impedir essa meta.

Nenhuma organização pode abordar esses desafios sozinha. Por isso, é importante combinar recursos e coordená-los de maneira eficaz. Trabalhando em conjunto, tanto organizações públicas quanto privadas saem ganhando.

Para construir confiança e espírito de comunidade, cada parte deve identificar barreiras e os caminhos para superá-las. Por exemplo: algumas organizações utilizam os protocolos existentes, tais como a estrutura de segurança cibernética do NIST, para desenvolver uma linguagem e terminologia comuns ao estabelecer parcerias com outras organizações. Há empresas que preferem priorizar a asseguração de que as informações de propriedade permanecerão na organização. Acordos de cooperação baseados em princípios operacionais comuns podem ajudar a estabelecer relações e respaldar a infraestrutura digital, mantendo a privacidade e reforçando a confiança mútua.

Há também a necessidade de reconhecer que o paradigma tradicional de segurança é menos relevante em um cenário interconectado; neste, o foco deve estar na resiliência. Por isso, em vez de tentar derrotar os maus atores por meio do isolamento e do controle dos sistemas, deve-se buscar uma abordagem mais coordenada e cooperativa.

Prasad Jayaraman
Sócio-líder de cyber security services
da KPMG nos Estados Unidos

4

A evolução do CISO

A contribuição do CISO para desenvolver a confiança

Integre o CISO

Os CISOs muitas vezes foram vistos como aqueles que refreavam as mudanças; agora, eles devem ser, cada vez mais, reconhecidos como "fundamentais" para viabilizá-las. Atuando como guardiões da confiança da organização, eles têm tudo para fornecer as bases para o sucesso.

"*Os CISOs podem aumentar e aprimorar a confiança; mas, normalmente, o que eles fazem é agir de acordo com suas prioridades organizacionais*", esclarece Mark Thompson, do IAPP. "*Há a necessidade de que eles comecem a ajudar a organização a impulsionar e transformar a dinâmica*", afirma.

Os próprios CISOs reconhecem o que está em jogo: 77% dos respondentes dizem que o aumento da confiança é um objetivo-chave de seus programas de risco cibernético.

E as organizações mostram altos níveis de confiança em suas capacidades de segurança cibernética: 74% afirmam ter observado melhorias na segurança cibernética nos últimos 12 meses. Essa confiança é combinada com uma grande crença na capacidade do CISO de realizar tarefas cruciais.

Mas esses profissionais estão confiantes na própria capacidade de satisfazer essas expectativas?

As organizações mostram altos níveis de confiança no CISO

O gráfico mostra a porcentagem de respondentes que classificam cada atividade como "efetiva".

- **80%** Atendimento das exigências legais enfrentadas pela empresa relativamente à segurança cibernética e à proteção de dados
- **80%** Colocação em prática de tecnologia que protege os dados do cliente/cliente/sócio de maneira eficaz
- **80%** PImplementação de tecnologia que protege os ativos de TI de ataques
- **79%** Investigação e mitigação do efeito de ataques cibernéticos e violações de dados
- **79%** Aumento da transparência em relação ao uso de dados e à privacidade/proteção de dados
- **78%** Disseminação e conscientização sobre questões de segurança cibernética
- **78%** Construção de relações com os órgãos reguladores, de modo a criar um sentimento de confiança mútua
- **78%** Tratamento das relações com os *stakeholders* e das mensagens públicas depois de uma violação cibernética
- **78%** Suporte aos parceiros internos à transformação dos negócios
- **77%** Fortalecimento da segurança cibernética de terceiros e da cadeia de suprimentos

É interessante que muitos CISOs estejam lutando para dispor de autonomia para perseguir seus objetivos. "*Pode haver conversas difíceis*", diz Ann Johnson, da Microsoft. "*Quais dados vamos compartilhar? Como vamos armazená-los e utilizá-los do ponto de vista da IA-ML? Como vamos protegê-los? O CISO tem que estar envolvido em cada uma dessas conversas, que nem sempre são fáceis*", acrescenta Johnson.

Quase dois terços dos respondentes (65%) dizem que a segurança das informações é vista por suas organizações como uma atividade de redução do risco, e não como indutoras de negócios. Além disso, 57% dizem que líderes seniores não entendem os benefícios competitivos da confiança aprimorada por uma melhor segurança das informações.

Construa um relacionamento com os líderes seniores

Seria irrealista e injusto esperar que os diretores de TI impulsionassem sozinhos a confiança na privacidade de dados e segurança cibernética. Suas interações com os demais setores e líderes são fundamentais. Uma colaboração eficaz pode produzir mudanças significativas, que de fato se reflitam no aumento da confiança

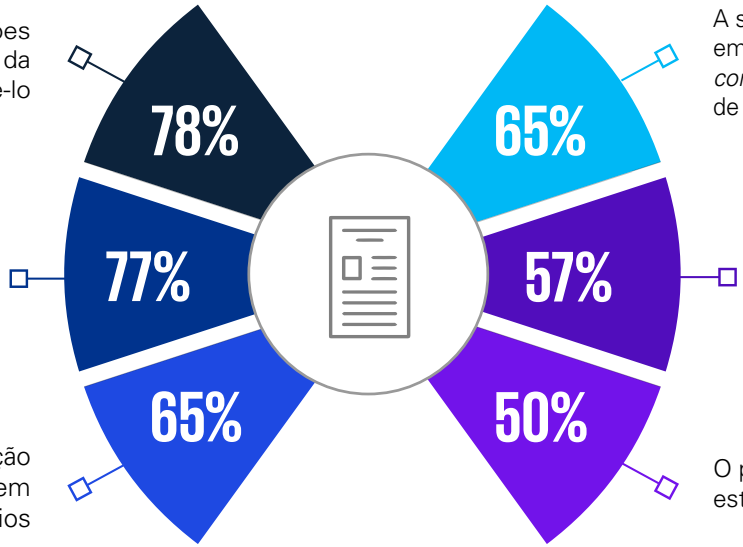
A boa notícia é que os líderes mais influentes das organizações acreditam que os CISOs e a área de segurança cibernética devem estar envolvidos na transformação desde o início.

De acordo com 45% dos respondentes que ocupam cargos de comando, o CISO é um executivo-chave, que teve sua importância impulsionada nos últimos cinco anos, graças à transformação digital, à necessidade de combater os crimes cibernéticos e ao aumento das expectativas dos órgãos reguladores.

Os CISOs precisam ter em perspectiva que as questões técnicas permanecerão em suas mãos; mas é importante que, no nível sênior, eles também enfoquem as necessidades do negócio e procurem assegurar que as estratégias cibernéticas devem se aliar às outras, como as de planejamento, investimento e entrega de resultados.

Os CISOs estão prontos para ir além — mas eles estão sendo autorizados a fazê-lo?

O gráfico mostra a porcentagem de respondentes que concordam ou concordam plenamente com as afirmações



Nossa equipe de segurança das informações entende seu papel na garantia da organização e sente-se confiante para fazê-lo

A segurança das informações em nossa empresa é moldada por requisitos de *compliance*, e não por uma visão estratégica de longo prazo

O aumento da confiança de todos os *stakeholders* é fundamental para nosso programa de riscos cibernéticos

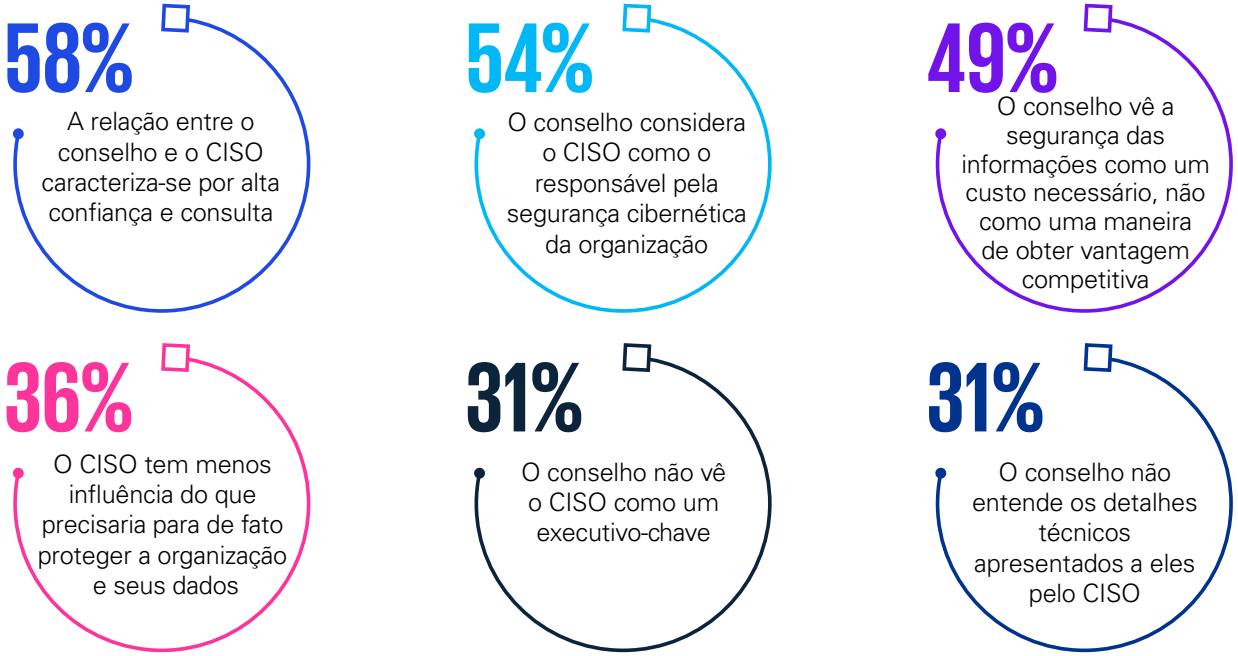
Nossos líderes seniores não entendem plenamente os benefícios competitivos do aumento da confiança viabilizados por uma melhor segurança das informações

A segurança das informações em nossa organização é vista como uma atividade de redução do risco em vez de um agente capacitador de negócios

O papel do CISO não é tão estratégico quanto deveria ser

Os conselhos têm opiniões mistas sobre a influência dos CISOs

O gráfico mostra a porcentagem de respondentes que concordaram com as afirmações.



O desafio de quantificar o risco

Muitas organizações estão fazendo um bom progresso na modelagem e avaliação de riscos em uma área que têm sido notoriamente resistente à análise. Três quartos das organizações dizem ter implementado uma modelagem de risco para quantificar e relatar visualmente o risco cibernético no conselho, mas somente 58% descrevem sua abordagem para quantificar os riscos cibernéticos como 'robustas' e concordam que os cenários de risco cibernético são adaptados às necessidades do negócio.

De maneira mais positiva, 69% dos respondentes dizem ter uma abordagem robusta para valorizar a confiança digital, em vez de vê-la como apenas um conceito abstrato. E 65% dizem que a modelagem de riscos impulsiona o investimento em segurança cibernética, com vínculos claros entre os projetos e a redução do risco.

Assim, os CISOs precisam atuar mais intensamente do que já fazem; precisam, também, reconhecer a natureza em evolução do trabalho, ampliando seu alcance em áreas nas quais existe potencial para estimular a confiança na organização.

Perspectiva da KPMG: a importância de mensurar o risco cibernético

Um trabalho cuidadoso de modelagem e quantificação pode ajudar os tomadores de decisão a entender o nível real de exposição ao risco cibernético da organização. Isso permite que administração identifiquem os controles que mais contribuem para a redução de determinadas exposições cibernéticas, ajudando a garantir que os recursos estão sendo direcionados para as áreas de maior retorno.

Para fazer isso direito, as organizações devem seguir cinco princípios:

1. Alinhar o modelo de risco com as estruturas de risco organizacionais.
2. Ser consistente na definição do risco cibernético, considerando possíveis eventos de perda para o negócio (traçar cenários é uma ótima maneira de fazer isso).
3. Utilizar a modelagem de caminhos de ataque para dimensionar como esses riscos poderiam materializar-se.
4. Utilizardados do mundo real nos cálculos — estimativas de probabilidade e impacto devem conter dados empíricos internos e externos.
5. Entender os benefícios e as limitações do modelo e ser transparente a respeito deles.

James Hanbury
Diretor de cyber security services
da KPMG no Reino Unido

Muitas organizações estão lutando para modelar e avaliar o risco cibernético

A tabela mostra a porcentagem de respondentes que apontaram as afirmações a seguir como mais (ou menos) alinhadas à realidade de suas respectivas organizações

A confiança digital permanece um conceito abstrato para nós	10% / 21% / 69%	Temos uma abordagem de valorização da confiança digital que inclui a proteção das informações dos clientes e dos sócios
As decisões sobre investimento em segurança cibernética e avaliação do risco são processos distintos e separados	12% / 22% / 65%	A modelagem dos riscos impulsiona o investimento em melhorias na segurança cibernética, com vínculos claros entre os projetos e a redução do risco
A modelagem de riscos baseia-se em premissas relativas à ameaça e à vulnerabilidade	12% / 22% / 67%	A modelagem de riscos baseia-se em dados abrangentes sobre ameaças e vulnerabilidades
Os cenários de risco cibernético perpassam toda a empresa, mas são desenvolvidos pelo CISO	16% / 26% / 58%	Os cenários de risco cibernético são desenvolvidos e de propriedade da empresa, adaptando-se às suas necessidades
As avaliações do risco cibernético baseiam-se julgamento subjetivo	16% / 26% / 58%	Temos uma abordagem robusta para quantificar os riscos cibernéticos à organização, incluindo a avaliação da exposição financeira
Nossa organização atualmente não tem capacidade de quantificar o risco cibernético	10% / 16% / 73%	Implementamos uma modelagem de risco para quantificar o risco cibernético e relatar o risco visualmente ao conselho

5

Missão alcançável

Como as organizações podem estimular a confiança com a ajuda do CISO

Os executivos entendem por que é importante aumentar a confiança em suas organizações e em seus ecossistemas. Eles estão empenhados em fazer do CISO um líder dessa jornada, visto que a segurança cibernética e a privacidade são elementos-chave para conquistar a confiança dos clientes, dos órgãos reguladores e do público, atendendo também às questões de ESG.

Os próprios CISOs reconhecem sua responsabilidade por impulsionar esse objetivo e valorizam que seus demais pares – ou seja, os outros líderes da organização – façam parte dessa jornada. No entanto, nossa pesquisa mostra que muitos estão lutando para cumprir esse papel, mas ainda não têm uma visão clara do que a confiança digital realmente significa e de que maneiras podem contribuir para alcançá-la.

Não que este seja um trabalho que qualquer CISO possa fazer sozinho. É indispensável que haja apoio da liderança sênior, colaboração de outras áreas e cooperação produtiva com parceiros externos e terceiros.

Ainda assim, o CISO é um campeão vital. A definição explícita da confiança pode ser um bom ponto de partida, seguida pela utilização da segurança cibernética e da privacidade como uma maneira de reforçar a confiança na organização, com todas as vantagens competitivas que isso pode proporcionar.

E como fazer isso?

Cinco passos cruciais para a construção da confiança por meio da segurança cibernética e da privacidade

01

Trate a privacidade e a segurança cibernética como prioridades

Insira a segurança cibernética e a privacidade nos processos de negócio, na governança e na cultura da organização, tornando-a parte integral dos negócios, em vez de um processo de custos operacionais exigido por *compliance*.

02

Construa colaborações internas e estimule a confiança

Trabalhe com colegas seus pares para ajudar a estabelecer, incorporar e manter a confiança digital.

03

Redimensione o papel do CISO

Adote uma pauta mais ampla e reconheça a capacidade de fazer contribuições abrangentes em áreas que abranjam desde as questões de ESG até a ética da IA.

04

Apoio dos líderes e investimento em confiança

Os CISOs que ganham o apoio da diretoria e do conselho enfrentam menos dificuldades para impulsionar a pauta de confiança. Isso significa transformar o papel do CISO: ele deixa de ser apenas um protagonista técnico e torna-se agente capacitador estratégico dentro da organização.

05

Entre em contato com o ecossistema

Identifique colaborações importantes no ecossistema da organização e colabore de maneira estreita com eles, buscando sempre aumentar a confiança e a resiliência.

Metodologia e reconhecimentos

Sobre a pesquisa *KPMG Cyber Trust Insights 2022*

Realizado pela KPMG entre maio e junho de 2022, este estudo baseia-se em entrevistas realizadas com 1.881 executivos e cinco líderes corporativos de todo o mundo. O objetivo central deste trabalho consiste em entender profundamente o papel que a segurança cibernética e a privacidade desempenham na construção e na manutenção da confiança.

Uma proporção significativa da amostra pesquisada é composta de líderes seniores: 42% são membros do conselho ou membros da diretoria. Dentre os respondentes, há líderes de 31 mercados (24% da região Ásia-Pacífico,, 50% da Europa, Oriente Médio e África, 16% da América do Norte e 10% da América do Sul) e seis setores-chave da indústria (energia e recursos naturais, serviços financeiros, *life sciences* e indústria farmacêutica, mídia, entretenimento e tecnologia, setor público e telecomunicações).

Entre os respondentes, 45% têm receitas anuais acima de US$ 500 milhões; 23% têm receitas acima de US$ 1 bilhão; e 7% têm receitas acima de US$ 5 bilhões.

A KPMG agradece aos seguintes executivos por suas contribuições:

- Bashar Abouseido, vice-presidente sênior e CISO da Charles Schwab
- Ulrich Baisch, CIO da Bechtle
- Allan Cocksaur, CISO da Shell
- Ann Johnson, vice-presidente corporativa da Microsoft Security Business Development
- Mark Thompson, CSO da Associação Internacional dos Profissionais de Privacidade (IAPP)

Sobre a KPMG

A KPMG é uma organização global de firmas independentes que prestam serviços profissionais nas áreas de auditoria, tributos e consultoria. Estamos presentes em 146 países e territórios. No exercício financeiro de 2020, o total de profissionais atuando nas firmas-membro em todo o mundo era de aproximadamente 227.000. Cada firma é uma entidade legal independente e separada e descreve-se como tal.

No Brasil, são aproximadamente 5.000 profissionais distribuídos em 13 Estados e Distrito Federal, 22 cidades e escritórios situados em São Paulo (sede), Belém, Belo Horizonte, Brasília, Campinas, Cuiabá, Curitiba, Florianópolis, Fortaleza, Goiânia, Joinville, Londrina, Manaus, Osasco, Porto Alegre, Recife, Ribeirão Preto, Rio de Janeiro, Salvador, São Carlos, São José dos Campos e Uberlândia.

Orientada pelo seu propósito de empoderar a mudança, a KPMG tornou-se uma empresa referência no segmento em que atua.

Compartilhamos valor e inspiramos confiança no mercado de capitais e nas comunidades há mais de 100 anos, transformando pessoas e empresas e gerando impactos positivos que contribuem para a realização de mudanças sustentáveis em nossos clientes, governos e sociedade civil.

Fale com o nosso time

Klaus Kiessling
Sócio de Cyber Security & Privacy da KPMG no Brasil
kkiessling@kpmg.com.br

Alguns dos serviços ou todos os serviços descritos neste item podem não ser permitidos para clientes de auditoria da KPMG e suas coligadas ou entidades relacionadas.

kpmg.com/socialmedia

Elaborado por Evalueserve.

Nome da publicação: insights sobre a confiança cibernética da KPMG para 2022 | Número da publicação: 138298-G | Data de publicação: outubro de 2022