Simplificando a segurança cibernética

As empresas se tornaram complexas demais para serem protegidas?

pwc

www.pwc.com.br

Onde estamos?

A digitização vertiginosa já está mudando os limites das empresas, impulsionando o surgimento de novas conexões, produtos e serviços, e tornando os cenários mais competitivos. Estar conectado em qualquer lugar e a qualquer momento é uma realidade mundial. Os processos industriais e a logística estão cada vez mais robotizados, apoiados por redes complexas de comando e controle. O uso intensivo de computação em nuvem e de inteligência artificial já são parte do cotidiano das pessoas e das empresas. O dispositivo móvel de um empregado, por exemplo, pode estar sendo utilizado para acessar os aplicativos da empresa, mas também de *wallet*, câmera, agenda, gravador de voz, televisor, biblioteca, console de jogos, entre outros, o que — sem dúvida — simplifica a vida.

Esse contexto faz com que os processos necessários para gerenciar e manter todo esse ecossistema interconectado – inclusive a segurança cibernética – também se tornem mais e mais complicados. Mas **há uma complexidade desnecessária**, nociva, e os executivos já perceberam isso.

77%

dos líderes brasileiros que participaram da pesquisa *Digital Trust Insights 2022* da PwC consideram que as organizações se tornaram complexas demais para serem protegidas.

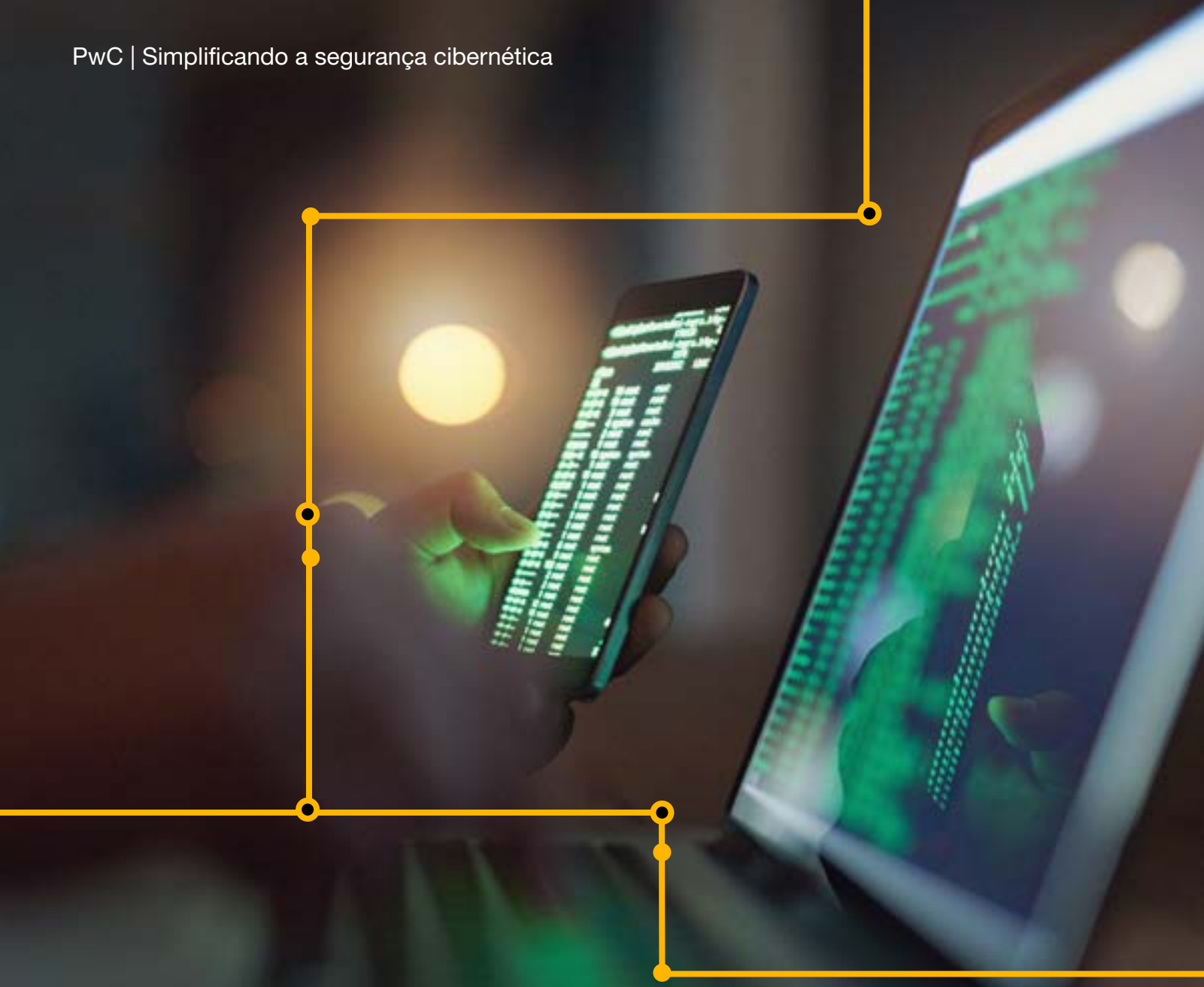
Fonte: *Global Digital Trust Insights 2022,* PwC, dados de outubro de 2021.

Além disso, muitos conselhos de administração, comitês de auditoria e CEOs ainda veem a segurança cibernética como um conjunto de iniciativas e normas técnicas que pertencem à esfera da área de Tecnologia, do diretor de segurança e de outros profissionais especializados. Com isso, acabam não usando dados e inteligência para tomar as melhores decisões de investimento e de gerenciamento de riscos cibernéticos que podem afetar os negócios.

1/3

Apenas 1/3 das organizações no mundo tem práticas avançadas de confiança de dados.

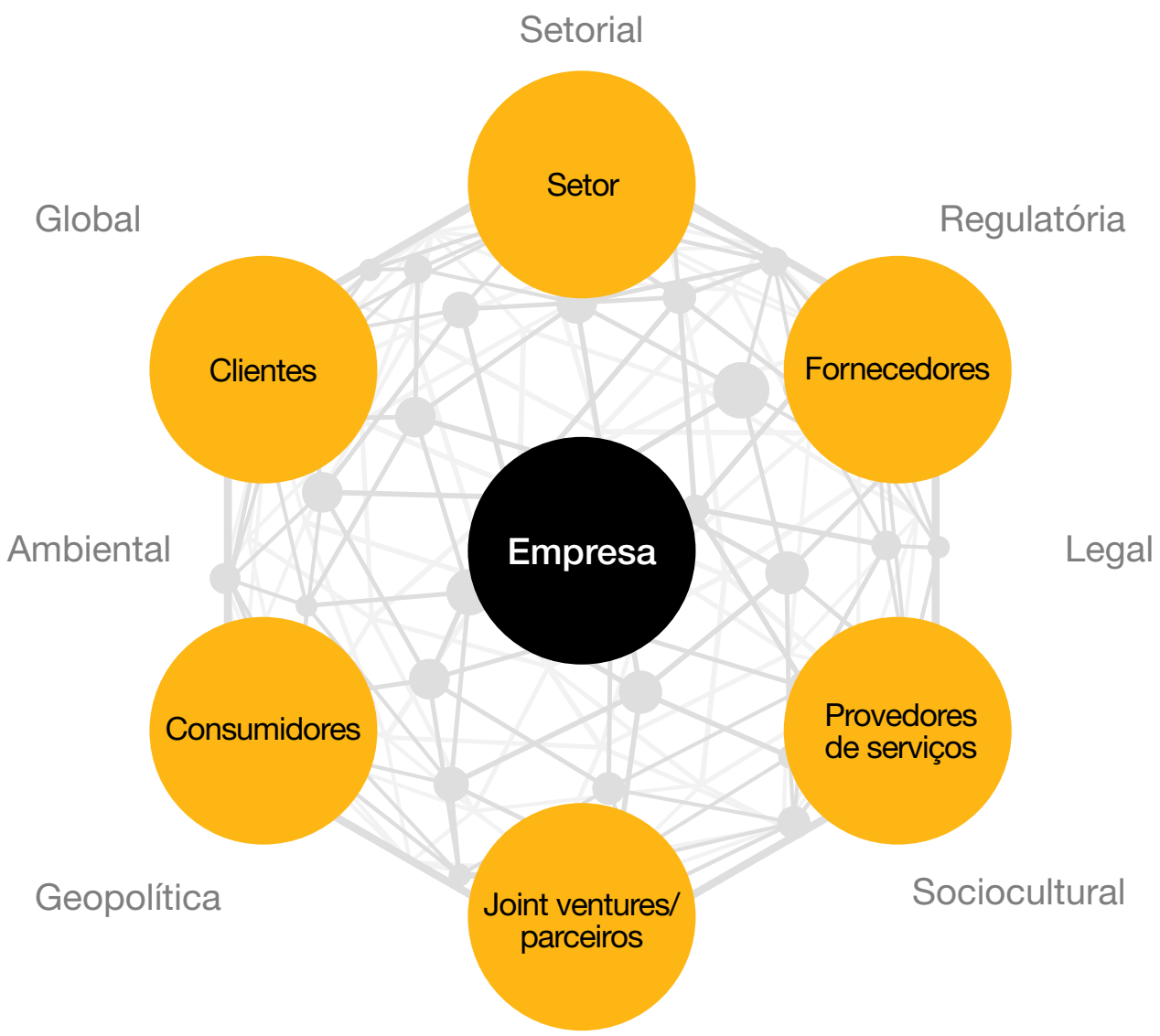
Fonte: *Global Digital Trust Insights 2022,* PwC, dados de outubro de 2021.



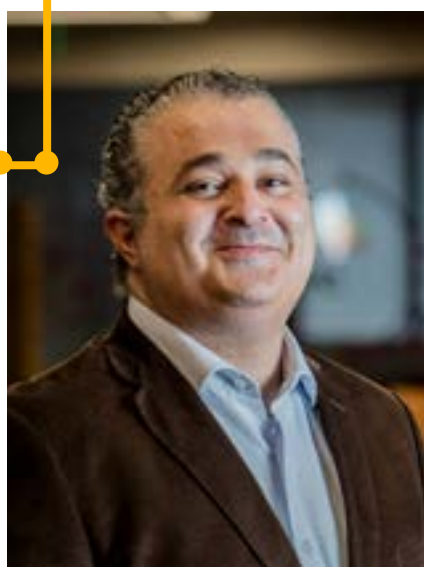
Complexidade desnecessária

A conexão digital exacerbou a questão da complexidade. As empresas criaram um número crescente de ecossistemas digitais, conectando uma variedade de novos parceiros, com o propósito de expandir seu alcance e obter resultados mais expressivos. Em contrapartida, a complexidade e a expansão do alcance digital trouxeram patamares superiores de exposição ao risco cibernético e de investimentos em segurança e proteção de dados.

Rede de interconexão digital



As empresas precisam considerar várias dimensões de risco cibernético que podem afetar o ecossistema de que fazem parte.



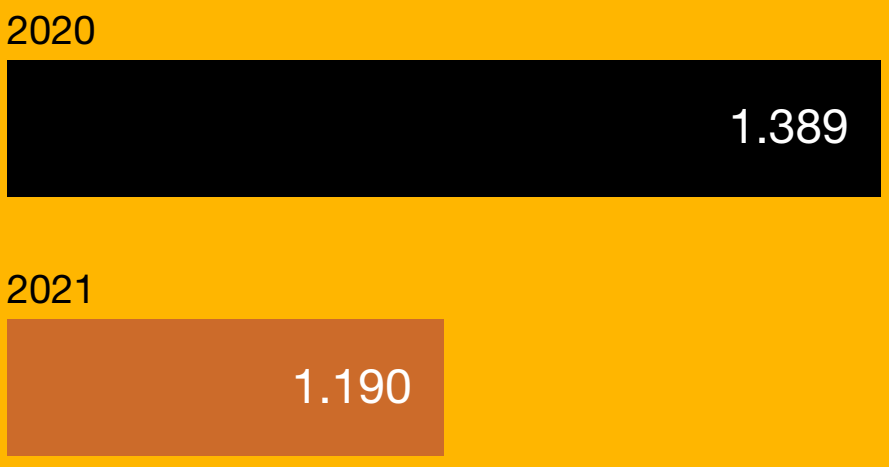
Eduardo Batista
Sócio e líder de *Cybersecurity*

“Além de estratégias e modelos de segurança cibernética para verificar a complexidade e os riscos abrigados em seus sistemas e processos, as empresas podem aprimorar sua segurança cibernética e proteger melhor seus dados, adotando novas abordagens, como a confiança zero (Zero Trust), que incorpora a análise da maneira como os sistemas são usados com privilégios equilibrados entre a necessidade de segurança e a performance do negócio.”

Ataques cibernéticos

O número de ataques cibernéticos em todo o mundo está aumentando, ano após ano, incluindo casos de *ransomware,* que são potencialmente devastadores para as operações das empresas privadas e públicas e visam a obtenção de ganhos financeiros por meio da extorsão (simples ou múltipla) decorrente do sequestro da infra-estrutura tecnológica ou de dados críticos da empresa (dados pessoais, financeiros, estratégicos etc.) empresa.

Total de vazamentos de dados de *ransomware* no mundo



Fonte: *Darktracer*, com dados de 2020 e 2021 (de janeiro a agosto).

Cada grande incidente expõe milhares de usuários, tanto em empresas quanto em agências governamentais, e os criminosos podem permanecer meses sem serem descobertos.

Em todas as indústrias, as principais consequências da complexidade são perdas financeiras, incapacidade de inovar e falta de resiliência

Pergunta:

Em sua opinião, quais são as consequências mais importantes da complexidade nos seus negócios?

	Geral	PI	SF	TMT	V&C	Saúde	EUR	G&SP
Perdas financeiras causadas por violações de dados ou ataques cibernéticos	1	3	3	1	1	1	1	5
Incapacidade de inovar tão rapidamente quanto as oportunidades de mercado oferecidas	2	2	1	3	2	3	2	2
Falta de resiliência operacional ou incapacidade de se recuperar de um ataque cibernético ou falha tecnológica	3	1	2	2	3	2	3	1

Participantes:

- Produção industrial: **789**
- Tecnologia, mídia e telecomunicações: **824**
- Serviços financeiros: **724**
- Varejo e consumo: **581**
- Energia, *utilities* e recursos: **299**
- Saúde: **255**
- Governo/serviços públicos: **126**

Para governo/serviços públicos, a terceira consequência mais importante é a "incapacidade de reter os melhores talentos".

Fonte: *Global Digital Trust Insights 2022,* PwC, dados de outubro de 2021.

3 questões primordiais

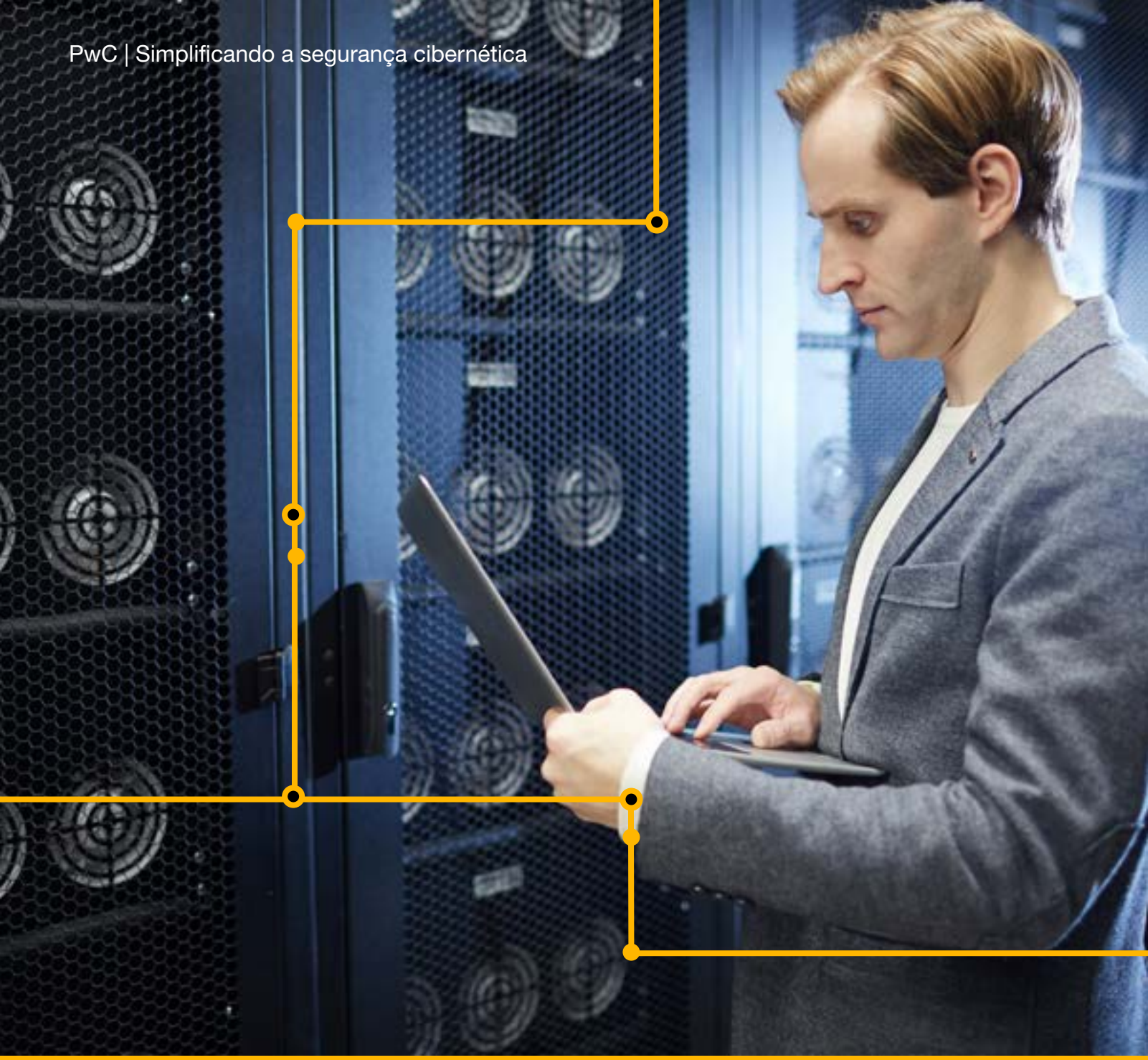
As equipes de liderança que lidam com questões como essas e adotam a simplicidade aumentam suas chances de tornar toda a empresa mais segura.

É essencial estabelecer um diálogo estratégico permanente sobre riscos cibernéticos entre conselho, comitê de auditoria, CEO e restante da diretoria.

01 Como o levantamento completo dos riscos cibernéticos afeta a atratividade do nosso modelo de negócios? Ele sugere a necessidade de uma “agenda de simplificação”?

02 Em que medida os riscos cibernéticos e os mecanismos de defesa das nossas parcerias externas são transparentes e eficientes? Quais seriam os prós e contras de simplificar nosso ecossistema para torná-las mais gerenciáveis?

03 Em que medida nossos processos legados de TI representam risco acentuado e como devemos priorizar os investimentos para protegê-los, simplificá-los e transformá-los a fim de obter vantagem competitiva?

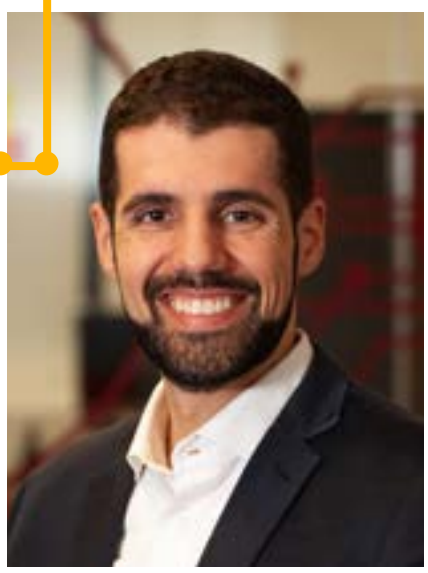


Até onde compensa terceirizar

Os líderes precisam de modelos eficientes para avaliar a complexidade dos acordos de negócios, das operações e da TI de suas organizações. Um modelo conceitual para pensar sobre a complexidade e o risco cibernético é o Teorema de Coase, formulado pelo economista Ronald Coase, ganhador do Prêmio Nobel. Ele postulou que as empresas deveriam usar fornecedores externos de bens e serviços até que os custos de transação ou complexidade associados a esses contratos excedam os custos de coordenação de fazer o trabalho internamente.

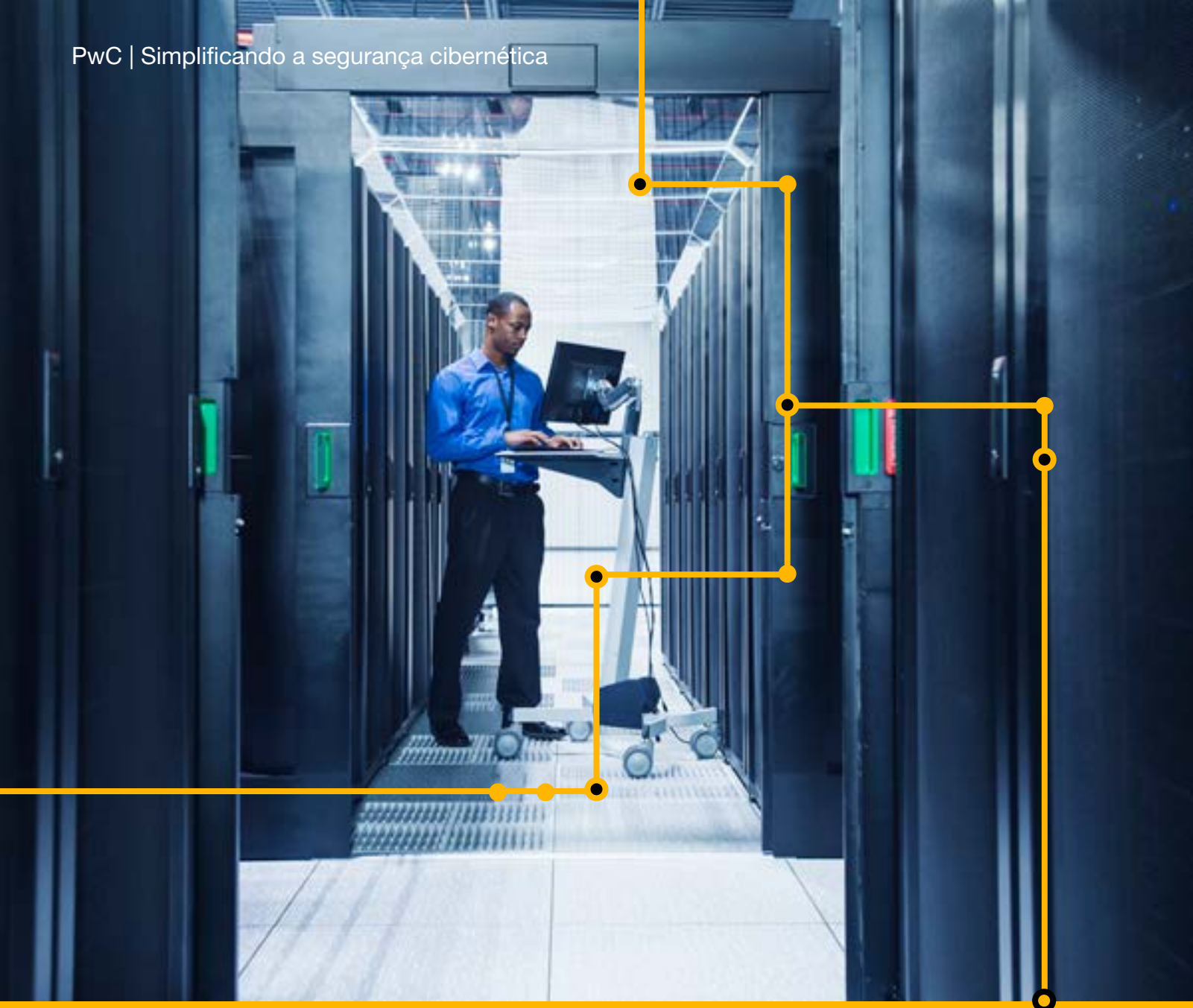
Uma dinâmica semelhante pode ser adotada para avaliar o risco cibernético. Seja gerado por um relacionamento com o fornecedor ou com o cliente ou ainda por acordos internos, o risco cibernético é uma espécie de custo externo, que aumenta à medida que as ameaças avançam e conseguem afetar a segurança e perenidade dos negócios.

Ao mesmo tempo, os custos de transação dentro da empresa para estabelecer vários canais de parcerias (onde os riscos ficam escondidos) realmente estão diminuindo, graças à onipresença e ao menor custo das interações digitais. Resultado: criou-se um ambiente no qual os custos de falhas de segurança aumentaram de forma acentuada, enquanto os custos de criar complexidade diminuíram.



Fernando Mitre
Sócio

“Reduzir a complexidade e, ao mesmo tempo, estabelecer uma estrutura de governança e responsabilidade compartilhada requer uma ação sustentável no longo prazo e direcionada aos principais riscos no curto prazo. Também exige a atenção e a energia de CEOs e conselhos de administração que entendem o valor dessa estrutura e estão prontos para investir na mudança de mentalidade sobre os benefícios da adoção da simplificação da segurança cibernética em toda a organização.”



Lidando com a complexidade em três áreas

Os líderes que buscam um melhor equilíbrio entre complexidade e simplificação podem partir de alguns princípios básicos. Um deles é garantir que seus movimentos estratégicos não aumentem o risco de complexidade e piorem a situação atual. Outro é entender que simplificar a segurança e a tecnologia da empresa pode significar mais do que uma pequena reconfiguração dos sistemas e, em vez disso, exigir modificações dos fundamentos e diretrizes estratégicas – geralmente de longo prazo – nas estruturas de TI e TO, para torná-las adequadas ao crescimento sustentável. Os desafios e oportunidades estão em três áreas.

Modelos de negócios

As empresas costumam responder às falhas na segurança cibernética e proteção de dados com ações que têm um foco restrito e, em última análise, são apenas remendos em um processo ineficiente. A nova intensidade das ameaças, entretanto, muitas vezes exige repensar a questão em um nível estratégico e delinear novos modelos para enfrentar problemas e riscos que se estendem aos negócios.

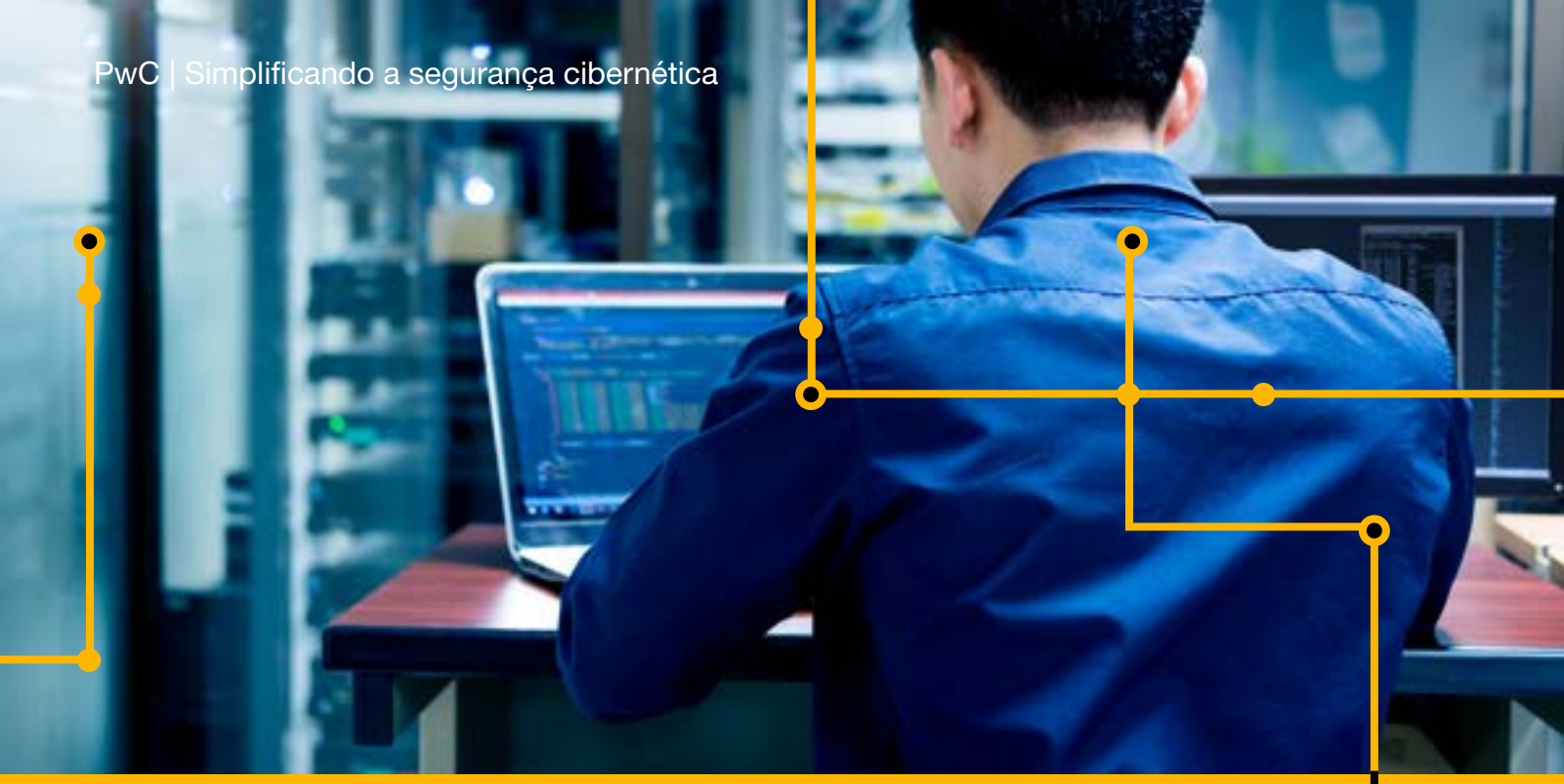
As organizações com as práticas mais avançadas e atuais têm duas vezes mais chances de ter alcançado progresso significativo em segurança cibernética nos últimos dois anos

Top 10% das empresas mais avançadas em quatro áreas: CEO engajado, organização simplificada, confiança de dados, ecossistemas seguros

Top 10% das empresas mais evoluídas, que relataram um progresso significativo em quatro aspectos: gestão do risco cibernético, cultura, alinhamento com o negócio e comunicação entre o conselho e a administração.

Outras empresas

Fonte: *Global Digital Trust Insights 2022,* PwC, dados de outubro de 2021.



Parceiros de negócios e terceiros

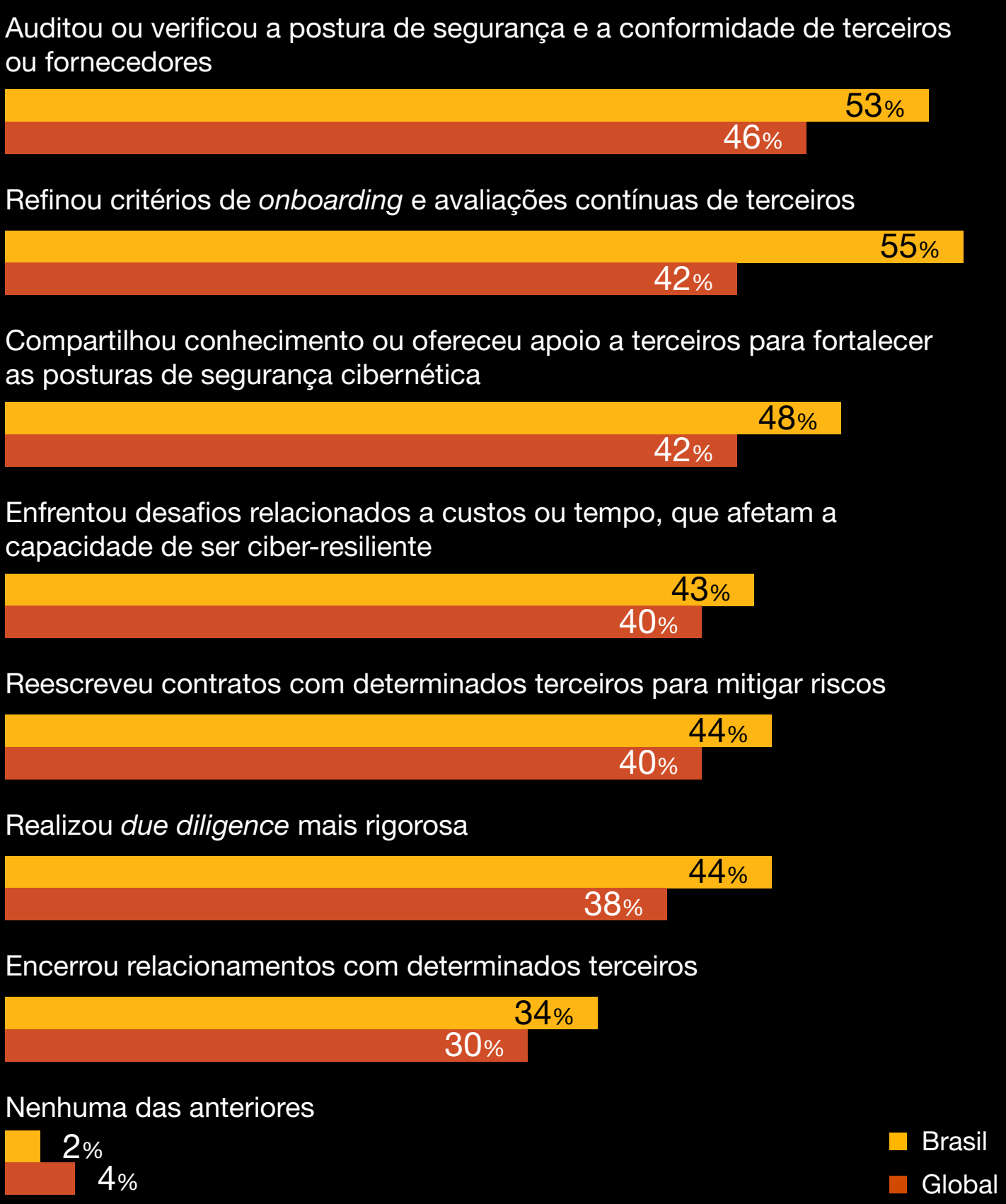
Reduzir o número de fornecedores aos *players* mais capazes e inovadores do setor – garantindo ao mesmo tempo a diversidade e a resiliência que criam confiança – pode ajudar a reduzir a complexidade da cadeia de suprimentos e aumentar a transparência.

A redução da complexidade permite que todas as partes entendam melhor suas funções individuais na proteção do ecossistema digital contra crises cibernéticas e de vazamento de dados pessoais

Criar proteções para acesso seguro às informações da empresa e manter uma vigilância mais próxima sobre as práticas de segurança e proteção de dados do fornecedor, por outro lado, contribui para tornar o ecossistema de dados mais seguro. Isso pode ser obtido a partir de um controle mais robusto sobre as responsabilidades da própria empresa e com modelos de governança para parceiros de negócios (fornecedores e terceiros em geral).

Dessa forma, é possível fazer uma melhor análise no processo de *due diligence*, antes da construção de uma relação mais longeva, definir as obrigações corporativas e individuais do parceiro para manter a relação e usar novas tecnologias para otimizar a eficiência na defesa cibernética e o monitoramento dos riscos de atividades digitais do parceiro de negócios.

Ações adotadas para reduzir riscos de terceiros ou fornecedores



? **Qual é o nível de compreensão da sua organização sobre os riscos cibernéticos e de privacidade decorrentes de terceiros ou fornecedores nas seguintes áreas?**

Fonte: *Global Digital Trust Insights 2022,* PwC, dados de outubro de 2021.

Olhando para dentro

Em muitas instituições financeiras, os sistemas de pagamento foram desenvolvidos ao longo de vários anos com uma combinação de aplicativos de vanguarda e legados. As interrupções que prejudicam a disponibilidade das aplicações geralmente estão associadas à tecnologia legada em sistemas centrais de pagamento.

Na verdade, a causa muitas vezes não é necessariamente a natureza da tecnologia mais antiga em si, mas os processos desatualizados que ela suporta.

Tradicionalmente, esses processos foram estruturados para fechar transações em um ciclo de pagamento de vários dias. À medida que os negócios passaram a exigir a conclusão das transações em tempo real, soluções alternativas cada vez mais complexas tiveram que ser incorporadas aos sistemas legados, com tecnologia que ajusta o pagamento instantâneo a um processo de vários dias.

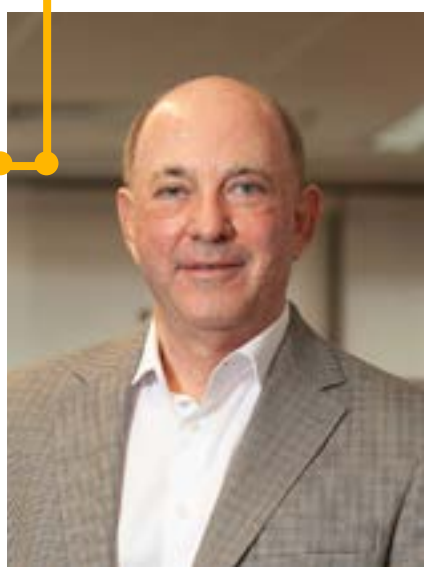
Essa complexidade levou a um aumento da probabilidade de grandes falhas e de interrupções menores se acumularem em cascata para gerar incidentes graves.

Como no caso das instituições financeiras, substituir sistemas existentes também requer decisões de negócios difíceis em outros setores, além de investimentos consideráveis e disposição para deixar de lado a atitude “se não está quebrado, não conserte”. Os custos crescentes da complexidade podem mudar esse comportamento.

Outra análise está relacionada às práticas de governança de privacidade adotadas nas empresas como decorrência da Lei Geral de Proteção de Dados (LGPD).

A eficiência na gestão de consentimentos e na compreensão dos riscos de tratamento de dados pessoais na empresa está diretamente associada à otimização da governança de dados. Sistemas e bases de dados legados se contrapõem com práticas analíticas em *data lakes* e proliferação de pastas de usuários com dados pessoais.

Essa complexidade na governança de dados vem exigindo das empresas não só uma reflexão a respeito, mas também uma ação efetiva com o propósito de otimizar e simplificar a governança de dados na organização.



Edgar D”Andrea
Sócio

“Para uma organização cuja orientação em segurança cibernética e proteção de dados é a simplificação, os executivos de segurança cibernética precisam ampliar seu alcance e repertório, indo muito além dos círculos tecnológicos – aprendendo com o diretor financeiro como falar sobre as implicações financeiras do risco, por exemplo, em uma linguagem que o conselho de administração e o comitê de auditoria compreendam, ou trabalhando com gerentes da “linha de frente” para conceber formas seguras de viabilizar negócios e direcionar inovação na empresa.”

Os líderes que estão prontos para dar um passo à frente e definir o tom da mudança criarão um modelo melhor para tornar sua empresa mais segura. Eles precisam incorporar às prioridades de negócios a busca pela simplicidade e pela redução da complexidade na área de segurança cibernética.

83%

das organizações no Brasil (69% no mundo) preveem um aumento nos gastos cibernéticos em 2022

45%

dos brasileiros (26% no mundo) preveem aumento de gastos cibernéticos acima de 10% – ano passado apenas 14% faziam essa previsão (8% no mundo).

“A complexidade dos desafios cibernéticos não representa apenas uma ameaça para o sucesso dos negócios de uma empresa. Ela também impede que uma organização seja capaz de criar oportunidades inovadoras e persegui-las rapidamente.”

Magnus Santos
Sócio

Veja mais: *Digital Trust Insights 2022*, em: https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2020/global-digital-trust-insights.html

Contatos

Eduardo Batista
Sócio e líder de *Cybersecurity*
eduardo.batista@pwc.com

Fernando Mitre
Sócio
fernando.mitre@pwc.com

Edgar D”Andrea
Sócio
edgar.dandrea@pwc.com

Magnus Santos
Sócio
magnus.santos@pwc.com

www.pwc.com.br

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil