Como a cibersegurança impulsiona a reinvenção da empresa para reforçar a resiliência corporativa

State of Cybersecurity Resilience 2023

Conteúdo

Garantia de sucesso na transformação

O mundo mudou

e a segurança cibernética também – embora nem sempre rápido o suficiente para resultar em alto desempenho.

Garantia de sucesso na transformação

A ruptura de mercados – alimentada por mudanças tecnológicas, regulações complexas, tensões geopolíticas e incertezas econômicas – está testando a abordagem das organizações globais para riscos e resiliência.

Conforme mostra nossa pesquisa Total Enterprise Reinvention, a maioria das grandes organizações está se transformando mais rápido e com mais frequência.

Nosso estudo mais recente sobre cibersegurança revela que algumas companhias vêm usando a segurança cibernética como um diferenciador para entregar melhores resultados corporativos. Essas empresas que alinham seus programas de cybersecurity aos objetivos de negócio são 18% mais propensas a incrementar sua habilidade para promover crescimento das receitas, aumentar sua participação no mercado e melhorar a satisfação e a confiança do cliente e a produtividade da força de trabalho.

Além disso, as organizações que incorporam ações-chave de cibersegurança em seus esforços de transformação digital e aplicam práticas operacionais de segurança cibernética forte na organização como um todo são quase 6x mais propensas a lograr transformações digitais mais efetivas do que aquelas que não o fazem.

Porém, algumas empresas não estão se comprometendo com cybersecurity com a devida antecedência para acelerar a transformação e assim poder enfrentar futuros desafios e explorar oportunidades.

Nós constatamos que quando o assunto é incorporar controles de segurança, 18% dos respondentes da nossa pesquisa ainda os implantam depois que finalizam um esforço de transformação – e mesmo isso só acontece se tiverem sido detectadas vulnerabilidades.

Poderia ser um caso típico de 'um pouco tarde demais'. Segundo um estudo recente, a descoberta de um erro devido a uma segurança fraca de uma aplicação numa fase de codificação de um app, em vez de ocorrer na fase de planejamento inicial, custa cinco vezes mais para consertar – e isso dispara para 30 vezes o custo quando a descoberta acontece após o lançamento.[1]

A próxima onda de transformação das empresas vai evoluir da gestão de capacidades digitais isoladas para a criação das fundações de uma realidade compartilhada. Ela vai convergir as vidas físicas que temos vivido com as digitais que vimos expandindo rapidamente. Num ambiente assim, as organizações deveriam incorporar a cibersegurança a cada passo do percurso para gerir melhor estes riscos altos.

Garantia de sucesso na transformação

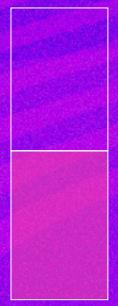
Ao converterem a cibersegurança de uma reação decorrente de um incidente em parte do programa de esforços para a transformação, as empresas podem não só reforçar a resiliência da segurança cibernética, mas também se posicionar para reinventar a empresa inteira e definir uma nova fronteira de performance, com segurança.

Cibersegurança como força transformadora

Cibersegurança como força transformadora

Nossa pesquisa anual State of Cybersecurity Resilience envolveu **3.000** respondentes globais de **15** indústrias, em **14** países.

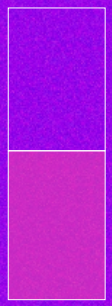
As respostas mostram que mais da metade das companhias está começando a reconhecer a importância de estar segura desde o começo de qualquer esforço de transformação.



53%

disseram que cibersegurança é parte da equipe principal de transformação

&



53%

afirmaram que cibersegurança é exigida antes que qualquer solução seja implementada

Fonte: Accenture State of Cybersecurity Resilience 2023;
N=3.000 executivos de segurança e líderes empresariais

Cibersegurança como força transformadora

Descobrimos que a maioria das organizações submetidas à transformação digital, em nossa pesquisa, aumenta suas chances de plena satisfação com a cibersegurança presente em seus esforços de transformação digital em **10%** se elas seguirem três ações.

Três ações de cibersegurança para potencializar a transformação:

1.

Exigir controles de segurança cibernética antes de todas as novas soluções serem implementadas

2.

Aplicar cibersegurança incrementalmente à medida que cada marco da transformação digital seja atingido

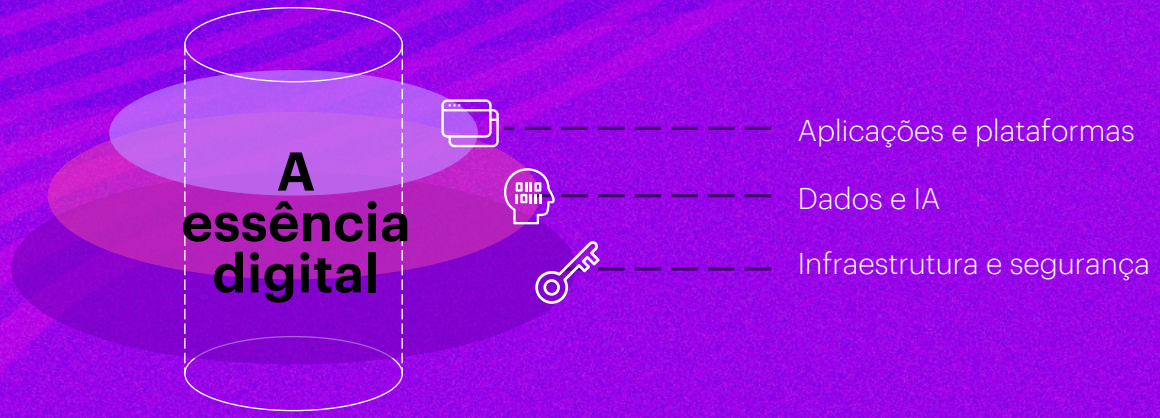
3.

Designar um representante de cibersegurança para integrar a equipe principal da transformação e indicar uma pessoa para orquestrar cibersegurança em todas as iniciativas de transformação

Cibersegurança como força transformadora

Nosso recém-lançado estudo Resilience for Reinvention[2] expõe que as companhias que alcançam crescimento rentável duradouro demonstram um comprometimento com o desenvolvimento de uma essência digital, a qual consiste de três camadas: infraestrutura e segurança; dados e IA; aplicações e plataformas.

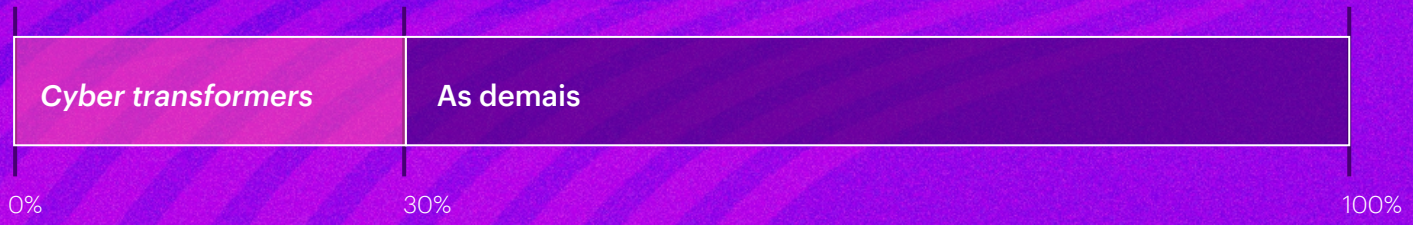
Elas também evidenciam uma parcela consistentemente mais alta de investimentos em novas tecnologias, inovação e cybersecurity.



Cibersegurança como força transformadora

Nesta mais nova pesquisa State of Cybersecurity Resilience, observamos que algumas empresas – representadas por **30%** dos respondentes – já vêm provando como faz uma diferença priorizar a cibersegurança. Estas organizações – nós as chamamos de cyber transformers – aceleraram os esforços para a transformação digital e planejam continuar a fazê-lo à medida que as ações de segurança cibernética de alta performance as propulsionam adiante (Figura 1).

Figure 1. *Cyber transformers* aceleram a transformação digital



Cibersegurança como força transformadora

E, como as cyber champions em nosso relatório de 2021, este ano as cyber transformers buscam um equilíbrio entre se superar em resiliência cibernética e se alinhar com a estratégia da empresa a fim de alcançar melhores resultados corporativos.

Cibersegurança como força transformadora

Cyber transformers mantêm programas de cibersegurança muito proximamente alinhados com os objetivos da empresa. Ao fazerem isso, elas são 18% mais propensas a aumentar os seguintes resultados:

- Habilidade para atingir metas de crescimento de receitas e market share
- Maior satisfação e confiança do cliente
- Maior produtividade da força de trabalho

Além disso, cyber transformers são quase duas vezes melhores do que as demais no envolvimento da equipe de cybersecurity desde o início do planejamento corporativo. E estão muito mais confortáveis com o planejamento interno de cibersegurança da sua organização.

73%

das cyber transformers envolvem a equipe de cibersegurança desde o início do planejamento dos negócios

contra

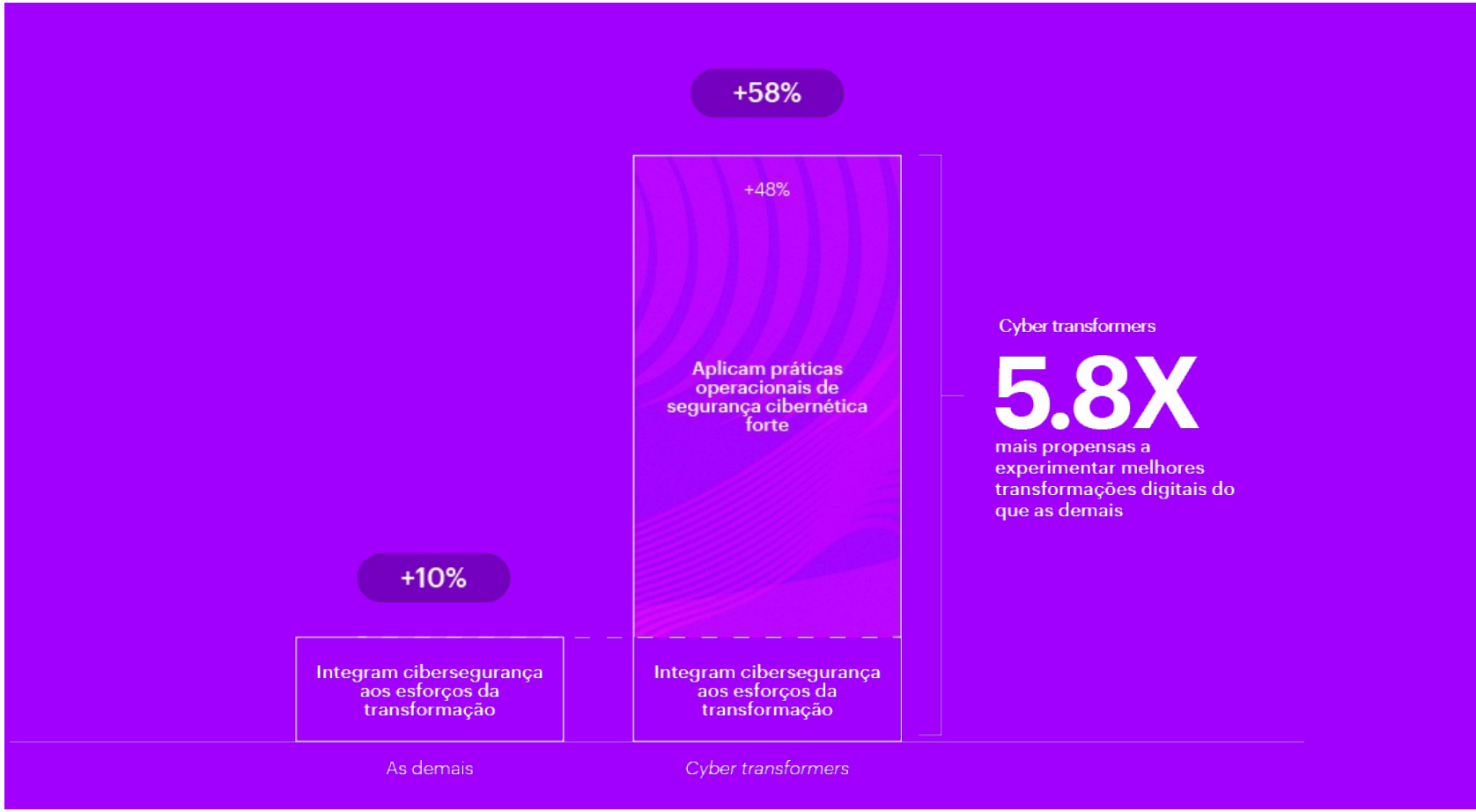
37%

das demais envolvem a equipe de cybersecurity desde o começo do planejamento dos negócios

Cyber transformers constroem as fundações da transformação de duas maneiras

Elas não só integram três ações de cibersegurança aos seus esforços de transformação como também estabelecem uma base melhor quando aplicam práticas operacionais de cibersegurança forte desde o início. Como resultado, elas são 5,8x mais propensas a lograr transformações digitais mais efetivas do que as demais (Figura 2).

Figure 2. Cyber transformers constroem as fundações da transformação de duas formas



Fonte: Análise da Accenture Research de regressão logística nos dados da State of Cybersecurity Resilience 2023; probabilidade premium estimada com a aplicação de melhores práticas na condução da transformação digital. N=2.500 executivos de segurança.

Cibersegurança como força transformadora

Cyber transformers superam as demais companhias com o uso de práticas operacionais de cibersegurança forte.

Destacam-se na integração de cibersegurança e gestão de riscos

Alavancam cibersegurança-como-serviço mais frequentemente a fim de aprimorar as operações de segurança

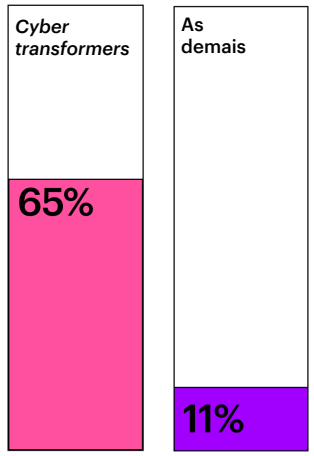
São mais comprometidas com a proteção de seus ecossistemas contra ataques externos

Confiam mais fortemente em automação

O que leva a ser uma cyber transformer

O que leva a ser uma *cyber transformer*

Existem vários fatores que ilustram as diferenças entre as cyber transformers e as demais companhias.



Fonte: Accenture State of Cybersecurity Resilience 2023; N=2.500 executivos de segurança

65% das cyber transformers aplicam três práticas líderes para operar a gestão de riscos com excelência. Do outro lado, apenas 11% das demais adotam esta abordagem "best-in-class".

1. **Integrar o risco cibernético:** um modelo estruturado baseado em risco cibernético é totalmente integrado ao seu programa corporativo de gestão de riscos

2. **Concordar com as prioridades:** suas operações de cibersegurança e a liderança executiva concordam de forma consistente sobre os ativos e operações prioritários a proteger

3. **Olhar os riscos holisticamente:** elas consideram o risco da cibersegurança muito importante quando avaliam o risco geral da empresa

Estudo de caso

Por exemplo, ao decidir integrar o risco cibernético ao seu amplo framework de gestão de riscos da empresa, uma companhia de viagens global conseguiu alcançar uma melhor gestão de riscos, aprimorou o compliance com os requerimentos regulatórios e aumentou a proteção de suas atividades e de seus clientes.
Esta abordagem abrangente e líder no setor para a gestão de riscos corporativos capacitou a empresa para obter um entendimento mais profundo e holístico dos riscos de segurança associados a fornecedores e sistemas de TI terceirizados, assim como um melhor planejamento da prontidão e da recuperação no caso de uma violação.

O que leva a ser uma *cyber transformer*

Cyber transformers usam cibersegurança-como-serviço mais frequentemente para aprimorar as operações.

40% das cyber transformers usam empresas terceirizadas ou provedores de serviços gerenciados para administrar as operações de cybersecurity e resolver as carências de talento contra **24%** das demais companhias.

Estudo de caso

Quando uma rede de varejo norte-americana se tornou uma empresa independente de capital aberto, ela precisou repensar suas operações de TI. A Accenture foi acionada para apoiar a equipe de segurança da varejista por meio da expansão de um modelo de cibersegurança-como-serviço, inicialmente executando as operações de segurança da companhia, como inteligência contra ameaças e estabelecimento de um Security Operations Center (SOC).

Hoje, a Accenture presta uma série de serviços, incluindo proteção de dados, gestão de identidades, segurança de rede, gestão de vulnerabilidades, conscientização de segurança e gestão de riscos.
A melhora nas operações de cibersegurança capacitou a empresa para inovar continuamente, executar suas operações nas lojas sem rupturas e manter a confiança do consumidor. A rede de varejo logrou uma resiliência cibernética aumentada e resultados comerciais melhores ao garantir a segurança desde o início.

O que leva a ser uma *cyber transformer*

Cyber transformers são mais comprometidas em proteger seu ecossistema.

Com base em nossa análise, cyber transformers performam melhor do que as demais companhias quando precisam agir para proteger seus ecossistemas.

Por exemplo, cyber transformers incorporam mais frequentemente seus parceiros de ecossistema ou de supply chain a seu plano de resposta a incidentes **(45% contra 37%)** e também exigem deles que adotem padrões rígidos de cibersegurança **(41% contra 29%)**. Embora estas ações do ecossistema assegurem às cyber transformers uma vantagem de 10% sobre as demais companhias, existe espaço para melhorias.

Estudo de caso

Uma companhia farmacêutica líder colaborou com a Amazon Web Services (AWS) para acelerar o desenvolvimento de medicamentos, aumentar a agilidade operacional, reduzir os custos de tecnologia e desenvolver a força de trabalho do futuro.
Para criar uma arquitetura escalável, confiável e segura, a empresa migrou 80% de suas aplicações para a nuvem, removendo tecnologia não diferenciadora, reduzindo sua pegada do data center interno, diminuindo suas despesas de capital e reforçando a resiliência.

Clientes, funcionários e parceiros podem se beneficiar da habilidade da empresa para reagir com maiores velocidade, agilidade e insights ao longo da cadeia de valor, a qual, por sua vez, melhora a experiência dos pacientes.

Acelerar a entrega de serviços e capacidades de dados pode ajudar a organização a aumentar a conectividade segura e a colaboração com o ecossistema do setor de ciências da vida e parceiros externos.

O que leva a ser uma *cyber transformer*

Cyber transformers confiam fortemente em automação.

89% das cyber transformers confiam fortemente em automação, comparadas com apenas **57%** das demais companhias.

Além disso, **96%** dos respondentes cujas empresas automatizaram substancialmente seus programas de cybersecurity reconhecem que a automação os ajuda a atenuar a escassez de talento em cibernética, um desafio-chave para qualquer companhia em busca de resiliência cibernética. Como evidência de uma abordagem homem+máquina dominando a cena, a análise da Accenture observou que a parcela de patentes de IA relacionadas a cibersegurança cresceu **2,7x** entre janeiro de 2017 e outubro de 2022.

Estudo de caso

Em nossa própria organização com 738 mil funcionários, adotamos IA e automação por meio da nossa Intelligent Application Security Platform. A plataforma usa as melhores ferramentas de scanning comercial para testar em escala o desempenho da segurança em aplicações e descobrir vulnerabilidades e problemas de código. Ela também automatiza, coordena e escala aplicações entrantes assim como testes em aplicações e controles no pipeline.

A plataforma usa um filtro alimentado por IA que remove e reduz vulnerabilidades – de vários milhares a algumas – resultando num processo mais apurado e mais gerenciável. Como resultado, o serviço de scanning ajudou as equipes de aplicações a economizar milhares de horas através da remoção automatizada de conclusões falso-positivas geradas pelas ferramentas de scanning.

O que leva a ser uma *cyber transformer*

Desenvolvimentos emergentes de inteligência artificial como a IA generativa podem impulsionar uma nova onda nos avanços da cibersegurança.

Com o tempo, a IA generariva poderia dar suporte à governança corporativa e à segurança da informação, protegendo contra fraudes, melhorando a conformidade regulatória e identificando riscos proativamente por meio de projetos de conexões multidisciplinares e interferências dentro e fora da organização.[3]

De fato, o surgimento do ChatGPT já trouxe disrupção e oportunidades, oferecendo avanços rápidos nas capacidades de segurança cibernética como detecção de ameaças, análise e resposta e uso acelerado da automação a fim de reduzir a carga de trabalho e ampliar a alocação de pessoas.

Como comentou um CISO:

Existe um argumento para automatizar o suporte de nível um do Security Operations Center (SOC) – coisas como a criação de regras Yara e questões mais complexas. A IA generativa já possui esta capacidade. No entanto, eu acredito que vocês ainda vão precisar da supervisão humana."

O que leva a ser uma *cyber transformer*

Conforme mostra a nossa pesquisa, Total Enterprise Reinvention é uma estratégia deliberada que visa a estabelecer uma nova fronteira de performance para as companhias e, na maioria dos casos, para os setores em que elas operam.

Cyber transformers estão bem posicionadas para executar essa estratégia de reinvenção através de ganhos que resultam diretamente de práticas e comportamentos diferenciados de cibersegurança.

E embora incidentes de cybersecurity continuem a ocorrer todos os dias, em média, as cyber transformers reportam custos **26%** menores do que as demais empresas diante de violações e incidentes de cibersegurança nos últimos 12 meses – isso é mais do que um quarto de todos os custos que poderiam ser alocados na empresa para otimizar as operações, alimentar o crescimento e melhorar os resultados.

Estudo de caso

Um grande banco comercial e de varejo introduziu uma tomada de decisões ágil relativa a cibersegurança enquanto se submetia a duas transformações digitais: a migração para uma nuvem privada e a criação de novos produtos com uso de nuvem pública.

O modelo operacional descentralizado do banco, associado à incorporação desde cedo de cibersegurança ao processo de transformação digital, ajudou a reduzir riscos e vulnerabilidades, aumentou a proteção dos dados e aprimorou a sua postura de segurança geral.

E o mais importante: o banco diminuiu custos e interrupções e aumentou o compliance – melhorando sua reputação como uma organização segura e confiável.

Pontos de pressão extra

Pontos de pressão extra

Embora a gestão de uma transformação digital segura seja uma consideração importante, nossa pesquisa revela a existência de outras questões permanentes que colocam pressão em todas as organizações e influenciam o estado da resiliência da cibersegurança. Olhando o nosso conjunto inteiro de respondentes globais, estes pontos de pressão adicionais ficaram claros.

Um panorama geopolítico incerto acelera as ameaças e os ataques

A resiliência da cibersegurança das empresas está sob pressão decorrente de tensões geopolíticas em curso, especialmente vinculadas às suas cadeias de suprimento, infraestrutura física e redes externas.

Toda a abordagem contra riscos cibernéticos está sob análise, interna e externa

As companhias não conseguem acompanhar o ritmo do aumento do escopo e da escala dos riscos cibernéticos.

Ainda há espaço para melhorias em cibersegurança e alinhamento aos negócios

As empresas estão alinhando melhor a cibersegurança com a liderança corporativa, mas existem lacunas na efetividade da sua abordagem.

Pontos de pressão extra

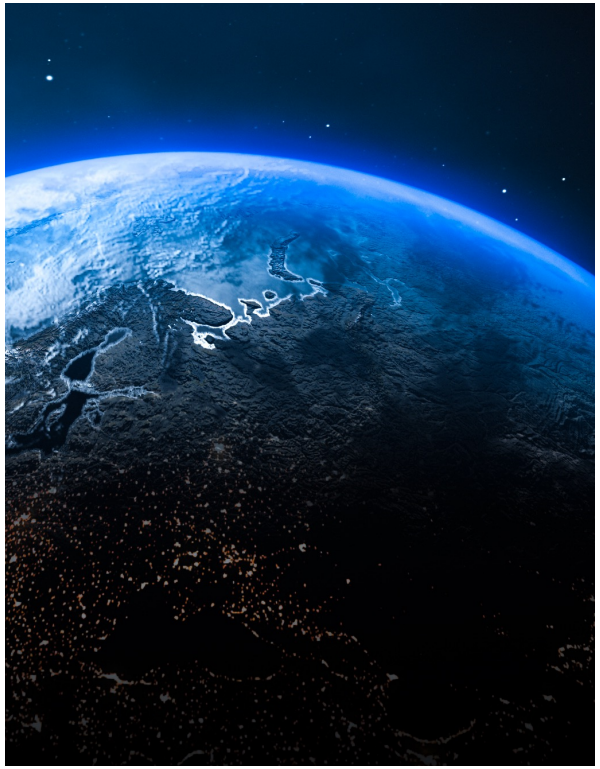
Um panorama geopolítico incerto acelera as ameaças e os ataques

A resiliência da cibersegurança das empresas está sob pressão decorrente de tensões geopolíticas em curso, especialmente vinculadas às suas cadeias de suprimento, infraestrutura física e redes externas, como parceiros investidores.

A influência das agressões da Rússia na Ucrânia tem sido sentida por praticamente todos. Quase todas as organizações (97%) viram um aumento das ameaças cibernéticas desde o começo da guerra Rússia-Ucrânia e quase todos os respondentes da pesquisa tomaram alguma medida.

51% das companhias atualizaram seus planos de continuação dos negócios e risco corporativo, e perto da metade aprimorou suas capacidades de resposta a incidentes. Ao mesmo tempo, só 39% das empresas estão priorizando uma colaboração estreita com agências governamentais acerca de políticas e recomendações em resposta à guerra. Mais da metade **(54%)** vê terceiros e redes externas como as áreas mais suscetíveis a ataques.

De fato, em linha com as conclusões do ano passado, a porcentagem de violações bem-sucedidas originadas fora da empresa continua alta, tendo subido de 60% para 61% este ano, enquanto para algumas indústrias, como utilities, as ameaças junto a parceiros de supply chain estejam de novo mais elevadas – em **62%.**



Pontos de pressão extra

Toda a abordagem contra riscos cibernéticos está sob análise, interna e externa

As companhias não conseguem acompanhar o ritmo do aumento do escopo e da escala dos riscos cibernéticos.

A gestão de riscos cibernéticos é desafiadora dentro das organizações. Menos da metade de todos os respondentes da pesquisa disse que apenas um aspecto da gestão de riscos corporativos – seu framework baseado em riscos cibernéticos – está completamente integrado ao programa de gestão de riscos da empresa.

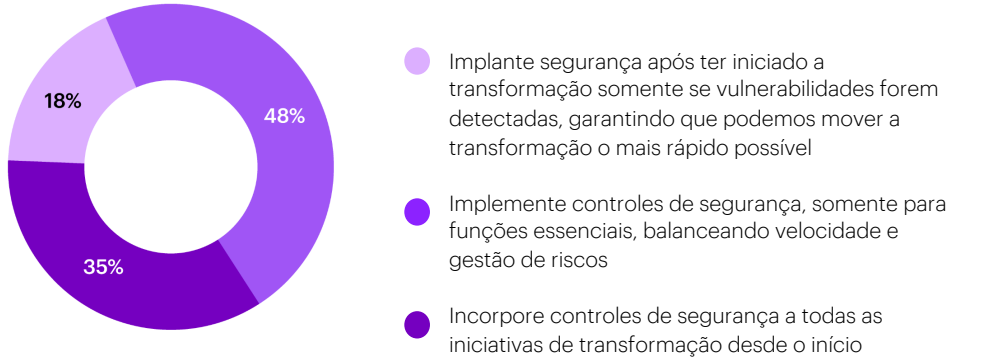
O cenário regulatório tem um papel aqui, com a integração dos riscos saltando para **81%** no setor bancário altamente regulado ou para **65%** na indústria de software e plataformas.

E acelerar a transformação sem endereçar a segurança em paralelo pode abrir a porta para riscos maiores.

Enquanto **35%** dos respondentes disseram que integram controles de segurança a todas as iniciativas de transformação desde o começo, ainda existem **18%** que implantam segurança após o evento. Para transformar rápido, a segurança deveria ser fundida, senão as organizações podem esperar incorrer em mais custos ou retrabalho mais adiante (Figura 3).

O risco cibernético também vem aumentando fora da organização, onde as ameaças estão crescendo devido a mudanças no panorama das ameaças, e as omissões em cybersecurity deixam as empresas expostas.

Figure 3. A segurança dos esforços da transformação digital



Fonte: Accenture State of Cybersecurity Resilience 2023; N=2.500 executivos de segurança e 500 líderes empresariais

Por exemplo, a invasão da Ucrânia pela Rússia impulsionou a reação dos executivos para endereçar práticas de cibersegurança, como atualizações para a continuação dos negócios, resposta a incidentes e aumento do conhecimento cibernético dos funcionários.

De fato, somente um terço de todos os respondentes (35%) considera riscos de cibersegurança "de grande relevância" quando avaliam o risco geral da empresa; isto evidencia que ainda existe muito a fazer pela frente para tornar cibersegurança uma necessidade proativa e estratégica dentro da companhia.

Pontos de pressão extra

Ainda há espaço para melhorias em cibersegurança e alinhamento aos negócios

As empresas estão alinhando melhor a cibersegurança com a liderança corporativa, mas existem lacunas na efetividade da sua abordagem.

Os líderes empresariais (respondentes CEOs e CFOs em nossa pesquisa) esperam que os CISOs vão além do seu papel técnico tradicional para agir como um representante da organização. Os líderes reportaram a importância de os CISOs adotarem certas características, como a tradução dos aspectos técnicos da cibersegurança para o CEO e o board (**44%**), conduzindo a reação durante as violações (**42%**) e estabelecendo confiança com os clientes (**41%**).

Como reportou um CISO:

A maior barreira que os líderes de segurança têm é a presença executiva. Você precisa demonstrar capacidade empresarial e valorizar e engajar em conversas que sejam acerca de outros temas além de segurança."

Estas conclusões ressaltam a importância de ter um CISO orientado pelo negócio, que atue como um educador e colaborador com interlocutores non-security.

Em especial, existe uma lacuna entre CISOs e líderes de empresa quando o assunto é uma estratégia de comunicação pós-violação dirigida ao público em geral. E contudo, como toda organização que já teve experiência de ataque sabe, no meio de uma crise, é fundamental preparar comunicados rápidos e transparentes a fim de informar e tranquilizar os stakeholders.

Quase metade de todos os CISOs disse que nenhum executivo foi definido como responsável pela comunicação externa durante uma violação.

Pontos de pressão extra

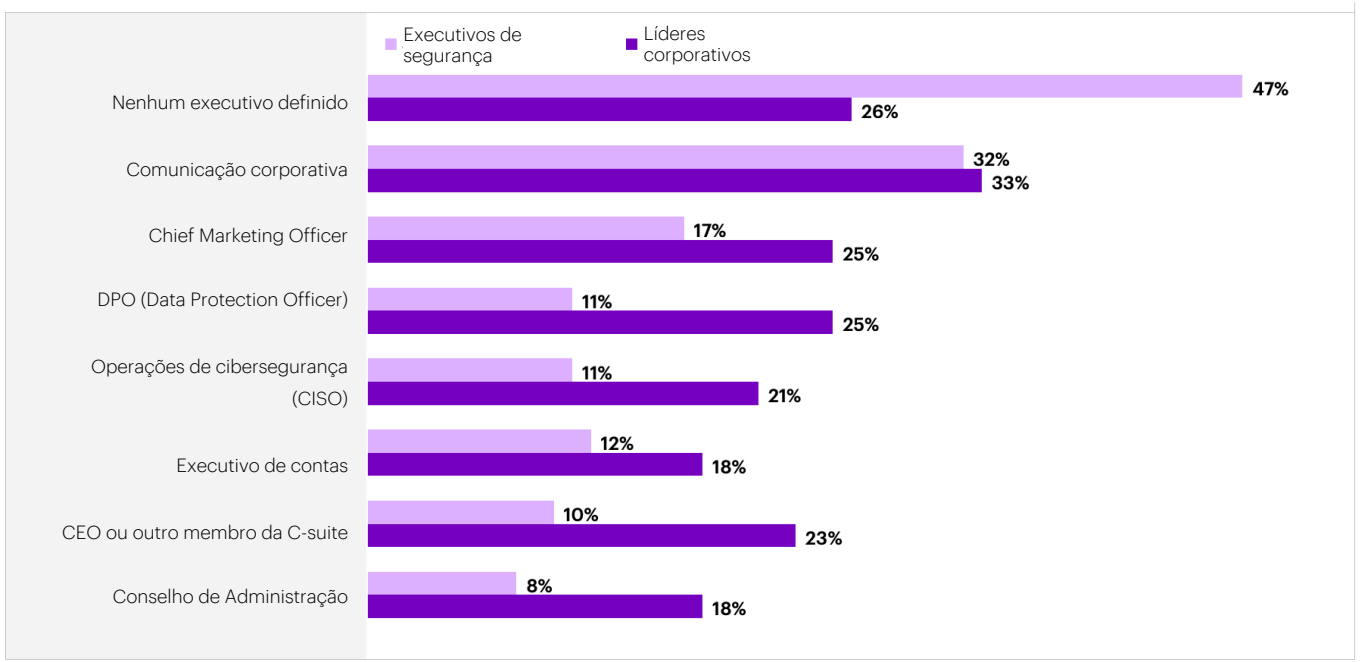
Ainda há espaço para melhorias em cibersegurança e alinhamento aos negócios

Além disso, as diferenças das opiniões entre CISOs e líderes empresariais sobre esta responsabilidade podem indicar uma falta de clareza para a comunicação pós-violações (Figura 4).

Este é um alerta vermelho para a empresa inteira, na medida em que a comunicação tenta limitar o estrago de uma violação para a marca e para a graduação da satisfação dos clientes. Foi identificada como a consideração mais importante após uma violação por 50% dos respondentes da nossa pesquisa.

As empresas têm a responsabilidade de definir a estratégia de comuncação de uma crise; que ela seja ágil, que considere as complexidades de eventos cibernéticos e que aponte claramente os papéis e responsabilidades pela comunicação dirigida aos stakeholders.

Figure 4. Responsabilidade pela comunicação durante uma violação



Fonte: Accenture State of Cybersecurity Resilience 2023. N=2.500 executivos de segurança e líderes empresariais

O que fazer agora?

O que fazer agora?

Realisticamente falando, se você não está olhando para a cibersegurança holisticamente, você não está protegendo sua empresa plenamente

O que fazer agora?

Veja como você pode empregar cibersegurança para impulsionar resultados melhores

Incorporar cibersegurança para proteger sua essência digital

Segurança é fundamental para capacitar agilidade e escalabilidade nas empresas assim como para estimular a inovação contínua e estabelecer a essência digital de uma organização – uma que empodere funcionários e departamentos para experimentar e escalar enquanto mitiga riscos.

O que você pode fazer

Empreenda as três ações de cybersecurity e estabeleça uma base forte com práticas operacionais de cibersegurança a fim de melhorar os resultados e a performance geral.

Aplicar cibersegurança para reconciliar os mundos digital e físico

Aumentos de acessos, dispositivos, software e conectividade na continuidade da nuvem e de ambientes legados resultaram num território de ameaças em constante expansão. E apesar de a IA generativa[4] poder anunciar uma nova era de agilidade e proteção cibernética, ela também atua como um novo vetor de ameaças para os criminosos cibernéticos.

O que você pode fazer

Invista em compreender seus dados, o valor deles e quem os acessa. Verifique identidades na empresa e de clientes para fazer a ponte ideal entre os mundos físico e digital. Estabeleça monitoramento e visibilidade aprimorados nos ambientes legados e na nuvem com uso de tecnologias de endpoint detection and response (EDR) e security orchestration, automation and response (SOAR).

Tornar a cibersegurança parte da estrutura de transformação

A abordagem tradicional para cibersegurança é insustentável. Uma escassez global de talento em cybersecurity para fazer frente às ameaças atuais é agravada pela menor disponibilidade de pessoas para lidar com os efeitos dos ciberataques sobre a continuação dos negócios de uma organização, sua saúde financeira e sua reputação. As linhas vão ficando indefinidas quando a transformação começa e quando acaba.

O que você pode fazer

Torne cibersegurança uma pedra angular em seus esforços de transformação e eleve a relatoria do CISO de modo que a função seja fundamental para os esforços de transformação da empresa.

O que fazer agora?

Da análise e gestão de riscos à implementação de controles de segurança, e do conhecimento e treinamento em segurança à resposta e recuperação de incidentes, a cibersegurança é essencial para manter uma proteção dinâmica em todo programa de transformação. Além disso, como mostram nossas cyber transformers, os líderes empresariais têm uma oportunidade de estender o impacto da cybersecurity além da proteção da companhia aqui e agora a fim de influenciar ativamente a reinvenção contínua e dinâmica.

Sobre a pesquisa

Dados demográficos

Nossa pesquisa State of Cybersecurity Resilience 2023 envolveu 3.000 respondentes de 15 setores econômicos, em 14 países. Queríamos compreender o papel da cibersegurança na abordagem das organizações para a transformação e as práticas mais amplas de segurança cibernética que facilitam a transformação digital segura. Os respondentes representam organizações com receitas anuais de US$ 1 bilhão ou mais nas regiões América do Norte, América do Sul, Europa e Ásia-Pacífico.

3,000

Total de respondentes

2.500 executivos de segurança
500 líderes empresariais (CEO, CFO)

US$ 1 bi+

Receitas anuais

14

Countries

Alemanha (223)
Arábia Saudita (55)
Austrália (234)
Brasil (100)
Canadá (115)
Espanha (100)
Estados Unidos (888)
França (201)
Irlanda (102)
Itália (200)
Japão (221)
Noruega (100)
Países Baixos (101)
Reino Unido (360)

15

Setores

Alta tecnologia (209)
Bancos (265)
Bens de consumo e serviços (288)
Biotecnologia (199)
Energia – óleo e gás (277)
Mercado de capitais (177)
Químicos (186)
Pagadores de saúde (102)
Provedores de saúde (130)
Seguros (209)
Serviços federais - EUA (100)
Software e plataformas (135)
Telecomunicações (202)
Utilities (262)
Varejo (259)

Metodologia

Análise dos dados da pesquisa

Usamos análise de dados de pesquisa padrão para compreender o panorama geral assim como as características de vários grupos em nossa amostra; em especial, comparamos as cyber transformers que somaram 30% dos executivos de segurança na amostra (741 respondentes) com o restante dos executivos de segurança (1.759 respondentes). Definimos como cyber transformers as organizações que aceleraram seus esforços de transformação digital e que planejam continuar a acelerá-los nos próximos dois anos.

Indicadores compostos

Construímos dois índices independentes a fim de capturar como as empresas avançadas estão em áreas mais complexas

1. **Índice de proteção do ecossistema.** Incorpora dados da nossa pesquisa e é baseado no número de respostas positivas a perguntas sobre ações de proteção do ecossistema que uma organização esteja fazendo. A mesma importância foi aplicada. O índice é distribuído numa escala de 0-100.
2. **Índice de alinhamento e governança.** Com o uso da definição de alinhamento do ano passado, aplicamos os dados da pesquisa deste ano para construir o índice. Este é baseado em respostas quanto ao modo como as organizações alinham sua segurança aos objetivos de negócio e quais práticas de governança elas adotam. Foi aplicada a mesma importância. O índice é distribuído numa escala de 0-100 e foi parte da métrica usada em nossa análise de regressão logística.

Algoritmo econométrico de regressão logística

Para estimar a relação entre a probabilidade de um resultado bem-sucedido e as práticas das organizações, aplicamos uma abordagem de regressão logística. Ambos os modelos foram controlados com respeito ao tamanho das organizações, localização geográfica e setor em que operam:

1. **Análise dos resultados da empresa** – analisamos a relação entre o nível do alinhamento da empresa e a governança, medida com o índice de alinhamento e governança e a probabilidade de que uma organização impacte positivamente por meio da cibersegurança em todos os seguintes resultados:
   - Aumento da habilidade para alcançar meta de crescimento da receita
   - Aumento do market-share
   - Aumento da satisfação e da confiança do cliente
   - Aumento da produtividade da mão de obra
2. **Análise dos esforços de transformação segura** – verificamos a probabilidade de a empresa estar altamente satisfeita com os esforços de transformação segura. Testamos a relação com as práticas-chave de transformação segura para camadas selecionadas na amostra da pesquisa.

NLP e análise de tendências de dados disponíveis publicamente

Usamos dados de patentes LexisNexis em nossa abordagem de processamento de linguagem natural (NLP) a fim de selecionar patentes relacionadas a cibersegurança, incluindo IA. Usando dados de publicação entre janeiro 2017 e outubro de 2022, executamos análise de tendências para compreender a evolução de parcela de patentes de IA no número geral de patentes focadas em cybersecurity.

Glossário

Transformação comprimida é a transformação de várias partes da empresa ao mesmo tempo ou a execução de uma única grande transformação mais rapidamente do que nunca.

Essência digital é fundamental para todas as outras necessidades estratégicas de uma empresa. Amplificar o papel da tecnologia na reinvenção significa se deslocar de um panorama tecnológico composto por partes estáticas e standalone para peças interoperáveis integradas intencionalmente e alavancar a nuvem. A essência digital consiste de três camadas: a camada de infraestrutura e segurança; a de dados e IA; e a de aplicações e plataformas. A construção de uma essência digital forte não é um projeto pontual. Ele precisa ser contínuo a fim de incorporar novas tecnologias e capacidades corporativas.

Total Enterprise Reinvention é uma estratégia deliberada que visa a estabelecer uma nova fronteira de performance para as companhias e, na maioria dos casos, para os setores em que elas operam. Centrada em torno de uma forte essência digital, ela ajuda a impulsionar crescimento e a otimizar as operações. Ela requer uma estratégia para a reinvenção contínua e dinâmica. Esta torna-se uma força unificadora entre a alta direção e todas as funções e áreas de negócio, porque, por definição, todas são envolvidas e responsáveis pelo seu sucesso. Ela demanda uma perspectiva de fora para dentro que conecte o que está ocorrendo na organização com o que acontece no mundo. E ela exige novas habilidades e uma maior profundidade no entendimento de tecnologia, gestão de mudança, comunicação e do modo como trabalhar com parceiros para alcançar resultados mais rápidamente (Figura 5).

Figura 5. As seis características diferenciadoras da Total Enterprise Reinvention

1. **A reinvenção é a estratégia.** Não se trata mais de uma alavanca de execução.
2. **A essência digital torna-se uma fonte primária de vantagem competitiva.** Ela alavanca o poder de nuvem, dados e IA através de um conjunto de sistemas interoperáveis na empresa inteira que permite o rápido desenvolvimento de novas capacidades.
3. **A reinvenção vai além dos benchmarks, abraçando a arte do possível.** Tecnologia e novas formas de trabalhar criam uma nova fronteira de desempenho.
4. **Talent strategy and people impact are central to reinvention,** not an afterthought. These companies consider change management a core competency.
5. **Estratégia de talento e impacto nas pessoas são vitais para a reinvenção, não uma consideração a posteriori.** Estas companhias consideram a gestão da mudança uma competência fundamental.
6. **A reinvenção é contínua.** Não se trata de uma atitude pontual com princípio e fim, mas uma capacidade contínua em benefício da organização.

Referências

1. Dig8ital — Link
2. Reinventing for resilience, Accenture 2023 — Link
3. Uma nova era de IA generativa para todos, Accenture 2023 — Link
4. Ibid — Link

Sobre os autores

Paolo Dal Cin
Líder
Accenture Security

Jacky Fox
Senior Managing Director
Accenture Security
Líder na Europa

Harpreet Sidhu
Senior Managing Director
Accenture Security
Líder na América do Norte

James Nunn-Price
Senior Managing Director
Accenture Security
Líder nos Growth Markets

Agradecimentos
Os autores gostariam de agradecer a Sarah Bird, Edward Blomquist, Katarzyna Furdzik, Corbin Lazier, Anna Marszalik, Eileen Moynihan, Juan Pablo Romero e Ann Vander Hijde por suas contribuições para este estudo.

Sobre a Accenture

A Accenture é uma empresa líder global de serviços profissionais que ajuda grandes companhias, governos e outras organizações a construir sua essência digital, otimizar suas operações, acelerar o crescimento das receitas e aprimorar serviços ao cidadão – criando valor tangível com velocidade e escala. Somos uma empresa liderada por talento e inovação com 732 mil pessoas atendendo a clientes em mais de 120 países. Tecnologia está hoje no coração da mudança, e nós somos uma das líderes mundiais a ajudar a impulsionar essa atitude, com fortes relacionamentos no ecossistema. Combinamos nossa força em tecnologia com experiência setorial incomparável, expertise funcional e capacidade de entrega global. Somos exclusivamente capazes de entregar resultados tangíveis graças ao nosso amplo portfólio de serviços, soluções e ativos em Strategy e Consulting, Technology, Operations, Industry X e Accenture Song. Estas capacidades, junto com nossa cultura de compartilhar sucesso e o compromisso de gerar valor 360o, nos permitem construir relações confiáveis e duradouras com nossos clientes e ajudá-los a alcançar o sucesso. Medimos nosso êxito pelo valor 360o que entregamos a nossos clientes, mutuamente, stakeholders, parceiros e comunidades.

Visite-nos em www.accenture.com.br

Sobre a Accenture Security

A Accenture Security é um provedor líder de serviços de cibersegurança end-to-end, incluindo estratégia, proteção, resiliência e serviços cibernéticos setoriais específicos. Nós criamos inovação em segurança, em escala global e com capacidade de entrega mundial, através de nossa rede de Cyber Fusion Centers. Ajudados por nossa equipe de profissionais altamente habilitados, capacitamos clientes para inovarem com segurança, construírem resiliência cibernética e crescerem com confiança.

Visite-nos em www.accenture.com/security

Sobre a Accenture Research

A Accenture Research molda tendências e cria insights baseados em dados acerca dos mais relevantes problemas enfrentados pelas organizações. Por meio da combinação do poder de técnicas de pesquisa inovadoras e de um profundo conhecimento dos setores de atuação de nossos clientes, nossa equipe de 250 pesquisadores abrange 23 países e publica centenas de relatórios, artigos e pontos de vista todos os anos. Nossos estudos instigantes – apoiados sobre dados proprietários e parcerias com organizações de ponta globais como MIT e Harvard – conduzem nossas inovações e nos permitem transformar teorias e novas ideias em soluções reais para nossos clientes.

Visite-nos em www.accenture.com/research