KnowBe4 Research

RELATÓRIO DE CULTURA DE SEGURANÇA NA AMÉRICA DO SUL 2024

O Relatório de cultura de segurança da KnowBe4 de 2024 apresenta uma análise profunda de como as medidas de segurança afetam as organizações e como os funcionários agem e se sentem no trabalho. Ele se destaca como a análise mais completa e aprofundada da cultura de segurança disponível atualmente, apresentando resultados de pesquisas de milhares de organizações no mundo todo, além de uma importante visão comparativa de cinco anos.

O relatório apresenta um estudo extenso e detalhado de seis regiões globais, no qual avalia o preparo da cultura de segurança em cada uma delas, incluindo América do Norte, América do Sul, Europa, África, Ásia e Oceania.

Este guia oferece uma visão geral das principais descobertas relacionadas à América do Sul.

Dimensões da cultura de segurança

Avaliamos sistematicamente a cultura em sete dimensões distintas:

Atitudes

As opiniões e os sentimentos que os funcionários têm em relação aos protocolos e problemas de segurança.

Comportamentos

As ações e atividades dos funcionários que têm um impacto direto ou indireto na segurança da or ganiz aç ão.

Conhecimento

O entendimento, o discernimento e a consciência dos funcionários em relação aos problemas e atividades de segurança.

Comunicação

A qualidade dos canais de comunicação para: debater assuntos relacionados à segurança, promover um senso de pertencimento e oferecer suporte em questões de segurança e relatórios de incidentes.

Conformidade

O conhecimento das políticas de segurança por escrito e do quanto os funcionários as seguem.

Normas

O conhecimento e o cumprimento das regras de conduta não escritas da or ganiz aç ão.

Responsabilidades

O modo como os funcionários veem sua própria função como um fator essencial para manter a segurança da organização ou para colocá-la em risco.

Cultura de segurança

O Índice da cultura de segurança (Security Culture Index, SCI) é o índice global que classifica as organizações com base na sua pontuação de cultura de segurança. O índice foi criado pela KnowBe4 Research e é calculado analisando a cultura de segurança de milhares de organizações em todo o mundo.

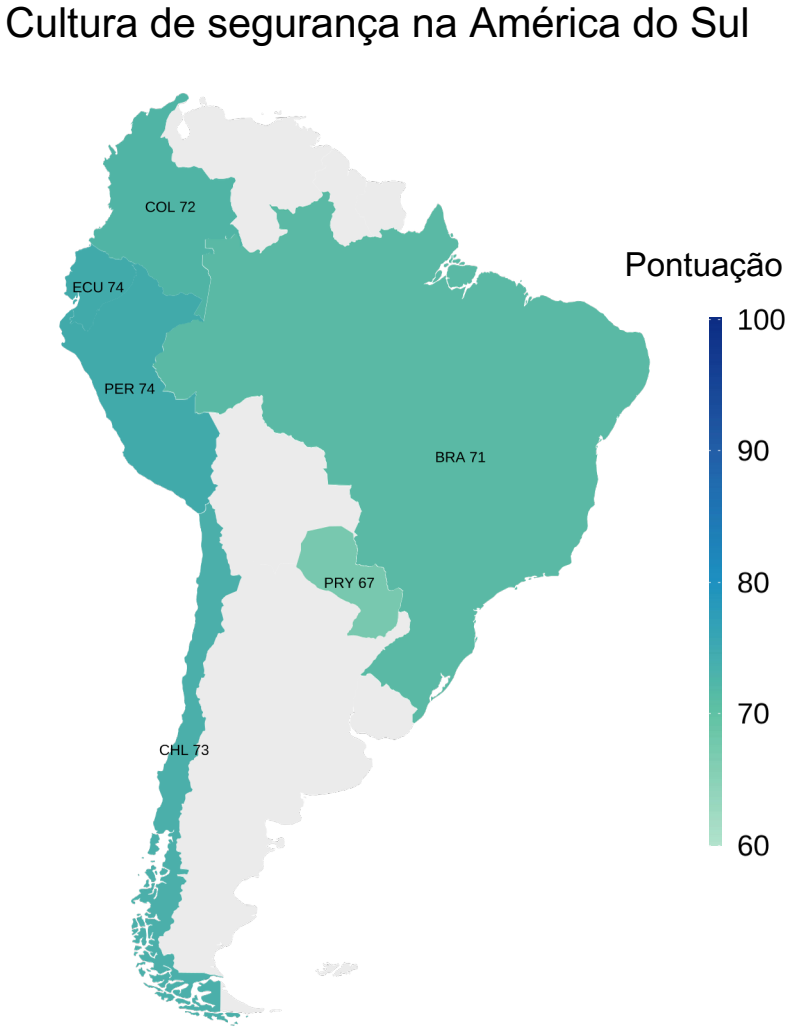
90 a 100	**Excelente**
80 a 89	**Boa**
70 a 79	**Moderada**
60 a 69	**M e diana**
0 a 59	**Fraca**

Observação: nenhum dos setores obteve uma cultura de segurança Excelente ou Boa neste ano.

América do Sul

Por Joanna Huisman, vice-presidente sênior de Pesquisas e percepções estratégicas

Adoção cultural



As organizações da América do Sul estão enfrentando desafios cada vez maiores com os ataques cibernéticos. Segundo oConselho de Relações Exteriores, a região costuma ser negligenciada por diversos motivos convincentes. Para começar, as empresas de inteligência de ameaças têm pouca motivação para priorizar a América do Sul em relação a mercados mais amplos. Além disso, os domínios de segurança cibernética tendem a se concentrar em agentes de ameaças bem conhecidos e proeminentes, ignorando os que estão surgindo. Por último, os níveis desiguais de desenvolvimento em todo ocontinente resultam em requisitos de segurança cibernética totalmente diversos entre os vários países.

Existe também uma grande falha de comunicação entre as nações. Os líderes influentes não participam dos diálogos necessários que ultrapassam fronteiras, levando a um despreparo sistêmico das organizações para lidar de forma eficaz com os problemas centrais. Essa deficiência acaba chegando à força de trabalho, e os funcionários não recebem o treinamento necessário para detectar, relatar e evitar os ataques. A raiz do problema está no fato de que os funcionários podem se sentir desconectados da responsabilidade, demonstrar indiferença ou simplesmente não ter consciência sobre a situação.

Para corrigir esse problema, as organizações devem, primeiramente, olhar os fatores humanos e oferecer treinamentos e testes contínuos e abrangentes para promover práticas robustas de higiene cibernética entre os funcionários. Aliado a planos sólidos de continuidade dos negócios e estratégias proativas de prevenção, isso ajudará a fomentar uma cultura em que os funcionários adotem comportamentos mais seguros e assumam a responsabilidade adequada pela segurança cibernética.

Atitudes gerais

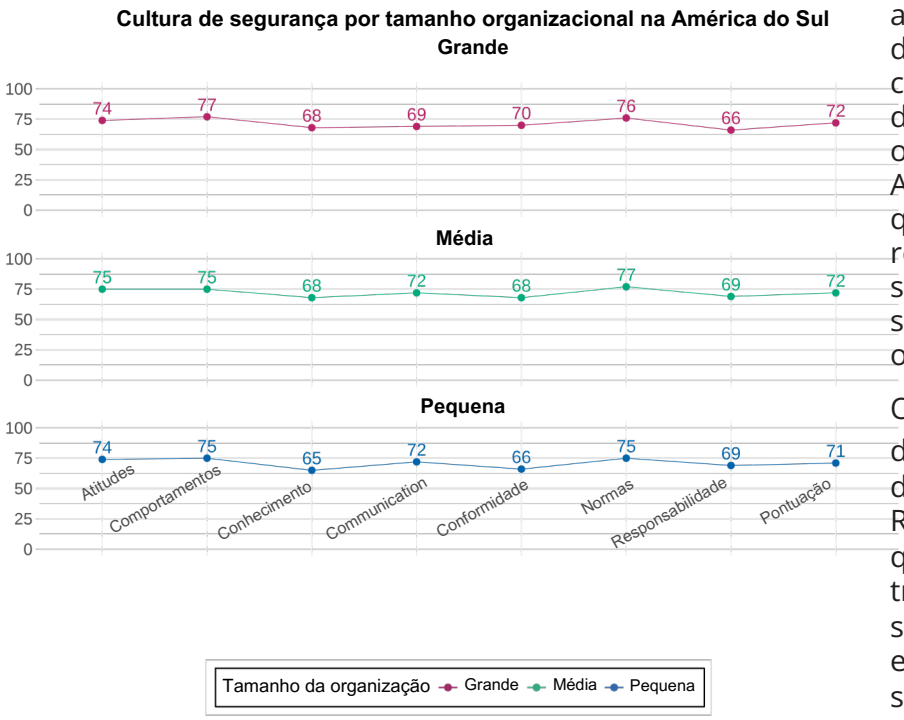
Pesquisas recentes indicam que os ataques cibernéticos estão crescendo rapidamente na América do Sul, com phishing e ransomware despontando como as principais táticas. Para combater essas ameaças, o treinamento de conscientização em segurança continua sendo uma contramedida essencial. Para melhorar a cultura de segurança nas empresas da América do Sul, é necessária uma análise minuciosa de várias dimensões culturais para detectar pontos fracos específicos.

Ao reavaliar e refinar devidamente suas estratégias, as organizações podem promover uma cultura de segurança mais robusta. Esse estado elevado de preparação, em que os funcionários estão bem-informados e a empresa promove e transmite o conhecimento ativamente, pode ter um impacto positivo e transformador na cultura de segurança. A pontuação baixa na dimensão Responsabilidades evidencia a falta de investimento no aspecto humano da segurança, que é fundamental para reconhecer e responder aos ataques de engenharia social.

Principais requisitos regulamentares (legislativos)

As estruturas de segurança cibernética em toda a América do Sul exibem diferentes níveis de desenvolvimento. A Colômbia está na liderança, com um conjunto sólido de estratégias de segurança cibernética, defesa cibernética e gerenciamento de riscos descritos no documento do Conselho Nacional de Política Econômica e Social (CONPES). Essa política define um esquema forte de medidas de segurança cibernética projetadas para reforçar a segurança digital das pessoas e do país, detalhando as entidades encarregadas de aplicar as regulamentações e gerenciar os riscos.

No Brasil, a coordenação de segurança de informações fica a cargo do Gabinete de Segurança Institucional (GSI) da presidência. Alinhado a uma diretiva presidencial, o GSI teve um papel fundamental na criação da Política Nacional de Segurança da Informação com cinco pilares estratégicos: segurança cibernética, defesa cibernética, proteção da infraestrutura crítica, segurança de informações confidenciais e prevenção de violações de dados. A Argentina dá grande importância à privacidade de dados, respaldada por sua Lei de Proteção de Dados Pessoais. A lei é aplicada rigorosamente pela Agência de Acesso à Informação Pública (AAIP) e obteve reconhecimento da Comissão Europeia pela sua equivalência a regulamentações internacionais de privacidade, como o Regulamento Geral de Proteção de Dados (General Data Protection Regulation, GDPR). A política de segurança cibernética do Chile para o período de 2023 a 2028 busca criar uma estrutura digital resiliente que priorize os direitos dos usuários, cultive uma cultura de segurança consciente e promova a colaboração nacional e internacional. Essa política também busca estimular o setor de segurança cibernética e as consultas científicas no campo.



Eventos de segurança/ Principais problemas

Segundo a Infosecurity Magazine, em 2023, a América do Sul foi uma das duas regiões que não observou queda nas violações de dados, com incidentes que impactaram mais de dois milhões de contas. A outra região, Antártida, não foi incluída nesta avaliação. Curiosamente, em setembro do mesmo ano, a Colômbia sofreu um enorme ataque cibernético a inúmeros sites. Foi um dos maiores ataques contra sua infraestrutura digital e, com certeza, um dos maiores também da América do Sul nos últimos tempos.

Dimensões

Na América do Sul, a pontuação geral da cultura de segurança foi classificada como levemente moderada, ficando em 71. Recomendamos veementemente que as entidades dessas áreas adotem práticas robustas de cultura de segurança, que devem incluir treinamento e medidas de avaliação. O Peru e o Equador ficam na extremidade superior da faixa, cada um com a pontuação relativamente moderada de 74. O Paraguai está na extremidade inferior, com 67 de pontuação, indicando uma cultura de segurança relativamente mediana. A avaliação do Paraguai revela uma disparidade entre a percepção e o conhecimento. A pontuação de apenas 59 em Conhecimento demonstra uma lacuna considerável na compreensão das ameaças à segurança. Por outro lado, a pontuação de Atitude ficou em 75, indicando que embora os funcionários reconheçam a importância da segurança, falta entendimento sobre as ameaças e como aplicar otreinamento de modo eficaz.

O Peru e o Equador enfrentam desafios semelhantes nas dimensões Conhecimento e Responsabilidades, o que indica que os funcionários não recebem treinamento essencial nem insights sobre preocupações de segurança e práticas pertinentes a seus setores. Essa deficiência prejudica a capacidade desses países de incorporar a cultura de segurança em seus comportamentos diários. No Brasil, onde está omais extenso conjunto de dados da América do Sul, a principal dificuldade dos setores está em Responsabilidades e Conhecimento. Isso indica que, apesar do reconhecimento da importância da segurança, existe um problema abrangente no que diz respeito a assumir a responsabilidade e compreender as ameaças, atrapalhando a implementação de medidas de segurança eficazes.

É importante destacar que as amostras dos vários países sul-americanos são pequenas, o que sugere uma ausência geral de medidas de segurança fundamentais em diversas organizações. O Brasil se destaca por ter contribuído com a amostra de maior tamanho na América do Sul.

Localização do idioma

Como o espanhol e o português são as línguas mais faladas na América do Sul, a maioria dos fornecedores de treinamento e conscientização oferece um grande volume de materiais de conscientização de segurança cibernética e conteúdo de treinamento nesses idiomas. Essa estratégia ajuda a deixar o material relevante e útil para os usuários, promovendo melhor engajamento e resultados de aprendizado.

Influência da IA

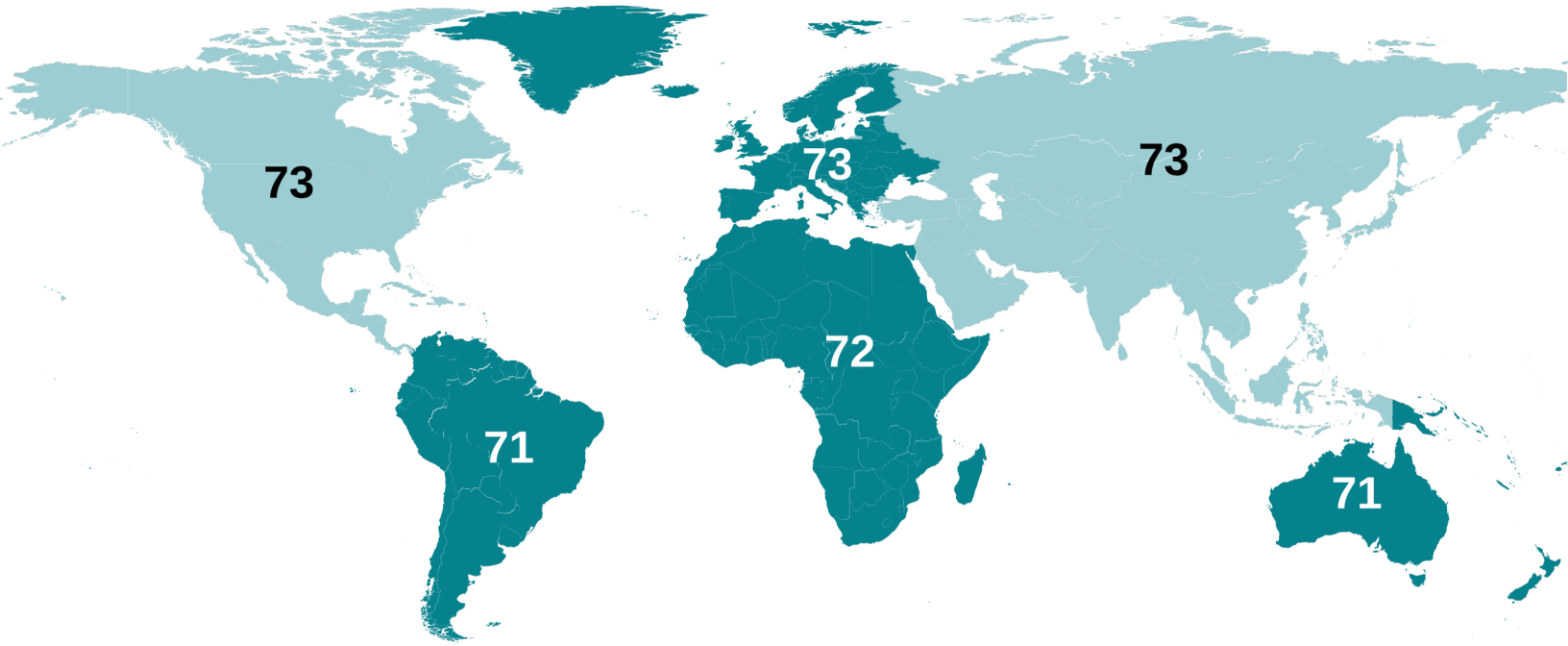
O empenho em nutrir talentos é fundamental para um ecossistema próspero de IA na América do Sul, que é complementado pelo desenvolvimento de sólidas estruturas regulamentares capazes de garantir o uso responsável e o avanço da IA. Pesquisas sugerem que o incentivo à adoção da IA na região será alimentado pela ampla necessidade de as empresas passarem por uma transformação digital. Além disso, os benefícios gerados pelo fortalecimento do poder computacional e da resiliência a flutuações inesperadas do mercado estimularão esse crescimento. No setor público, a IA apresenta uma oportunidade inédita para os governos da América do Sul abordarem e corrigirem desafios arraigados e ineficiências que, historicamente, já impediram o avanço social e econômico da região.

Pontos principais

O panorama de ameaças à segurança cibernética na América do Sul é preocupante, e as projeções indicam uma tendência de agravamento.
Para fortalecer as defesas contra o aumento nas táticas de engenharia social que têm levado a ataques inéditos de ransomware, é essencial realizar um investimento importante na preparação da força de trabalho. As empresas devem se empenhar rigorosamente na formulação de políticas e exigir a adesão dos funcionários a essas diretrizes. Além disso, os países da América do Sul seriam beneficiados com o aumento na colaboração de inteligência referente a ameaças cibernéticas e deveriam contribuir ativamente para um ecossistema global de compartilhamento de informações.
A participação em iniciativas como a Rede de Pesquisa de Segurança Cibernética da América Latina também é fundamental, pois fornece insights mais aprofundados sobre a evolução das ameaças, bem como acesso a teorias e metodologias avançadas em segurança cibernética.

Visão geral global

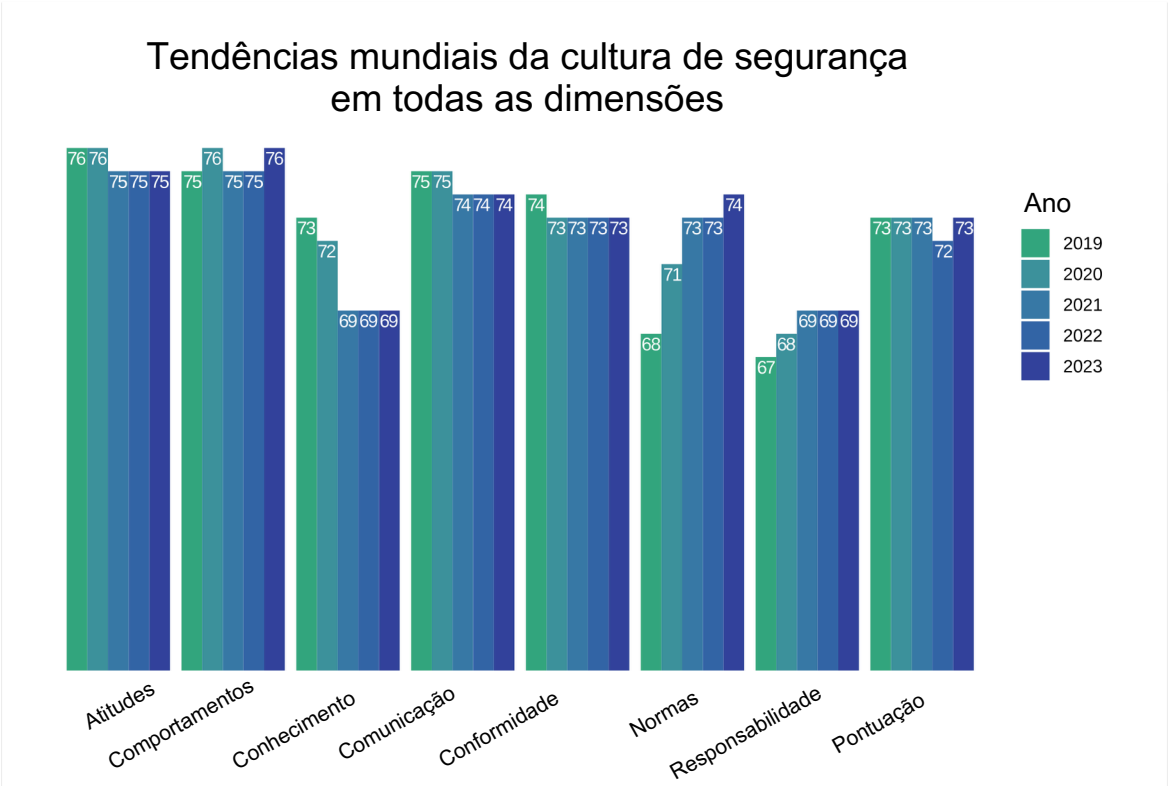
Por Javvad Malik, Defensor de conscientização em segurança



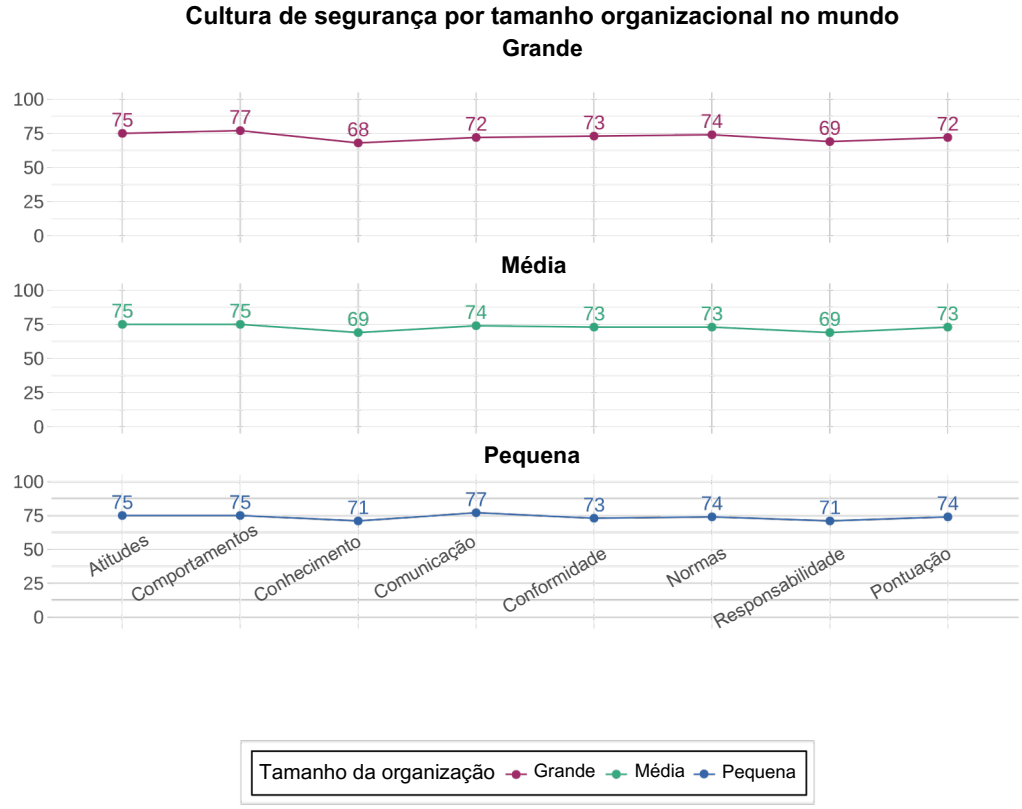
Adoção cultural

O mundo pode ser a sua casa, mas como é o desempenho dele em termos de cultura de segurança cibernética? Cerca de 5,35 bilhões de pessoas possuem acesso à internet, o que significa que 66,2% da população mundial são alvos em potencial para criminosos. Com esse cenário, o fortalecimento das culturas de segurança é mais do que um desafio corporativo. É um dever social.

No mundo todo, as organizações apresentam várias diferenças na sua intenção de construir uma cultura de segurança forte que esteja alinhada à sua tolerância a riscos e à cultura geral. Embora vários governos e organizações tenham tentado implementar algum tipo de estratégia de segurança cibernética, os resultados obtidos mostraram diferentes níveis de sucesso.



Várias organizações lidam com a cultura da segurança cibernética da mesma forma que lidam com um projeto de tecnologia. No entanto, o que funciona com computadores e redes não funciona bem com pessoas. Pode ser por isso que medidas práticas para criar uma cultura forte falham ou se tornam um exercício de conformidade. Essas falhas refletem os modelos ultrapassados de conscientização e treinamento em segurança de antigamente, quando os funcionários recebiam um só treinamento em conscientização por ano.



Atitudes gerais

Os níveis de maturidade da cultura de segurança variam muito em todo o mundo. Em algumas áreas, as pessoas têm mais consciência e estão mais atentas às ameaças em nível pessoal, mas isso não se reflete automaticamente nas organizações. Em outras áreas, as ameaças são vistas mais como um desafio organizacional que não afeta as pessoas individualmente.

Empiricamente, parece que a cultura de segurança fica mais forte quando é relevante não só para a organização, mas também para as pessoas — quando é algo que elas podem levar para casa para compartilhar com amigos e familiares.

No lado positivo, é como se mais organizações estivessem incorporando iniciativas de segurança cibernética além dos controles tecnológicos e compreendendo que as pessoas são um aspecto importante na criação de uma cultura de segurança forte.

Principais requisitos regulamentares (legislativos)

No mundo todo, são muitos os requisitos regulamentares existentes, novos e atualizados que tentam colocar a segurança cibernética como prioridade nas organizações. No entanto, vários deles falham ao se concentrar em controles tecnológicos, requisitos de notificação de violações ou conscientização básica. Embora todos eles sejam peças fundamentais para criar uma cultura de segurança, sozinhos não são capazes de mudar a situação significativamente.

Eventos de segurança/Principais problemas

Quando se trata de cultura de segurança, há muitos problemas no mundo causando impacto nas organizações. Os crimes cibernéticos continuam sendo uma prioridade em várias organizações. O foco principal está em problemas como ransomware, enquanto se ignora o fato de que a engenharia social continua sendo o método mais predominante de implementar ransomware.

Em 2023, esses eventos causaram um impacto duradouro. As mudanças para os modelos de trabalho remoto ou híbrido exigiram a implementação rápida de tecnologia e implicaram uma dívida cibernética no processo, afetando negativamente várias organizações.

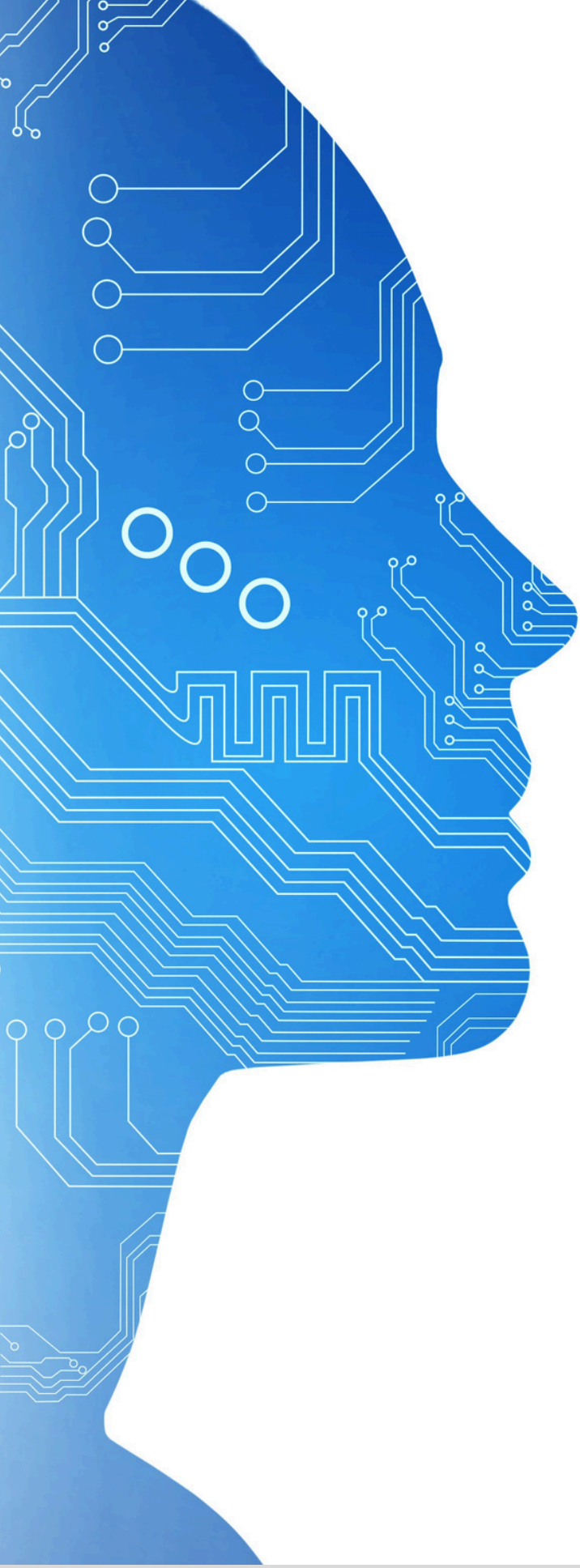
À medida que as compras de papel higiênico motivadas pelo pânico causado pela COVID diminuíam, os eventos mundiais apresentavam uma nova série de riscos complexos. Em 2022, a Rússia invadiu a Ucrânia, e, no ano seguinte, o conflito no Oriente Médio ganhou novas proporções. Esses fatos são importantes porque mostram como a segurança cibernética tem exercido um papel relevante não só entre as pessoas envolvidas diretamente nesses conflitos, como também entre apoiadores distantes.

Dimensões

Em 2023, coletamos insights sobre 816.733 funcionários que representavam 4.078 organizações. A pontuação geral da cultura de segurança no mundo todo é 72 (levemente moderada), permanecendo inalterada em relação ao ano anterior. Como seria de se esperar, as organizações menores tendem a apresentar pontuações mais altas na cultura de segurança. É muito mais fácil mudar a cultura de um grupo pequeno do que a de um grupo grande. Na verdade, Comportamentos foi a única dimensão na qual as grandes organizações tiveram uma nota mais alta do que as outras.

Em termos mundiais, parece que há menos entendimento, conhecimento e conscientização de segurança, bem como menos responsabilidade.

Embora os números variem bastante conforme a localização geográfica, o tamanho da organização e o setor, o fato preocupante é que ainda há muito por fazer para aumentar o padrão em cultura de segurança.



Influência da IA

De todas as tecnologias novas, a inteligência artificial (IA) será, provavelmente, a que terá os impactos mais profundos em segurança cibernética nas organizações e nas pessoas. A IA já está sendo usada para: disseminar desinformação e campanhas com informações erradas, fortalecer ataques de engenharia social e automatizar ataques de várias camadas e facetas em grande escala — até mesmo por criminosos com pouco conhecimento técnico.

Nos próximos meses e anos, sempre que houver eleições, guerras e outros eventos importantes, a IA surgirá como uma ferramenta cada vez mais importante no arsenal dos criminosos. Com um nível baixo de conscientização e a ausência de uma regulamentação eficaz, quando os governos e órgãos reguladores finalmente resolverem avançar pode ser tarde demais.

Pontos principais

A cultura de segurança varia bastante em todo o mundo. Esse é um problema no nosso mundo totalmente conectado, em que um celular no meio do deserto pode interagir com uma conta do mercado acionário ou com um banqueiro em Wall Street. A abordagem isolada não é sustentável. Os governos precisam colaborar mais entre si e com os órgãos reguladores não só para definir leis, mas também para demonstrar e incorporar as medidas práticas necessárias para criar uma cultura forte.

Por sua vez, as organizações precisam olhar o desafio humano e não tratá-lo como um problema tecnológico. Diferentemente do conserto de computadores, o "conserto" de pessoas requer um trabalho constante de conscientização e treinamento.
Citando Nelson Mandela, "A educação é a arma mais poderosa que podemos usar para mudar o mundo".

Ler o relatório completo