UNINDO AS PESSOAS E A IA: O FUTURO DA RESILIÊNCIA CIBERNÉTICA

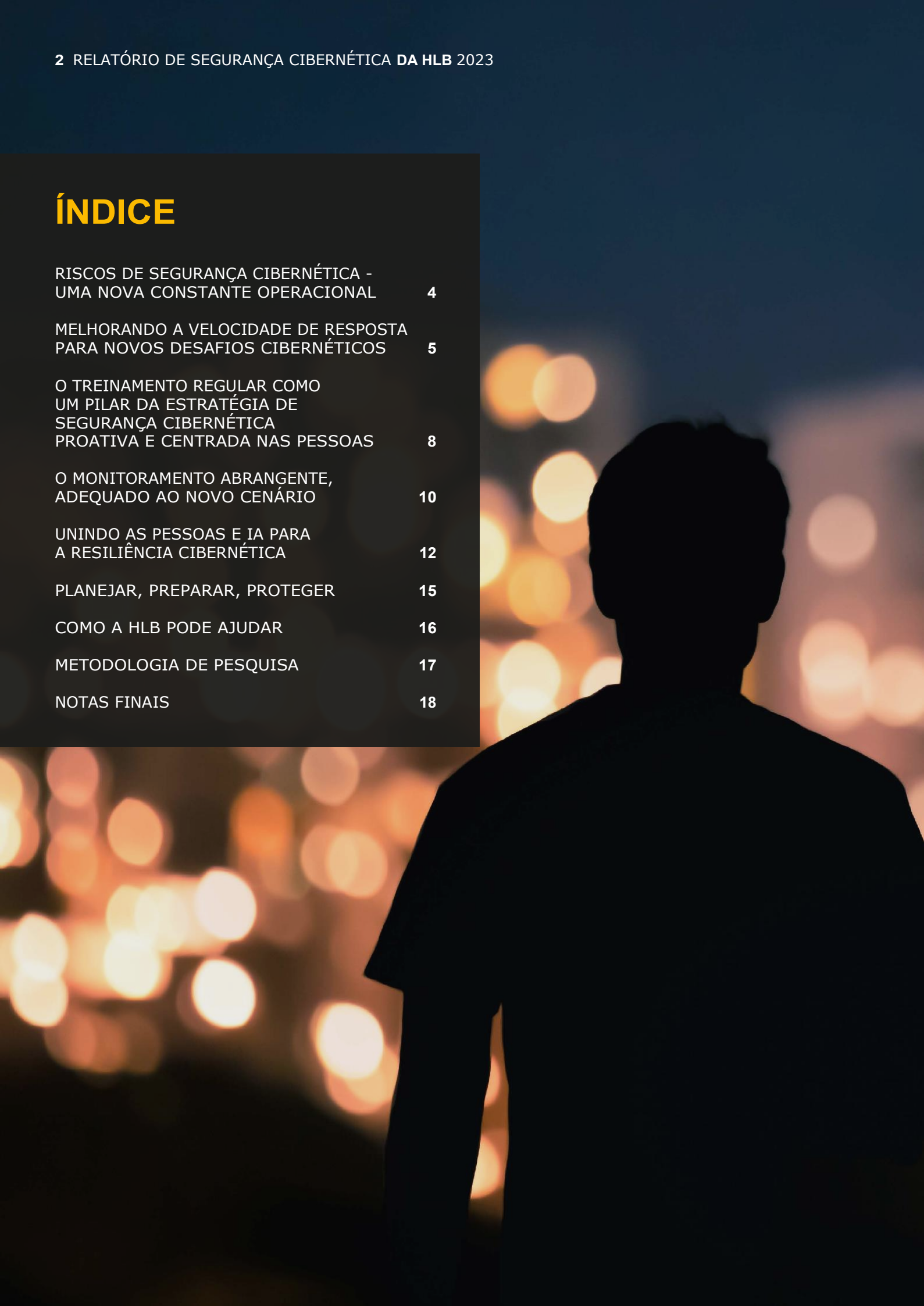
RELATÓRIO DE SEGURANÇA CIBERNÉTICA DA HLB 2023

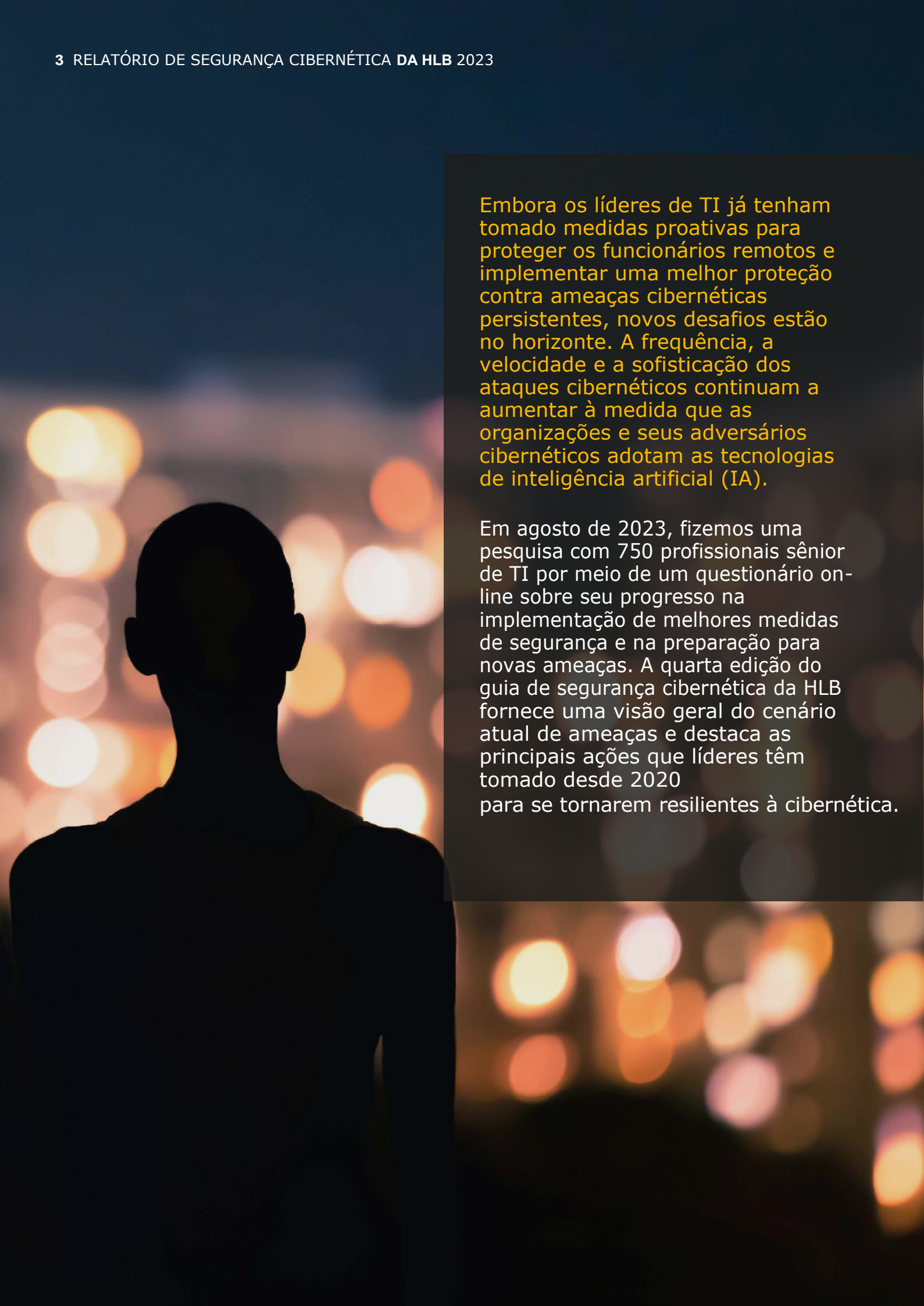
A CONSULTORIA GLOBAL
E A REDE DE CONTABILIDADE

www.hlb.global

JUNTOS FAZEMOS ACONTECER

ÍNDICE





Embora os líderes de TI já tenham tomado medidas proativas para proteger os funcionários remotos e implementar uma melhor proteção contra ameaças cibernéticas persistentes, novos desafios estão no horizonte. A frequência, a velocidade e a sofisticação dos ataques cibernéticos continuam a aumentar à medida que as organizações e seus adversários cibernéticos adotam as tecnologias de inteligência artificial (IA).

Em agosto de 2023, fizemos uma pesquisa com 750 profissionais sênior de TI por meio de um questionário on-line sobre seu progresso na implementação de melhores medidas de segurança e na preparação para novas ameaças. A quarta edição do guia de segurança cibernética da HLB fornece uma visão geral do cenário atual de ameaças e destaca as principais ações que líderes têm tomado desde 2020
para se tornarem resilientes à cibernética.

RISCOS DE SEGURANÇA CIBERNÉTICA - UMA NOVA CONSTANTE OPERACIONAL

Na segurança cibernética, nunca estamos "lutando a última guerra". Desde 2020, a HLB tem medido a exposição das empresas globais às ameaças cibernéticas. Embora os líderes de TI tenham feito um progresso significativo na melhoria de sua postura de segurança, ainda há mais trabalho a ser feito.

Em 2023, 50% dos líderes empresariais observaram um aumento nos ataques cibernéticos, com outros 35% dizendo que os níveis de ataque permaneceram os mesmos do ano passado. Isso é 3 pontos percentuais maior do que em 2021, quando 47% dos líderes de negócios relataram um aumento[1], embora tenha havido um ligeiro atenuamento em comparação com 2020, quando 53% observaram um aumento no número de ataques cibernéticos.

A frequência e a sofisticação dos ataques cibernéticos continuam a aumentar proporcionalmente aos esforços de digitalização das organizações. Atualmente, as empresas do mundo todo enfrentam 1.248 ataques por semana [2]- e toda organização é um alvo. Desde o início do ano, os agentes de ameaças têm atacado com sucesso instituições públicas (Polícia Metropolitana do Reino Unido, agência francesa de desemprego Pôle emploi, Diretoria Geral de Imigração da Indonésia) e empresas privadas como: Empresas de telecomunicações dos EUA, T-Mobile e AT&T; a Australian Latitude Financial, a varejista Cortina Holdings, com sede em Cingapura, entre outras.

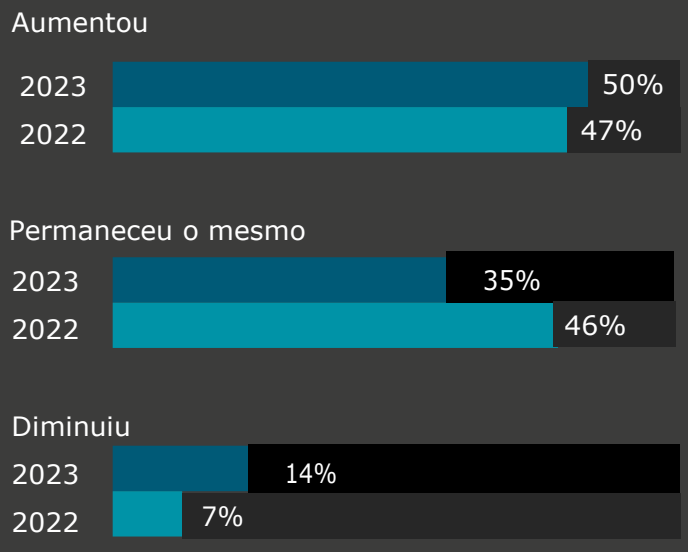
"Uma estratégia robusta de segurança cibernética inclui três princípios fundamentais: monitoramento contínuo por especialistas que estão totalmente atualizados com o cenário de ameaças em constante mudança, a capacidade de responder aos problemas imediatamente para reduzir as perdas e o estabelecimento de programas abrangentes de treinamento e conscientização."

Mark Butler, sócio-gerente da HLB Ireland

A democratização de software mal-intencionado, o ritmo acelerado da transformação digital, os conflitos geopolíticos em andamento e a incerteza econômica, criaram o ambiente perfeito para o crescimento perpétuo das ameaças cibernéticas. De fato, 62% dos líderes esperam que os riscos de segurança cibernética se tornem ainda mais proeminentes em um panorama de cinco anos, segundo a pesquisa global da HLB de 2023 de líderes empresariais [3].

A exposição ao risco cibernético é persistente. Para garantir uma proteção de longo prazo, as empresas precisam se concentrar nos três pilares da resiliência cibernética: resposta rápida, treinamento regular e monitoramento abrangente.

FIG.1: ATAQUES CIBERNÉTICOS AINDA EM ASCENSÃO



MELHORANDO A VELOCIDADE DE RESPOSTA AOS NOVOS DESAFIOS CIBERNÉTICOS

TRABALHO REMOTO E HÍBRIDO COMO PRINCIPAIS CATALISADORES DA TRANSFORMAÇÃO CIBERNÉTICA

A segurança cibernética tem sido o ponto focal de atenção para líderes empresariais desde o início da transição para o trabalho remoto. De aplicativos de videoconferência a locais de armazenamento em nuvem desprotegidos, são poucos os caminhos que os criminosos cibernéticos não tentaram explorar.

Embora 57% dos líderes de TI admitam não estarem preparados inicialmente para os desafios do trabalho remoto, 88% conseguiram executar mudanças efetivas em suas estratégias e protocolos de segurança cibernética em resposta à pandemia [4]. Do fornecimento de acesso a redes privadas virtuais (VPNs) aos funcionários e ferramentas seguras de troca de dados na nuvem à iniciativas de treinamentos cibernéticos regulares, os líderes de TI conseguiram realizar mudanças significativas em um curto espaço de tempo.

Até 2021, 44% dos líderes de TI disseram ter mudado a infraestrutura tecnológica para uma arquitetura de confiança zero, com outros 44% indicando que adotaram alguma tecnologia para dar suporte à nova força de trabalho híbrida.[5] Além disso, os líderes se concentraram em promover uma conscientização mais forte sobre a segurança cibernética por meio de sessões de treinamento regulares. Mais de 57% dos líderes de TI com quem conversamos em 2021 implementaram uma política de "sem exceção" para a educação cibernética de suas equipes [6].

Em 2023, os investimentos em segurança cibernética estão trazendo dividendos tangíveis. 64% disseram que veem os impactos positivos na forma de uma implementação mais fácil de sua estratégia de educação em segurança cibernética, maior conscientização geral e redução dos riscos.

"Embora o volume de ataques tenha aumentado, o mesmo ocorreu com os níveis gerais de conscientização cibernética. Graças ao trabalho remoto, os funcionários agora entendem mais sobre segurança e se sentem mais capacitados."

Anurag Sharma, sócio e líder de mercado, System and Process Assurance services, Withum.

FIG.2: A MAIORIA DOS PROFISSIONAIS DE TI ACREDITA QUE O TRABALHO REMOTO TEVE UM IMPACTO POSITIVO NAS EMPRESAS

Como você acha que o novo mundo do trabalho remoto afetou sua estratégia de inteligência/educação em segurança cibernética e a conscientização geral dos funcionários?

10%	26%	64%
Nenhum impacto	**Impacto negativo** Aumento dos riscos, maior dificuldade para implementar nossa estratégia de educação sobre segurança cibernética, redução da conscientização	**Impacto positivo** Diminuição dos riscos, maior facilidade para implementar nossa estratégia de educação sobre segurança cibernética, aumento da conscientização

AUMENTO DOS NÍVEIS DE MATURIDADE DA SEGURANÇA CIBERNÉTICA

A maioria dos líderes avaliou positivamente seu progresso com a segurança cibernética. No entanto, um quarto das organizações também percebeu os impactos negativos do trabalho remoto na segurança, citando o aumento dos riscos e os desafios na implementação da estratégia educacional correta.

Um patrimônio de TI crescente e uma força de trabalho híbrida exigem novos processos e tecnologias para o gerenciamento da segurança cibernética. Para dar início a um novo programa de segurança cibernética, inicie uma auditoria do seu ambiente atual - uma área em que os profissionais da HLB podem ajudar.

Muitas das soluções de local de trabalho digital baseadas em nuvem vêm com controles de segurança integrados e aplicação de políticas automatizadas. Certifique-se de que todas as configurações recomendadas sejam implementadas. Avalie suas políticas de segurança atuais para entender se elas se adequam a um modelo operacional híbrido. Procure novos fornecedores de segurança de TI, que ofereçam soluções contínuas de monitoramento de ameaças e recomendações baseadas em dados para melhorar a postura de segurança.

"Além das campanhas de conscientização, algumas medidas de segurança foram reforçadas pelas empresas para proteger os pontos remotos, como VPNs, softwares de antivírus e firewalls de última geração (NGFWs)", diz Gustavo Solis, CEO da Cynthus. Ao combinar o treinamento dos funcionários com melhorias direcionadas na tecnologia de segurança, as organizações podem atenuar as ameaças de forma proativa, em vez de lidar reativamente com as consequências de um ataque.

"Além das campanhas de conscientização, algumas medidas de segurança foram reforçadas pelas empresas para proteger pontos remotos, como VPNs, software de antivírus e firewalls de última geração (NGFWs)."

Gustavo Solis, CEO, Cynthus

ESTUDO DE CASO:

A FANE VALLEY USOU O TRABALHO REMOTO COMO UMA OPORTUNIDADE PARA TRANSFORMAÇÕES CIBERNÉTICAS

A Fane Valley é uma das empresas agrícolas e de processamento de alimentos mais avançadas da Irlanda. Por estar no setor de manufatura e varejo, a empresa enfrenta demandas exclusivas de conformidade do setor e precisa manter altos níveis de segurança cibernética.

Para estabelecer um novo programa de segurança cibernética, a Fane Valley optou primeiro por uma auditoria. "Nossa primeira etapa foi entender onde a empresa era vulnerável, pois, dada a escala de nossos negócios, queríamos garantir que lidássemos primeiro com os riscos potenciais mais significativos", diz o porta-voz. A investigação ajudou a empresa a estabelecer padrões de referência para medir sua postura de segurança e priorizar as lacunas de segurança mais urgentes, que poderiam ser abordadas de forma estruturada.

"Acreditamos firmemente em fazer da segurança cibernética uma responsabilidade coletiva, abrangendo a todos em nossa organização, desde a liderança até os funcionários da linha de frente. Isso se tornou parte da nossa maneira de fazer as coisas, e nossa equipe é o pilar da nossa defesa."

Essa mudança para o trabalho remoto estimulou uma reformulação holística de sua estrutura de segurança cibernética, com políticas de senha robustas, medidas adicionais de verificação de usuários e treinamento anti-phishing sendo implementados, juntamente com outras ferramentas e políticas.

"Acreditamos firmemente em fazer da segurança cibernética uma responsabilidade coletiva, abrangendo a todos em nossa organização, desde a liderança até os funcionários da linha de frente. Isso se tornou parte do nosso modo de fazer as coisas, e nossa equipe é o pilar da nossa defesa", diz o porta-voz da empresa.

Para obter uma proteção contínua, a Fane Valley optou por oferecer "Cyber-as-a-Service" (Cibernética como Serviço), com uma equipe experiente monitorando seu patrimônio de TI, abordando possíveis vulnerabilidades e garantindo a implementação das melhores práticas do setor. Essa abordagem permitiu que a Fane Valley obtivesse uma proteção abrangente e escalar, adaptada às mudanças no tamanho da equipe, nas práticas operacionais e no cenário de ameaças.

O TREINAMENTO REGULAR COMO UM PILAR DA ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA PROATIVA E CENTRADA NAS PESSOAS

O TREINAMENTO EM SEGURANÇA CIBERNÉTICA E A CONSCIENTIZAÇÃO NÃO É NEGOCIÁVEL

Os esforços contínuos de digitalização resultaram em um portfólio de TI maior e em um cenário de dados complexo. Terabytes de informações mudam de mãos digitalmente em questão de segundos. No entanto, as operações orientadas por dados têm o custo de aumentar os riscos de segurança, especialmente quando seu pessoal não compreende totalmente suas funções nos processos de segurança.

Como diz o ditado, 'Uma corrente é tão forte quanto seu elo mais fraco'. Nesse caso, esse elo geralmente é um funcionário não conscientizado", diz Mark Butler. Uma senha de e-mail fraca, um clique em um link desconhecido ou um documento carregado em um local de armazenamento não seguro podem ser uma alavanca para um criminoso cibernético.

No ano passado, 95% dos líderes de TI concordaram que mudar o comportamento humano era a maior barreira para uma defesa cibernética mais segura[7]. De fato, o fator humano pode aumentar os riscos de segurança cibernética. Todos cometem erros, especialmente quando trabalham remotamente. Penalizar as pessoas por erros de segurança, no entanto, só resultará em mais ocultação e soluções alternativas, tornando o trabalho dos profissionais cibernéticos ainda mais difícil.

Para cultivar uma cultura de responsabilidade de alta segurança, os líderes de TI devem procurar mudar alguns dos principais comportamentos humanos por meio de educação regular e treinamento proativo. É admirável que 87% das empresas tenham algum tipo de treinamento cibernético após a contratação.

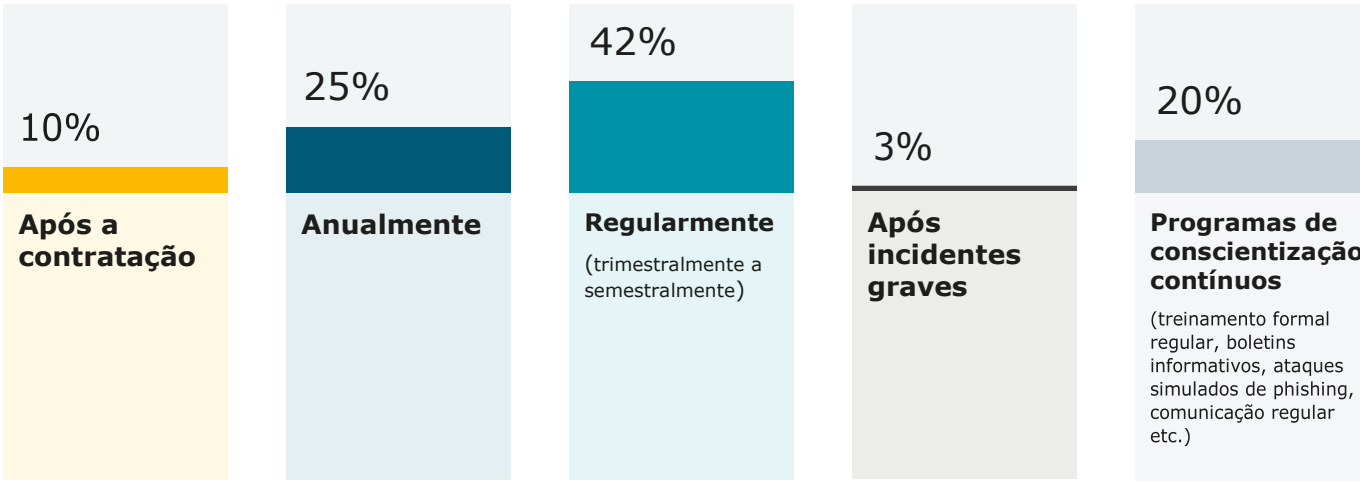
No entanto, apenas 18% têm programas de conscientização contínua em vigor, o que pressupõe treinamento formal regular, ataques simulados de phishing e comunicação regular. A maioria dos entrevistados (42%) investe em treinamento cibernético trimestral ou semestralmente e 25% - apenas uma vez por ano.

Jim Bourke, Líder de Consultoria global da HLB, insiste em uma ocorrência mais regular. "Eu recomendaria fazer o treinamento cibernético mensalmente e, no mínimo, trimestralmente". A regularidade ajuda os funcionários a reter e atualizar o conhecimento para acompanhar o ritmo das ameaças em evolução.

"Eu recomendaria fazer o treinamento cibernético mensalmente e, no mínimo, trimestralmente."
Jim Bourke, Líder de Consultoria Global da HLB

FIG.3: O INVESTIMENTO REGULAR EM TREINAMENTO EM SEGURANÇA CIBERNÉTICA AGORA É A NORMA

Com que frequência sua empresa investe em treinamento de segurança cibernética?



A CRIAÇÃO DE UM PROGRAMA EFICAZ DE TREINAMENTO EM SEGURANÇA CIBERNÉTICA

Um bom treinamento em segurança cibernética deve ser orientado para enfatizar a função da responsabilidade compartilhada, do esforço colaborativo e da correção contínua do comportamento, com a compreensão da importância da segurança cibernética no centro das atenções.

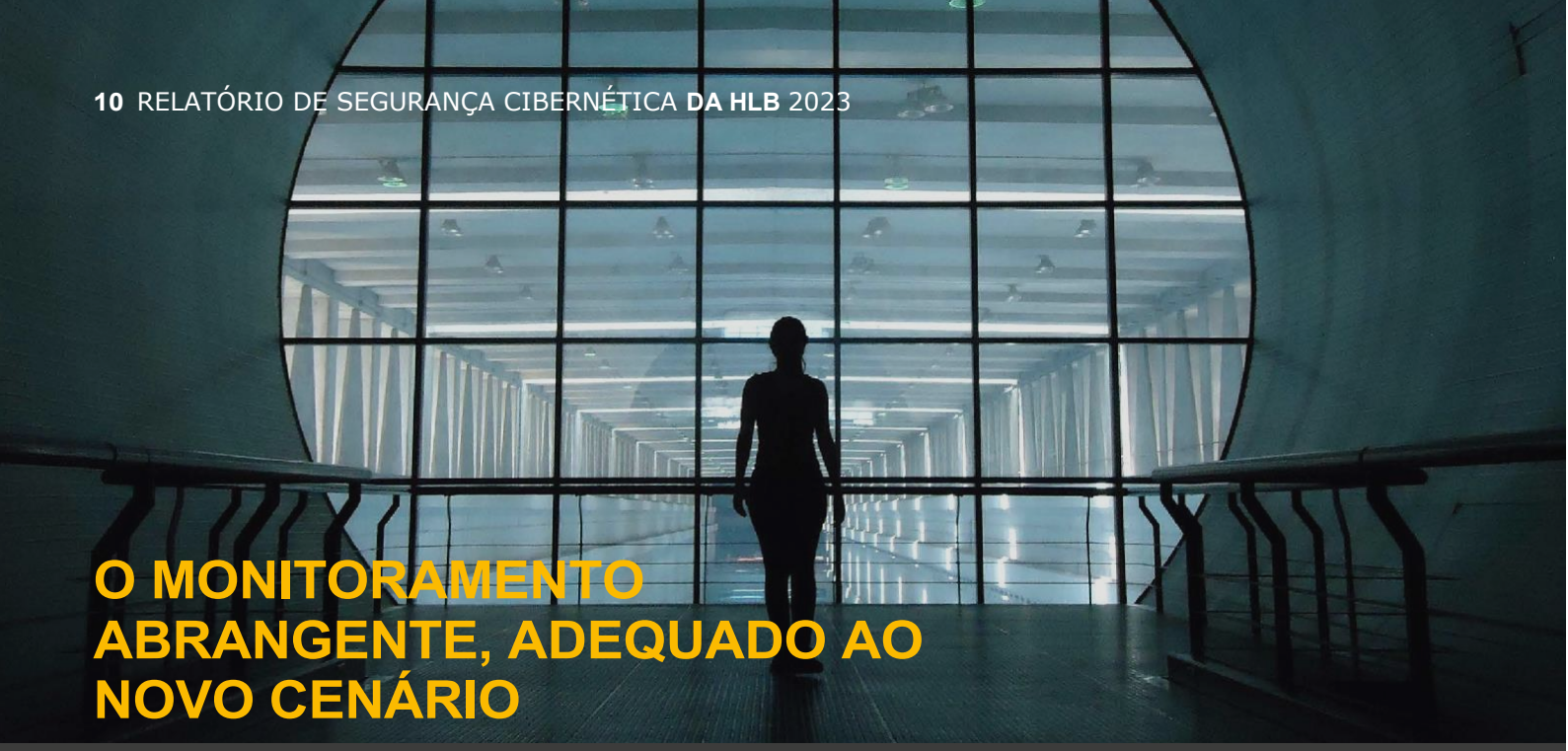
"A qualidade do treinamento em segurança cibernética é tão importante quanto sua frequência. Os exercícios de conscientização de segurança do tipo "caixa de seleção" não trazem resultados impactantes. Muitas vezes, os programas de treinamento são projetados de uma forma em que o usuário clica em um e-mail falso de treinamento e é redirecionado para um link de treinamento, no qual é forçado a entrar", diz Abu Bakkar, Diretor de Inovação da HLB. De acordo com Bakkar, esse tipo de treinamento pode ter uma eficiência questionável a longo prazo e não prepara totalmente os usuários para as ameaças emergentes.

O treinamento cibernético de qualidade tem como objetivo mudar a percepção e a compreensão dos usuários sobre a tecnologia e os riscos que ela acarreta, juntamente com estímulos suaves para melhorar seus comportamentos.
O uso regular de senhas fortes, o compartilhamento seguro de dados e a comunicação oportuna sobre os riscos - essas ações fundamentais criam uma forte cultura de segurança. E, portanto, deve fazer parte dos exercícios regulares.

Ao avaliar um novo programa de treinamento cibernético, faça as seguintes perguntas: ele se concentra na correção de comportamento? Ele está adaptado ao seu setor e tipo de operações? Ele leva em conta os riscos recém-surgidos, como a IA generativa? "As empresas devem avaliar continuamente a qualidade de seus programas de treinamento em segurança cibernética. Apenas para garantir que estamos acompanhando o ritmo de avanço da tecnologia", observa Jim Bourke.

Ao capacitar as equipes com o conhecimento e as habilidades, as organizações podem diminuir substancialmente os riscos de violações e comprometimento de dados.
Os investimentos feitos na educação em segurança cibernética se manifestam como um compromisso de longo prazo para reforçar a resiliência e o sucesso geral de uma organização.

"A qualidade do treinamento em segurança cibernética é tão importante quanto sua frequência. Os exercícios de conscientização de segurança do tipo "caixa de seleção" não trazem resultados impactantes. Muitas vezes, os programas de treinamento são projetados de uma forma em que o usuário clica em um e-mail falso de treinamento e é redirecionado para um link de treinamento, no qual é forçado a entrar."
Abu Bakkar, Diretor de Inovação da HLB



O MONITORAMENTO ABRANGENTE, ADEQUADO AO NOVO CENÁRIO

A IA COMO UM AGENTE DE AMEAÇA EMERGENTE

A inteligência artificial (IA) tem feito incursões constantes nas operações da empresa, com 50% dos líderes vendo a IA como a tecnologia mais importante para seus negócios nos próximos 5 anos [8].
No entanto, quando cai em mãos erradas, a IA também pode representar novos riscos de segurança.

Para realizar atividades mal-intencionadas, os criminosos cibernéticos agora estão usando diferentes tecnologias de inteligência artificial, como aprendizado de máquina, aprendizado profundo, grandes modelos de aprendizado de linguagem (LLMs) e redes adversárias generativas (GANs). DeepFakes, e-mails de spear phishing gerados por IA e botnets autônomos e auto-evolutivos são apenas alguns exemplos das novas ameaças que causam preocupações globais.

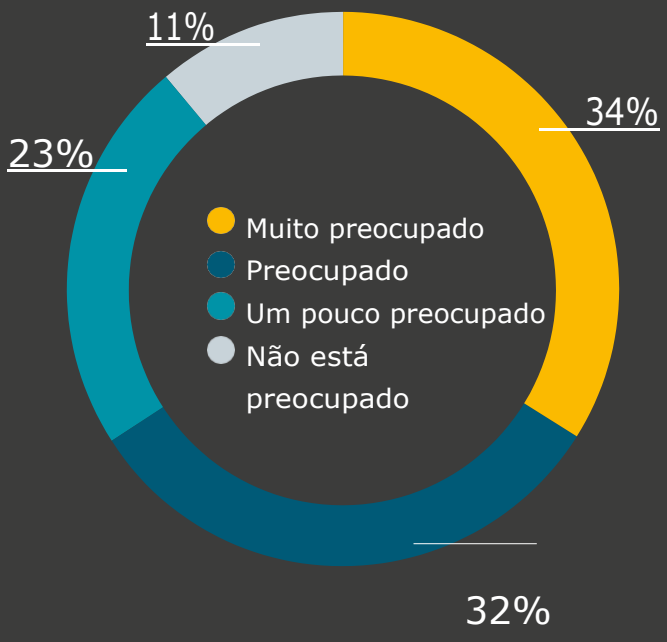
Apesar da notável novidade, os ataques de IA geralmente tomam emprestada a mecânica de ataque subjacente das ameaças tradicionais. "Ainda pode ser engenharia social, por exemplo", explica Abu Bakkar. "Mas isso é feito com um novo nível de personalização, escala e velocidade".

Os sistemas de IA generativa, como o ChatGPT, podem ser treinados com eficiência em dados públicos, produzidos por seus funcionários, para imitar com precisão o tom de voz do CEO da empresa em um e-mail de phishing. Ou usado para criar personas falsas de clientes em ataques de isca. Reconhecer se algo é falso ou real ficou mais difícil por causa da IA.

É compreensível que 89% dos líderes estejam preocupados com o ritmo atual da inovação tecnológica, especialmente na IA generativa, e com o possível aumento do risco cibernético, dos quais 34% dos líderes estão muito preocupados.

FIG.4: OS PROFISSIONAIS DE TI SE PREOCUPAM COM O RITMO ATUAL DAS INOVAÇÕES TECNOLÓGICAS E COM O AUMENTO POTENCIAL DE RISCOS CIBERNÉTICOS

Até que ponto você está preocupado com o ritmo atual da inovação tecnológica, especialmente na IA generativa, e com o possível aumento do risco cibernético?



AS SOLUÇÕES DE IA TAMBÉM EXIGEM PROTEÇÃO

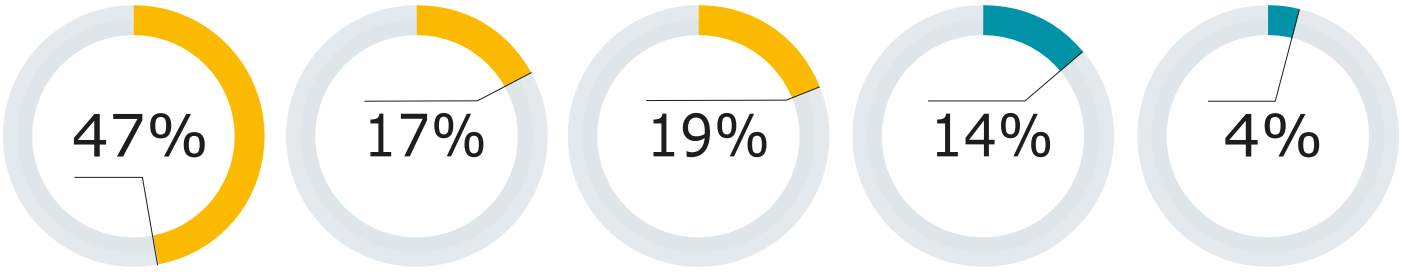
Coletivamente, confiamos cada vez mais decisões à IA, desde aprovações de solicitações de empréstimos até controles de redes de energia. Embora raros no momento, os ataques direcionados por IA podem, em breve, ter consequências visíveis no mundo real na forma de operações rodoviárias interrompidas, atividades de financiamento fraudulentas ou linhas de transporte com mau funcionamento.

Sistemas de IA mal projetados e operados podem produzir resultados tendenciosos, expor dados privados ou até mesmo negar serviço a usuários legítimos. Os modelos de IA geradores de código aberto, usados pelos funcionários, também podem armazenar dados corporativos privados ou confidenciais que podem violar as normas de privacidade. A AI Red Team (Equipe Vermelha de IA) do Google também apresentou recentemente um conjunto de táticas, técnicas e procedimentos (TTPs) voltados para sistemas de IA: Envenenamento de dados, extração de dados de treinamento, injeções de prompt, invasão de backdoor, ataques adversariais e exfiltração de dados [9]. As empresas que projetam e/ou adotam soluções de IA precisarão adaptar seus processos de segurança cibernética para levar em conta esses novos vetores de ataque.

No entanto, atualmente, a maioria das organizações admite não estar totalmente preparada para as ameaças de IA. Mais de 50% das empresas não têm estratégias de defesa suficientes contra ataques de IA, apesar de estarem preocupadas com sua proliferação. A melhor notícia é que a IA é uma ferramenta que cada um pode usar a seu favor.

FIG. 5: OS ATAQUES RELACIONADOS À IA REPRESENTAM UMA AMEAÇA, MAS OS PROFISSIONAIS DE TI ESTÃO PRONTOS PARA A DEFESA

Sua empresa está preocupada com os ataques orientados por IA e tem estratégias de defesa correspondentes para combatê-los?



Estamos preocupados com os ataques relacionados à IA e temos estratégias de defesa correspondentes

Estamos preocupados com os ataques relacionados à IA, mas não temos estratégias de defesa correspondentes

Estamos preocupados com os ataques relacionados à IA, não temos estratégias de defesa correspondentes, mas estamos investigando opções no momento

Não estamos preocupados com ataques relacionados à IA, mas temos estratégias de defesa correspondentes

Não estamos preocupados com ataques relacionados à IA e não temos estratégias de defesa correspondentes

UNINDO AS PESSOAS E A IA PARA A RESILIÊNCIA CIBERNÉTICA

A IA não apenas possibilita ataques mais sofisticados, mas também ajuda os profissionais cibernéticos e os funcionários comuns a estabelecerem melhores mecanismos de defesa. Ao combinar a inteligência humana com os recursos de processamento de dados em grande escala dos sistemas de IA, as empresas podem ficar um passo à frente dos invasores.

A segurança cibernética é um problema de dados. Os analistas de segurança precisam examinar muitos sinais de segurança para entender a exposição às ameaças. No entanto, há falta de pessoal especializado. A escassez de talentos em segurança cibernética é um dos desafios para a implementação de melhores práticas de mitigação cibernética, de acordo com a pesquisa de 2022 do HLB[10]. As soluções de aprendizado de máquina podem atuar como um multiplicador de força, permitindo que o talento humano capture, analise e atue com base em mais dados.

Embora a IA na segurança cibernética seja relativamente nova, ela já provou sua eficácia. Algoritmos inteligentes podem fazer uma varredura automática em todo o patrimônio técnico para identificar possíveis vulnerabilidades, alertar sobre anomalias e caçar ameaças de forma proativa.
Algoritmos supervisionados de aprendizado de máquina podem classificar ataques malignos de e-mail com 98% de precisão[11]. Um algoritmo de aprendizagem profunda apresentou taxas de precisão de 99,9% para a detecção de invasão de rede[12].

Entre os participantes da pesquisa, 100% estão cientes das novas soluções de segurança habilitadas para IA, mas apenas 30% implementaram pelo menos uma ferramenta de segurança habilitada para IA em seu ambiente. Outros 36% estão explorando ativamente essas soluções.

Fornecedores como NVIDIA, IBM e Microsoft, entre outros, já lançaram soluções de segurança cibernética baseadas em IA para detecção de ameaças, gerenciamento de segurança de endpoints e monitoramento da infraestrutura de TI. Essas plataformas permitem que os profissionais cibernéticos mantenham visibilidade total dos ambientes corporativos, concentrem sua atenção em sinais de segurança significativos e respondam mais rapidamente a possíveis ameaças cibernéticas.

47% dos profissionais de TI estão preocupados com ataques relacionados à IA e implementaram estratégias de defesa correspondentes.

FIG.6: MENOS DE UM TERÇO DOS PROFISSIONAIS DE TI IMPLEMENTARAM FERRAMENTAS DE SEGURANÇA HABILITADAS PARA IA EM SUA ESTRATÉGIA DE DEFESA

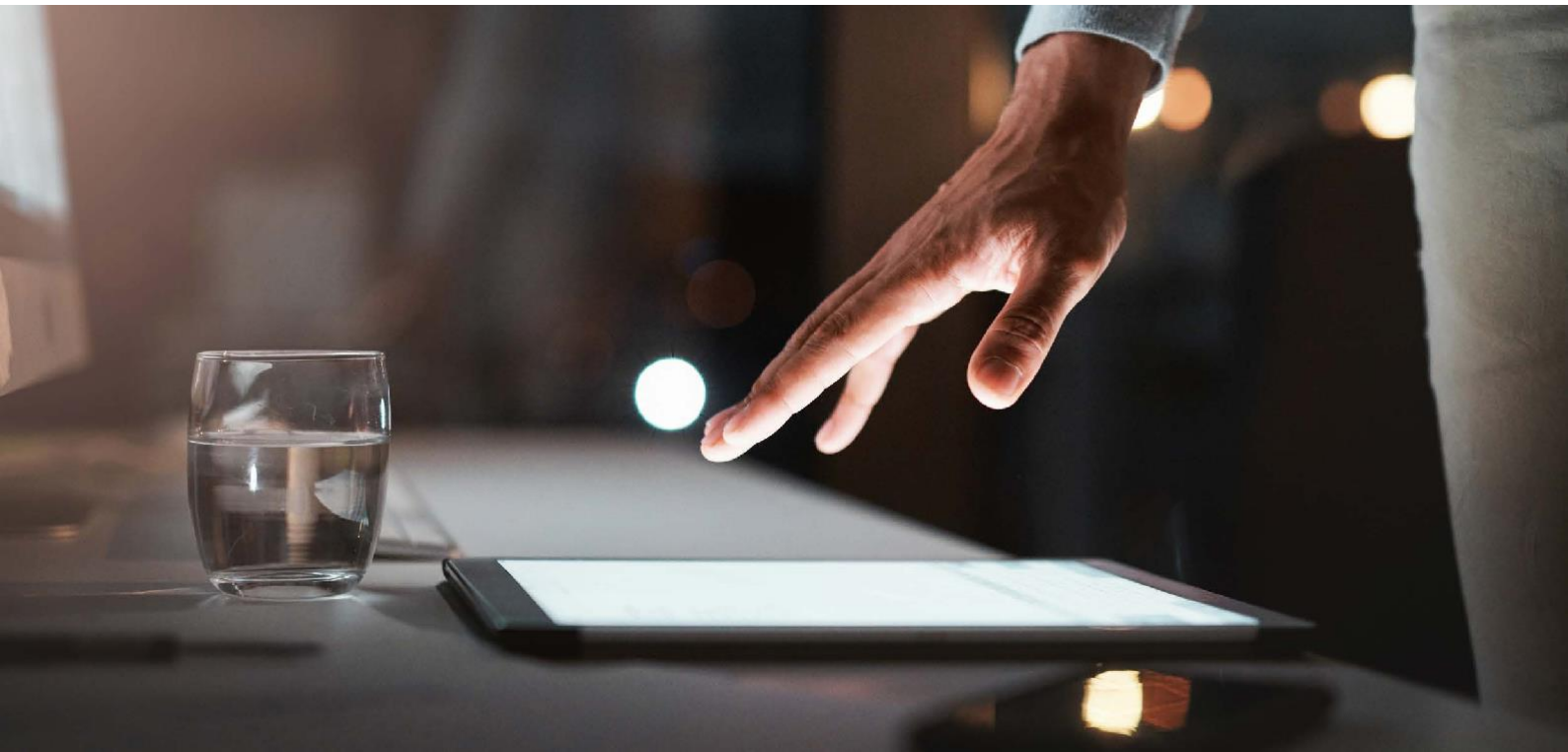
Sua empresa está explorando o uso de alguma ferramenta de segurança habilitada para IA como parte de sua estratégia geral de defesa?

34%	36%	30%
Estamos cientes de uma variedade de ferramentas de segurança habilitadas para IA no mercado, mas não exploramos a opção de implantá-las em nosso ambiente	Estamos **explorando** ativamente as ferramentas de segurança habilitadas para IA a serem implantadas, mas ainda não implementamos nenhuma ferramenta	**Implementamos** pelo menos uma ferramenta de segurança habilitada para IA em nosso ambiente

A IA generativa também pode melhorar a experiência do usuário de soluções de segurança cibernética, tornando-as mais acessíveis para profissionais seniores e juniores. Em março de 2023, a Microsoft lançou o Security Co-Pilot, um assistente de conversação inteligente que os profissionais de segurança podem usar para ajustar suas defesas. O assistente é treinado com base na inteligência global de ameaças exclusiva da Microsoft e em mais de 65 trilhões de sinais diários. O Security Co-Pilot sugere melhorias nas configurações do sistema, destaca inconsistências nas políticas e ajuda a investigar incidentes cibernéticos juntamente com analistas humanos.

Dito isso, é importante não depositar uma confiança inquestionável na IA. "Ficamos felizes em receber os avanços tecnológicos para nos proteger de nosso próprio comportamento descuidado ou imprudente e ficarmos 'livres da culpa', já que podemos transferir a culpa do erro humano para a IA. Com certeza, esse não é um resultado feliz para as empresas, portanto, a necessidade de educar, alertar, treinar e gerenciar o comportamento humano continua sendo tão importante quanto antes, se não mais", afirma o Dr. Tomas Chamorro-Premuzic, professor de Psicologia Empresarial da University College London e da Columbia University[13].

As organizações podem obter os melhores resultados de segurança combinando inovações tecnológicas com investimentos contínuos em pessoas e processos.



ESTUDO DE CASO:

matillion

A MATILLION AVANÇA PARA ESTABELECER A SEGURANÇA CONTRA AMEAÇAS ORIENTADAS POR IA

A Matillion é a nuvem de produtividade de dados, que permite que empresas globais projetem, implementem e operem soluções de dados, tornando os dados prontos para os negócios mais rapidamente. Confiada pelas empresas orientadas por dados mais progressistas do mundo e por empresas da Fortune 500, a Matillion deve manter padrões excepcionais de segurança cibernética.

"Vimos um aumento nas campanhas de phishing de qualidade e sabemos que o malware está sendo gerado por meio de IA. A IA reduz a barreira de entrada e acelera exponencialmente as habilidades de um atacante ou adversário."

Graeme Park, Diretor de Segurança da Informação (CISO) da Matillion

A equipe já utiliza a IA nas ferramentas de segurança atuais e usou a IA generativa para ajudar a criar novos roteiros de segurança em um ritmo mais rápido. No que diz respeito às pessoas, a Matillion realiza programas contínuos de conscientização, baseados em vídeos curtos e nítidos. "Esses vídeos oferecem uma série envolvente no estilo Netflix sobre segurança, abordando tópicos como DeepFakes e ameaças de IA. Além disso, temos uma comunicação regular da equipe de segurança com a empresa em geral para explicar os quase-acidentes e outros eventos importantes para manter a segurança na mente da nossa equipe", diz Graeme Park.

PLANEJAR, PREPARAR, PROTEGER

O desenvolvimento de uma defesa cibernética robusta não é um caso isolado - é um exercício contínuo que evolui junto com o ambiente de ameaças e o seu portfólio de tecnologia. Processos e soluções que antes eram considerados de última geração perdem a eficácia com o tempo. O compromisso regular com a auditoria, a otimização e a modernização dos mecanismos de defesa da segurança cibernética corporativa é essencial para a resiliência de longo prazo.

Há três etapas que as organizações podem adotar para criar um ciclo de vida positivo de transformações cibernéticas:

COMO A HLB PODE AJUDAR

A segurança cibernética é um processo de ciclo de vida, que recruta diligência contínua. Investir em novos treinamentos e tecnologias uma única vez não é suficiente para garantir a resiliência contínua. Os melhores programas de segurança cibernética concentram-se em obter impactos de longo prazo: melhor visibilidade dos ambientes operados, mitigação proativa de ameaças e treinamento de funcionários orientado por resultados. Os profissionais de segurança cibernética do HLB ajudam as organizações a avaliar de forma holística sua postura de segurança e a priorizar investimentos nas áreas certas, nos eixos pessoas-processos-tecnologia. Entre em contato conosco para uma auditoria inicial.

NOSSOS SERVIÇOS

CONSULTORIA EM RISCOS CIBERNÉTICOS

- ANÁLISE DE LACUNAS NA CONFORMIDADE COM AS NORMAS
- AVALIAÇÃO DE RISCOS
- AVALIAÇÃO DA MATURIDADE DA SEGURANÇA
- ESTRATÉGIA EM CIBERSEGURANÇA

SOC COMO UM SERVIÇO

- MONITORAMENTO DE EVENTOS DE SEGURANÇA
- RESPOSTA A INCIDENTES
- COMPUTAÇÃO FORENSE
- CAÇA AO TESOURO

CYBERDRILLS

- AVALIAÇÃO DA RESPOSTA A INCIDENTES

CAPACIDADES

- AVALIAÇÃO DA RESILIÊNCIA CIBERNÉTICA
- EXERCÍCIOS CIBERNÉTICOS NACIONAIS

AVALIAÇÕES TÉCNICAS DE SEGURANÇA

- AVALIAÇÃO DE VULNERABILIDADE
- TESTES DE PENETRAÇÃO
- REVISÃO DO CÓDIGO-FONTE
- EXERCÍCIOS DA RED TEAM

SEGURANÇA GERENCIADA

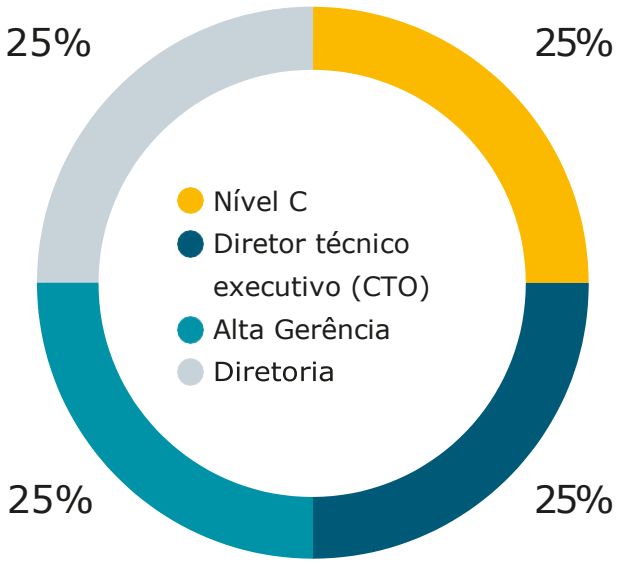
- AUDITORIAS INTERNAS
- INTELIGÊNCIA DE AMEAÇAS
- GERENCIAMENTO E SUPORTE DE TECNOLOGIA
- CONSCIENTIZAÇÃO SOBRE SEGURANÇA

METODOLOGIA DE PESQUISA

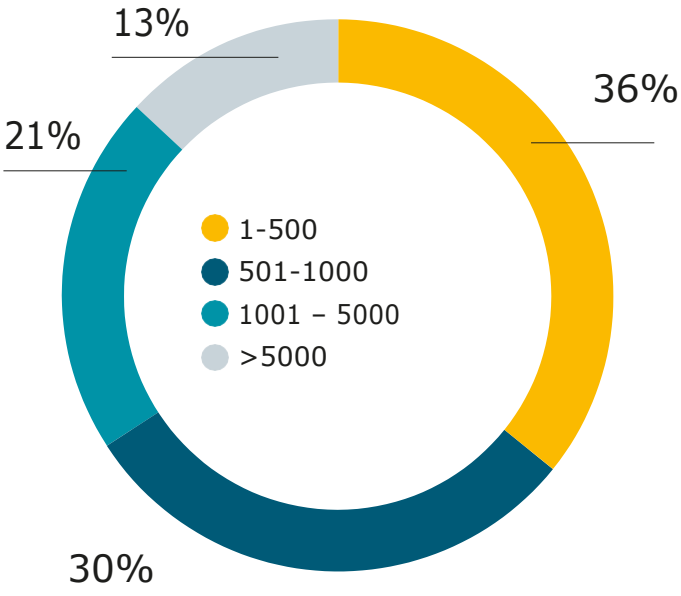
Em agosto de 2023, a HLB coletou 750 respostas de pesquisa de líderes de TI de quatro países e de diversos históricos do setor. As respostas foram coletadas por meio de uma ferramenta de pesquisa on-line. Além disso, foram realizadas duas trocas de e-mails de estudos de caso para coletar dados de especialistas externos no assunto.

Observe que nem todos os números deste relatório somam até 100% como resultado de porcentagens de arredondamento, excluindo respostas neutras ou quando os respondentes poderiam escolher mais de uma resposta.

Entrevistados por título de funcionários



Tamanho da empresa pelo número de funcionários



NOTAS FINAIS

1. HLB International, 2023. HLB Cybersecurity Report 2022: Hidden Risks in Cyber-Defence Laying a Foundation for Effective Cybersecurity Risk Mitigation
2. Check Point Software, 2023. 2023 Cyber Security Report
3. HLB International, 2023. HLB Survey of Business Leaders 2023: Leading Through a Perfect Storm
4. HLB International, 2023. Relatório de Segurança Cibernética de 2020 da HLB: Navegando no cenário de risco cibernético na era do trabalho remoto
5. HLB International, 2023. HLB Cybersecurity Report 2021: Addressing the cyber-risk landscape in the age of hybrid work
6. HLB International, 2023. HLB Cybersecurity Report 2021: Addressing the cyber-risk landscape in the age of hybrid work
7. HLB International, 2023. HLB Cybersecurity Report 2022: Hidden Risks in Cyber-Defence Laying a Foundation for Effective Cybersecurity Risk Mitigation
8. HLB International, 2023. HLB Survey of Business Leaders 2023: Leading Through a Perfect Storm
9. Google 2023. Why Red Teams Play a Central Role in Helping Organizations Secure AI Systems
10. HLB International, 2023. HLB Cybersecurity Report 2022: Hidden Risks in Cyber-Defence Laying a Foundation for Effective Cybersecurity Risk Mitigation
11. MDPI 2023. IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model
12. IEEE Access 2023. A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection
13. HBR 2023. Human Error Drives Most Cyber Incidents. Could AI Help?

www.hlb.global

TOGETHER WE MAKE IT HAPPEN

HLB International Limited, registrada na Inglaterra & País de Gales No. 02181222, escritório registrado: Lynton House 7-12, Tavistock Square, Londres, WC1H 9LT.