CYBER READINESS
INSTITUTE

A necessidade urgente de fortalecer a prontidão cibernética de pequenas e médias empresas

Uma proposta para a administração Biden

"À medida que o mundo se torna mais imerso e dependente da revolução da informação, o ritmo das intrusões, interrupções, manipulações e roubos também se acelera. O avanço tecnológico está a ultrapassar a segurança e continuará a fazê-lo, a menos que mudemos a forma como abordamos e implementamos estratégias e práticas de segurança cibernética. Ataques recentes nos quais dispositivos de consumo diários foram comprometidos para uso malicioso deixaram bem claro que agora vivemos num mundo muito mais interdependente."

— Comissão sobre o reforço nacional de segurança cibernética, relatório sobre a proteção e crescimento da economia digital, 1 de dezembro de 2016

Quase cinco anos depois, essas palavras continuam a soar verdadeiras. Continuamos atolados num jogo de Whack-A-Mole com os nossos adversários cibernéticos. Mas agora o cenário digital é maior e não temos ideia de onde virá o próximo ataque cibernético. O que sabemos com certeza é que virá. A descoberta das principais ações adversas, por meio dos compromissos SolarWinds e Microsoft Exchange, ocorre quando emergimos de um ano pandémico de operações comerciais remotas que viram um aumento dramático nos ataques de ransomware contra hospitais, escolas e outras infraestruturas críticas. Estamos num ponto de inflexão e há necessidade urgente de ação.

info@cyberreadinessinstitute.org

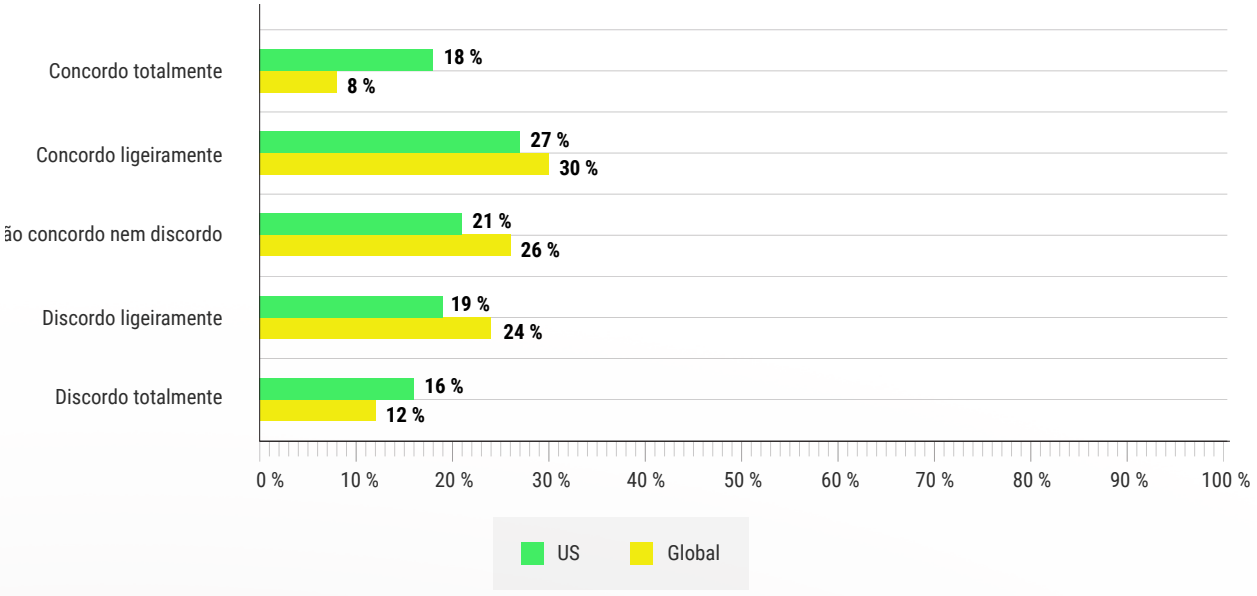
Chocantemente expansivos e sofisticados, os eventos SolarWinds e Microsoft Exchange eram apenas sintomas dos desafios que enfrentamos. Esforços corretivos, como atualização e correção do nosso software, alteração de palavras-passe e remoção de código malicioso, não são suficientes. Devemos reconhecer e abordar a nossa falha em incentivar comportamentos seguros e implementar as políticas necessárias para fortalecer as nossas defesas cibernéticas, para tornar a nossa nação protegida contra ataques cibernéticos.

Os eventos SolarWinds e Microsoft Exchange comprometeram dezenas de pequenas e médias empresas (PMEs) que formam elos vitais nas cadeias de abastecimento e na economia do nosso país. As pequenas e médias empresas são visadas por invasores cibernéticos porque, muitas vezes, não têm os recursos para investir em ferramentas e formação em segurança cibernética. A intenção deste White Paper é fornecer à Administração Biden ações específicas para melhorar a resiliência e a prontidão cibernética das pequenas e médias empresas dos EUA.

Embora não possamos acabar com as intrusões cibernéticas, existem ações básicas que podemos tomar para proteger os nossos cidadãos, empresas e infraestrutura crítica. Ao concentrarmo-nos no papel que o comportamento humano desempenha em hacks bem-sucedidos e ao fornecer às PMEs as ferramentas e recursos para melhorar a sua preparação para ataques cibernéticos, podemos construir uma base forte e resiliente para a segurança cibernética.

Também podemos ajudar a promover a força e a sobrevivência dos negócios. Dado que 60 % das PMEs irão fechar as suas portas dentro de um ano após uma violação cibernética, de acordo com a National Cyber Security Alliance, é vital para as PMEs, e para todos nós, que fiquemos preparados para ataques cibernéticos.

Apenas 18 % das PMEs nos EUA estão confiantes ("concordo totalmente") de que a sua empresa está preparada para um incidente cibernético.



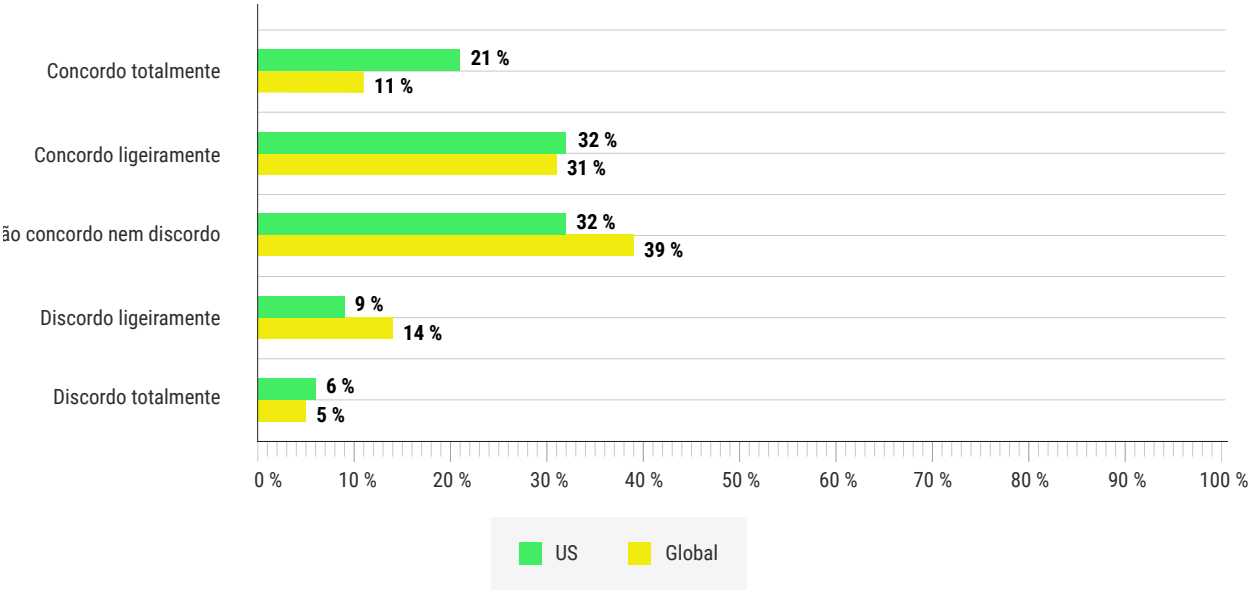
Questão: Até que ponto concorda que a sua empresa está preparada para um incidente cibernético e saberia como responder?

Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

Cenário e desafios da segurança cibernética

A pandemia COVID-19 desencadeou uma corrida global para facilitar operações remotas por parte de trabalhadores, empresas e agências governamentais. Embora as empresas e a sociedade beneficiem com essa transformação digital, ela aumentou as vulnerabilidades a nível mundial e em todos os setores da indústria. Em nenhum lugar a nossa exposição é maior do que entre as pequenas e médias empresas. No entanto, muitas pequenas e médias empresas não têm recursos financeiros ou talentos humanos para enfrentar os desafios da segurança cibernética e veem pouco retorno sobre o investimento com o gasto de recursos escassos em segurança cibernética. De acordo com um estudo do CRI de 2021, apenas 21 % das PMEs estão confiantes de que o tempo e o dinheiro que a sua empresa investe em segurança cibernética diminuirá o seu risco. A maioria das PMEs tem muito mais incerteza sobre o valor de investir em segurança cibernética. Enquanto isso, muitas empresas de maior dimensão não possuem requisitos básicos de segurança cibernética para os seus fornecedores ou estão apenas a começar a resolver o problema.

Apenas 21 % das PMEs nos EUA estão confiantes ("concordam totalmente") de que o tempo e o dinheiro investidos em segurança cibernética diminuem o seu risco.

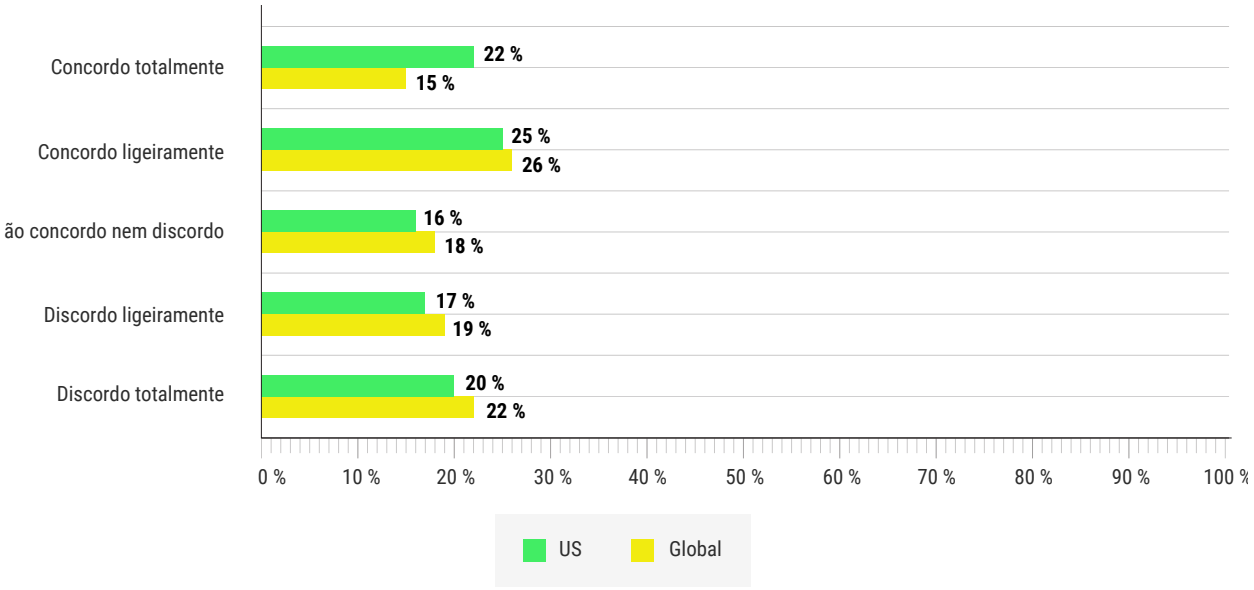


Questão: Até que ponto concorda que o tempo e o dinheiro que a sua empresa investe em segurança cibernética estão a diminuir o seu risco?

Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

Existem várias ameaças para pequenas e médias empresas, mas ransomware, phishing e roubo de credenciais estão entre as mais sérias. Essas ameaças só deverão crescer à medida que as indústrias continuam a colocar todas as operações online devido à pandemia COVID-19 e à mudança na natureza do trabalho. Essa rápida mudança gerou lacunas na resiliência cibernética, pois as empresas, especialmente aquelas com menos recursos, lutam para acompanhar. Essas vulnerabilidades crescentes estão a ser rápida e frequentemente exploradas por agentes mal-intencionados.

Apenas 22 % das PMEs nos EUA estão confiantes ("concordo totalmente") de que têm um funcionário ou equipa de funcionários com responsabilidade clara pela segurança cibernética.



Questão: Até que ponto concorda com a seguinte declaração: “Temos um funcionário ou equipa de funcionários com responsabilidade clara pela nossa segurança cibernética”?
Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

As consequências de um comprometimento de segurança cibernética não são apenas relevantes para a empresa em questão, mas também expõem outros negócios na sua cadeia de abastecimento. Considerando que mais de dois terços das grandes empresas terceirizam uma parte das suas funções e permitem o acesso de terceiros aos seus dados, a proteção cibernética insuficiente entre as pequenas e médias empresas também pode ter consequências para empresas de maior dimensão. **Um relatório de 2020 compilado pela Accenture descobriu que até 40 % das violações cibernéticas são indiretas, o que significa que visam elos fracos nas cadeias de suprimentos ou ecossistemas de negócios.**

Recomendações

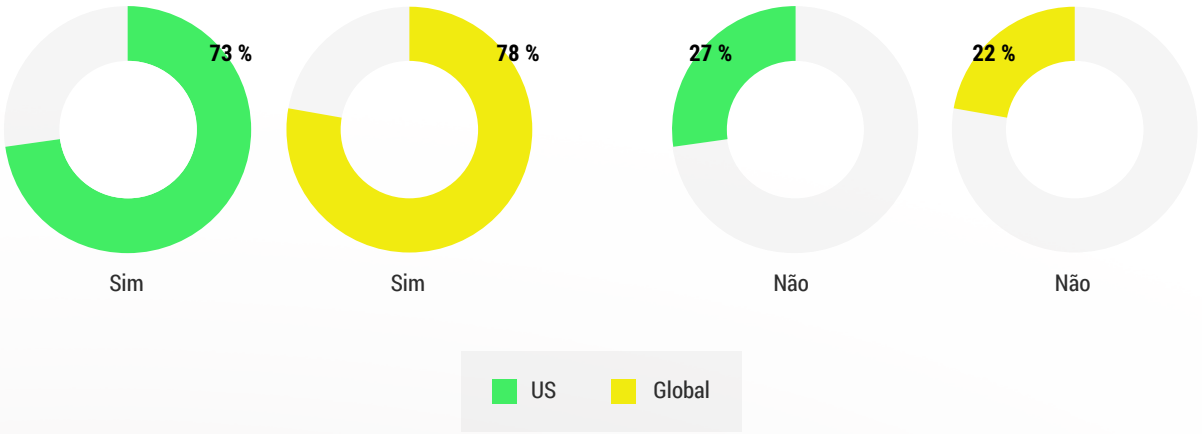
A segurança cibernética das pequenas e médias empresas dos EUA é parte integrante da operação desimpedida das nossas instituições públicas e privadas e do bem-estar económico da nossa nação. Seguem-se cinco recomendações para ajudar as pequenas e médias empresas americanas a prepararem-se para ataques cibernéticos.

- Criar uma campanha de sensibilização nacional para promover a prontidão cibernética para pequenas e médias empresas
- Criar um centro de recursos de segurança cibernética para PMEs dentro do governo federal
- Oferecer créditos fiscais para incentivar as pequenas e médias empresas a investir em segurança cibernética
- Estabelecer colaboração pública/privada para definir padrões mínimos de segurança cibernética
- Criar Cyber Squads financiados pelo governo, em colaboração com a comunidade e faculdades de 4 anos

Criar uma campanha de sensibilização nacional para promover a prontidão cibernética para pequenas e médias empresas

Como nação, temos uma longa história de campanhas de sensibilização pública para salvar vidas e mudar comportamentos - de incêndios florestais à segurança do cinto de segurança e aos anúncios pós-11 de setembro "Se vir algo, fale". Agora é o momento para uma campanha nacional de sensibilização que foque o papel do comportamento humano na segurança cibernética e eduque todos sobre as ações que nos tornarão todos seguros. Há apoio público para uma campanha do governo: mais de 60% das pequenas e médias empresas americanas e globais, de acordo com uma pesquisa do CRI de 2021, acreditam que o governo deve criar uma campanha nacional de sensibilização pública para promover a prontidão cibernética.

Mais de 70 % das pequenas e médias empresas dos Estados Unidos querem que o governo faça mais para ajudar a tornar as empresas da cadeia de abastecimento preparadas para ataques cibernéticos



Questão: O governo deve oferecer mais apoio para ajudá-lo a melhorar a segurança cibernética da sua empresa e de outras pessoas na cadeia de abastecimento?

Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

info@cyberreadinessinstitute.org

A cibersegurança é uma área complexa, não facilmente reduzida a uma simples mensagem. Uma campanha de serviço público eficaz deve concentrar-se numa questão única e básica de segurança cibernética - como a utilização de palavras-passe fortes. Focar num único tópico com uma mensagem recorrente simples ajudará a proteger as PMEs de um dos métodos preferidos pelos hackers.

Criar um centro de recursos de segurança cibernética para PMEs dentro do governo federal

Uma campanha nacional de sensibilização focada na prontidão cibernética irá naturalmente direcionar as PMEs a uma lista de recursos públicos e privados disponíveis. Hoje, esses recursos estão distribuídos por várias agências governamentais, às vezes com conselhos muito técnicos para muitos proprietários de negócios que não têm uma equipa interna de TI ou que terceirizam a segurança cibernética. Dado o trabalho em andamento para PMEs pela Agência de Segurança Cibernética e Infraestrutura (CISA), recomendamos que a CISA seja a agência mais bem posicionada para ser responsável pela preservação de recursos de segurança cibernética para PMEs. A agência contratada para preservar recursos também deve ter como missão principal a tarefa de simplificar os conceitos em torno da segurança cibernética para torná-los compreensíveis e acessíveis aos proprietários de negócios.

Oferecer créditos fiscais para incentivar as pequenas e médias empresas a investir em segurança cibernética

Para estimular os investimentos das PMEs em segurança cibernética, o governo federal deve fornecer um incentivo na forma de créditos fiscais. O Departamento do Tesouro, em colaboração com a Small Business Administration (SBA) e a CISA, deve estabelecer diretrizes para que o investimento das PMEs em segurança cibernética se qualifique para créditos fiscais. Embora os créditos fiscais reduzam a receita tributável que o governo arrecada, a segurança cibernética aprimorada reduzirá os danos económicos causados por invasores cibernéticos e terá um impacto líquido positivo sobre a segurança, a força e a resiliência da economia digital.

Trabalhando com outras agências e solicitando informações do setor, a administração fiscal pode estabelecer requisitos para que as empresas indiquem que tomaram medidas para se tornarem preparadas para ataques cibernéticos antes de receberem qualquer crédito fiscal. Estes padrões devem exigir treino e educação em segurança cibernética para que os funcionários se qualifiquem para o crédito. A educação deve enfatizar a necessidade de criar uma cultura de segurança cibernética no local de trabalho. A consciência dos riscos associados às violações cibernéticas e os comportamentos que mitigam esses riscos devem ser incorporados nas ações de todos, desde os funcionários até à liderança da empresa, para que os funcionários entendam as suas responsabilidades e sejam tomadas ações para garantir que a empresa está preparada para ataques cibernéticos.

Estabelecer colaboração pública/privada para definir padrões mínimos de segurança cibernética

Não podemos mais depender das forças do mercado ou de ações voluntárias para melhorar a segurança cibernética das nossas instituições públicas e privadas. Atualmente, "primeiro no mercado" supera "seguro no mercado". As forças do mercado priorizam o lucro em vez da segurança - e permitem vulnerabilidades, que os nossos adversários facilmente expõem. Esta estrutura é inaceitável e deve mudar. Devemos criar padrões que priorizem a segurança no mercado. Alinhados com uma campanha eficaz de educação e sensibilização, os padrões de mercado para segurança também ajudarão os consumidores a priorizar a segurança.

Estabelecer padrões por meio da colaboração da indústria e do governo é vital para proteger as cadeias de abastecimento. Estabelecemos com sucesso regulamentos que melhoram a segurança das nossas estradas, saúde e sistemas financeiros. Devemos estabelecer padrões mínimos de segurança cibernética.

Não existe uma solução única para todos para preparar as empresas para estarem prontas para ataques cibernéticos. O número de funcionários, setor, conhecimento técnico e capacidade financeira são apenas alguns fatores que variam de acordo com a empresa. Mas a indústria e o governo podem trabalhar juntos para estabelecer padrões, com foco numa abordagem de gestão de risco, que tenha esses fatores em consideração.

Criar Cyber Squads financiados pelo governo, em colaboração com a comunidade e faculdades de 4 anos

Já existe um programa governamental financiado por doações concedidas pela National Science Foundation - CyberCorps: Scholarship for Service. Esse programa, no entanto, é projetado para recrutar e treinar profissionais de TI e gestores de segurança cibernética para cargos em agências federais, estaduais e locais. Um novo programa Cyber Squad expandiria o leque de talentos disponíveis para PMEs e também facilitaria o envolvimento multidisciplinar e especialização na criação de culturas de prontidão cibernética entre PMEs.

Os Cyber Squads podem resolver vários problemas que atrapalham os esforços das PMEs para se tornarem preparadas para ataques cibernéticos - incluindo a escassez de talentos e de recursos financeiros. Um programa Cyber Squad modelado após o Peace Corps ou uma campanha semelhante à iniciativa educacional de Ciência, Tecnologia, Engenharia e Matemática (STEM) permitirá que os alunos explorem o interesse em procurar a segurança cibernética como uma carreira profissional, ao mesmo tempo em que fornece uma ligação com as suas comunidades locais.

Em colaboração com faculdades e universidades comunitárias, estudantes estagiários com experiência multidisciplinar receberiam formação adicional sobre o papel que o comportamento humano desempenha em tornar as PMEs seguras - questões como gestão de palavras-passe, atualização de software e alerta de phishing - que não são abordadas em muitos programas de cibersegurança. Cyber Squads seriam enviados à comunidade para ajudar PMEs locais a melhorar a sua prontidão cibernética. Inicialmente, o programa concentraria-se em ajudar empresas subfinanciadas de propriedade de minorias.

Conclusão

Estas recomendações e ações destacam a necessidade de colaboração público/privada urgente para abordar as graves vulnerabilidades que colocam a nossa segurança nacional e bem-estar económico em risco. **Agora, mais do que nunca, precisamos de colaboração proativa e deliberada e ação coletiva entre o governo e a indústria.**

Os eventos cibernéticos do ano passado demonstram como os nossos adversários cibernéticos estão cada vez mais sofisticados na identificação das nossas vulnerabilidades e fraquezas e na sua exploração. Devemos reforçar as nossas capacidades de defesa cibernética e, ao mesmo tempo, continuar a investir no nosso ataque.

As pequenas e médias empresas precisam de acesso a recursos de segurança cibernética que sejam prescritivos e acessíveis. Recursos, ferramentas e técnicas para pequenas e médias empresas exigem uma abordagem diferente daquela que as empresas maiores precisam. O objetivo é o mesmo, criar uma empresa protegida saudável, mas o caminho para chegar lá é diferente. Não podemos simplesmente reduzir as ferramentas e técnicas empregadas por grandes corporações em versões menores para pequenas e médias empresas.

Devemos ser proativos no apoio às PMEs para que se tornem uma força no nosso ecossistema, não uma fraqueza. Devem tornar-se mais resilientes e preparadas para ataques cibernéticos para garantir que a nossa nação tem uma base sólida e uma cultura de segurança.

Sobre o Cyber Readiness Institute

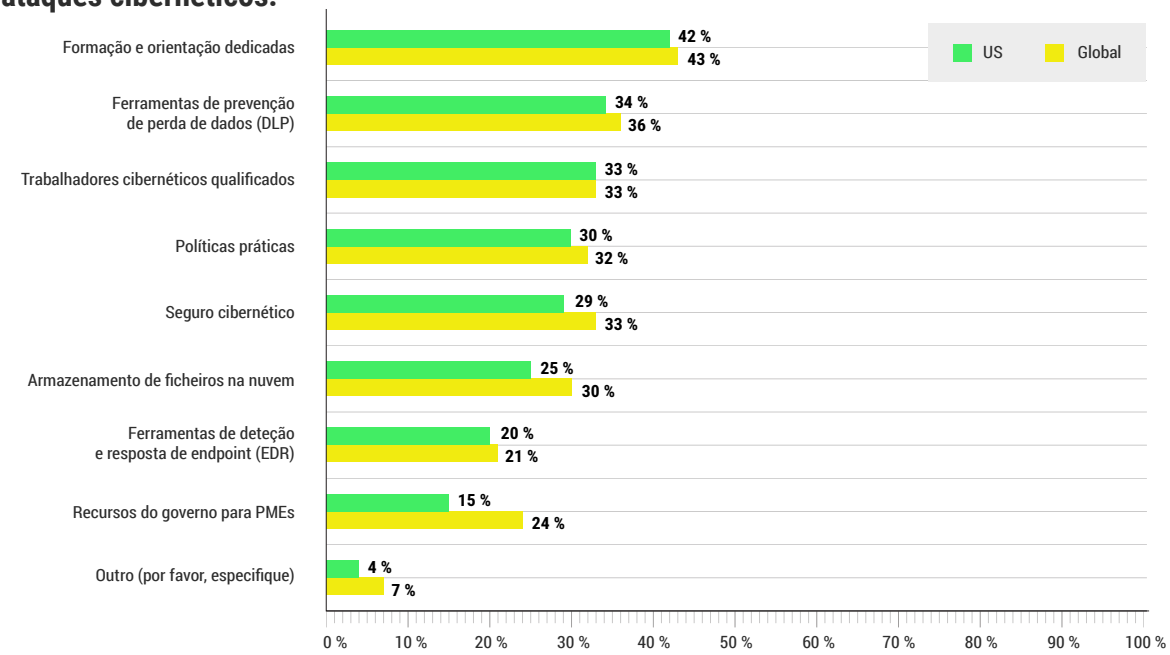
CYBER READINESS INSTITUTE

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para partilhar recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). O CRI foi cofundado pelos CEOs do The Center for Global Enterprise, Mastercard, Microsoft, PSP Partners, como uma ação de acompanhamento do trabalho da Comissão de Melhoria da Segurança Cibernética Nacional. Nossos membros também incluem ExxonMobil, General Motors e Principal. A nossa missão é promover a prontidão cibernética das PMEs para melhorar a segurança das cadeias de abastecimento globais. Os recursos do CRI concentram-se no comportamento humano e enfatizam a educação e a sensibilização dos funcionários. Para saber mais, visite www.BeCyberReady.com.

Apêndice

Pesquisa Global de Segurança Cibernética do Cyber Readiness Institute*, janeiro de 2021

A maioria das PMEs precisa de treino e orientação dedicados para se tornarem mais preparadas para ataques cibernéticos.

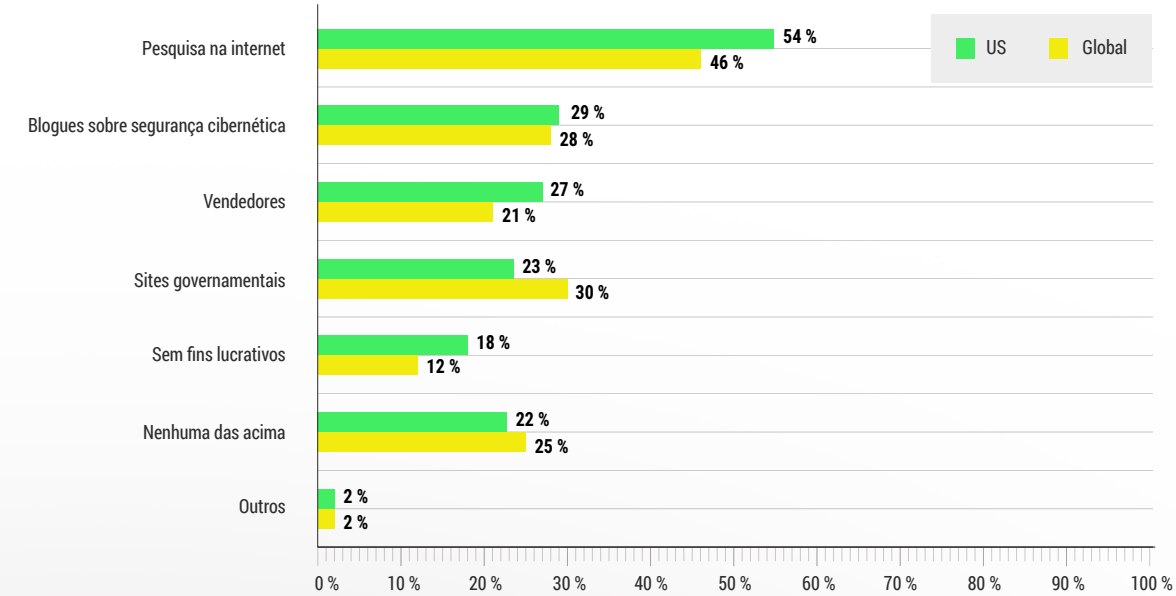


Questão: Qual das opções a seguir precisa para tornar a sua empresa mais segura? (selecione tudo o que se aplica)

Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

**Dimensão da pesquisa: U.S. é 576 e Global é 517*

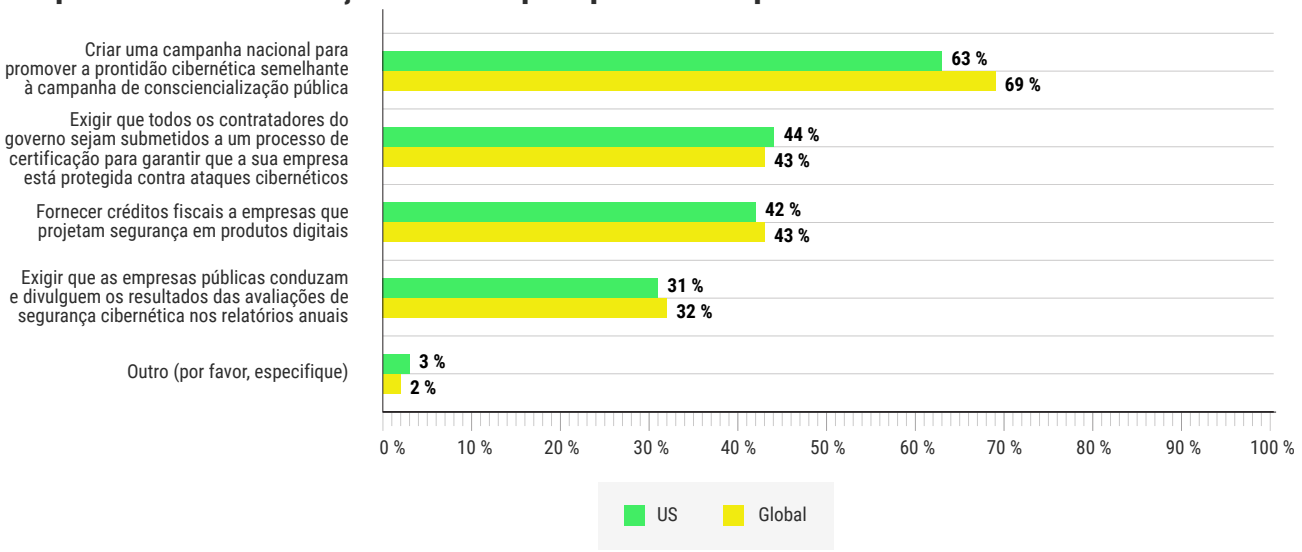
A maioria das PMEs depende de pesquisas na Internet para encontrar recursos de segurança cibernética.



Questão: Qual das seguintes fontes visitou para encontrar recursos de segurança cibernética para a sua empresa?

Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

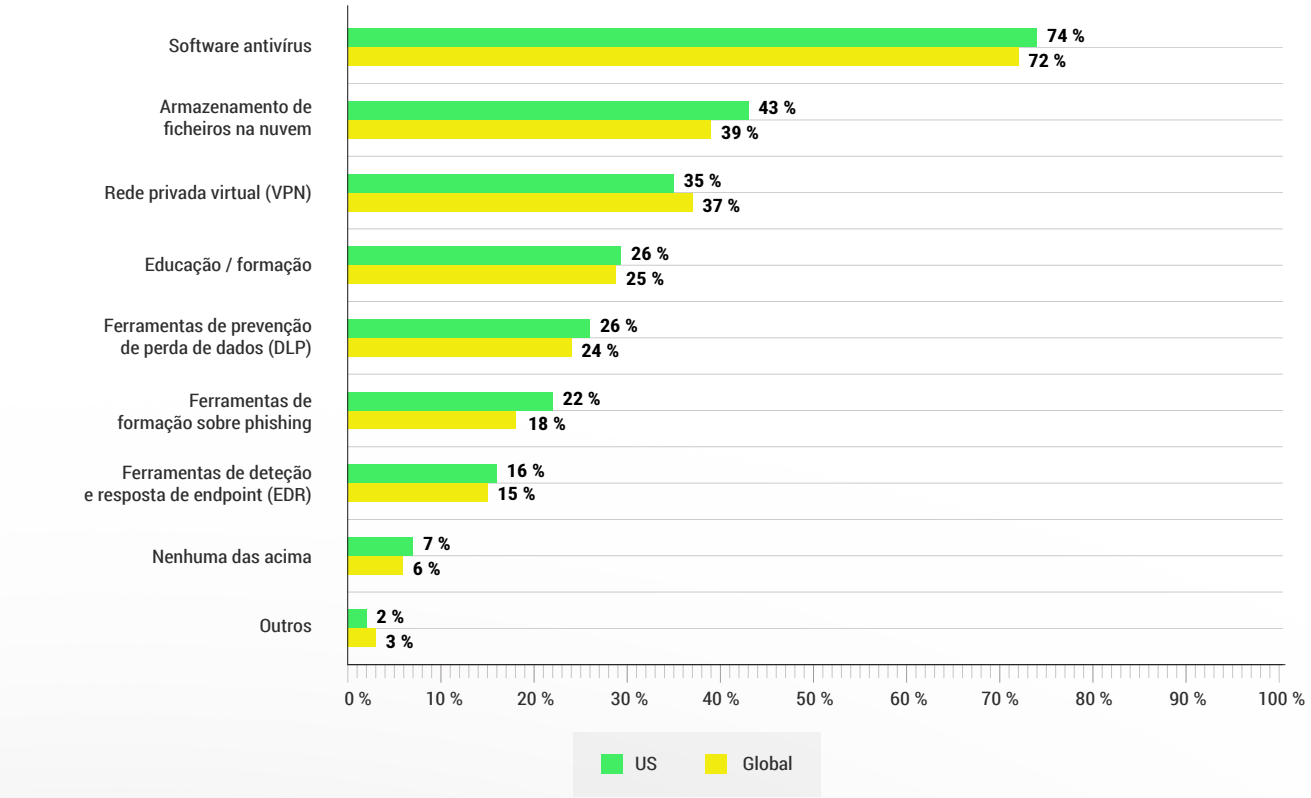
Mais de 60% das pequenas e médias empresas dos EUA querem que o governo crie uma campanha de sensibilização nacional para promover a prontidão cibernética.



Questão: Qual dos passos a seguir o governo deve tomar?

Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

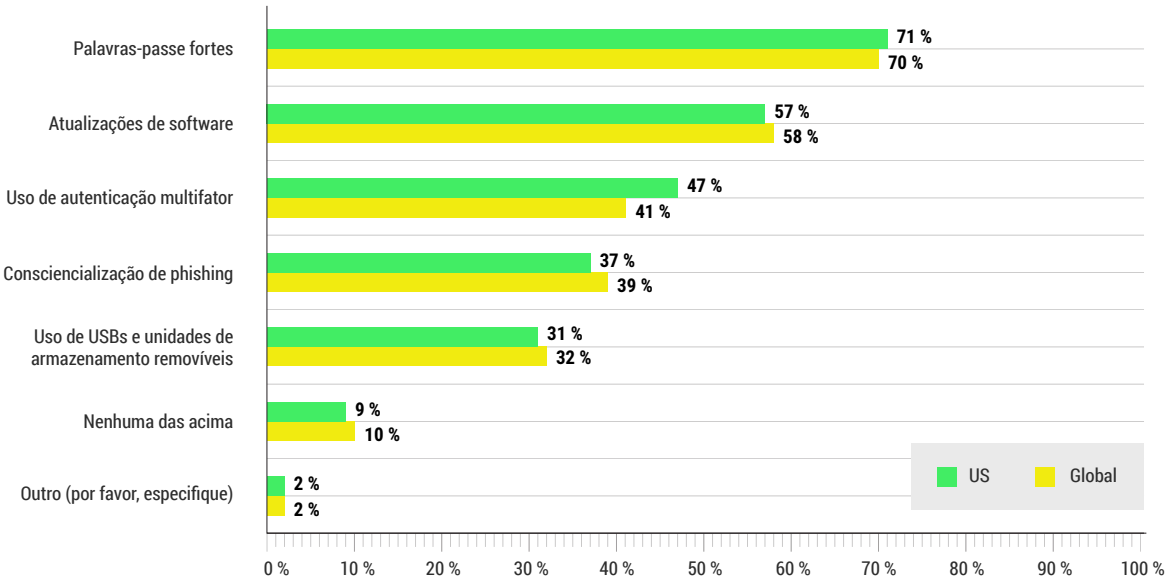
Software antivírus, armazenamento de ficheiros na nuvem e rede privada virtual (VPN) são as três principais ferramentas de segurança cibernética com as quais as PMEs contam.



Questão: Qual das seguintes tecnologias e/ou ferramentas usou para ajudar a manter a segurança cibernética da sua empresa?

Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

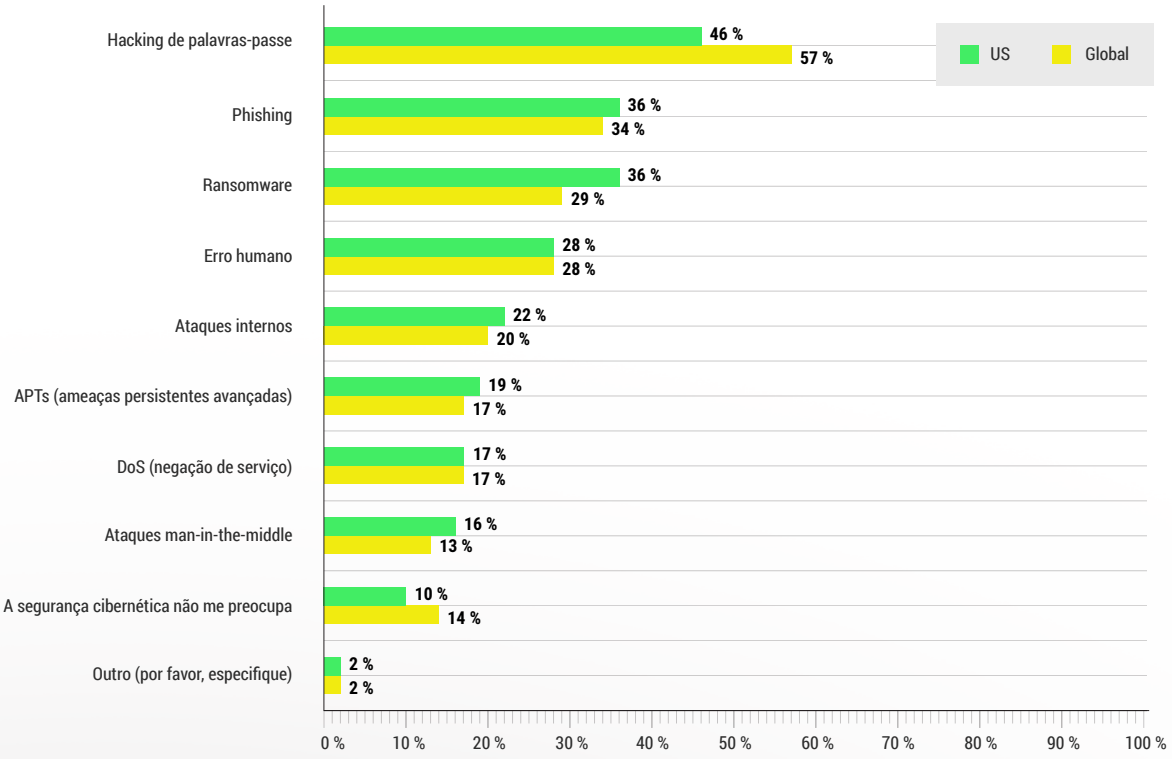
71 % das PMEs nos EUA afirmam que os seus funcionários são treinados para usar palavras-passe fortes. MAS as palavras-passe fracas ainda são o principal motivo dos hacks recentes.



Questão: Para qual dos seguintes tópicos relacionados com a segurança cibernética os funcionários da sua empresas receberam formação?

Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

Hacking de palavras-passe está no topo da lista de preocupações com a segurança cibernética entre as pequenas e médias empresas, junto com phishing, ransomware e erro humano.



Questão: Qual a sua maior preocupação em relação à segurança cibernética da sua empresa?

Fonte: Pesquisa Global do Cyber Readiness Institute, Pequenas e Médias Empresas, janeiro de 2021

info@cyberreadinessinstitute.org