CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Roteiro para a prontidão cibernética das pequenas e médias empresas (PME)

Índice

Resumo executivo

O Cyber Readiness Institute (CRI) convocou com êxito líderes de topo de empresas globais para recolher as melhores práticas de gestão de pessoas, processos e tecnologias que são fundamentais para melhorar a cibersegurança. Esta colaboração serviu de base ao desenvolvimento de conteúdos e ferramentas destinadas a proteger, responder e recuperar de incidentes ocorridos em toda a comunidade global de pequenas e médias empresas (PME).

Os co-presidentes e membros do CRI representam vários setores empresariais e têm uma presença em todo o mundo. Estas organizações continuam a ter um impacto positivo na proteção das PME globais contra as ciberameaças com os seus recursos, tecnologia e liderança. Os nossos co-presidentes pertencem à Apple, The Center for Global Enterprise (CGE), Mastercard e Microsoft, e nossos membros incluem a ExxonMobil, a General Motors e a Principal.

O Roteiro para a prontidão cibernética das pequenas e médias empresas (PME) do CRI faz uma retrospetiva dos nossos primeiros cinco anos ao recolher informações de dados, testemunhos, iniciativas-piloto, análise de conteúdos e participação das partes interessadas para avaliar o nosso alcance e impacto. Estas informações e o feedback direto dos debates aprofundados com os nossos membros e outros participantes chave no programa do CRI forneceram orientações para a continuação do trabalho específico necessário para cumprir a missão do CRI: permitir que as PME globais acelerem a sua prontidão em termos de cibersegurança e a resiliência operacional.

Sensibilização

Aumentar o nível de sensibilização e compreensão que as PME têm sobre as ameaças à cibersegurança relacionadas com a continuidade do negócio e as melhores práticas

1. Alcance global: assegure que os recursos do CRI cheguem às PME em todo o mundo ao estabelecer parcerias com organizações de âmbito global
2. Desenvolvimento e partilha de dados: recolha e publique informações exclusivas não específicas de fornecedor

Implementação

Apoiar as PME na implementação de políticas e procedimentos cibernéticos para criar uma cultura de prontidão cibernética ao focar-se no comportamento humano

1. Padrões de prontidão cibernética: desenvolver e dimensionar o Programa de prontidão do CRI como base para um processo de certificação padrão para PME que seja reconhecido e apoiado pelos Membros do CRI e pelas indústrias globais
2. Rede de formação global: estabelecer uma rede global de Formadores de cibersegurança qualificados

Incentivos

Explorar os mecanismos para incentivar as PME a melhorar a resiliência empresarial e a prontidão cibernética

- Seguro cibernético: recolher informações das PME para partilhar com o setor ao sermos a voz autorizada das PME
  - Desenvolver diretrizes para as PME selecionarem a cobertura mais adequada à respetiva organização
  - Ajudar as PME a apresentar provas da sua prontidão cibernética para dar uma resposta adequada ao risco
    - Alimentar os futuros modelos de negócio para os mercados de seguros
  - Fornecedor preferencial: implementar o Programa de prontidão cibernética com fornecedores de segundo e terceiro nível ao longo das cadeias de abastecimento globais para as PME obterem vantagens competitivas com a sua certificação.
    - Analisar a forma como nós, com os nossos membros e parceiros, podemos utilizar recompensas monetárias

Resumo executivo

Continuação

Para continuarmos a cumprir a missão do CRI estabelecida há cinco anos, temos de continuar a desempenhar um papel de liderança para as PME enquanto voz e intérprete das suas questões cibernéticas chave. Ao tirar partido da experiência dos nossos membros e parceiros, o CRI pretende tornar-se o primeiro destino para as PME que procuram melhorar a sua prontidão cibernética ao focarem-se no comportamento humano e nos passos essenciais para reduzir os ciberataques. Com muitas organizações já a trabalhar para promover estes princípios, o CRI continuará a focar-se em ser uma voz das PME a nível mundial nas questões cibernéticas fundamentais, representando a sua perspetiva junto dos decisores chave para assegurar que são tidas em conta as suas necessidades.

O CRI gostaria de agradecer à Apple, GM, Mastercard, Microsoft, ExxonMobil, Principal e ao Center for Global Enterprise pelo papel desempenhado no desenvolvimento deste Roteiro. As informações resultantes dos debates com os representantes destas organizações foram vitais para moldar o rumo a seguir pelo CRI.

Introdução

Revisão de cinco anos

O Cyber Readiness Institute (CRI) convocou com êxito líderes de topo de empresas globais para recolher as melhores práticas de gestão de pessoas, processos e tecnologias que são fundamentais para melhorar a cibersegurança. Esta colaboração serviu de base ao desenvolvimento de conteúdos e ferramentas destinadas a proteger, responder e recuperar de incidentes ocorridos em toda a comunidade global de PME. Segundo um inquérito global do CRI de 2021, apenas 18% das PME nos Estados Unidos estão confiantes de que a sua organização está preparada para um incidente cibernético.[1]

O Roteiro para a prontidão cibernética das pequenas e médias empresas (PME) do CRI faz uma retrospetiva dos nossos primeiros cinco anos ao recolher informações de dados, testemunhos, iniciativas-piloto, análise de conteúdos e participação das partes interessadas para avaliar o nosso alcance e impacto. Estas informações e o feedback direto dos debates aprofundados com os nossos membros e outros participantes chave no programa do CRI forneceram orientações para a continuação do trabalho específico necessário para cumprir a missão do CRI: permitir que as PME globais acelerem a sua prontidão em termos de cibersegurança e a resiliência operacional.

Co-presidentes e membros

Os co-presidentes e membros do CRI representam vários setores empresariais e têm uma presença em todo o mundo. Estas organizações continuam a ter um impacto positivo na proteção das PME globais contra as ciberameaças com os seus recursos, tecnologia e liderança. São inúmeros os seus contributos desde o início do CRI, mas destacamos alguns trabalhos:

- Apple: patrocinou um programa-piloto do CRI para melhorar a segurança dos fornecedores
- The Center for Global Enterprise (CGE): lançou o Digital Supply Chain Institute (DSCI) para se focar na evolução das cadeias de abastecimento das empresas e na aplicação prática das melhores práticas de gestão da cadeia de abastecimento
- Mastercard: criou o Trust Center para partilhar informações, ferramentas e recursos para ajudar as empresas a melhorar a sua cibersegurança
- Microsoft: lançou o Microsoft Defender para Empresas para oferecer às PME capacidades de deteção e resposta nos pontos terminais para proteção contra ransomware e outras ciberameaças sofisticadas

Os membros do CRI, a ExxonMobil e a Principal também desempenharam um papel importante na promoção da missão do CRI, e a GM realizou um programa-piloto com os seus fornecedores críticos. Os nossos membros fornecem feedback direto sobre o desenvolvimento de conteúdos e as melhorias ao programa.

[1] CRI-The-Urgent-Need-to-Strengthen-the-Cyber-Readiness-of-Small-and-Medium-Sized-Businesses (2).pdf

Conteúdo e recursos

Formação

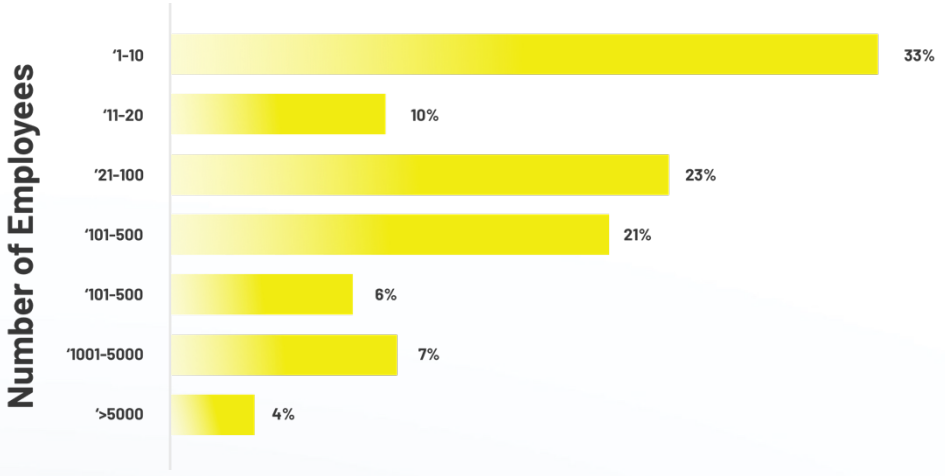
O CRI lançou o Programa de prontidão cibernética em 2017 e atualizou-o em 2020. O Programa está focado no comportamento humano com informações sobre os 4 principais problemas de cibersegurança para ajudar as PME a desenvolver políticas, procedimentos e dar formação aos colaboradores. Estes "quatro pilares" continuam a ser relevantes para as PME.

1. Palavras-passe: 4 em 5 falhas de segurança de dados resultam de palavras-passe fracas ou roubadas[2]
2. Atualizações de software: 60% das vítimas de falhas de segurança afirmaram que estas ocorreram devido a uma vulnerabilidade conhecida não corrigida, em que a correção não foi aplicada[3]
3. Phishing: pouco mais de um em cada quatro colaboradores (26%) afirmou ter sido vítima de um esquema de phishing no trabalho nos últimos 12 meses, um pequeno aumento em relação aos 25% registados em 2020.[4]
4. Suportes amovíveis/pen USB: as ameaças capazes de se propagarem através de USB, ou que exploram especificamente suportes USB para a infeção inicial, aumentaram de 19% em 2019 para 52% em 2021[5]

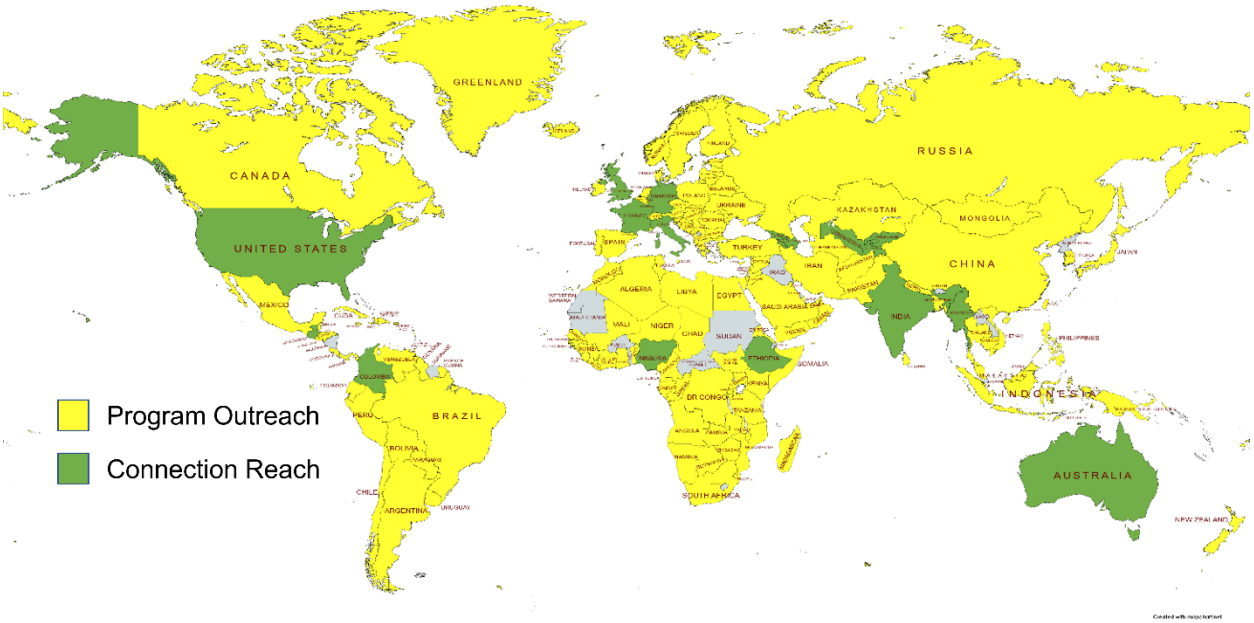
O Programa de prontidão cibernética foi traduzido para espanhol, português, francês, árabe, japonês e russo para facilitar o acesso de PME em todo o mundo.

Em outubro de 2020, o CRI alargou o Programa de prontidão cibernética com o Programa de certificação de líderes cibernéticos. Trata-se de um programa de gestão focado no reforço da capacidade dos colaboradores das PME para criar e manter uma cultura de prontidão cibernética na sua organização. Este programa mais aprofundado ensina os utilizadores a gerir as pessoas, os processos e a tecnologia essenciais para proteger a sua organização.

Destas PME, 33% têm 1 a 10 colaboradores, 10% têm 11 a 20, 23% têm 21 a 100, 21% têm 101 a 500, 6% têm 501 a 1000, 7% têm 1001 a 5000 e 4% têm mais de 5000.



[2] https://www.verizon.com/business/resources/reports/dbir/
[3] Estudo da Ponemon sobre lacunas na resposta às vulnerabilidades - ServiceNow
[4] **Tessian - Understand The Mistakes That Compromise Your Company's Cybersecurity**
[5] Case Study_SMX_Pulp and Paper 2_Cybersecurity_Honeywell (honeywellforge.ai)



Até à data, as inscrições nestes programas atingiram quase 5000 PME em 178 países, com uma representação de mais de noventa setores específicos. O mapa acima mostra o alcance global das inscrições e parcerias do programa do CRI. A maioria das inscrições que representam PME são organizações com menos de 100 trabalhadores. É evidente que o CRI está a chegar ao público-alvo.

Guias

Desde 2017, o CRI lançou 25 guias para PME sobre tópicos como a Autenticação multifator (MFA), MSPs, telessaúde, trabalho híbrido e muito mais. Estes guias são recursos de fácil consulta sobre tópicos em que se verificou que as PME têm lacunas de conhecimento.

Redes sociais

O conteúdo e os recursos exclusivos do CRI publicados no Twitter, LinkedIn, Facebook e Instagram alcançaram mais de sete milhões de pessoas, tendo gerado cerca de 350 mil interações e levando 118 mil pessoas ao Web site para obterem mais informações.

Estes feitos são apenas uma parte do trabalho do CRI nos últimos cinco anos e proporcionaram uma visão clara do caminho a seguir. Por exemplo, apesar das quase 5000 inscrições, apenas 1390 PME concluíram os nossos programas. É evidente que, devido à pouca sensibilização, à falta de orientações para a implementação e à ausência de incentivos adequados, as PME demoram a adotar as políticas e os procedimentos disponíveis para melhorar a sua segurança.

Roteiro de CRI

O CRI vê a melhoria da resiliência e a preparação das PME globais como uma estrada de três faixas, em que todas se movem à mesma velocidade e na mesma direção. Em cada uma destas faixas, o CRI identificou ações específicas para ajudar as PME de todo o mundo. Seguem-se as ações:

Sensibilização

Aumentar o nível de sensibilização e compreensão que as PME têm sobre as ameaças à cibersegurança relacionadas com a continuidade do negócio e as melhores práticas

3. Alcance global: assegure que os recursos do CRI cheguem às PME em todo o mundo ao estabelecer parcerias com organizações de âmbito global

4. Desenvolvimento e partilha de dados: recolha e publique informações exclusivas não específicas de fornecedor

Implementação

Apoiar as PME na implementação de políticas e procedimentos cibernéticos para criar uma cultura de prontidão cibernética ao focar-se no comportamento humano

3. Padrões de prontidão cibernética: desenvolver e dimensionar o Programa de prontidão do CRI como base para um processo de certificação padrão para PME que seja reconhecido e apoiado pelos Membros do CRI e pelas indústrias globais

4. Rede de formação global: estabelecer uma rede global de Formadores de cibersegurança qualificados

Incentivos

Explorar os mecanismos para incentivar as PME a melhorar a resiliência empresarial e a prontidão cibernética

- Seguro cibernético: recolher informações das PME para partilhar com o setor ao sermos a voz autorizada das PME
  - Desenvolver diretrizes para as PME selecionarem a cobertura mais adequada à respetiva organização
  - Ajudar as PME a apresentar provas da sua prontidão cibernética para dar uma resposta adequada ao risco
    - Alimentar os futuros modelos de negócio para os mercados de seguros
  - Fornecedor preferencial: implementar o Programa de prontidão cibernética com fornecedores de segundo e terceiro nível ao longo das cadeias de abastecimento globais para as PME obterem vantagens competitivas com a sua certificação.
    - Analisar a forma como nós, com os nossos membros e parceiros, podemos utilizar recompensas monetárias

Com as PME a representarem cerca de 99% das empresas nos países da Organização para a Cooperação e o Desenvolvimento Económico (OCDE),[1] estas ações vão reforçar as cadeias de abastecimento mundiais do zero ao colmatar as lacunas de conhecimentos básicos e de recursos para criar uma rede global de PME mais preparada e resiliente para o ciberespaço.

Sensibilização

Uma questão que continuou a surgir nos debates com as partes interessadas foi a falta global de sensibilização para o risco que as PME enfrentam se não melhorarem as suas políticas e procedimentos básicos de cibersegurança. Mais de metade dos proprietários de pequenas empresas inquiridos pelo CNBC afirmam não estar preocupados com o facto de a sua empresa vir a ser vítima de um ciberataque. Este ponto de vista deixa claro que existe uma lacuna de conhecimentos[1]. É compreensível, uma vez que a maioria das PME está focada no trabalho quotidiano necessário para gerir uma empresa com recursos limitados, pelo que têm pouco tempo para se informarem sobre as mais recentes e surpreendentes estatísticas de falhas de segurança informática ou para reverem os padrões técnicos preferenciais. Por conseguinte, o CRI tem a oportunidade e a permissão do mercado para se estabelecer como a "fonte de referência" em matéria de cibersegurança para PME, com recursos GRATUITOS focados nas questões cibernéticas fundamentais, tudo num único lugar. Uma forte aposta em parcerias com organizações globais, e um foco na disponibilização de dados relevantes e imparciais serão fundamentais para melhorar a sensibilização das PME para as principais questões cibernéticas.

Alcance global

As futuras campanhas de sensibilização e apoio direcionadas do CRI devem continuar a focar-se nas PME fora da América do Norte. Este foco internacional está alinhado com a natureza global das cadeias de abastecimento digitais e fornece informações sobre as realidades do funcionamento em diferentes regiões. Colocar os recursos do CRI nas mãos de mais PME em África e na América do Sul aumentará a sensibilização global para as questões da prontidão e resiliência cibernéticas. Para chegar eficazmente a estas diferentes regiões, o CRI irá orientar os seus esforços de recrutamento e parceria com as organizações e PME adequadas que operam nestes países. Esta representação fornecerá novas perspetivas ao nosso atual processo de desenvolvimento de recursos e ajudará o CRI a transmitir eficazmente mensagens para diferentes culturas. A tradução contínua dos programas de formação do CRI, entre outros recursos, é fundamental para o êxito deste alcance global. Os futuros esforços de tradução serão determinados pelas necessidades dos nossos membros e parceiros para permitir que os nossos recursos aumentem a sensibilização para as questões de cibersegurança em todo o mundo.

Desenvolvimento e partilha de dados

Uma lacuna importante que o CRI identificou na melhoria da sensibilização para a cibersegurança entre as PME a nível global é uma despreocupação com as consequências. Muitas vezes, estas PME não compreendem as consequências que não melhorar a sua higiene cibernética básica pode ter para a sua atividade. Mesmo quando as PME e outros profissionais no setor da cibersegurança procuram dados, deparam-se frequentemente com resultados de fornecedores que tentam vender um produto. Reforçar as credenciais do CRI como uma origem de dados fidedigna para as PME ajudará a aumentar a adoção do nosso programa. Ao recolher dados únicos dos nossos programas, realizar inquéritos e tirar partido dos recursos dos nossos membros, o CRI pretende quantificar e comunicar melhor o efeito de um evento cibernético para as PME.

Implementação

Oferecer às PME recursos para melhorar a sua prontidão cibernética é apenas parte do desafio. Os colaboradores estão cada vez mais conscientes do impacto dos seus comportamentos na segurança, com 36% dos colaboradores a considerarem que cometeram um erro no trabalho que comprometeu a segurança nos últimos 12 meses. Ainda assim, sem as políticas e a formação adequadas, não conseguem aprender a evitar o mesmo erro na oportunidade seguinte. Ao compreender os desafios que as PME enfrentam, o CRI deve criar mecanismos para melhorar a prontidão cibernética sem criar confusão, trabalho desnecessário ou esgotar os recursos. Com a realização de iniciativas-piloto com os nossos membros e parceiros, esclarecemos um aspeto fundamental: uma abordagem passo-a-passo e de grande proximidade é a forma mais eficaz de levar as PME a concluírem o Programa de prontidão cibernética, que inclui as características fundamentais de políticas e procedimentos cibernéticos, bem como planos de resposta a incidentes. O CRI planeia expandir esta capacidade ao oferecer um envolvimento próximo às PME à medida que trabalham para melhorar a sua cibersegurança com uma base normalizada e uma rede global formadores qualificados em cibersegurança.

Padrões de prontidão cibernética

Com as normas, os regulamentos, as tecnologias e outros aspetos fundamentais da cibersegurança a avançarem a um ritmo alucinante, a maioria das PME não está equipada para os acompanhar. Mas será que precisam? Em vez disso, o CRI debe estabelecer um conjunto básico de políticas e procedimentos que as PME possam aplicar para provar a sua prontidão cibernética. Estas políticas dão às PME um ponto de partida no seu percurso, algo que muitas vezes têm dificuldade em encontrar. Uma vez atingido, o padrão do CRI dará aos clientes, parceiros da cadeia de abastecimento, seguradoras e outras partes interessadas a garantia de que uma empresa está preparada para o ciberespaço. O desenvolvimento destas políticas e procedimentos exige uma forte colaboração entre os setores público e privado, bem como o contributo direto das PME para assegurar a sua viabilidade e eficácia. O atual Programa de prontidão cibernética do CRI e o processo de certificação associado servirão de ponto de partida para um processo dimensionável no qual as PME podem trabalhar com Formadores de cibersegurança aprovados pelo CRI. À medida que o padrão evolui ao longo do tempo, procuraremos expandir os nossos programas e materiais para tópicos como a gestão de vulnerabilidades e outras questões identificadas como vitais para melhorar a cibersegurança das PME.

Rede de formação global

Para aumentar as taxas de conclusão e a eficácia global do programa, o CRI tenciona desenvolver uma rede global de Formadores de cibersegurança qualificados. Ao replicar e ampliar um esforço bem-sucedido da parceria do CRI com o Cyber Hawaii, o CRI formará pessoas em áreas geográficas locais para ajudar as PME a avançar no seu percurso de prontidão cibernética e verificar se o programa foi concluído com êxito. Esta rede de suporte localizada ajudará o CRI a personalizar as necessidades das PME afetadas, o que permite aos parceiros globais trabalhar nos Programas do CRI ao seu próprio ritmo. Esta abordagem tem dois objetivos: ajudar as PME através do programa e verificar externamente a conclusão do programa para o CRI atribuir a certificação. Além disso, o desenvolvimento desta rede irá reforçar a força de trabalho e expandir o conjunto de recursos para iniciativas futuras.

Incentivos

A sensibilização e a oferta de apoio à implementação são necessárias, mas não suficientes, para ajudar as PME a investir na sua preparação e a manter a sua resiliência. Os incentivos financeiros e, eventualmente, os desincentivos, têm-se revelado mecanismos eficazes que têm um efeito nas práticas e nos procedimentos cibernéticos. Um inquérito do CRI feito em 2021 concluiu que apenas 21% das PMEs estão confiantes de que o tempo e o dinheiro que a sua organização investe em cibersegurança diminuirá a sua exposição ao risco[1]. À medida que procurarmos melhorar a prontidão cibernética das PME, temos de oferecer mais novas abordagens para aumentar a segurança e a proteção da marca. Duas áreas, o Seguro cibernético e o Estatuto de fornecedor preferencial, surgiram como incentivos favoráveis nos debates com as principais partes interessadas.

Seguro cibernético

Normalmente, as PME não dispõem de pessoal, processos e tecnologias para desenvolver os programas de segurança robustos necessários para se habilitarem a um seguro cibernético. Muitas seguradoras e subscritores também não têm uma visibilidade adequada das realidades da gestão de uma pequena empresa. Isto criou uma situação cada vez mais confusa, tanto para as seguradoras como para as PME que procuram a apólice adequada às suas necessidades. Para esclarecer esta confusão, o CRI deve aproveitar a sua capacidade de reunir as partes interessadas para identificar as lacunas de conhecimentos e desenvolver material para as colmatar. Para tal, será necessário que o CRI forneça às PME orientações para a seleção de apólices e que trabalhe com as seguradoras para criar descontos ou outros incentivos financeiros que encorajem as PME a adotar práticas cibernéticas sólidas.

Estatuto de fornecedor preferencial

À medida que continuamos a estabelecer o Programa de prontidão cibernética como o padrão de "higiene cibernética", o CRI quer dar às PME a capacidade de demonstrar a sua prontidão cibernética aos seus parceiros. O CRI irá tirar partido da nossa capacidade de reunião ao colaborar com os nossos membros e parceiros para ajudar a estabelecer um estatuto de fornecedor preferencial para os fornecedores de segundo e terceiro nível e, em seguida, ajudar as PME a alcançar esse estatuto. Além disso, o CRI irá analisar se a oferta de incentivos monetários poderá aumentar a adoção deste padrão de prontidão cibernética.

Perspetiva de futuro

Para continuarmos a cumprir a missão do CRI estabelecida há cinco anos, temos de continuar a desempenhar um papel de liderança para as PME enquanto voz e intérprete das suas questões cibernéticas chave. Ao tirar partido da experiência dos nossos membros e parceiros, o CRI pretende tornar-se o primeiro destino para as PME que procuram melhorar a sua prontidão cibernética ao focarem-se no comportamento humano e nos passos essenciais para reduzir os ciberataques.

O presente Roteiro, que aborda a prontidão cibernética das PME, descreve o que o CRI e os nossos parceiros devem fazer para apoiar as PME a nível mundial. Ao planear o futuro, é importante reconhecer a dimensão dos problemas atuais que não só as PME enfrentam, mas também as organizações de todos os sectores e dimensões. Por conseguinte, o CRI acredita que o nosso percurso para o êxito assenta nos princípios de parcerias fortes, desenvolvimento e retenção da força de trabalho, e soluções tecnológicas acessíveis.

Parcerias

As instituições públicas e privadas de todo o mundo precisam de abrir as linhas de comunicação, privilegiando a colaboração e não a concorrência. A partilha de dados, melhores práticas, políticas eficazes e lições aprendidas é fundamental para melhorar o ecossistema global das PME.

Desenvolvimento e retenção da força de trabalho

O crescimento da força de trabalho global no domínio da cibersegurança proporciona uma maior reserva de talentos, o que coloca à disposição das PME colaboradores mais capazes. Fornecer os conhecimentos adequados para reter esta força de trabalho irá assegurar a continuidade e a resiliência das operações comerciais globais.

Soluções tecnológicas acessíveis

As PME beneficiam muito com a disponibilização de ferramentas e sistemas fáceis de utilizar e acessíveis para gerir a sua posição de risco. O desenvolvimento destas tecnologias exigirá investimentos focados nas necessidades reais de cibersegurança das PME, e não apenas em mais uma funcionalidade para vender.

Com muitas organizações já a trabalhar para promover estes princípios, o CRI continuará a focar-se em ser uma voz das PME a nível mundial nas questões cibernéticas fundamentais, representando a sua perspetiva junto dos decisores chave para assegurar que são tidas em conta as suas necessidades.