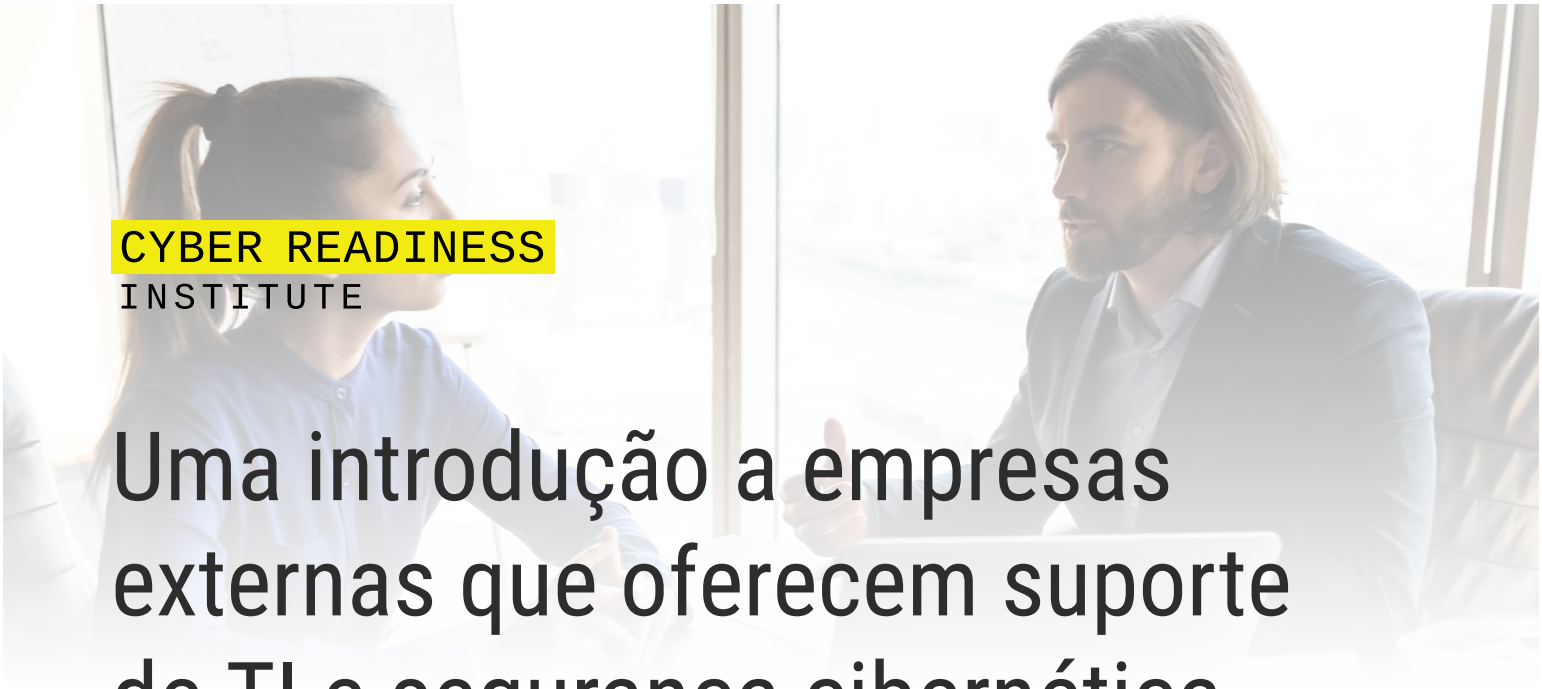

CYBER READINESS
INSTITUTE

Uma introdução a empresas externas que oferecem suporte de TI e segurança cibernética

O segundo de uma série sobre como usar empresas externas para reduzir o risco de segurança cibernética.

Como muitas pequenas empresas, chegou à conclusão de que precisa de suporte externo de tecnologia da informação (TI) e cibersegurança. Talvez tenha ouvido falar de mais violações de segurança cibernética nas notícias. Talvez conheça uma empresa que sofreu um ataque de ransomware. Se ainda não tem a certeza se precisa de ajuda, dê uma vista de olhos no **primeiro guia** desta série, "Devo obter suporte externo para gerir o meu risco de segurança cibernética?"

Percebe que a TI e a segurança cibernética estão a tornar-se "fundamentos" da gestão de negócios - como finanças e vendas. Mas não tem tempo para descobrir tudo. Se é como a maioria dos proprietários ou gestores de pequenas empresas, pode não ter a certeza do tipo de suporte de que precisa ou mesmo que perguntas fazer. Esta série do Conselho Consultivo para Pequenos Negócios do Cyber Readiness Institute ajudará a orientá-lo no processo de determinar se precisa de ajuda externa e como obter a ajuda necessária.

Lembre-se sempre de que, em última análise, é responsável pela prontidão cibernética da sua empresa. Pode terceirizar certas funções, como a instalação de atualizações de software, mas é responsável por definir as políticas, construir uma cultura de prontidão cibernética e cumprir quaisquer obrigações de conformidade de privacidade e segurança.

À medida que a ameaça de ataques cibernéticos aumenta, também aumenta o número e os tipos de empresas que oferecem a sua assistência. É um mercado confuso com ofertas de serviços sobrepostas e mais siglas do que possa imaginar.

info@cyberreadinessinstitute.com

Uma das primeiras decisões é se deseja contratar um consultor de TI/cibernético confiável para orientá-lo durante o processo ou percorrer os fornecedores por conta própria. Sabemos que a ideia de contratar um consultor para escolher o(s) fornecedor(es) certo(s) pode parecer uma despesa adicional. No entanto, pode ser menos dispendioso a longo-prazo porque podem garantir que recebe os serviços de que precisa por um preço justo. Em última análise, precisa de determinar em quem confiar para obter a ajuda de que precisa.

Eis uma lista dos **tipos de empresas** que irá encontrar e uma breve descrição. Lembre-se de que haverá alguma sobreposição nos tipos de serviço que fornecem. O próximo guia da série discutirá como selecionar o nível certo de suporte externo.

Consultor de TI

Análogo a um faz-tudo de TI. De modo geral, o consultor de TI ajuda a prevenir a ocorrência de problemas e corrige os problemas que ocorrem. Eles ajudam a configurar a sua rede e/ou Wi-Fi, a construir e manter sites, a recomendar e instalar software, a configurar e-mails, a configurar contas de utilizador, a criar e a testar cópias de segurança e muito mais.

Fornecedor de serviços geridos (MSP)

Os MSPs são normalmente pequenas empresas que oferecem serviços semelhantes a consultores de TI. Geralmente são instaladores certificados ou consultores de vários fornecedores de hardware e software. Alguns MSPs dizem que se especializam em segurança cibernética, o que significa que os seus serviços se sobreporiam em maior medida aos de um MSSP.

Fornecedor de serviços de segurança geridos (MSSP)

O MSSP verificará se o MSP está a construir e a manter a rede para maximizar o valor e reduzir o risco, uma vez que alguns MSPs e consultores de TI têm conhecimento limitado sobre tecnologia ou monitorização de segurança cibernética. Os MSSPs realizam frequentemente atividades como mapeamento de intrusão, verificação de registos, avaliação de risco de tecnologia, planeamento e consultoria, conformidade com políticas, desenvolvimento de procedimentos, suporte ao utilizador, resposta de segurança proativa, monitorização e resposta a incidentes.

Diretor de informação virtual (vCIO)

Para empresas que podem precisar de um CIO na sua força de trabalho, os vCIOs oferecem uma maneira de terceirizar a função, semelhante a como pode terceirizar as funções de Conselheiro Geral ou Diretor Financeiro. Esta abordagem tende a ser para empresas um pouco maiores na escala de pequeno a médio porte. Os vCIOs irão gerir, implementar e recomendar produtos e serviços para melhorar os seus níveis de TI e segurança.

Aqui está uma lista dos **tipos mais comuns e respeitados de certificações** ou credenciais profissionais que pode encontrar ao avaliar aqueles que fornecem suporte externo.

Credenciais gerais de segurança cibernética:

CISSP - Profissional Certificado de Segurança de Sistemas de Informação

- Uma certificação avançada que é amplamente aplicável, pois não é específica do fornecedor. Requer 5 anos de experiência para adquirir.

CISM - Gestor de Segurança da Informação Certificado

- Uma certificação avançada que requer cinco anos de experiência para ser adquirida. Aqueles que adquiriram essa credencial geralmente gerem a segurança no nível organizacional (por exemplo, CISOs).

CompTIA Security+

- Uma certificação básica que fornece uma boa base para desenvolver outras credenciais mais avançadas.

Credenciais especializadas (dependendo da necessidade):

SANS

- O SANS oferece uma variedade de certificações técnicas, divididas em áreas de foco como Segurança na Nuvem, Teste de Penetração e Hacking Ético e Gestão de Segurança, Legal e Auditoria.
- A certificação SANS GIAC Security Essentials (GSEC) atinge um bom equilíbrio ao sinalizar que o titular da credencial tem uma base de conhecimento amplamente aplicável, bem como capacidades técnicas específicas.

CISA - Auditor Certificado de Segurança da Informação

- Como o nome sugere, essa credencial destina-se a funções com foco em auditoria e conformidade.

CIPP - Profissional Certificado de Privacidade de Informação

- Esta credencial concentra-se na privacidade de dados no que se refere a questões legais e regulatórias.

CEH - Hacker Ético Certificado

- Esta credencial significa que o indivíduo aprendeu a pensar como um hacker, mas usa essas capacidades para proteger e prevenir ataques, em vez de penetrar num sistema com intenção maliciosa.

Este guia forneceu informações sobre os tipos de empresas e credenciais que pode encontrar. Se agora se está a perguntar como selecionar o tipo certo de suporte externo para a sua empresa, procure o nosso próximo guia nesta série, **“Como selecionar o nível certo de suporte externo.”**

info@cyberreadinessinstitute.com

A lista completa de guias desta série:

Devo obter suporte externo para gerir o meu risco de segurança cibernética?

Introdução aos tipos de suporte externo de TI e segurança cibernética

(ESTE GUIA)

Como selecionar o nível certo de suporte externo

Revisão e compreensão do contrato

As suas responsabilidades contínuas de segurança cibernética

Autores contribuidores

Agradecimentos especiais

- Marc Pillon, IT Ally
- Brian Kelly, EDUCAUSE
- Dawn Yankeelov, TALK
- Faye Francy, Auto-ISAC
- Ilene Klein, Cybercrime Support Network
- Jill Tokuda, CyberHawaii
- John Bryk, DNG-ISAC
- Michael Pritchard, Netchex
- Tanya Bolden, AIAG
- Walter Bran, ICC Guatemala
- Stan Stahl, SecureTheVillage

Sobre o CRI

O Cyber Readiness Institute é uma iniciativa sem fins lucrativos que reúne líderes empresariais de vários setores e regiões geográficas para a partilha de recursos e conhecimento que informam o desenvolvimento de ferramentas gratuitas de segurança cibernética para pequenas e médias empresas (PMEs). Explore os blocos de construção de uma boa segurança cibernética com o nosso Kit de Iniciação ou crie uma cultura de prontidão cibernética na sua empresa com o programa de prontidão cibernética online. Os nossos recursos de trabalho remoto e guias de local de trabalho híbrido oferecem dicas oportunas para lidar com os desafios cibernéticos em evolução nos dias de hoje. Para saber mais, visite www.BeCyberReady.com.