CYBER READINESS
INSTITUTE

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

Este é o primeiro guia de uma série de cinco partes sobre como usar empresas externas para reduzir o risco de segurança cibernética.

Se for como a maioria dos proprietários ou gestores de pequenas empresas, terá muitas funções. O seu foco geralmente está nos fundamentos da gestão e construção do seu negócio. Sabe que a segurança cibernética é uma área de risco crescente porque há mais notícias sobre ela - especialmente mais notícias sobre ameaças e ataques cibernéticos. A segurança cibernética é multifacetada. Sim, firewalls e filtros de spam ajudam, mas também precisa de uma força de trabalho com a devida formação que conheça os elementos básicos da segurança cibernética. O Cyber Readiness Institute concentra-se no comportamento humano e na educação para criar uma cultura de segurança dentro de cada empresa. Afinal, basta um clique equivocado numa ligação de phishing para potencialmente derrubar a sua empresa. Se isso parece opressor, não há problema em procurar orientação. Esta série de cinco partes do Cyber Readiness Institute, em consulta com o seu Small Business Advisory Council, ajudará a orientá-lo no processo de determinar se precisa de ajuda externa e, em caso afirmativo, como obtê-la.

Talvez pensasse que não seria um alvo para hackers, mas agora está claro que eles estão a atacar pequenas empresas para obter ganhos financeiros, como plantando ransomware, bem como usando pequenas empresas como portas de entrada para atacar empresas maiores. Sabe que precisa de fazer algo, mas não tem a certeza do que deve fazer ou se precisa de ajuda externa. **Lembre-se de que pode terceirizar algumas das suas responsabilidades de segurança cibernética, mas não pode terceirizar a sua responsabilidade pela segurança cibernética.** Com ou sem ajuda externa, será sempre da sua responsabilidade criar e fomentar uma cultura de prontidão cibernética dentro da sua empresa.

info@cyberreadinessinstitute.com

O primeiro passo é examinar honestamente o risco de segurança cibernética. Priorize os sistemas e dados de que precisa para administrar a sua empresa. Aqui estão algumas dicas rápidas para começar:

1. Liste as **informações e dados que são mais importantes** para o sucesso da sua empresa (por exemplo, informações do cliente, informações comerciais confidenciais).
2. Liste as **ferramentas de hardware e software de computador que são mais importantes** para administrar a sua empresa (por exemplo, site, e-mail, armazenamento de ficheiros, sistema de contabilidade, bases de dados).
3. Nas listas acima, identifique os três a cinco principais itens que causariam mais danos à sua empresa se não estivessem disponíveis, fossem perdidos ou roubados. Vamos chamá-los de **joias da sua coroa**.
4. Identifique quem tem **acesso às suas joias da coroa**. Determine de forma realista o quão bem protegidos eles estão e se se sente confortável com o **nível de proteção**.
5. Se não consegue dizer o quão bem protegidos eles estão, precisa de suporte externo.
6. Se eles precisarem de melhor proteção, sabe o que fazer e é capaz de o fazer? Caso contrário, precisa de suporte externo.
7. Determine se há alguma proteção de dados, segurança cibernética ou requisitos de privacidade de dados dos seus clientes ou leis e regulamentos federais ou locais aplicáveis.

CYBER READINESS
INSTITUTE

Não se preocupe se parecer que precisa de considerar a possibilidade de obter suporte externo. A maioria das pequenas empresas precisa de algum suporte externo para TI e segurança cibernética. Como uma organização sem fins lucrativos, estamos aqui para lhe dar conselhos gratuitos e diretos. Podemos ajudá-lo a compreender a diferença entre um consultor de TI, um fornecedor de serviços geridos (MSP) e um fornecedor de serviços de segurança geridos (MSSP). Podemos fornecer algumas orientações sobre onde e como usar os serviços em nuvem para ajudar a sua empresa a ficar mais protegida contra ataques cibernéticos e resiliente.

Houve uma altura em que a segurança cibernética não era considerada um “fundamento” da gestão de uma empresa - esse tempo já passou. Precisa de se concentrar nisso da mesma forma que prioriza as suas finanças, relações com clientes e recursos humanos. Nos últimos anos de ataques cibernéticos e violações, aprendemos que não deve esperar até que ocorra um desastre para prestar atenção à segurança cibernética.

Volte em breve para ver os próximos guias da série ou **inscreva-se aqui** para receber uma notificação por e-mail quando forem lançados.

Ao avaliar o risco de segurança cibernética, pense na perda de dados e na continuidade dos negócios.

Se é uma empresa de contabilidade, por exemplo, perder dados de clientes é provavelmente muito pior do que ter o seu site bloqueado durante uma semana. Se vende produtos e serviços online, deixar o seu site bloqueado durante uma semana pode ser extremamente prejudicial.

info@cyberreadinessinstitute.com

A lista completa de guias desta série:

Devo obter suporte externo para gerir o meu risco de segurança cibernética?
(ESTE GUIA)

Introdução aos tipos de suporte externo de TI e segurança cibernética

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
- **Jennifer Khoury**, NCMS
- **Pam Hurt**, NCMS
- **Brian Kelly**, EDUCAUSE
- **Dawn Yankeelov**, TALK
- **Lee Ann Lyle**, 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
- **Lisa McAuley**, GTPA
- **Kiersten Todt**, CRI
- **Chris Caine**, CRI
- **Craig Moss**, CRI
- **Marion Lewis**, CRI
- **Lessie Longstreet**, CRI
- **Ira Sager**, CRI
- **Monica Consiglio**, CRI
- **Vivek Ghelani**, CRI

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.