IBM **Center for Applied Insights**

Um novo padrão para líderes de segurança

Insights do Estudo IBM Chief Information Security Officer de 2013

Estou fazendo o suficiente? Estou concentrado nas coisas certas? Como eu me comparo aos meus colegas? Estas perguntas surgem cada vez mais para Executivos de Segurança da Informação (CISOs) e outros líderes de segurança. Nossa pesquisa descobriu um conjunto das principais práticas de negócios, tecnologia e medição que ajudam a responder a essas perguntas. Ela também revelou uma série de desafios. Até mesmo os líderes de segurança mais experientes lutam com a forma de gerenciar diversos interesses de negócio, criar políticas de segurança móvel e integrar plenamente as métricas de negócio, risco e segurança. Aqueles que têm a combinação certa de práticas e que estão enfrentando esses desafios principais estão evoluindo para líderes de segurança mais versáteis - e estabelecendo um novo padrão.

Sobre o estudo

Ao continuar a expandir o trabalho do Estudo IBM CISO de 2012, intitulado ***Encontrando uma Voz Estratégica***, o IBM Center for Applied Insights, em colaboração com IBM Security Systems e IBM Security Services, realizou entrevistas detalhadas com 41 líderes seniores que são responsáveis pela segurança da informação em suas organizações. O objetivo das entrevistas era identificar práticas e comportamentos organizacionais específicos que poderiam fortalecer o papel e a influência de outros líderes de segurança.

Para manter a continuidade, os entrevistados foram recrutados a partir do grupo de participantes da pesquisa realizada em 2012 - 80 por cento dos recrutados eram participantes anteriores - com ênfase em líderes de segurança mais maduros. Os entrevistados eram de uma ampla gama de indústrias e quatro países. Mais de 80 por cento eram associados a grandes empresas, e cerca de um terço tinha orçamentos de segurança de mais de US$ 1 milhão.

O ambiente de segurança global, conforme descrito no Estudo de CISO 2012, continua a ser exigente. Ameaças cada vez mais sofisticadas e expectativas crescentes de mobilidade são desafios significativos. Talvez como consequência, os líderes de segurança estão ganhando maior atenção dos executivos seniores. Ao mesmo tempo, os líderes de segurança estão aumentando seus esforços para ganhar influência em sua organização.[1] Há também um coro crescente exigindo que os líderes de segurança evoluam para se tornarem especialistas em riscos de informação para suas organizações.[2] Com foco maior no CISO e pedidos para ampliar essa função além de simplesmente defender a empresa, os líderes da organização enfrentam uma série de perguntas-chave: Eu tenho a equipe e as competências certas? Como eu me comparo em relação a outros líderes de segurança na minha indústria? Quais práticas eu devo seguir que atualmente não sigo?

Em nosso Estudo CISO anterior, *Encontrando uma voz estratégica*, começamos a responder a essas perguntas.[3] Nossa análise delineou três tipos diferentes de líder de segurança - Influenciador, Protetor e Respondedor - e examinou a maturidade global e as características de cada um. Nós estabelecemos na época que líderes de segurança mais maduros colocam em funcionamento abordagens de estrutura e gerenciamento mais robustas, têm maior alcance organizacional e medem o desempenho mais rigorosamente.

No estudo deste ano, verificamos um padrão semelhante, mas, indo mais fundo, descobrimos conclusões importantes, principais práticas e um conjunto de deficiências que mesmo líderes de segurança maduros estão lutando contra. Analisando profundamente três áreas - práticas de negócios, maturidade tecnológica e capacidade de medição - um caminho emerge que pode atuar como um guia para novos e experientes líderes de segurança.

.

Práticas de negócios: Falando a linguagem e aliviando as preocupações

Quando foi questionado sobre qual conselho daria a um novo CISO, quais habilidades serão importantes no futuro e como construir a confiança das partes interessadas, os líderes de segurança mais maduros compartilharam um conselho semelhante. Eles recomendam uma ênfase em forte visão, estratégia e políticas, gestão de risco global e relações de negócios eficazes. Eles relatam que constantemente constroem a confiança por meio da comunicação de forma transparente, frequente e com credibilidade. Os líderes de segurança acreditam que essas atividades são cada vez mais importantes, pois são baseadas em suas competências tecnológicas e expandem sua perspicácia empresarial.

"Segurança é difícil, e as pessoas de segurança são únicas. Elas têm um jeito diferente de ver as coisas. Nós tentamos nos afastar da "confusão tecnológica", que não é importante para os negócios. A empresa precisa de praticidade, e não de teoria."

— Diretor de Tecnologia, Seguros

O que os líderes de segurança experientes dizem sobre alcançar o sucesso em sua função

Estratégia e política fortes	"O que é importante ao tomar decisões de segurança? Uma visão estratégica, avaliações de risco e priorização em torno da segurança, compreensão do impacto de novas tecnologias, tendo a capacidade de diferenciar as soluções e escolher os vencedores." (Diretor de TI, Seguros)	"Você precisa de uma consistência global em sua política – em estrutura. Processo é a chave. As pessoas questionam o que elas precisam fazer se você não tem os processos de segurança consistentes." (Vice-presidente executivo de TI, Serviços financeiros)
Gestão de risco global	"As informações da avaliação de risco são usadas para determinar nossa política de segurança. Elas nos ajudam a decidir o quê, onde, quando e como proteger, bem como o custo de fazer isso - o custo para a empresa." (Diretor do Grupo de TI, Manufatura)	"O gerenciamento de risco holístico exige que você compreenda o negócio - o modelo, os pontos de contato com as partes externas, a estrutura regulamentar, os riscos do negócio, e não apenas os riscos de TI." (Diretor de informações, Mídia e entretenimento)
Relações de negócios eficazes	"Conseguir apoio do negócio trata-se de venda. Você precisa de alguém que tenha tino comercial, mas também entenda de tecnologia - que possa falar o valor do negócio e entenda o risco." (Diretor de tecnologia, Seguros)	"Ao trabalhar com a empresa, líderes de segurança devem demonstrar a maior transparência possível, mostrar casos de negócios e alternativas, falar sobre as soluções que correspondem à abordagem de negócios ." (Diretor de TI, Farmacêutica)
Esforços de comunicações combinados	"Para comunicar totalmente o risco, você precisa dar muitos exemplos específicos do que outros hospitais estão fazendo. Nós mostramos trechos de artigos, o que é uma violação em um hospital diferente, bem como as penalidades e as multas." (Diretor de informações, Saúde)	"Relações eficazes requerem muita comunicação, prestando assistência a líderes empresariais e solicitando espaço em suas reuniões para comunicar a importância da segurança, falar sobre vitórias e comunicar os riscos. Você abre mentes quando tem canal constante de comunicação." (Diretor de infraestrutura, Utilitário)

Desafio das práticas de negócios: Gerenciar diversas preocupações de negócios

Muitos líderes de segurança sabem quais são as preocupações de seus executivos seniores. Isso é bom, pois mostra que eles estão envolvidos e se comunicam com toda a organização. Os líderes mais maduros tendem a se reunir regularmente com seu Comitê e executivos seniores, melhorando assim o relacionamento. Não é de surpreender, porém, que cada executivo sênior tem uma preocupação principal de segurança diferente (Figura 1). Os entrevistados disseram que seus CEOs são mais sensíveis em relação ao impacto negativo na reputação da marca ou confiança do cliente. Os CFOs preocupam-se com perdas financeiras devido a uma violação ou incidente. Os COOs perdem o sono com o tempo de inatividade operacional. Finalmente, os CIOs têm um amplo conjunto de preocupações, incluindo violações, perda de dados e execução de investimentos em tecnologia.

	Perda da reputação/ confiança da marca	Perda financeira	Indisponibilidade operacional	Violação de conformidade	Outros
CEO	49%	6%	15%	9%	21%
CIO	26%	0%	24%	18%	32%
CFO	14%	47%	6%	21%	12%
COO	38%	4%	42%	8%	8%
Média	32%	14%	22%	14%	18%

Figura 1 - De acordo com os líderes de segurança, cada membro do C--suite tem uma diferente preocupação principal de segurança.

Esse amplo espectro de preocupações é um desafio difícil. Para ajudar a aliviar essas diversas preocupações, os líderes de segurança que entrevistamos regularmente se reúnem com seu Comitê e executivos seniores, geralmente uma vez por trimestre. Quando eles se encontram, os principais tópicos que discutem incluem identificação e avaliação de riscos (59 por cento), resolução de questões de orçamento e solicitações (49 por cento) e implementação de novas tecnologias (44 por cento). O foco no risco é bom. Ele dá aos líderes de segurança a chance de ajudar a resolver todas as diversas preocupações dos executivos seniores.

O fato de que os líderes de segurança acreditam, em média, que uma perda de reputação da marca ou confiança do cliente é a preocupação de negócio mais importante em suas organizações, isso levanta questões interessantes. Hoje é quase impossível controlar o impacto de violações de segurança e outros incidentes na reputação da marca - mesmo que possa haver um impacto no preço das ações ou percepção do público. Poucos líderes de segurança com quem falamos têm qualquer recurso na área. As preocupações do CEO podem finalmente se concentrar na reputação da marca e na confiança do cliente, mas cabe ao líder de segurança ter as habilidades de negócios e comunicação para descrever realisticamente o que é possível para o executivo sênior. É evidente que é uma área em que a indústria, como um todo, precisa fazer progresso.

Perspectiva do CISO: Encontrar um equilíbrio com líderes de negócio

Por Shamla Naidoo
Vice-presidente, Risco e segurança de informação
Starwood Hotels & Resorts Worldwide, Inc.

A Starwood desenvolveu uma estratégia de segurança abrangente que foi revisada e aprovada pela liderança executiva e o Comitê para certificar que nós protegemos vigorosamente os ativos da empresa e os dados de nossos associados e convidados. Para manter nossos líderes conscientes sobre mudanças na indústria e ameaças em evolução, a equipe de segurança de TI fornece relatórios regulares sobre nossa estratégia e os possíveis riscos de segurança. A natureza orientada ao serviço da indústria de hospitalidade, que opera em um ambiente de negócios em rápida mutação, aumenta o nosso perfil de segurança significativamente. Consequentemente, o debate saudável e o diálogo franco, juntamente com a tomada de decisão ponderada e responsiva, ajudam a garantir que estamos avançando nosso negócio e gerenciando de forma apropriada os riscos de segurança.

O melhor conselho que posso dar aos novos líderes de segurança:

1. Desenvolva uma estratégia de segurança e obtenha adesão executiva para metas e plano.
2. Treine ou contrate experiência prática; você não poderá proteger, se não souber como.
3. Mantenha-se informado sobre a constante mudança de riscos de segurança e considere as questões legais na tomada de decisões de segurança.
4. Entenda como seu negócio gera receitas e encontre formas produtivas para suportar e gerenciar de forma agressiva os riscos que podem afetar o crescimento e a inovação da empresa.
5. Comunique-se com as partes interessadas da empresa para informar e educá-las sobre os riscos e as possíveis soluções, ajudando-as a tornar-se parte de sua organização de segurança.

"Você tem que estar na vanguarda absoluta da tecnologia de negócios e tecnologia de consumo. Bring-your-own-device (BYOD) está começando a abranger quase tudo. Os dispositivos estão proliferando. Os líderes de segurança precisam ser inteligentes, ser esclarecidos. Pensar como o usuário. Pensar no que os usuários estão fazendo."

—Diretor de informações, Financeiro

Tecnologia: Indo além dos princípios básicos

Embora o foco de líderes de segurança esteja mudando para gerenciamento de risco, relações de negócio mais fortes e melhor comunicação, a tecnologia de segurança continua a ser a ferramenta mais importante para o líder de segurança holístico. Na verdade, os entrevistados gastam tempo significativo avaliando a tecnologia (24 por cento, a área global número um).

Muitos dos líderes de segurança veem tecnologias de segurança fundamentais e funcionais como os componentes mais importantes para sua organização. Essas tecnologias incluem Gestão Corporativa de Identidades e Acessos (51 por cento), prevenção de intrusão de rede e análise de vulnerabilidades (39 por cento) e segurança de banco de dados (32 por cento). As tecnologias mais avançadas ou estratégicas ainda não superaram as tecnologias fundamentais em importância, incluindo a detecção avançada de malware (20 por cento), análise de inteligência de segurança (15 por cento) e mecanismos de autenticação alternativos (12 por cento). Vai ser interessante ver como isso muda no futuro.

Apesar das preocupações conhecidas, os líderes de segurança estão avançando com a implementação de segurança móvel e serviços de segurança baseados em nuvem. A segurança móvel é a tecnologia de segurança número um "implantada mais recentemente", com um quarto dos líderes de segurança implantando nos últimos 12 meses. E, embora privacidade e segurança em um ambiente de nuvem ainda sejam preocupações, três quartos (76 por cento) implantaram algum tipo de serviço de segurança em nuvem - o mais popular sendo monitoramento e auditoria de dados, juntamente com identidade federada e gerenciamento de acesso (ambos em 39 por cento).

Muitos dos entrevistados estão escorando suas fundações de segurança ao testar lentamente uma tecnologia mais avançada e estabelecer recursos de nuvem e móveis. Os líderes de segurança não devem perseguir toda nova tecnologia, mas sim concentrar-se naqueles que irão transformar sua abordagem e avançarão seus objetivos de negócio.

Desafio de tecnologia: Avançando todos os aspectos da segurança móvel

No último Estudo CISO, a segurança móvel foi a principal preocupação tecnológica, com mais da metade dos líderes de segurança classificando-a como um grande desafio de tecnologia nos próximos dois anos. A segurança móvel continua a receber atenção significativa: de 14 áreas tecnológicas diferentes, foi classificada como a "mais importante" e a "mais implantada" ao longo dos últimos 12 meses. Embora a mobilidade seja primordial e apoiada por investimentos, os recursos ainda estão amadurecendo.

Hoje, a segurança móvel está em um estágio fundamental do desenvolvimento. As práticas mais frequentemente implantadas estão equipando os dispositivos com uma função de gerenciamento de dispositivos móveis (78 por cento) e criando inventário de dispositivos que usam a rede corporativa ou dados (76 por cento) - primeiros passos típicos ao estabelecer com segurança a mobilidade dentro de uma empresa (Figura 2).

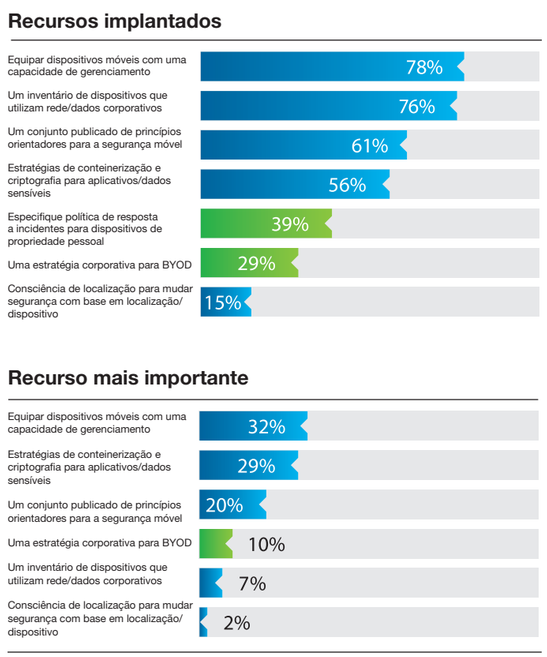

Figura 2 - Política e estratégia de segurança móvel ainda não se tornaram prioridade.

O desafio móvel primário para líderes de segurança é avançar além dos passos iniciais e pensar menos em tecnologia e mais sobre política e estratégia. Para a maioria dos entrevistados, uma política móvel abrangente e estratégia para dispositivos pessoais ainda não são amplamente utilizadas ou consideradas importantes. Menos de 40 por cento das organizações implementou políticas de resposta específicas para dispositivos de propriedade pessoal ou uma estratégia corporativa para *bring-your-own-device* (BYOD), e muito poucos consideram essas ações como "mais importantes".

No entanto, os líderes de segurança estão reconhecendo e abordando esta lacuna. Estabelecer uma estratégia corporativa para BYOD (39 por cento) e uma política de resposta a incidentes para dispositivos de propriedade pessoal (27 por cento) são as duas principais áreas planejadas de desenvolvimento para os próximos 12 meses.

Perspectiva do CISO: Construindo confiança para aliviar a preocupação

Por Ken Kilby, Diretor da Segurança das Informações BB&T

O nosso banco existe há 141 anos, e esperamos estar presente por pelo menos mais 141 anos. Para permitir isso, abordamos segurança e risco como uma equipe, é responsabilidade de todos. No final das contas, tudo que a organização tem é seu nome. Se você não puder manter o acesso seguro para seus clientes, apenas recolha suas coisas e saia do circuito. Assim, nossos controles e políticas, em última análise, têm de se concentrar na reputação.

Para alcançar este objetivo, eu gasto muito do meu tempo construindo a confiança com os executivos C-level e o Comitê. Estou constantemente conversando com os membros individuais do Comitê e a equipe de gerenciamento executivo, desenvolvendo relações pessoais. Diferentes membros do C-level têm diferentes preocupações que eu tenho que resolver.

BYOD também é uma grande preocupação para nós. Estamos tentando acompanhar a tecnologia, mas sempre sentimos como se estivéssemos brincando de pegar o mais recente e maior. Temos que gerenciar e proteger muitas plataformas móveis diferentes - e dado o grande número de malwares emergentes, isso é extremamente difícil.

Há duas recomendações que eu dou aos meus colegas em busca de orientação. A primeira é que os líderes de segurança têm seu jogo. Eles têm que ser capazes de se comunicar com seu Comitê na linguagem que esse Comitê entende. Fiquem envolvidos, e não fiquem presos na rotina do dia a dia. A segunda é algo essencial para meu trabalho: Desenvolver relacionamentos com os contatos que aplicam as leis, parceiros da indústria e legisladores. Promover uma maior comunicação pública e privada, em última instância ajuda a reduzir a superfície de ataque total. Nós podemos fazer mais juntos.

Medição: Criando o ciclo correto de *feedbacks*

Hoje, os líderes de segurança usam métricas principalmente para orientar o orçamento e defender a tese de investimento de novas tecnologias. Em alguns casos, eles usam medidas para ajudar a desenvolver prioridades estratégicas para a organização de segurança. Em geral, porém, as métricas técnicas e de negócios ainda estão focadas em questões operacionais. Por exemplo, mais de 90 por cento dos entrevistados rastreiam incidentes de segurança, registros perdidos ou roubados, dados ou dispositivos e status de auditoria e conformidade - dimensões fundamentais que você espera que todos os líderes de segurança controlem. Poucos entrevistados (12 por cento) estão alimentando métricas de negócio e de segurança em seu processo de risco corporativo, apesar de líderes de segurança afirmarem que o impacto da segurança no risco empresarial geral é o fator de sucesso mais importante.

"Nós usamos métricas para melhorar continuamente nossos processos e conscientização. Elas ajudam a determinar o que acontece a seguir, a fim de permanecer à frente do jogo."

—Vice-presidente executivo de TI, Serviços financeiros

Desafio de medição: Traduzir as métricas de segurança na linguagem da empresa

Essa lacuna entre a importância percebida de alimentar métricas em processos de risco corporativos e realmente fazer isso reflete o desafio que os CISOs e líderes de segurança estão enfrentando. No Estudo de CISO 2012, verificou-se que os líderes de segurança mais maduros medem mais coisas, mais frequentemente (como educação e formação, risco e assim por diante). Mas o que deve ser feito com as informações, como isso deve se comunicar com a empresa para estimular a ação?

Quase dois terços dos líderes de segurança não traduzem métricas em resultados financeiros. Eles carecem de recursos ou requisitos de negócio para fazê-lo, ou é simplesmente muito complexo para calcular. Além disso, mais da metade não integra plenamente métricas de segurança com medidas de risco de negócio (Figura 3). Essa incapacidade de combinar medidas relacionadas de sucesso pode restringir a capacidade dos líderes de segurança para se comunicar com outros líderes empresariais - o que torna mais difícil para eles representarem de forma eficaz e precisa a condição da organização internamente.

Perspectiva do CISO: Medição para o benefício da empresa

Por Felix Mohan, Vice-Presidente Sênior e Diretor Global da Segurança das Informações

Bharti Airtel Limited

Originalmente, nós começamos nosso programa de medição matriz em um nível de gerenciamento tático muito mais operacional. Foi para ajudar a justificar os recursos que precisávamos como um centro de custo. À medida que nos informamos e amadurecemos mais, mudamos o modo de medição para ficar mais estratégico - adicionando risco, conformidade, continuidade de negócios, conscientização e treinamento e tempo de atividade de aplicativo crítico.

Hoje, ainda estamos melhorando o nosso processo matriz, tentando ficar mais automatizado, chegando ao nível de risco da empresa e traduzindo as medidas de segurança em impacto nos negócios. Estamos tentando persistentemente entender melhor a tolerância ao risco da empresa e como medi-la.

Como parte da nossa mais recente iteração matriz, foram identificados todos os processos críticos que sustentam nossos produtos e serviços - coisas que geram receita para a empresa. Nós identificamos toda a infraestrutura de TI e tecnologia da qual esses processos dependem (por exemplo, sistemas e aplicativos, ativos críticos). Nós também respondemos à pergunta: Se esses processos e ativos não estiverem disponíveis, qual seria o tempo de recuperação? Então, classificamos esses processos como ultrassensível, alto, médio e baixo. A classificação determina o quão rápido precisamos recuperar a infraestrutura, variando de algumas horas a alguns dias.

Medida do impacto financeiro

"Medir o impacto financeiro é importante quando queremos implementar a tecnologia. Qual é o ROI, a eliminação de custos de um incidente? Usamos isso para provar que há valor."
(Diretor de Tecnologia, Seguros)

Integrar métricas de TI e risco de negócio

"As métricas de segurança são combinadas com a satisfação do cliente como parte de um escopo mais amplo de continuidade e análise de impacto nos negócios. Cibersegurança é integrada na análise de risco, juntamente com outras questões." (Diretor de TI, Utilitário)

Figura 3 - As deficiências são aparentes na aferição do impacto financeiro, integrando segurança e risco.

Rumo a um líder de segurança mais versátil

O que esses insights e desafios podem nos dizer sobre o foco e a abordagem de líderes de segurança da informação? Eles podem nos ajudar a construir um modelo para medir o progresso? Ou encontrar um caminho para seguir?

Para começar, eles sugerem que os líderes de segurança devem combinar uma estratégia de segurança forte com gerenciamento de risco holístico que considera o impacto econômico da segurança de TI, desenvolvendo relações de negócio eficazes e gerando confiança com líderes seniores. Eles têm que manter as tecnologias de segurança fundamentais, mas não à custa da implementação de recursos mais avançados e estratégicos. Os líderes precisam abordar a segurança móvel de forma mais abrangente - enfatizando a política e permitindo o uso de dispositivos de propriedade pessoal.

Eles também devem criar os ciclos corretos de *feedbacks*. Tanto a tecnologia de segurança quanto as métricas de negócios devem ser incorporadas no processo de gerenciamento de risco, não apenas como itens de linha, mas por meio de uma integração profunda. Essas métricas devem ser traduzidas na linguagem da organização. Sem isso, a segurança não pode permitir as iniciativas de negócios, e torna-se mais difícil de racionalizar a necessidade de gastos com projetos de segurança em toda a organização.

Traçando um caminho para maior desempenho do CISO

Alguns dos líderes de segurança entrevistados estavam mais próximos desse modelo de versatilidade do que outros, no entanto, poucos estavam fazendo tudo o que o modelo implicava. Aqueles que têm a combinação certa de práticas de negócios, tecnologia e capacidade de medição e estão abordando os principais desafios definem o padrão de maturidade na liderança de segurança. Eles estão transformando o papel que a segurança da informação desempenha em suas organizações. Eles estão demonstrando o domínio de uma série de disciplinas, relacionadas tanto à tecnologia quanto ao negócio - e avançando no que está rapidamente se tornando um renascimento na liderança de segurança.

Para obter mais informações

Você pode saber mais sobre a mudança de papel da liderança de segurança acessando ibm.com/ibmcai/ciso.

Práticas de negócios

Etapas essenciais
Formalize seu papel como CISO para ter a certeza de que é reconhecido como o líder de segurança sênior único com autoridade organizacional e orçamentária.
Estabeleça uma estratégia de segurança que seja atualizada regularmente, amplamente divulgada e desenvolvida em conjunto com outras estratégias da organização (como desenvolvimento de produto, risco e crescimento).
Desenvolva relações de negócio eficazes e se reúna com os executivos seniores e o Comitê com frequência e desenvolva uma abordagem para gerenciar suas diversas preocupações. Leve essas preocupações em consideração ao determinar o que medir.
Construa confiança ao se comunicar com as partes interessadas da empresa de forma transparente, frequente e com credibilidade.

Tecnologia

Etapas essenciais
Invista em tecnologia avançada quando esta suportar uma meta de negócio. Não gaste todos os seus recursos apenas em tecnologias de segurança fundamentais; busque tecnologias avançadas e métodos que irão transformar a sua abordagem.
Fortaleça sua segurança móvel, não apenas com tecnologia, mas também com um conjunto de práticas e políticas de negócios - para dispositivos de propriedade individual e da empresa.
Compartilhe informações com outros grupos, incluindo colegas da indústria. Isto irá melhorar a sua confiança [como você faz investimentos em tecnologia] e ajudar a responder a perguntas sobre prioridades de segurança e práticas de liderança.

Medição

Etapas essenciais
Concentre-se no impacto econômico de risco geral para a organização ao invés de apenas na auditoria e conformidade. Determine como proteger a empresa e entenda o impacto da segurança no valor e reputação da marca.
Aborde preocupações sobre o risco reputacional e a satisfação do cliente com seu Comitê e executivos seniores (C-level), descrevendo de forma realista o que for possível.
Traduza métricas em impactos financeiros e integre totalmente as métricas de risco de TI e negócios.

Figura 4 - Etapas essenciais para se tornar um líder de segurança mais forte.

Sobre os autores

Marc van Zadelhoff, Vice-Presidente, Gerenciamento de Estratégia e Produto, IBM Security Systems
Nessa função, ele é responsável pelo gerenciamento geral de ofertas, orçamento e posicionamento para o portfólio global de serviços e software de segurança da IBM. Seu e-mail marc.vanzadelhoff@us.ibm.com.

Kris Lovejoy, Gerente Geral, IBM Security Services
Nessa função, ela é responsável pelo desenvolvimento e entrega de serviços de segurança gerenciados e profissionais para os clientes da IBM em todo o mundo. Antes de sua função em Serviços, Kris foi vice-presidente da IBM de Risco de Tecnologia da Informação e CISO Global, responsável pelo gerenciamento, monitoramento e testes de funções de resiliência e segurança corporativa da IBM em nível mundial. Seu e-mail é klovejoy@us.ibm.com.

David Jarvis, Gerente, IBM Center for Applied Insights Insights
David é especialista em pesquisa baseada em fatos sobre tópicos emergentes de tecnologia estratégia e empresarial. Ele é coautor de uma série de estudos de segurança da IBM, incluindo a 2012 IBM CISO Assessment e *Educação em cibersegurança para a próxima geração*
Seu e-mail é djarvis@us.ibm.com.

Agradecimentos especiais

Caleb Barlow, *Diretor, Segurança móvel, Segurança de aplicativo, Segurança de dados, Segurança de infraestrutura crítica*

David Puzas, *Executivo de Marketing Global, IBM Security Services*

Adam Trunkey, *Gerente de Marketing Global, IBM Security Services*

Sobre o IBM Center for Applied Insights

ibm.com/ibmcai

O IBM Center for Applied Insights apresenta novas maneiras de pensar, trabalhar e liderar. Através de pesquisa baseada em evidências, o Center equipa os líderes com orientação pragmática e o caso de mudança.

Notas e fontes

[1] Gottlieb, Joe. “Being great: Five critical CISO traits.” SC Magazine. 13 de junho de 2013. http://www.scmagazine.com/being-great-five-critical-ciso-traits/article/298686/

[2] Ashford, Warwick. “CISOs must shape up or ship out, says Forrester.” *ComputerWeekly.com.* 11 de junho de 2013. http://www.computerweekly.com/blogs/david_lacey/2013/07/where_next_for_the_enterprisin.html

[3] *Encontrando uma voz estratégica: Insights do 2012 IBM Chief Information Security Officer Assessment.* IBM. Maio de 2012. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=CIE03117USEN

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produzido nos Estados Unidos da América

Outubro de 2013

CIW03087-USEN-00