- **Alavancar a inteligência proveniente de diversas fontes** utilizando a segurança como serviço, incluindo os serviços de segurança baseados em nuvem da IBM, o serviço de proteção de presença na web da IBM e a Proteção Avançada contra Fraudes da Trusteer
- **Realizar um benchmarking da maturidade com relação a seus pares** e definir um roadmap de transformação com o benchmarking de maturidade de segurança da IBM e a Avaliação de Riscos de Segurança da IBM
- **Integrar sua plataforma de segurança** com o IBM Security Framework de soluções e com os Serviços de Otimização de Operações de Segurança da IBM
- **Tirar proveito da profunda experiência em segurança** com os serviços de Consultoria de Segurança da IBM, o IBM X-Force® e as pesquisas da Trusteer

Para obter mais informações

Para saber mais sobre as Soluções IBM Security, entre em contato com seu representante de vendas IBM ou Parceiro Comercial IBM, ou visite: **ibm.com**/security/ciso

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produzido nos Estados Unidos da América em
Março de 2014

[1] "2013 Cost of Cyber Crime Study," *Ponemon Institute*, outubro de 2013. http://media.scmagazine.com/documents/54/2013_us_ccc_report_fi l_6-1_13455.pdf
[2] "A new standard for security leaders: Insights from the 2013 IBM Chief Information Security Officer Assessment," *IBM Corp.*, outubro de 2013. http://public.dhe.ibm.com/common/ssi/ecm/en/ciw03087usen/CIW03087USEN.PDF
[3] IBM Global Technology Services, "Understanding the economics of IT risk and reputation: Making the business case for business continuity and IT security," *IBM Corp.*, novembro de 2013. http://www-935.ibm.com/services/us/gbs/bus/html/risk_study.html
[4] Jon Oltsik, Kristine Kao e Jennifer Gahm, "Security Management and Operations: Changes on the Horizon," *ESG Research*, 23 de julho de 2012. http://www.esg-global.com/research-reports/security-management-and-operations/
[5] A Trusteer, Ltd. foi adquirida pela IBM em setembro de 2013.
[6] A Fiberlink Communications foi adquirida pela IBM em dezembro de 2013.

WGF12346-BRPT-00

Prepare-se para uma nova era de segurança

Beneficie-se da experiência, análise e da abordagem sistemática com a IBM Security

Vivemos uma nova realidade de segurança

Atualmente, os ataques à segurança são bem financiados e realizados com uma precisão semelhante à com que negócios são conduzidos. E à medida que tecnologias como as de nuvem, dispositivos móveis, big data e mídias sociais são mais difundidas, os ataques a empresas se tornam mais sofisticados e custosos. Estima-se que o custo de apenas uma violação chegue a inacreditáveis US$ 11 milhões.[1]

Para os Chief Information Security Officers (CISOs), as ameaças crescentes configuram uma prioridade. Líderes de segurança indicam que a segurança de dispositivos móveis é a tecnologia implantada mais recentemente.2 No entanto, para todas as empresas que estão implementando defesas, outras seguem desprotegidas. Enquanto isso, os perímetros de rede da forma que os conhecemos estão desaparecendo, e a tecnologia que as organizações vinham utilizando para proteger essas fronteiras está se tornando obsoleta. Os negócios deixaram de ser conduzidos dentro dos limites da organização. E à medida que os pontos de extremidade se proliferam, os ambientes de segurança se tornam mais complexos - e as lacunas na qualificação continuam se expandindo.

Mais de um terço dos executivos de segurança não têm uma estratégia de riscos.[3]

A chave para que os líderes de segurança superem esses desafios é adotar uma estratégia de proteção dinâmica que possa evoluir com o panorama de ameaças - e encontrar um parceiro de segurança capaz de fornecer a tecnologia, a especialização e a experiência para ajudar a assumir o controle da nova realidade da segurança.

Tome medidas para fazer com que a segurança seja estratégica

Todas as empresas e todos os setores são vulneráveis a ataques. Ainda assim, frequentemente se passam meses antes que muitas delas sequer saibam que foram invadidas. Organizações despreparadas para a nova era da segurança estão assumindo riscos perigosos. Na verdade, apenas cerca de metade das organizações integram métricas de TI e de negócios para compreender o impacto financeiro potencial de uma violação de segurança.[2] A seguir, os aspectos imprescindíveis para estar melhor protegido:

Proteger os negócios

Riscos de segurança representam uma ameaça cara e persistente para os negócios em termos de vendas, perda de confiança do cliente e, algumas vezes, um duradouro desgaste da marca. Líderes de negócios esperam que os CISOs forneçam uma muralha de proteção.

Adotar as tecnologias disruptivas

Conforme tecnologias disruptivas como as tecnologias de nuvem, dispositivos móveis, big data e mídias sociais assumem residência permanente no mundo dos negócios, os líderes de segurança buscam maneiras de utilizá-las estrategicamente para fortalecer a segurança.

Abandonar medidas tradicionais

A abordagem tradicional de implantar uma nova ferramenta de segurança para lidar com cada novo risco deixou muitas organizações com uma rede fragmentada que é cara, complexa e privada de uma visibilidade integral do cenário de segurança.

Preparar-se hoje

Ao adotar uma nova estratégia de segurança — e compreender as habilidades que conferem eficácia a essa estratégia —, os CISOs são capazes de posicionar estrategicamente a organização, hoje, para enfrentar ameaças que ainda serão criadas.

Prepare-se para o ataque inevitável

Para evitar violações de segurança, os CISOs precisam fornecer às suas equipes de segurança um treinamento sólido e as ferramentas líderes do setor de que elas precisam - e, então, complementar as habilidades internas por meio de parcerias com consultores, utilizando serviços gerenciados e compreendendo pesquisas avançadas em segurança.

Sua equipe deve estar treinada para pensar como os invasores e agir estrategicamente. Comece identificando os ativos de maior importância para seus negócios - funcionários, dados ou transações - e proteja-os colocando em prática um robusto sistema de inteligência em segurança capaz de:

- Monitorar o acesso a dados para ajudar a bloquear ameaças
- Conhecer seus usuários para ajudar a evitar fraudes
- Identificar anomalias e acessos não autorizados
- Aplicar análise em tempo real para detectar indicadores de ataques.

Oitenta e três por cento das empresas consideram que é difícil contratar profissionais de segurança.[4]

Para estar preparado para as inevitáveis violações de segurança, sua estratégia de segurança deve capacitá-lo a:

- **Limitar o impacto de uma violação** com um plano e uma equipe de resposta a incidentes
- **Certificar-se de que as tecnologias de nuvem, dispositivos móveis, mídias sociais e big data sejam ainda mais seguras** do que as tecnologias localizadas nas instalações
- **Empregar alternativas baseadas em riscos** onde for possível
- **Testar incansavelmente a conformidade** com padrões
- **Implementar prontamente mudanças** de controles e políticas
- **Aplicar inteligência e automação** para reduzir surpresas e facilitar tarefas rotineiras

Soluções da IBM para proteger os negócios

A IBM compreende suas necessidades como CISO. Nós oferecemos tecnologias testadas e comprovadas, criadas para proteger contra uma gama de ameaças à segurança e ajudá-lo a:

- **Transformar big data em inteligência de segurança acionável,** com as soluções de inteligência em segurança da IBM e os serviços de gerenciamento e monitoramento de ameaças da IBM.
- **Proteger ativos sensíveis** com o Programa de Proteção "Crown Jewels" da IBM, os Serviços de Gestão de Acesso e Identidade da IBM® e a Segurança de Aplicativos e Dados da IBM.
- **Implementar defesas de última geração** utilizando os Serviços de Respostas a Emergências da IBM, os dispositivos do IBM Security Network Protection e as soluções da Trusteer[5] contra crimes cibernéticos.
- **Manter o controle da nuvem** com as soluções de segurança de nuvem da IBM.
- **Garantir a segurança de dispositivos móveis** com as soluções de segurança IBM MobileFirst, as soluções contra fraudes em dispositivos móveis da Trusteer e as soluções de segurança para dispositivos móveis IBM Fiberlink[6].