IBM Center for Applied Insights

Encontrando uma voz estratégica

Insights do Estudo com IBM Chief Information Security Officer 2012

IBM

Sobre o estudo

Para obter uma visão global das estratégias e abordagens dos líderes de segurança, o IBM Center for Applied Insights conduziu entrevistas não identificadas com 138 desses líderes, os executivos de TI e de linha de negócios responsáveis pela segurança da informação em suas empresas. Entre esses líderes, alguns eram Chief Information Security Officer (CISO), mas não todos, dada a diversidade das estruturas organizacionais. O Center complementou essa pesquisa quantitativa com conversas detalhadas com 25 líderes de segurança da informação.

Os participantes abrangiam diversos segmentos de mercado e sete países diferentes. Cerca de 20% dos entrevistados comandam a segurança da informação em empresas com mais de 10 mil funcionários e 55% estão em empresas com 1.000 a 9.999 funcionários.

Este estudo e os outros recursos de gerenciamento de risco e segurança para CIOs e CISOs estão disponíveis em ibm.com/smarter/cai/security.

Com o grande aumento da conectividade e da colaboração, o gerenciamento da segurança da informação está se tornando cada vez mais complexo e difícil. Apesar disso, algumas organizações de segurança estão enfrentando o desafio. Nossa pesquisa revela um padrão de progressão distinto – e as características que distinguem aqueles que são mais confiáveis e capazes.

Esses pensadores com ideias avançadas estão adotando abordagens mais estratégicas, proativas e integradas para a segurança, destacando os modelos que devem ser seguidos e as funções de liderança de negócios emergentes do Chief Information Security Officer (CISO).

No mundo atual, extremamente conectado, a segurança da informação está se expandindo além de seu campo técnico para uma prioridade estratégica corporativa. Basta dar uma rápida olhada sobre as notícias recentes para entender o motivo. Em 2011, o mundo corporativo observou a segunda maior perda de dados desde 2004[1].

Os líderes de segurança estão passando por um período de mudanças significativas. A TI não está mais limitada aos departamentos administrativos ou mesmo à empresa. Cadeias de valores inteiras, de fornecedores a clientes, estão conectadas eletronicamente e em colaboração como nunca antes visto. Os dispositivos e as formas de acesso à informação estão se proliferando. Espera-se que o número de funcionários remotos chegue a 1,3 bilhão em 2015. Ao mesmo tempo, as ameaças à segurança remota cresceram quase 20% em 2011[2]. Esse cenário aumenta bastante a vulnerabilidade.

Enquanto muitas organizações continuam no modo de resposta à crise, algumas adotaram uma postura reativa e estão desenvolvendo ações para reduzir o risco futuro. Elas se consideram mais desenvolvidas em seus recursos relacionados à segurança e mais preparadas para enfrentar as novas ameaças. O que essas empresas fizeram para gerar mais confiança? E o mais importante, as ações dessas empresas podem mostrar uma solução para as outras?

"Os líderes de segurança estão se integrando cada vez mais aos negócios, e se tornando mais independentes da tecnologia da informação."

– VP Sênior de TI, Energia e Serviços Públicos[3]

O cenário de segurança em transformação: O que aprendemos

Com o desafio de proteger alguns dos bens mais importantes das empresas, como ativos financeiros, dados de clientes, propriedade intelectual e até a própria marca, os líderes de segurança estão sob grande pressão. As descobertas do nosso estudo apontam para maiores mudanças na atitude e no reconhecimento claro da importância estratégica da segurança da informação:

- **Os líderes de negócios estão cada vez mais preocupados com as questões de segurança.** Quase dois terços dos líderes de segurança dizem que seus executivos seniores se preocupam mais com segurança hoje do que há dois anos, principalmente pela atenção à mídia.
- **Espera-se que os orçamentos aumentem.** Dois terços dos líderes de segurança esperam que o investimento em segurança da informação aumente nos próximos dois anos. Entre eles, quase 90% prevê um crescimento de dois dígitos. Um em cada dez espera um aumento de 50% ou mais.
- **A atenção está se voltando ao gerenciamento de risco.** Em dois anos, os líderes de segurança esperam investir mais tempo na redução de futuros riscos em potencial, e menos em mitigação das ameaças atuais e no gerenciamento de questões regulamentares e de conformidade.

- **As ameaças externas representam o principal desafio de segurança.** Atraindo muito mais atenção que as ameaças internas, a introdução à tecnologia ou a conformidade regulamentar, as ameaças externas estão no topo das listas de preocupações com segurança.
- **A segurança remota é o foco principal.** Com o crescimento da mão de obra remota e a alta taxa de adoção de dispositivos wireless, mais da metade dos líderes de segurança dizem que a segurança remota será o maior desafio tecnológico nos próximos dois anos.

Em todas as categorias, há um consenso sobre a grande importância da segurança da informação. E muitas empresas dizem ter uma função de segurança centralizada. Entretanto, ao olhar com mais cuidado para as ações, planos e estratégias dos líderes de segurança, percebe-se uma grande diferença no modo como as organizações realmente implementam a segurança "centralizada".

Autoavaliação da maturidade e do preparo

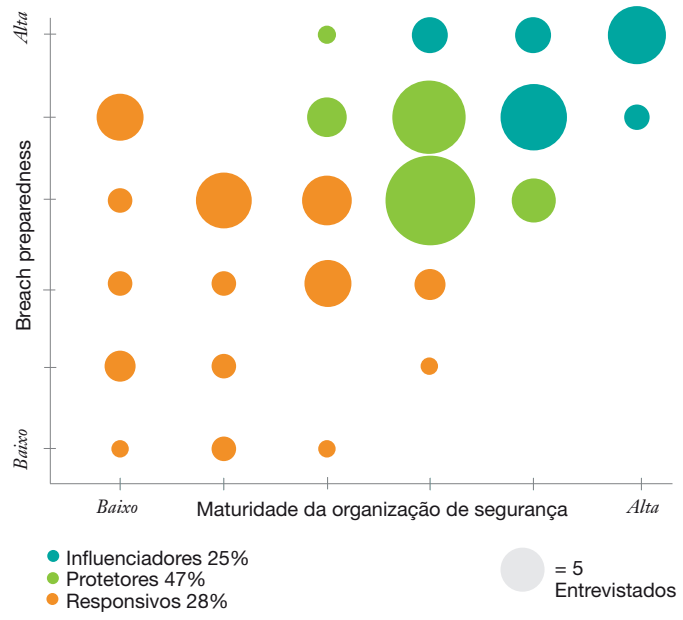

Figura 1: Apenas um quarto dos líderes de segurança acredita que suas organizações são maduras e possuem grande confiança em suas habilidades para evitar ou conter uma violação.

"Os líderes de segurança estão mais responsáveis pelos negócios agora. O público está se expandindo".

– CIO, Seguro

As organizações estão realmente preparadas?

Quando os líderes de segurança classificam a si mesmos em relação à maturidade e habilidade de suas organizações para lidar com violações, ou impedi-las, três tipos de organizações se destacam, como mostra a Figura 1:

- **Influenciadores:** os membros deste grupo, 25% dos entrevistados, veem suas organizações de segurança como avançadas, e se consideram muito bem-classificados em maturidade e preparo. Esses líderes de segurança possuem influência de negócios e autoridade, uma voz estratégica na empresa.
- **Protetores:** abrangendo quase metade dos entrevistados, esses líderes de segurança reconhecem a importância da segurança da informação como uma prioridade estratégica. Entretanto, há uma falta significativa de insight de medida e da autoridade de orçamento necessária para a transformação completa da abordagem de segurança de suas empresas.
- **Responsivos:** este grupo permanece em grande parte no modo de resposta, trabalhando para proteger a empresa e cumprir com os regulamentos e padrões, esforçando-se para fazer uma estratégia progredir. Eles podem ainda não ter os recursos ou a influência de negócios para impulsionar uma mudança significativa.

Saber que algumas empresas estão muito confiantes enquanto outras veem obstáculos levanta uma questão importante. O que os Influenciadores fazem de diferente?

O que faz os Influenciadores se destacarem

Curiosamente, esses três segmentos de segurança não são tendências para determinadas localidades. A combinação de tamanhos de segmentos de mercado, geografias e empresas é, em geral, consistente em todos os grupos. As diferenças principais são encontradas em seus perfis de segurança da informação, sua estrutura, escopo e prestação de contas. Por meio de uma análise das respostas dos líderes de segurança, foi descoberto um padrão de evolução diferente entre as organizações de segurança (consulte a Figura 2) e as características distintivas entre aquelas mais avançadas.

"Os líderes de segurança da informação terão mais autoridade sobre o assunto. A influência e o poder de tomada de decisão aumentarão na empresa."

– Líder da Divisão de TI, Mídia e Entretenimento

Perfis de segurança

		Responsivos	Protetores	Influenciadores
Estrutura e gerenciamento	CISO dedicado	26%	42%	56%
	Comitê de segurança/risco	26%	52%	68%
	Item de linha de orçamento	27%	45%	71%
	Autoridade de orçamento	CIO (30%) VP/Diretor/Gerente de TI (24%) CFO (18%)	CIO (32%) CFO (20%) CEO (20%)	CIO (26%) CEO (26%) CISO (13%)
Alcance organizacional	Atenção da liderança ampliada	50%	68%	77%
	Tópico de comitê regular	22%	58%	60%
	Foco principal nos próximos dois anos	Novas tecnologias de segurança (46%) Atualização de processos de negócios (36%)	Formação de funcionários (53%) Novas tecnologias de segurança (42%)	Formação de funcionários (59%) Comunicação/ colaboração (24%)
Medida	Métricas padronizadas	26%	43%	59%

Figura 2: Influenciadores são mais suscetíveis a elevar a segurança da informação a uma prioridade estratégica.

Estrutura e gerenciamento

Como as equipes de gerenciamento sênior reconhecem a necessidade de uma abordagem coordenada, as organizações no grupo de Influenciadores estão mais suscetíveis à nomeação de um CISO, um líder dedicado com alcance corporativo estratégico. Os Influenciadores também devem possuir um comitê de direcionamento de segurança liderado por um executivo sênior, geralmente o CISO. O principal objetivo do comitê é avaliar os problemas de segurança holisticamente e desenvolver uma estratégia corporativa integrada. É responsável pelas mudanças sistêmicas que ampliam as funções, incluindo a área jurídica, de operações de negócios, finanças, recursos humanos entre outras.

A grande maioria dos Influenciadores se beneficia de um item de linha de orçamento de segurança dedicado que suporta seus esforços. Entre todos os entrevistados, os CIOs geralmente controlam o orçamento da segurança da informação. Entretanto, nas organizações Protetoras e Influenciadores, as autoridades de investimento confiam em líderes de negócios com mais frequência. Na realidade, os Influenciadores dizem que os CEOs direcionam os orçamentos de segurança da informação tanto quanto os CIOs.

Entre os Responsivos, CISOs e comitês de direcionamento não são tão comuns, o que sugere que sua abordagem de segurança seja mais tática e fragmentada. A ausência de um item de linha de orçamento dedicado pode levar as organizações de segurança a negociarem constantemente por financiamento ou limitar o escopo de iniciativas para funções ou áreas específicas.

Uma perspectiva de um CISO: Visão mais ampla, função mais extensa

Por Paul Connelly

Vice-Presidente e Chief Information Security Officer, Hospital Corporation of America

A função do líder de segurança está mudando em razão de diversas dinâmicas essenciais. O valor e o volume das informações aumentam em muitas empresas. As ameaças a essas informações se tornam mais sofisticadas e prejudiciais, e o impacto dos colapsos de segurança se tornam mais custosos. As expectativas para a proteção das informações estão maiores entre os líderes de negócios, clientes e o público em geral.

Como resultado, os líderes de segurança precisam se concentrar em maneiras inovadoras e eficientes para proteger os dados da empresa, além de ter uma visão ampliada da proteção da informação, que vai além das medidas de segurança. A prioridade e os investimentos na proteção da informação devem ser uma decisão de negócios, que conduz uma mudança nas estruturas de relatório tradicionais em TI. O alinhamento com gerenciamento de risco e privacidade, recuperação de desastre, planejamento de continuidade de negócios e segurança física oferece uma vantagem clara. É possível eliminar potencialmente a sobreposição, criar sinergias e conduzir o desempenho da empresa para a proteção da informação, permitindo que o líder de segurança se torne um protagonista do gerenciamento de risco de informações extensivas.

Alcance organizacional

Os Influenciadores possuem a atenção dos líderes de negócios e de seus comitês. A segurança não é um tópico ad hoc, mas sim uma parte regular dos debates de negócios e, progressivamente, da cultura. Esses líderes compreendem a necessidade de uma consciência generalizada do risco, e estão mais concentrados na formação, colaboração e comunicação corporativa (consulte a Figura 3). Eles trabalham junto com as funções de negócios para criar uma cultura na qual os funcionários adotem posturas mais proativas em relação à proteção da empresa. Como estão mais integradas aos negócios, essas organizações de segurança também são capazes de influenciar o design de novos produtos e serviços, incorporando considerações de segurança no início do processo.

Diferenças de foco nos próximos dois anos

Responsivos		Influenciadores
	Aprimoramento da comunicação e colaboração corporativas	**4x** *mais*
	Fornecimento de formação e desenvolvimento de consciência	**2x** *mais*
2x *mais*	Incorporação de novas tecnologias para preencher as lacunas atuais	

Figura 3: Com tecnologias de segurança de base e práticas em vigor, os Influenciadores estão voltando a atenção às pessoas e criando uma cultura de consciência do risco.

Os Responsivos são mais voltados às táticas. Eles se concentram na construção de bloqueios na base: incorporam novas tecnologias de segurança para preencher as lacunas, desenvolvem os processos de negócios e contratam novas equipes. Embora a tecnologia e os processos de negócios ainda sejam importantes para os Influenciadores, eles continuam inovando e aprimorando ao invés de estabelecer recursos básicos.

Nos três grupos, a segurança remota é o maior desafio técnico, dominando as pautas dos Responsivos (60%) e Protetores (63%). Entretanto, entre os Influenciadores, a segurança remota é parte de uma estratégia de ponta a ponta. Esses Influenciadores se concentram não apenas na segurança do acesso remoto (33%), mas também em proteção da nuvem (30%) e armazenamento de banco de dados (30%).

"Os líderes de segurança se tornarão essenciais para suas organizações. Seus orçamentos aumentarão e eles sairão da margem e serão incorporados."

– Líder da Divisão de TI, Mídia e Entretenimento

Medida

Os Influenciadores são duas vezes mais suscetíveis a rastrear seu progresso que os Responsivos. Considerando a intenção de criar uma cultura de consciência do risco, essas organizações medem mais a consciência e os programas educacionais do usuário que os Protetores e os Responsivos (consulte a Figura 4). Como estão preocupados com riscos mais amplos e sistêmicos, os Influenciadores também são mais propensos a avaliar suas habilidades para lidar com ameaças futuras e a integração de novas tecnologias. De maneira geral, os Influenciadores não apenas ganham a atenção dos líderes de negócios e trabalham de forma colaborativa na empresa, como também estão se tornando responsáveis pelo processo de medidas formais.

"Em geral, a função da segurança da informação está se deslocando de riscos específicos para riscos gerais. A função será muito mais ampla do que costumava ser".

– Diretor Financeiro, Seguros

Perfis de segurança

Figura 4: Os Influenciadores são mais propensos a medir o progresso por meio de uma ampla variedade de métricas e se preocupam mais com a mudança sistêmica que os outros grupos.

A perspectiva de um CISO: Por que a medida é importante?

Por John Meakin

Líder Global de Soluções de Segurança e Arquitetura, Deutsche Bank

Considerando a natureza dinâmica do desafio, a medida do estado de segurança nas organizações é cada vez mais importante. Como as ameaças estão sempre mudando e as soluções são mais complexas, dinâmicas e, muitas vezes, parciais, é essencial saber onde você está.

Os indicadores de liderança poderiam incluir uma variedade de medidas do número de aplicativos que tiveram requisitos de segurança específicos definidos e foram testados antes de serem lançados na mesma rapidez e integridade na correção das vulnerabilidades conhecidas.

À medida que as pessoas acessam as informações a partir de uma variedade cada vez maior de dispositivos, é mais difícil protegê-las. As organizações precisam rastrear os servidores e terminais que armazenam grandes quantidades de informações.

Ainda que as métricas sejam um desafio para definição e captura, elas não devem impedir que as organizações as implementem. As medidas podem ser imprecisas a princípio, mas serão aprimoradas ao longo do tempo. E o próprio processo pode conduzir insight de valor.

O caso para a liderança de segurança

Apesar das constantes ameaças e do crescimento da variedade de riscos, algumas organizações estão mais confiantes e capazes. Suas abordagens destacam a importância de um objetivo mais amplo para a função da segurança, além de uma função mais estratégica para os líderes de segurança da informação. Ainda assim, a adoção desta estratégia mais holística envolve uma mudança significativa.

Os líderes de segurança devem assumir uma posição de liderança de negócios e desfazer a ideia de que a segurança da informação é uma função de suporte de tecnologia. Seu escopo deve abranger uma mudança educacional e cultural, e não apenas dos processos e das tecnologias de segurança. Os líderes precisarão reorientar suas organizações de segurança para o gerenciamento proativo de risco ao invés de orientar para resposta e conformidade à crise. O gerenciamento da segurança da informação deve migrar de iniciativas distintas e fragmentadas para uma abordagem sistêmica e integrada. A segurança deve ser projetada para proteger e empresa toda, e não apenas algumas partes dela.

Para atingir esses objetivos, os líderes de segurança devem criar um plano de ação com base em seus recursos atuais e suas necessidades mais urgentes. Eles também precisarão obter suporte de todo o nível C de executivos para conduzir a mudança corporativa.

Os Responsivos podem se deslocar para além do foco tático ao:

- Estabelecer uma função de liderança de segurança dedicada (como um CISO), formar um comitê de segurança e risco e medir o progresso
- Automatizar os processos de segurança de rotina para dedicar mais tempo e recursos às inovações de segurança

Os protetores podem fazer da segurança mais do que uma prioridade estratégica ao:

- Investir mais em seus orçamentos para reduzir riscos futuros
- Alinhar as iniciativas de informações de segurança para ampliar as prioridades da empresa
- Aprender e colaborar com uma rede de parceiros de segurança

Os Influenciadores podem continuar a inovar e promover suas abordagens de segurança ao:

- Fortalecer a comunicação, a formação e as habilidades de liderança de negócios para cultivar uma cultura de consciência do risco
- Usar insights de métricas e análise de dados para identificar áreas de aprimoramento de grande valor

A abordagem, o alcance estratégico e os sistemas de medida integrados dos Influenciadores apontam para um novo tipo de organização de segurança e uma nova geração de líderes. Esses líderes de segurança com pensamento avançado podem progredir constantemente, pois possuem autoridade, responsabilidade na prestação de contas e impacto. Ao seguir esse exemplo, aqueles que não seguem esse modelo podem começar a encontrar suas vozes estratégicas.

Para mais informações

Visite o website IBM Center para Applied Insights information security (**ibm.com**/smarter/cai/security) para insights adicionais, incluindo perspectivas de líderes de segurança da IBM. Além disso, é possível colaborar com parceiros em todo o mundo como parte do IBM Institute for Advanced Security (instituteforadvancedsecurity.com).

Sobre os autores

David Jarvis é Senior Consultant no IBM Center for Applied Insights, onde é especialista em pesquisa baseada em fatos sobre negócios emergentes e tópicos de tecnologia. Além de suas responsabilidades de pesquisa, David é professor de previsão de negócios e resolução criativa de problemas. Pode ser contatado através do email: djarvis@us.ibm.com.

Marc van Zadelhof é Vice President of Strategy para o IBM Security Systems. Nesta função, ele é responsável pelo gerenciamento geral de ofertas, orçamento e posicionamento para o portfólio de serviços e software de segurança global da IBM. Pode ser contatado através do email: marc.vanzadelhof@us.ibm.com.

Jack Danahy é Director for Advanced Security do IBM Security Systems. Ele é palestrante nacional e escreve sobre redes de computador e segurança de dados. É membro distinto do Ponemon Institute. Além disso, Jack contribui com frequência em grupos de segurança governamental e de segmento de mercado nas áreas de privacidade de dados, cibersegurança, ciberameaças e proteção de infraestrutura essencial. Ele pode ser contatado através do email: jack.danahy@us.ibm.com.

Colaboradores

IBM Center for Applied Insights

Angie Casey, Steve Rogers, Kevin Thompson

IBM Market Development & Insights

Subrata Chatterjee, Doron Shiloach, Jill Wynn

Escritório do IBM CIO

Sandy Hawke, Kris Lovejoy

IBM Security Systems

Tim Appleby, Tom Turner

Sobre o IBM Center for Applied Insights

O **IBM Center for Applied Insights (ibm.com/smarter/cai/value)** apresenta novas maneiras de pensar, trabalhar e liderar. Por meio de pesquisas com base em evidências, o Center oferece aos líderes um guia pragmático e o caso para a mudança.

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo - SP
Brasil

A página inicial da IBM pode ser localizada em:
ibm.com

[1] *Verizon 2012 Data Breach Investigations Report.* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

[2] "Mobile Worker Population to Reach 1.3 Billion by 2015, According to IDC." Janeiro de 2012. http://www.idc.com/getdoc.jsp?containerId=prUS23251912

[3] Todas as citações de mercado foram extraídas da pesquisa IBM Center for Applied Insights.

Por favor, recicle

CIE03117-BRPT-00