Ernst & Young agora é EY.

APOIADOR OFICIAL

COM RIO 2016

Criando confiança no mundo digital

Pesquisa Global da EY sobre Segurança da Informação - 2015

Insights sobre governança, risco e compliance

EY
Building a better working world

Conteúdo

Bem-vindo à pesquisa **Criando Confiança no Mundo Digital**

Paul van Kessel
Líder Global de Riscos da EY

Ken Allan
Líder Global de Segurança da Informação da EY

A Pesquisa Global da EY sobre Segurança da Informação – 2015, em sua 18ª edição, investiga as questões mais críticas relacionadas à segurança cibernética enfrentadas atualmente pelas organizações.

Este ano nos sentimos realizados em ter 1.755 organizações participando da pesquisa, que tem como base as visões extraídas dos resultados e da nossa vasta experiência global em trabalhar com clientes, no sentido de melhorar suas soluções de segurança cibernética.

No ano passado identificamos como as organizações podem estar à frente do crime cibernético seguindo uma jornada de três fases - Ativar, Adaptar e Antecipar. Este conceito ainda se aplica, mas como ataques cibernéticos estão continuamente mudando suas táticas, aumentando sua persistência e expandindo suas capacidades, a natureza das ameaças cibernéticas evoluiu. Ataques cibernéticos estão atualmente encontrando novas e melhores maneiras de tirar vantagem da rápida expansão da digitalização, da crescente conectividade dos negócios e das formas às quais nossa vida pessoal está cada vez mais relacionada às tecnologias móveis e à internet.

Se você está com dificuldades de entender como gerenciar essa situação, você não está sozinho - mais de um terço dos participantes da nossa pesquisa ainda pensa que é improvável detectar um ataque sofisticado e, de acordo com nossa experiência, sabemos que somente as organizações mais vigilantes seriam capazes de detectar pequenas anomalias, indicativas de uma brecha de longa duração.

Segurança cibernética é mais do que uma questão tecnológica, e seu domínio não pode se restringir apenas à equipe de TI, tampouco ser uma simples responsabilidade de um diretor. Ela afeta todos os níveis de um negócio e todos os níveis executivos, de formas sutis e não facilmente detectáveis. O foco deste relatório é como várias partes de uma organização precisam estar unidas e compartilhar experiências. Dessa forma, é possível acumular evidências, identificando onde criminosos já tiveram acesso e se eles estão, agora mesmo, coletando informações que poderão afetar o valor de sua organização.

Seu foco deve permanecer em estar um passo à frente dos criminosos cibernéticos, o que atualmente significa aprender os meios de se manter em um estado constante de "Defesa Ativa". Neste relatório, nós exploramos quais são os meios e como a EY pode apoiá-lo nessa caminhada.

Gostaríamos de agradecer pessoalmente nossos clientes por dedicar seu tempo ao preenchimento da pesquisa, e esperamos que apreciem este relatório.

Paul van Kessel
Líder Global de Consultoria em Gestão de Riscos da EY
paul.van.kessel@nl.ey.com

Ken Allan
Líder Global de Segurança da Informação da EY
kallan@uk.ey.com

Entendendo os desafios para a segurança cibernética

O mundo digital está repleto de oportunidades em rápida expansão para a inovação e, com isso, negócios, governos e indivíduos focaram sua atenção nos significativos benefícios de se adaptar a esse movimento. Ao criar novos mercados e produtos, surgiu um melhor entendimento dos consumidores, dos cidadãos e de como encontrar formas diferentes de se conectar a eles. O mundo digital oferece um enorme potencial.

Infelizmente, na pressa, muitas precauções foram negligenciadas, e riscos subestimados. A identificação de que há um outro lado da moeda e que o mundo digital também oferece grande potencial de exploração por parte dos criminosos surgiu muito tarde. Adicionalmente, consequências complexas e imprevistas da interconectividade entre as pessoas, as organizações e o ambiente estão emergindo.

Para que essas organizações reconheçam os desafios atuais e entendam o que precisam fazer, elas deveriam pensar nos quatro tópicos:

Ataques atuais no mundo digital

- Como o mundo está mudando para você?
- Quais são as ameaças e as vulnerabilidades que você deve temer?
- Como você gerencia os ataques?

Como os ataques se desdobram

- Quais são os piores cenários para você?
- Como detectar sinais pequenos e sutis?
- Por que devemos estar constantemente em "alerta máximo"?

Por que ainda estamos tão vulneráveis?

- Medidas insuficientes no ambiente atual
- Sem mecanismos para se adaptar à mudança
- Lenta aproximação proativa para neutralizar ataques sofisticados

Transição para a Defesa Ativa

- O que é Defesa Ativa?
- O que precisa ser melhorado?
- Como construir a Defesa Ativa?

Cenário atual de ataques no mundo digital

88%

dos respondentes não acreditam que a sua segurança da informação atenda totalmente às necessidades da organização

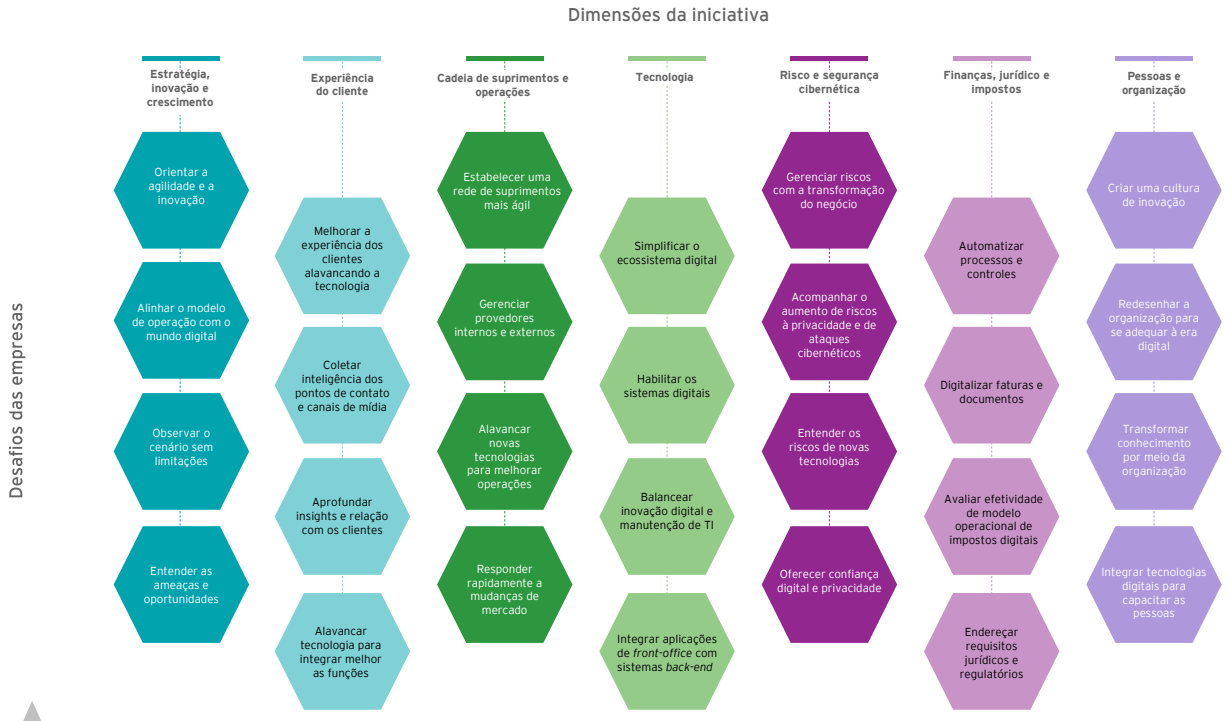
Como o mundo está mudando para você?

Organizações não têm escolha a não ser operar neste ambiente; por este motivo, inevitavelmente, existe uma crescente preocupação dos governos e da mídia com o que pode estar ocorrendo de errado onde o espaço cibernético e o mundo físico se encontram. Clientes tendo seus dados pessoais roubados e usados é inaceitável, assim como o roubo de propriedade intelectual e os custos subsequentes de remediação. A manipulação e a deturpação da mídia, comunicações, administração governamental e sistemas de defesa são vistos como ameaças significativas à segurança nacional.

Então, qual é o significado da sobrevivência no mundo digital para você e sua organização?

Sua organização precisa estar inserida por completo na dimensão "cibernética", e todas estas áreas precisam ser consideradas, relacionando segurança cibernética com oportunidades digitais e sustentáveis.

Aproveitar a segurança cibernética para canalizar as oportunidades digitais e a sustentabilidade



Catalisadores de aceleração

Internet das Coisas
US$626b
Em gastos dos consumidores por meio de dispositivos móveis até 2018 (US$)
Fonte: Goldman Sachs, 2014

Móvel
85%
dos relacionamentos de negócios sem interação humana até 2020
Fonte: Gartner Group, 2011

Impressão 3D
99%
de todos os dispositivos que algum dia poderão fazer parte da rede ainda não estão conectados
Fonte: CISCO, Rob Soderbury, 2013

Nuvem
36%
das organizações ainda não conseguem detectar um ataque cibernético sofisticado
Fonte: Pesquisa Global da EY sobre Segurança da Informação, 2015

Cibernético
81%
dos executivos seniores concordam que os dados devem estar no centro de toda tomada de decisões
Fonte: EY Tornando-se uma organização conduzida por dados analíticos para criar valor, 2015

Detectores

Análises

Social

Inteligência artificial

Operando no mundo digital - O que há de novo?

- Serviços e dispositivos "inteligentes" que resultam em consequências indesejadas e uma massa de dados que aumenta o número de vulnerabilidades a ser exploradas, além de humanos que geralmente são removidos do processo de tomada de decisão.
- Mídia social e BYOD, com empregados, clientes, cidadãos "sempre conectados" e compartilhando informação - não apreciando totalmente as implicações resultantes da privacidade e confidencialidade.
- Organizações inserindo mais dados na nuvem e compartilhando com terceiros: atrativo, mas perigoso. Com a perda de controle, há o aumento das ameaças e a conectividade inesperada, criando um ecossistema complexo.
- Comportamentos humanos estão mudando, de forma positiva e negativa.
- O surgimento de novas legislações e regulações está forçando mudanças nos processos. Estas, por sua vez, criam novas vulnerabilidades que futuramente modificarão o cenário de ameaças (normalmente as aumentando e não diminuindo) e a superfície de ataque de uma organização.

68%

dos respondentes não consideram o monitoramento do seu ecossistema de negócios um desafio à segurança da informação na Internet das Coisas

Quais são as ameaças e vulnerabilidades que você deve temer?

Para que sua organização se mova para um ambiente mais seguro e sustentável no mundo digital, é necessário observar todas as ações tomadas sob uma perspectiva de risco cibernético.

Muitas organizações estão gerenciando seus riscos e vulnerabilidades pontualmente, expondo todos nós a grandes ameaças. Esta não é uma responsabilidade que possa ser delegada para um ou dois indivíduos; preferencialmente, uma ampla gama de responsabilidades individuais deve ser considerada e detalhada internamente na organização e no seu ecossistema, convergindo para uma visão simples, acessível e coerente. Essa visão poderá parecer diferente para diretoria, executivos e funcionários, assim como poderá parecer diferente também para parceiros, fornecedores e outros terceiros.

O problema é como não afundar nesse mar de dados e criar mais trabalho e riscos do que o necessário. Em vez disso, você deve priorizar, simplificar e mapear qual seria uma abordagem eficiente e abrangente para a companhia em particular. Os blocos de construção básicos devem ser comuns (como demonstrado na nossa abordagem 3A, ver em www.ey.com/GISS2014), porém o valor verdadeiro está na adaptação de sua abordagem de segurança cibernética às suas estratégias de negócio, riscos e prioridades.

Então, para guiar sua organização de forma eficiente por meio das camadas de riscos e ameaças, líderes devem ter confiança para definir o apetite ao risco e estar preparados para tomar ações decisivas para lidar com qualquer tipo de incidente. Por exemplo, um tema que vem emergindo nos últimos anos é que o impacto de um incidente é muito reduzido quando a liderança assegura a existência de uma forma inteligente e apropriada de lidar com incidentes cibernéticos e de uma comunicação efetiva, tanto interna quando externa, para gerenciar as consequências.

67%

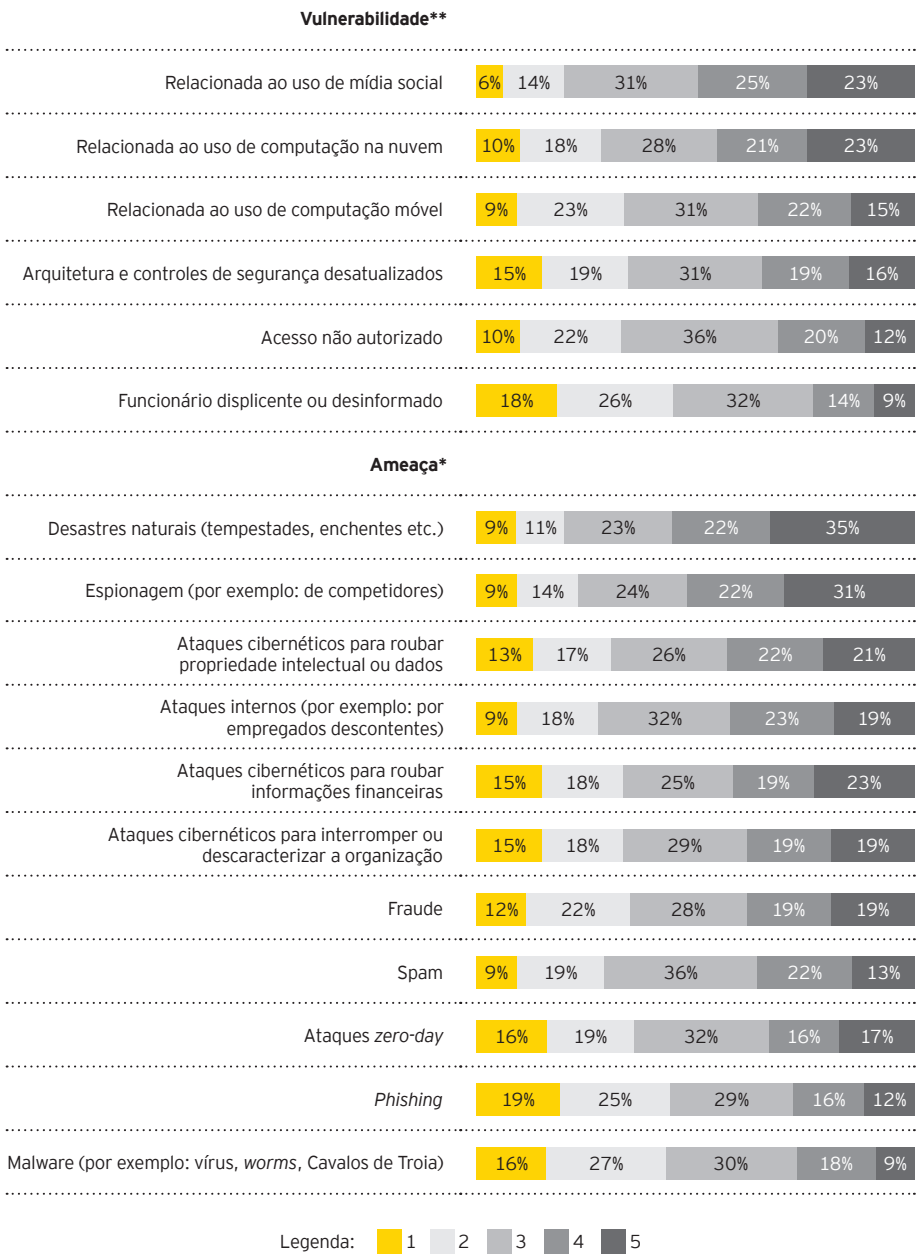
dos respondentes não consideram administrar o crescimento nos pontos de acesso à sua organização um desafio à segurança da informação na Internet das Coisas

Questões para sua organização considerar:

- Você realmente tem confiança no seu entendimento das ameaças e vulnerabilidades no mundo digital?
- Você realizou um trabalho de reflexão sobre os requerimentos necessários para determinar como o cenário de ameaças se aplica a sua organização, estratégia e priorização de medidas de segurança cibernética?
- Você sabe como definir seu apetite ao risco para determinar os níveis aceitáveis e não aceitáveis de perda e danos oriundos de potenciais incidentes como parte do desenvolvimento do seu programa de gerenciamento de resposta a incidentes de segurança?

Apenas quando o apetite ao risco é definido no nível em que a diretoria está confortável e a organização pode alcançá-lo, suas transformações digitais serão sustentáveis.

Quais ameaças e vulnerabilidades mais aumentaram seu risco de exposição nos últimos 12 meses? (Dê uma nota para todos os itens, sendo 1 a de maior prioridade, e 5, a de menor prioridade)



**Ameaça é definida como o potencial de ocorrência de uma ação hostil proveniente de atores em um ambiente externo.*
***Vulnerabilidade é definida como existência da possibilidade de ser atacado e sofrer danos.*

Como 2015 se compara a 2014?

Se observarmos as duas maiores vulnerabilidades:

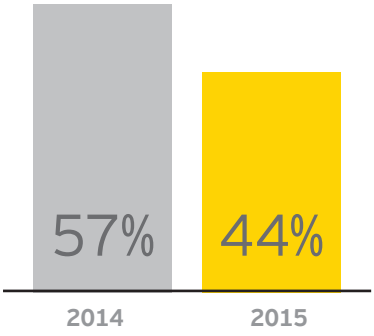
- Funcionários displicentes ou desinformados.
- Arquitetura e controles de segurança da informação desatualizados.

Em 2014, essas duas mesmas vulnerabilidades foram consideradas como prioridades altas, porém, a percepção de vulnerabilidade sentida pelas organizações diminuiu nessas áreas. Atualmente, somente 44% se sentem vulneráveis em relação a funcionários displicentes, comparado com 57% em 2014; somente 34% se sentem vulneráveis devido a sistemas desatualizados, comparado a 52% em 2014. Isso mostra que as organizações acreditam que estão cobrindo suas vulnerabilidades de forma mais eficiente.

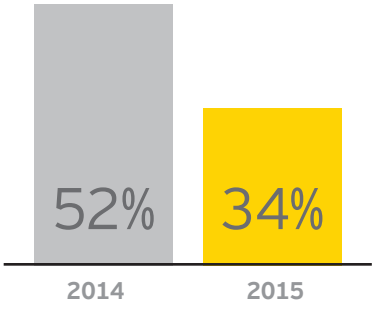
Entretanto, quando olhamos para as maiores ameaças atuais:

- Phishing
- Malware

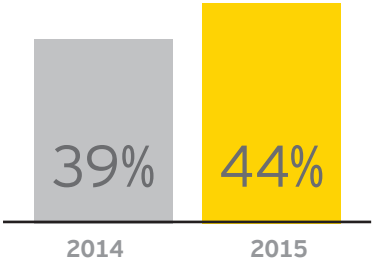
Estas ameaças, que ficaram em 5º e 7º lugares em 2014, junto com o roubo de informações financeiras, propriedade intelectual, ameaça de fraude, espionagem e ataques *zero-day*, todas parecem maiores. Essa elevada percepção de *phishing* e *malware* como ameaças demonstra uma clara mudança de perspectiva, mas essa é a mudança correta ou um desvio na direção errada?



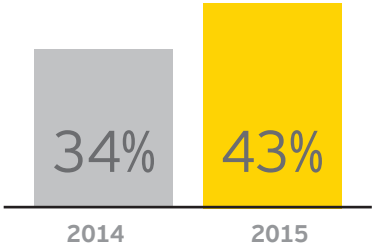
Hoje, apenas 44% se sentem vulneráveis em relação a funcionários displicentes, em comparação a 57% em 2014



Apenas 34% se sentem vulneráveis devido a sistemas ultrapassados, em comparação a 52% em 2014



Atualmente, 44% consideram o *phishing* uma das principais ameaças, em comparação a 39% em 2014



Atualmente, 43% consideram o malware uma das principais ameaças, em comparação a 34% em 2014

42%

dos respondentes declararam que o conhecimento de todos os seus ativos é um sério desafio à segurança da informação

Você pode deter os ataques?

Sua organização irá sofrer incidentes cibernéticos. Isso é parte do mundo digital.

O ponto de partida para ganhar confiança como organização é a conscientização situacional – um entendimento de como um criminoso cibernético enxerga sua organização.

- Como você protege sua organização contra incidentes cibernéticos se você não sabe o que os criminosos estão almejando?
- Como eles poderão obter acesso aos seus dados e como isso afetaria você e seus ativos críticos?
- Como você pode ter confiança se não entende completamente a capacidade da sua organização de responder, conter e se recuperar de um ataque?

Princípios-chave de gerenciamento de riscos	Aplicado a riscos cibernéticos
1 **Focar no que é mais crítico** Deve estar alinhado com sua cultura de risco e negócio.	**Conhecer seus ativos críticos de informação** Identifique ativos críticos do negócio mais vulneráveis a ataques cibernéticos.
2 **Medir e reportar** Incluir medições qualitativas e quantitativas.	**Tornar riscos cibernéticos mais tangíveis** Defina claramente riscos cibernéticos e suas métricas.
3 **Natureza abrangente** Deve cobrir todos os tipos de risco, presentes e futuros.	**Estar alinhado a frameworks de riscos existentes** Financeiro, operacional, regulatório, clientes, reputação etc.
4 **Definição do apetite ao risco** Atribuição do apetite para unidades de negócio e tipos de risco.	**Tornar riscos cibernéticos relevantes para o negócio** Relacione os riscos de nível organizacional às unidades de negócio e seus ativos de informação.
5 **Integrar com planejamento de negócio** Reguladores estão continuamente procurando evidências.	**Considerar o apetite ao risco em decisões de investimento** Priorize o investimento onde for crítico, capacitando o negócio para que se tomem decisões locais com base em informações.

Incidentes cibernéticos geralmente são anunciados como eventos dramáticos e sensacionalistas – vazamentos massivos, sistemas e sites inoperantes resultando em danos e inconveniência para os consumidores. As manchetes focam em eventos de larga escala em que milhões de dados de contas são roubados, pilhas de informações confidenciais disponibilizadas online, propriedade intelectual roubada e sistemas danificados.

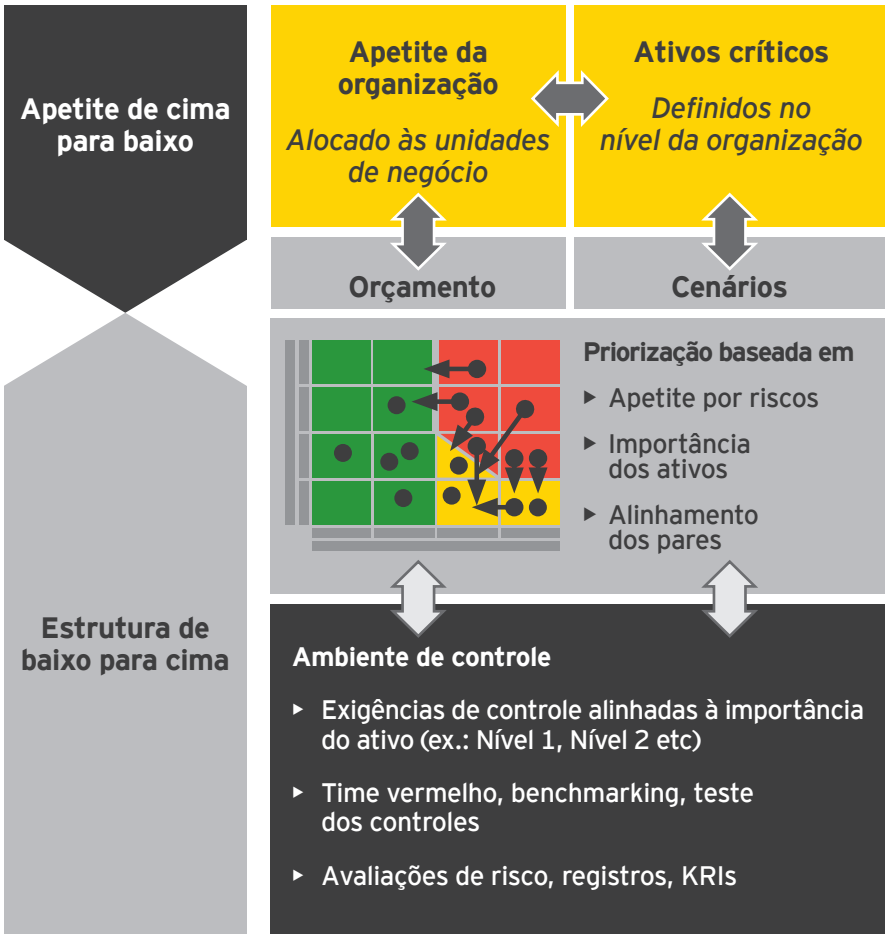
No entanto, a natureza desses eventos pode não estar sendo corretamente informada. A maioria desses ataques teve início semanas ou meses antes, quando criminosos cibernéticos encontraram um ponto de entrada e pacientemente começaram a explorar, localizando ativos valiosos e dando continuidade aos seus planos.

Além disso, incidentes cibernéticos não são casos isolados, não importa o quão complexos ou simples, direcionados ou aleatórios eles possam ou aparentam ser. Os sinais iniciais e os impactos acumulados dos repetidos ataques devem ser entendidos e considerados no planejamento do apetite ao risco.

$ $ $

20%

dos respondentes não conseguem estimar o prejuízo financeiro total relacionado a incidentes cibernéticos nos últimos 12 meses



Time vermelho: *é um grupo que desafia ativamente uma organização para aprimorar a sua segurança por meio de exercícios específicos, como testes de penetração, engenharia social etc.*

Identificar os riscos reais

- Definição descendente do apetite por riscos e dos ativos que contêm informações críticas.
- Mapear os ativos críticos entre os sistemas e negócios (e terceirizados).

Priorizar o mais importante

- Pressupor que violações irão ocorrer – aprimorar os controles e processos para identificar, proteger, detectar, responder e recuperar-se dos ataques.
- Equilibrar as partes essenciais com as ameaças emergentes e a capacitação dos pares.

Administrar e monitorar o desempenho

- Avaliar regularmente o desempenho e a posição do risco residual.
- Medir os principais indicadores para detectar problemas enquanto ainda são pequenos.

Otimizar os investimentos

- Aceitar os riscos administráveis quando não houver orçamento disponível.
- Assegurar que o impacto de "custos diretos" e das "atividades rotineiras do negócio" seja considerado para todo o investimento.

Permitir/ativar o desempenho nos negócios

- Tornar a segurança responsabilidade de todos
- Não restringir as novas tecnologias. usar as forças das mudanças para ativá-las.

Como os ataques acontecem

Quais são os piores cenários?

A fim de identificar que as coisas não estão "muito bem", é necessário primeiro conhecer o seu ambiente de dentro para fora – verificar o que é crítico para o sucesso da organização, determinar quais seriam os cenários de riscos cibernéticos críticos para o negócio e retratar o que seria mais prejudicial se fosse perdido ou comprometido. Então, torna-se possível priorizar suas precauções e criar contramedidas em torno das áreas mais críticas e dos cenários com maior chance de sofrer ataque.

Exemplo de cenário de ataque:

Com um ou com os mais altos tipos de negócio de mercado e cenários de riscos cibernéticos delineados, é possível identificar quais áreas na organização devem ser observadas com mais atenção:

- É o número de vendas em uma determinada região onde você suspeita de roubo de propriedade intelectual está sendo usado contra você?
- É uma queda em seu valor de mercado ao longo do tempo enquanto você está se preparando para a uma importante atividade de fusão e compra?
- É onde você tem um alto número de terceiros envolvidos em uma área crítica do seu negócio?

Quem ou o que você considera ser a fonte mais provável de ataque?

Eles já estão infiltrados na minha organização?

Uma vez que os criminosos cibernéticos podem passar meses dentro de sua organização, buscando informações que eles armazenarão para um futuro ataque ou colhendo pedaços de informações que juntas irão levá-los ao objetivo que buscam, eles também criarão medidas para se protegerem da sua detecção. Por vezes, criam táticas para desviar a atenção do que eles estão fazendo e onde foram bem-sucedidos. Frequentemente, os criminosos vão manter as informações roubadas e não as usarão por algum tempo - outras vezes, eles vão compartilhá-las entre a comunidade de criminosos cibernéticos (talvez por uma taxa), espalhando ainda mais as ameaças diretas a você.

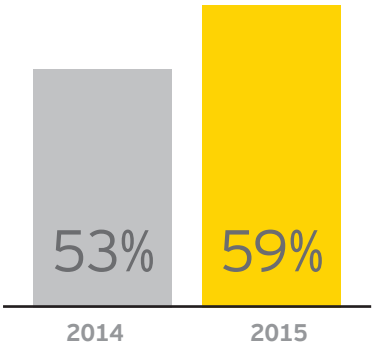
Ocasionalmente, essas explorações criminosas vão deixar vestígios, e sequelas serão sentidas, mas tais vestígios não são fáceis de detectar. Os sinais são tão sutis que pequenas perturbações nas operações ou aparentemente pequenas falhas em sistemas não são discutidas ou relatadas amplamente, assim não se tem uma fotografia panorâmica. Mesmo que a segurança cibernética seja um item permanente na agenda dos executivos, muitas vezes não se tornará aparente que os pequenos eventos inexplicáveis com os quais cada executivo está lidando individualmente possam ser parte de um ataque maior e mais sofisticado com potencial para causar grandes impactos.

Como detectar sinais pequenos e sutis

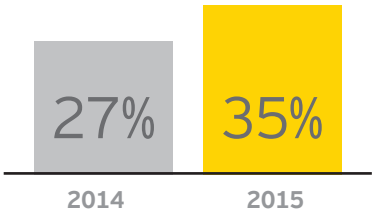
Focar a atenção, prevenir e desenvolver contramedidas em torno das áreas de maior valor e maior risco é um passo fundamental para minimizar os impactos decorrentes de incidentes cibernéticos. Ser capaz de detectar incidentes cibernéticos o mais cedo possível é o próximo passo crucial, o que só é possível por meio de radar abrangente que seja capaz de cobrir uma variedade de indicadores e que possa gerar alerta quando um determinado limite é cruzado. A determinação dos limites se refere novamente ao apetite ao risco e aos tipos de incidente que possam causar os maiores impactos à sua organização.

Alguns ataques serão inesperados e óbvios e, nesses casos, todo o foco muda para uma resposta eficaz. No entanto, lembre-se de que esses ataques óbvios também podem ser uma tática de distração, por isso, as organizações precisam ter capacidade de analisar cada incidente a fim de obter dados suficientes para verificar padrões que possam surgir ao longo do tempo.

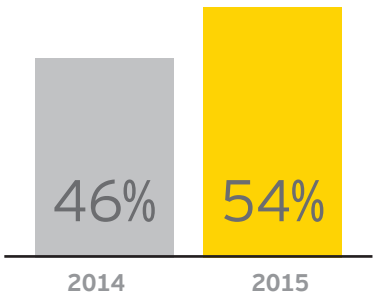
Existem muitas maneiras de invadir uma organização, e os criminosos cibernéticos encontrarão os pontos de entrada mais vulneráveis. Alguns deles serão óbvios e, portanto, mais fáceis de proteger, e eles devem ser monitorados. Porém, ao pensar criativamente em um cenário sobre como os criminosos cibernéticos podem operar,



Atualmente, 59% consideram os grupos criminosos a fonte mais provável de ataques, comparado a 53% em 2014



Atualmente, 35% consideram os agressores patrocinados pelo Estado a fonte mais provável de ataques, em comparação a 27% em 2014



Atualmente, 54% consideram os hacktivistas a fonte mais provável de ataques, em comparação a 46% em 2014

barreiras e monitoramentos extras podem ser adicionados em áreas não tão óbvias (por exemplo, sites voltados ao público, sistemas de terceiros que se conectam aos sistemas internos, conexões de sistemas industriais, na nuvem etc.).

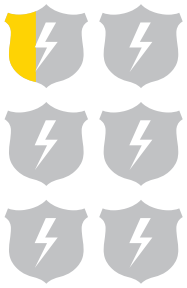
Uma vez dentro de seu ambiente, os criminosos cibernéticos irão focar no que há de maior valor para eles. Este é o momento em que conhecer seus pontos críticos para o negócio, os pontos (mais) prejudiciais, e que tenham valor para outra pessoa/empresa, é essencial – os pontos onde eles se cruzam é onde indicadores ou sinais mais sutis podem ser detectados.

Os departamentos Financeiro, Marketing, Operações, P&D, RH – todas essas áreas-chave – devem estar cientes dos riscos cibernéticos para a organização, incluindo a gama de responsabilidades individuais das áreas sobre esses riscos. Todos precisam estar alertas para identificar anormalidades no comportamento e prontos para reportá-las ao contato de segurança cibernética que irá adicioná-las a outros relatórios.

Assim como acontece em campanhas públicas antiterroristas, a ideia é que não custa nada relatar algo que levante suspeita. O fator crítico é que ele seja relatado para as partes interessadas que sejam capazes de juntar as peças do quebra-cabeça.

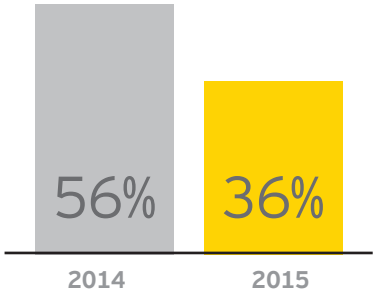
Exemplos de indicadores que um radar deve estar configurado para detectar são:

- Ataques muito visíveis sem uma finalidade óbvia: por exemplo, DDoS; dados roubados, mas sem uso óbvio aparente.
- Alterações inesperadas nos valores de ações.
- Novos produtos lançados por concorrentes que estão estranhamente semelhantes às suas P&D e propriedade intelectual e chegam ao mercado pouco antes do seu - caracterizando o roubo de propriedade individual e conhecimento da sua estratégia de crescimento e de seus timings.
- Interrupção em atividades de fusão e aquisição (M&A): ofertas rivais que mostram semelhanças e podem demonstrar conhecimento dos planos confidenciais; alvos de M&A sofrem incidentes cibernéticos (por exemplo: propriedade intelectual roubada).
- Comportamento incomum de cliente ou de uma joint venture: lembre-se de que esses podem nem sempre ser verdadeiros clientes ou parceiros, pois criminosos podem se filiar às organizações para obter acesso mais fácil aos seus sistemas e dados.
- Comportamento incomum de empregado: gerentes de equipe precisam ser mais conscientes de mudanças no comportamento, especialmente quando os funcionários trabalham em áreas mais sensíveis.
- Interrupção operacional sem uma causa clara.
- Anormalidade no processamento de pagamento ou sistemas de compras.
- Informações inconsistentes nas bases de dados de clientes ou de usuários.



7%

das organizações declaram que possuem um programa de respostas sólido, que inclui os colaboradores terceirizados e a aplicação da lei e é integrado à função mais ampla de gestão de ameaças e vulnerabilidade



36% declaram que é improvável que consigam detectar um ataque sofisticado. Trata-se de uma melhoria significativa em relação aos 56% de 2014, porém as organizações devem lembrar que o nível de sofisticação aumenta continuamente

56%

dos respondentes definiram a prevenção do vazamento de dados/ perda de dados como alta prioridade para suas organizações ao longo dos próximos 12 meses

49%

dos respondentes definiram os riscos e as ameaças internos como prioridade média, apesar de 56% afirmarem que os funcionários são uma das fontes mais prováveis de ataques e 36% mencionarem os fornecedores externos alocados na empresa como outra fonte provável

50%

dos respondentes definiram as mídias sociais como baixa prioridade

Quais das seguintes áreas de segurança da informação você definiria como de "alta, média ou baixa prioridade" para a sua organização nos próximos 12 meses?
(Selecione uma resposta para cada tópico)

	Alto	Médio	Baixo
Prevenção ao vazamento/roubo de dados	56%	33%	11%
Continuidade do negócio/Resiliência e Recuperação de desastres	55%	33%	12%
Gestão de acesso e identidade	47%	41%	12%
Conscientização e treinamento em segurança	44%	45%	11%
Capacidade de resposta a incidentes	44%	44%	12%
Operações de segurança (ex: antivírus, patches, criptografia)	41%	44%	15%
Testes de segurança (ex: ataques e penetração)	38%	46%	15%
Gestão de acesso privilegiado	38%	44%	17%
Proteção às tecnologias emergentes	38%	45%	18%
Gestão de eventos de incidentes de segurança e SOC	38%	42%	21%
Gestão de ameaças e vulnerabilidades	37%	45%	18%
Computação móvel	33%	47%	21%
Computação em nuvem	32%	34%	34%
Integração da Segurança de TI e tecnologias operacionais	29%	50%	21%
Medidas de privacidade	29%	44%	27%
Transformação da segurança da informação (redesenho fundamental)	25%	39%	35%
Gestão do risco de terceiros	24%	46%	30%
Ameaças/Riscos internos	23%	49%	28%
Redesenho da arquitetura de segurança	22%	46%	32%
Terceirização das atividades de segurança	21%	37%	42%
Suporte a fraudes	20%	40%	40%
Propriedade intelectual	19%	37%	44%
Suporte forense	13%	38%	49%
Mídias sociais	11%	39%	50%
Outros (favor especificar)	30%	21%	50%

Legenda: Alto Médio Baixo

Por que devemos estar constantemente em "alerta máximo"?

O mundo digital não permite que nenhuma organização se sinta confortável na área de ameaças e vulnerabilidades de segurança cibernética. Estar constantemente em alerta na detecção e resposta às mudanças do ambiente é essencial. Estar disponível 365 dias, 24x7, sem paradas, é essencial.

Porém, com esse grau de vigilância, é compreensível que algumas organizações estejam sentindo fadiga nessa área, e muitas perguntem "até quando ela será suficiente"?

Ser bombardeado constantemente por numerosos ataques durante anos (três a quatro anos) e ter que reagir a esses eventos cibernéticos pode facilmente provocar complacência. Um histórico extenso em repelir "ataques típicos" corriqueiros (ex: phishing) e conectar as lacunas evidentes (ex: gerenciamento de identidade e acesso funcionando de forma eficaz) pode levar as organizações a pensar que elas tenham "resolvido" o problema de segurança cibernética, quando, na realidade, a situação está piorando. Isso é especialmente verdade, pois pode ser muito difícil demonstrar o valor do investimento em termos reais quando os orçamentos são apertados.

Na realidade, a maioria das organizações tem colocado as bases adequadas à segurança cibernética em prática, não percebendo que este é apenas o começo, e o mundo digital requer uma abordagem firme e sensível quanto aos investimentos. Uma organização só pode considerar que está segura o "suficiente" quando esta é capaz de manter-se dentro dos limites do apetite ao risco estabelecido

No entanto, ao passo que a maturidade de segurança cibernética da organização aumenta, torna-se mais fácil demonstrar o valor desses investimentos. Fornecer avaliações mais precisas de custos para os danos causados por vários cenários de ataques cibernéticos pode ajudar a justificar investimentos e vigilância contínuos. Cada vez que seu Centro de Operações de Segurança (SOC) ou analistas de inteligência identificarem um ataque em fases muito iniciais, é possível demonstrar o valor deste para o negócio, extrapolando os danos que, de outra forma, seriam causados se o pior cenário possível acontecer.

Da mesma forma, quanto melhor for a sua consciência situacional, mais fácil será otimizar e priorizar seus gastos. Muito dinheiro é desperdiçado em controles ou equipamentos desnecessários que, na maioria das vezes, não aumentam a maturidade de segurança cibernética nas áreas onde ela é mais necessária.

$$$$$$

49%

afirmam que é necessário aumentar os recursos em até 25% para proteger a organização de acordo com a tolerância aos riscos da diretoria

$

84%

gastarão o mesmo ou menos em segurança da informação para IP ao longo do ano

70%

gastarão o mesmo ou menos em operações de segurança (antivírus, *patching*, criptografia etc)

62%

gastarão o mesmo ou menos na capacitação para a resposta a incidentes no próximo ano

Por que ainda estamos tão vulneráveis

Em nosso relatório GISS 2014, identificamos três etapas da jornada para a maturidade em segurança cibernética – Ativar, Adaptar e Antecipar (os "três As") – que precisam ser executadas em sequência com o objetivo de alcançar medidas de segurança cibernéticas cada vez mais avançadas e abrangentes em cada fase.

Os três As ainda são relevantes, e nossos resultados da pesquisa de 2015 mostram que ainda há progressos a ser feitos em todas as três fases. No entanto, tendo em vista as ameaças de hoje, muitas das ações que identificamos como sendo mais avançadas tornaram-se agora fundamentais.

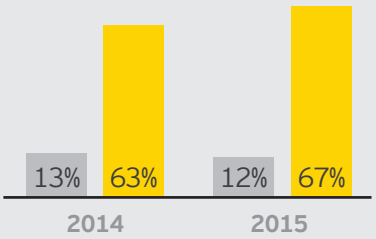
1. Ativar

Aqui é onde uma organização alcança uma base sólida de segurança cibernética para o ambiente **atual**, que compreende um conjunto de medidas de segurança cibernética que ajudam a fornecer a defesa básica. Isso exige que a organização:

- Realize uma avaliação da segurança e crie um roadmap.
- Obtenha apoio da diretoria para as transformações de segurança.
- Revise e atualize políticas de segurança, procedimentos e normas.
- Estabeleça um Centro de Operações de Segurança (SOC).
- Teste o plano de continuidade de negócio e os procedimentos de resposta a incidentes.
- Desenhe e implemente controles de segurança cibernética.

Hoje, com os riscos e as ameaças cibernéticos se tornando mais sofisticados, duas tarefas adicionais são fundamentais:

- Definir o ecossistema da organização.
- Introduzir treinamento de conscientização de segurança cibernética para os funcionários.

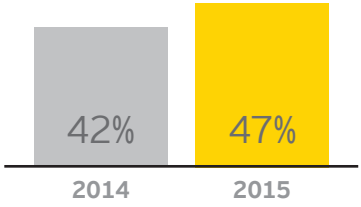


Percentual de entrevistados que acreditam que sua área de segurança da informação atende plenamente às necessidades da organização; percentual de entrevistados que acreditam que atendem parcialmente às necessidades, mas estão fazendo melhorias.

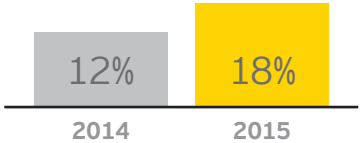
Então, onde estavam as empresas em 2015?

Não há ação suficiente no ambiente atual

- Apenas 12% acreditam atualmente que sua área de segurança da informação satisfaça plenamente às necessidades das organizações. 67% ainda estão em desenvolvimento.
  - Houve queda de 1% dentre aqueles que acreditam que as necessidades são plenamente atendidas, mas o número dos que estão em desenvolvimento aumentou apenas 4% desde 2014.
- 69% dizem que seu orçamento de segurança cibernética precisa aumentar até 50% para proteger a empresa de acordo com a sua tolerância ao risco.
- 47% não têm um SOC, em comparação com 42% em 2014.
- 37% não têm um programa de proteção de dados ou têm apenas políticas *ad hoc* ou processos em andamento, em comparação com 34% em 2014.
- 18% não têm um programa de Gerenciamento de Acesso e Identidade (IAM), enquanto em 2014 esse número era de 12% - o que representa uma queda grave.
- Apenas 40% possuem um inventário preciso de seu ecossistema (ou seja, todos os terceiros prestadores de serviços, conexões de rede e dados).
- 27% informaram que phishing em usuários finais foi a principal falha de controle ou processo que resultou em incidentes de segurança mais significativos no último ano.



Porcentagem dos respondentes que não têm um SOC (Centro de Operações de Segurança)



Porcentagem dos respondentes que não têm um programa de Gerenciamento de Acesso e Identidade (IAM)

54%

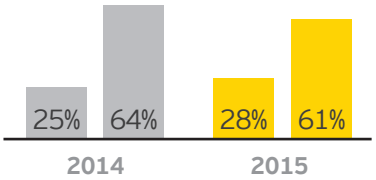
das organizações atualmente não têm um profissional responsável ou departamento na função de Segurança da Informação com foco nas tecnologias emergentes e no impacto que causam

2. Adaptar

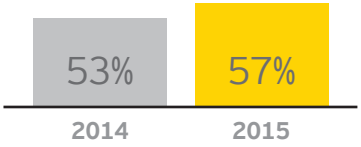
Aceitando que as medidas fundamentais de segurança da informação vão se tornar menos eficazes ao longo do tempo, esta fase foca no ambiente de mudança e destaca as ações necessárias para garantir que as organizações possam continuar a se adaptar, manter o ritmo e atender aos requisitos e às dinâmicas de mudança de negócios.

Hoje em dia, a fase Adaptar requer:

- Projetar e implementar um programa de transformação para alcançar uma melhoria gradual na maturidade de segurança cibernética, usando ajuda externa para acelerar ou incorporar as principais práticas na concepção do programa e fornecendo gerenciamento de programa.
- Decidir o que manter in-house e o que terceirizar.
- Definir uma matriz RACI para a segurança cibernética.



Porcentagem dos respondentes que pretendem gastar mais, ou a mesma quantia, na transformação da segurança da informação



Porcentagem que afirma que a falta de recursos capacitados está prejudicando a contribuição e o valor da segurança da informação para a organização

Então, estiveram os negócios em 2015?

Não há adaptações suficientes para mudanças

- 54% das organizações não possuem um ponto focal ou departamento na área de segurança da informação que esteja se concentrando em tecnologias emergentes e seus impactos - incluindo 36% que não têm planos para sua implementação.
- Apenas 34% avaliaram seu monitoramento de segurança como maduro ou muito maduro, que é apenas um aumento de 4% em comparação a 2014.
- Apenas 53% avaliaram sua segurança de rede como madura ou muito madura, que é apenas um aumento de 1% desde 2014.
- 57% informaram que a falta de recursos qualificados é um desafio à contribuição de segurança da informação à organização, enquanto em 2014 esse número era de 53%.
- Quando perguntados "em comparação com o ano anterior", 28% dos respondentes disseram que planejam gastar mais com a transformação da segurança da informação (uma reestruturação fundamental); este é apenas um aumento de
3% sobre as respostas à mesma pergunta em 2014.

3. Antecipar

Na fase Antecipar, uma organização precisa desenvolver táticas para detectar e neutralizar potenciais ataques cibernéticos de maneira proativa. Deve concentrar-se no estado **futuro** e tornar-se mais confiante em sua capacidade de lidar tanto com as ameaças mais previsíveis quanto com ataques inesperados.

Poucas organizações estão neste nível de capacidade, e hoje é necessário que elas:

- Projetem e implementem uma estratégia de Inteligência de Ameaças Cibernéticas.
- Definam e englobem um ecossistema de segurança cibernética para a organização de longo prazo.
- Adotem uma abordagem de *cyber-economics*.
- Utilizem análise de dados forense e inteligência de ameaças cibernéticas.
- Certifiquem-se de que todos compreendam o que está acontecendo.
- Preparem-se para o pior por meio do desenvolvimento de uma estratégia abrangente de gerenciamento de resposta a falhas de segurança cibernética.

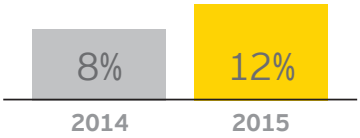
36%

dos respondentes não têm um programa de inteligência de combate a ameaças

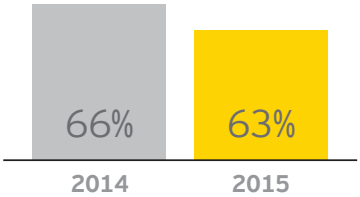
Então, onde estiveram os negócios em 2015?

Abordagem proativa lenta para neutralizar os ataques cibernéticos sofisticados

- 36% não têm um programa de inteligência de ameaças, outros 30% só possuem uma abordagem informal, enquanto 5% disseram que a sua organização possui/atingiu um estado avançado na sua área de inteligência contra ameaças; em comparação com 2014, estes números não mudaram, a não ser por uma queda de 2% daqueles que possuem a abordagem informal.
- 63% informaram que gerenciamento de ameaças e vulnerabilidade é uma prioridade média ou baixa, que é apenas uma pequena melhoria comparada a 2014.
- Apenas 12% atentam não só para seus fornecedores mas também para os fornecedores dos seus fornecedores (quarteirizados), que é apenas uma pequena melhoria de 4% comparada a 2014.
- Apenas 31% dos terceiros possuem classificação de risco e diligência apropriada aplicada, em comparação com 27% em 2014.
- 79% informaram que a ausência de conscientização ou o mau comportamento do usuário são os principais riscos associados a dispositivos móveis.



Porcentagem dos respondentes que procuram além de seus fornecedores possíveis parceiros quarteirizados



Porcentagem dos respondentes que alegam que a gestão de ameaças e da vulnerabilidade é uma prioridade média ou baixa

A transição para a Defesa Ativa

"A Defesa Ativa não substitui as operações tradicionais de segurança - mas as organiza e aprimora."

Ken Allan, Líder Global de Segurança da Informação da EY

O que é a Defesa Ativa?

A segurança cibernética é uma habilidade organizacional inerentemente defensiva. Os departamentos de Defesa do governo (e militares) podem estar preparando capacidades ofensivas, desenvolvendo técnicas de ataque e conduzindo ações intrusivas disruptivas, mas, para organizações que se mantêm fora deste escopo, operações ofensivas ainda são desnecessárias e ficam na zona cinzenta da legalidade. Entretanto, isso não significa que as empresas tenham que ser passivas e devam esperar para se tornarem vítimas.

Como mencionado antes neste relatório, entender os riscos cibernéticos críticos para o negócio e conhecer o que um criminoso cibernético quer em sua organização permite estabelecer uma defesa direcionada por meio da priorização (de ativos, pessoas e áreas de negócio) e da diminuição das vulnerabilidades. Avaliar o horizonte de ameaças que sejam particulares à sua organização (com base no seu ambiente operacional, ativos críticos e estratégia de negócio) permite que você entenda os vetores de ameaça mais prováveis e os métodos que eles possam usar, utilizando isso nos cenários como forma de se preparar. Tudo isso serve de informação para o SOC e deve ser utilizado como base para dar suporte para a sua organização.

Estabelecer um ASOC (*Advanced Security Operations Center*) e utilizar a inteligência em ameaças cibernéticas como forma de alinhar efetivamente as operações ajuda na condução da Defesa Ativa, ao ponto que você pode direcionar o foco para buscar ataques cibernéticos, analisar e avaliar ameaças e neutralizá-las antes que os ativos críticos da organização sofram algum dano. Da mesma maneira, você pode utilizar o ASOC para operar ativamente, combater anomalias indesejadas, "visitantes" ou criminosos cibernéticos já inseridos no seu ambiente.

O que precisa ser melhorado?

Inteligência Avançada em Ameaças Cibernéticas: diferentes níveis de análise de ameaça e criação de perfis podem ser feitos, variando desde questões mais básicas. Uma inteligência mais avançada em ameaças cibernéticas permite o gerenciamento proativo das ameaças e suas contramedidas.

Você precisa melhorar a sua inteligência em ameaças cibernéticas?

Algumas perguntas-chave a ser feitas em sua área de segurança da informação:

- Qual informação sobre a organização/o negócio está disponível para qualquer criminoso cibernético? Como ela pode ser usada?
- Qual é o perfil mais provável dos criminosos cibernéticos (hacktivistas, redes criminosas procurando por informações para ser vendidas, fraudadores, criminosos patrocinados por governos, por exemplo)?
- Quais são as suas aptidões (por exemplo, recursos prováveis, cronograma, capacidade técnica e possibilidade para recrutar informantes internos)?
- Para cada um dos prováveis criminosos cibernéticos, o que é mais provável que eles queiram? (Cruze essa lista com as informações do que mais importa para a sua organização/negócio – as joias da coroa).
- O quão vulnerável esses ativos/alvos estão e como eles podem ser explorados?
- Quais são os caminhos mais prováveis que seus concorrentes podem tomar para alcançar seus objetivos (por exemplo, por meio de um sistema de ar-condicionado, de um sistema de pagamento, recrutando um agente interno, pela realização de *spear-phishing* em membros do board ou de funcionários com os acessos necessários)?
- Quais as contramedidas mais eficientes?
- O que mais posso aprender dos incidentes ocorridos com meus concorrentes?

Munido das perguntas para essas respostas, a organização pode usar essas informações para comunicar as decisões estratégicas a nível executivo e à gerência, mudar o foco das atividades do SOC e utilizar informações de inteligência de mercado contra ameaças cibernéticas para alimentar as áreas mais relevantes da empresa neste momento.

24%

dos respondentes não possuem um programa de identificação das vulnerabilidades

34%

possuem um programa informal de identificação das vulnerabilidades executam testes automatizados regularmente

27%

declaram que as políticas e procedimentos de proteção de dados são informais ou que foram implantadas políticas ad hoc

59%

dos respondentes declararam que seu SOC (Centro de Operações de Segurança) não possui uma assinatura paga com feeds de informações sobre ameaças cibernéticas

Como construir uma Defesa Ativa

A Defesa Ativa estende as operações de segurança a duas formas-chave, mas antes ela deve ser guiada por uma inteligência de ameaças cibernéticas profissionalmente analisadas. Mais do que apenas receber informações de mercado, a análise de inteligência de ameaças permite que os praticantes de Defesa Ativa identifiquem possíveis criminosos cibernéticos, infiram os alvos mais prováveis no seu negócio e desenvolvam hipóteses sobre como esses ataques vão se desenrolar. Essas ideias ajudam na implementação de contramedidas específicas.

Um segundo fator-chave de diferenciação de uma abordagem-padrão de segurança cibernética é o ciclo operacional da Defesa Ativa. Por meio da interação dos processos definidos para análise das informações disponíveis, chegar a conclusões relevantes e agir, os adeptos da Defesa Ativa podem adicionar um componente dinâmico e proativo para as operações de segurança da organização.

Diferente de outros serviços, Defesa Ativa não é melhorar uma área específica ou implementar novas ferramentas. Em vez disso, ela busca integrar e melhorar as capacidades da organização em segurança da informação como forma de alcançar maior efetividade contra ataques persistentes. Ao implementar e executar um ciclo iterativo com mecanismos de melhoria contínua acoplados, a organização pode perceber ganhos em eficiência, responsabilidade e governança. Esses ganhos podem ser traduzidos em retorno sobre investimento para programas de segurança ao aumentar a eficiência das operações de segurança, que, por sua vez, reduzem a efetividade de ataques direcionados.

A Defesa Ativa também deve incluir a avaliação das implicações de risco no caso de incidentes críticos e o desenvolvimento de um framework de resposta centralizada como parte da estratégia de gestão de riscos da organização. O framework de gestão de incidentes, com um modelo claro de governança, deve cobrir o processo de investigação do incidente, coleta e análise de evidências, análise de impacto e suporte a litígios.

A Defesa Ativa é apropriada para a minha organização?

Se a resposta for sim para qualquer uma das perguntas abaixo, deve-se considerar a abordagem de Defesa Ativa:

- Nós temos um SOC, porém não estamos encontrando evidências de ataques avançados.
- Nós temos um SOC, porém tivemos um incidente grave.
- Nós temos um SOC terceirizado, mas nossa propriedade intelectual e sistemas de negócio não estão totalmente seguros.

Próximos passos na construção de um mundo digital confiável

Uma resposta simples para a pergunta "Do que minha organização precisa?" é o necessário para contemplar todos os itens a seguir:

- Conhecimento do que pode impactar negativamente a organização e impedir que se alcance sua estratégia.
- Clara identificação dos seus ativos críticos, ou seja, as joias da coroa.
- Cenário de riscos cibernéticos que figurem exatamente como um ataque pode ocorrer e impactar o negócio.
- Uma diretoria e executivos seniores que possam determinar o apetite ao risco para uma organização.
- Uma avaliação da maturidade atual da segurança cibernética e uma comparação com o nível de maturidade que é necessária para atingir o apetite ao risco.
- Um roadmap de melhorias.
- Inteligência avançada em ameaças de segurança cibernética e adaptação do perfil de ameaças e inteligência em ameaças cibernéticas.
- Um SOC mais avançado: *in-house*, cooperativo ou terceirizado.
- Uma estratégia proativa e multifuncional de gerenciamento de resposta a incidentes cibernéticos.

Para ir adiante com o roadmap e a implementação do plano de segurança cibernética, pode ser necessária uma mudança de cultura na organização e também um melhor esclarecimento do papel da diretoria – uma solução holística e um framework serão necessários para o completo alinhamento ao seu desempenho de negócio. É possível que recursos externos sejam necessários para ajudar a organização a alcançar este objetivo. Atualmente, uma avaliação no nível da diretoria sobre a perspectiva do seu nível de maturidade pode ser um exercício preliminar e altamente eficiente para preparar o cenário para a escala da mudança que possa ser necessária.

As páginas seguintes oferecem a perspectiva completa dos níveis de maturidade – onde você está hoje e onde você almeja estar? A abordagem de defesa almejada não sugere que o estado ideal seja essencial em todos os aspectos.

66%

dos respondentes que recentemente sofreram incidentes significativos não descobertos pelo SOC afirmam que o SOC não tem nenhuma assinatura paga com feeds de informações sobre ameaças cibernéticas

O espectro da maturidade - e a posição atual das empresas

Perguntas de maturidade	1 – Não existente	2
Qual é a maturidade do seu programa de inteligência de ameaças?	**36%** dos entrevistados não possuem um programa de inteligência de ameaças	**30%** possuem um programa informal de inteligência de ameaças que incorpora informações de terceiros e listas de distribuição de e-mail
Qual é a maturidade da sua capacidade de identificação de vulnerabilidade?	**24%** dos entrevistados não possuem um programa de identificação de vulnerabilidade	**34%** possuem um programa informal de identificação de vulnerabilidade e executam testes automatizados regularmente
Qual é a maturidade do seu programa de detecção de incidentes?	**18%** dos entrevistados não possuem um programa de detecção; outros 4% não possuem processos formais estabelecidos de resposta e escalonamento	**23%** possuem dispositivos de segurança de perímetro de rede (IDS); outros 21% utilizam uma solução de gerenciamento de eventos (SIEM) para monitorar ativamente a rede, IDS/IPS e logs do sistema
Qual é a maturidade da sua capacidade de resposta a incidentes?	**14%** não possuem capacidade de resposta a incidentes	**21%** possuem um plano de resposta a incidentes, por meio do qual podem se recuperar de ataques de malwares ou mau comportamento dos funcionários; investigações futuras sobre as causas não são realizadas
Qual é a maturidade do seu programa de proteção de dados?	**10%** dos entrevistados não possuem um programa de proteção de dados	**27%** informaram que as políticas e procedimentos de proteção de dados são informais ou que políticas *ad hoc* estão em vigor
Qual é a maturidade do seu gerenciamento de identidade e acesso?	**18%** dos entrevistados não possuem um programa de gerenciamento de identidade e acesso	**25%** possuem uma equipe para supervisão dos processos de gerenciamento de acesso; a condução de revisões não é formalmente estabelecida

3	4	5 – Muito maduro
20% possuem um programa formal de inteligência de ameaça que inclui feeds de assinaturas de ameaças de provedores externos e fontes internas assim como uma ferramenta de gerenciamento de incidentes e eventos de segurança	**10%** têm uma equipe de inteligência de ameaças que recolhe insumos de ameaças e vulnerabilidades internas e externas para analisar a credibilidade e a relevância em seu ambiente	**5%** têm uma função avançada de inteligência de ameaças, com insumos internos e externos assim como analistas de inteligência dedicados e consultores externos que avaliam as informações quanto a credibilidade, relevância e exposição a agentes de ameaças
20% usam uma variedade de abordagens de revisão, incluindo engenharia social e testes manuais	**18%** têm uma função formal de inteligência de vulnerabilidade com um programa de avaliação baseado em ameaças de negócios, utilizando ataque *deep dive* e testes de penetração de fornecedores, verificação periódica dos processos de negócio e testes de projeto (por exemplo, novos sistemas)	**5%** têm uma função de inteligência avançada de vulnerabilidade e realizam avaliações com base no risco, e os resultados e remediações são alinhados com a área de riscos ao longo do ano
6% têm processos informais de resposta e escalonamento estabelecidos; outros 5% utilizam processos pontuais para coleta, integração, resposta e escalonamento de ameaças	**13%** têm um programa formal de detecção que utiliza tecnologias modernas para monitoramento (e detecção de malware, detecção de anomalia comportamental etc. em rede baseado em host) do tráfego interno e externo	**11%** têm uma função formal e avançada de detecção que reúne cada categoria de tecnologia moderna (detecção de malware baseado em host, antivírus, detecção de malware baseado em rede, DLP, IDS, *next-generation firewalls*, agregação de log) e utilizam análises de dados sofisticadas para identificar tendências, anomalias e correlações. No entanto, apenas 2% têm processos formais para coleta, divulgação, a integração, a resposta, escalada e previsão de ameaça e ataques
43% têm um programa formal de resposta aos incidentes e de conduta de investigações na sequência de um incidente	**16%** têm um programa formal de resposta aos incidentes e acordos estabelecidos com os fornecedores externos para serviços mais completos de resposta e investigação de identidade	**7%** possuem um programa de resposta a incidentes robusto que inclui terceiros e aplicação de legislação, que seja integrado a uma função de gerenciamento de ameaças e vulnerabilidades mais amplo; eles também constroem *playbooks* para possíveis incidentes e os testam regularmente por meio de exercícios
19% dizem que as políticas e os procedimentos de proteção de dados são definidos no nível da unidade de negócios	**26%** dizem que as políticas e os procedimentos de proteção de dados são definidos no nível de grupo	**17%** dizem que as políticas e os procedimentos de proteção de dados são definidos no nível de grupo, refletindo supervisão corporativa e comunicada por meio do negócio; exceçõesde unidades de negócios específicassão documentadas, monitoradas e revisadas anualmente
34% têm uma equipe formal para supervisionar os processos definidos de gerenciamento de acesso, embora este seja, em grande parte, manual; um diretório central está em vigor, mas ele interage com um número limitado de aplicações e não é revisado regularmente		**23%** têm uma equipe formal que interage com unidades de negócios a fim de melhorar a supervisão de IAM; eles têm processos bem definidos, fluxos de trabalho limitadamente automatizados, fonte de Single Sign-on para a maioria dos aplicativos e realização de análises periódicas bem definidas

32%

dos respondentes declararam que a sua prioridade mais alta e de maior utilidade é o benchmarking das informações sobre a maturidade das organizações da mesma categoria

Coloque sua organização nos trilhos

Poucas organizações atualmente têm as habilidades e os recursos apropriados para proteger efetivamente seus ativos de informação e ao mesmo tempo otimizar o desempenho do negócio. Organizações de todos os setores podem se beneficiar de uma avaliação objetiva dos seus programas de segurança da informação e estruturas.

Uma avaliação eficiente deve buscar auxiliar sua organização:

- Entendendo o risco de exposição da organização.
- Avaliando a maturidade do seu atual programa de segurança cibernética e identificando áreas de melhoria.
- Construindo um roadmap priorizado para investimentos de projeto e iniciativas de mudanças organizacionais.
- Coletando informações para criar benchmarks de comparação com outras organizações.
- Verificando se seus investimentos em segurança melhoraram sua postura de segurança.

Esta avaliação precisa ser ampla e de alto nível, assim como totalmente imersa em áreas e componentes específicos: é onde a EY pode ajudar. Dashboard de métricas auxilia a organização na análise da transformação e da sustentabilidade da estratégia de segurança da informação.

Por outro lado, níveis de maturidade podem ajudar a organização a se posicionar em direção ao seu espectro mais adequado em relação a sua situação competitiva atual e futura.

A efetividade da segurança da informação

Quais são os principais obstáculos ou razões que impedem que a segurança da informação contribua operacionalmente e agregue valor à organização? (Marque todos que se aplicam)

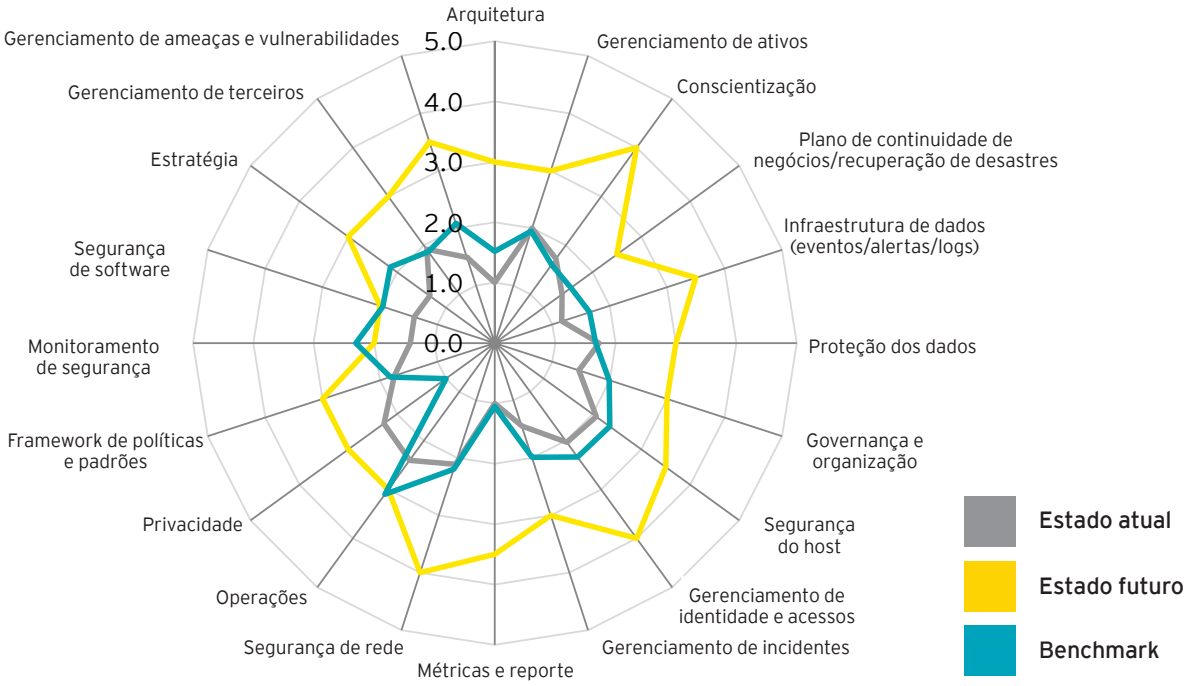
Você tem uma matriz RACI?

Com a diretoria definindo o tom e o nível de expectativa, a colaboração por meio da empresa é essencial, assim como a vigilância relacionada a "como riscos cibernéticos e ataques cibernéticos afetam o seu papel". O gerenciamento efetivo de segurança afeta todos os papéis e todas as partes da organização; uma matriz RACI, boa governança e funcionários cooperativos são essenciais – na nossa abordagem dos 3 As é um elemento-chave do nível de adaptação de segurança cibernética. Considere como uma matriz RACI deve parecer para sua organização, e seja claro no entendimento de que a segurança cibernética não é mais um problema somente de TI.

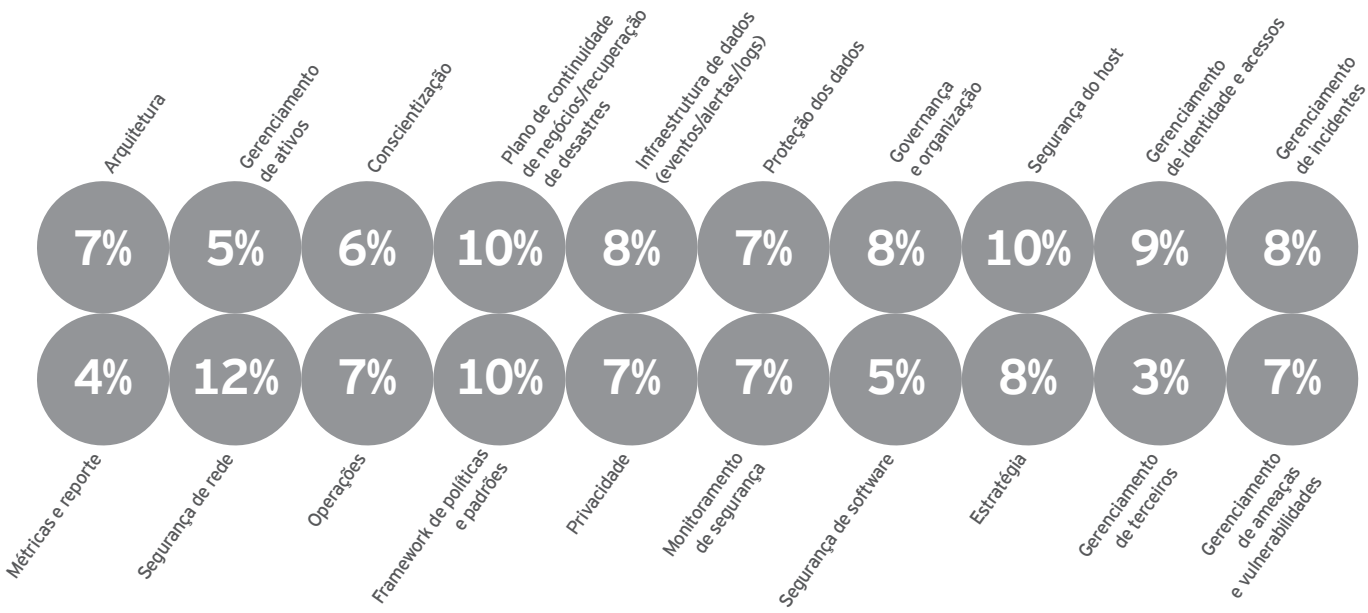
Estado atual da maturidade de segurança cibernética comparando organização e seus pares

O estado de maturidade atual da organização X está aproximadamente no mesmo nível em comparação com seus pares. Estados futuros definidos aumentam o estado de maturidade consideravelmente.

Organização X versus pares



Porcentagem dos respondentes da nossa pesquisa que indicaram que seu nível de maturidade era "muito alto"



A segurança cibernética é a capacitadora digital

A segurança cibernética não é apenas uma inibidora no mundo digital; mais do que isso, ela ajuda a tornar o mundo digital totalmente operacional e sustentável.

A segurança cibernética é fundamental para desvendar as inovações e expansões e, adotando uma organização personalizada e uma abordagem focada nos riscos, as organizações podem focar mais nas oportunidades e na exploração. Desenvolver a confiança em uma empresa bem-sucedida na operação da Internet das Coisas (IoT) e que oferece total suporte e proteção às pessoas e aos seus dispositivos móveis pessoais (de um simples celular a um dispositivo de controle da saúde; dos eletrodomésticos aos carros inteligentes), é um importante diferencial competitivo e deve ser prioridade.

Por meio de uma ação imediata, será possível ajustar o equilíbrio do mundo digital com foco na sustentabilidade e na segurança para ajudar a proteger melhor a sua organização e a gerar confiança na sua marca.

Metodologia da pesquisa

A Pesquisa Global da EY sobre Segurança da Informação foi realizada entre junho e setembro de 2015. Participaram da pesquisa 1.755 respondentes de 67 países que representaram todos os principais setores da economia.

Convidamos para participar da nossa pesquisa CIOs, CISOs, CFOs, CEOs e outros executivos de segurança da informação. Distribuímos os questionários aos profissionais designados pela EY em cada país participante, com as instruções para uma administração consistente do processo de pesquisa.

A maioria das respostas à pesquisa foi obtida durante entrevistas pessoais. Quando isso não foi possível, o questionário foi preenchido on-line.

Se você deseja participar das futuras Pesquisas Globais de Segurança da Informação da EY, por favor entre em contato com o seu representante ou escritório local da EY ou visite www.ey.com/giss e preencha um simples formulário.

Perfil dos participantes

1.755
respondentes

67
países do mundo

25
setores de atividade econômica

Respondentes por área (1.755 respondentes)

Legenda:

EMEIA	51%
Américas	29%
Ásia-Pacífico	15%
Japão	5%

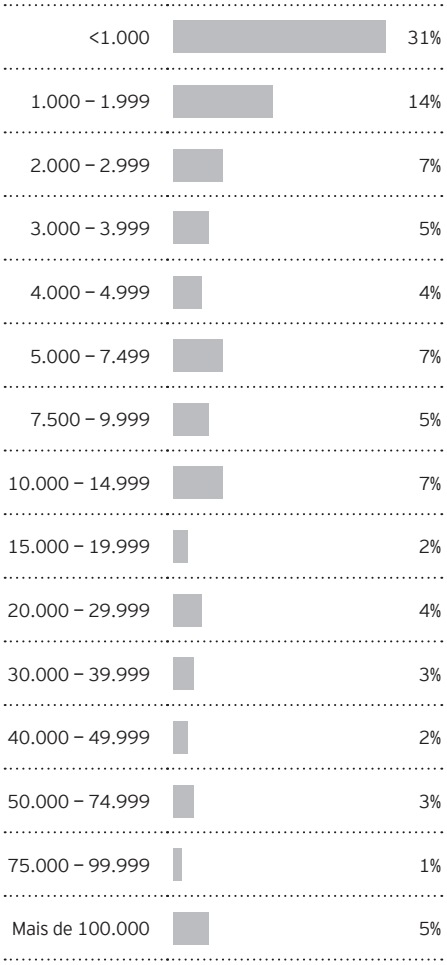
Respondentes distribuídos pela receita total anual da empresa

Todos os valores estão em dólar americano (USD)

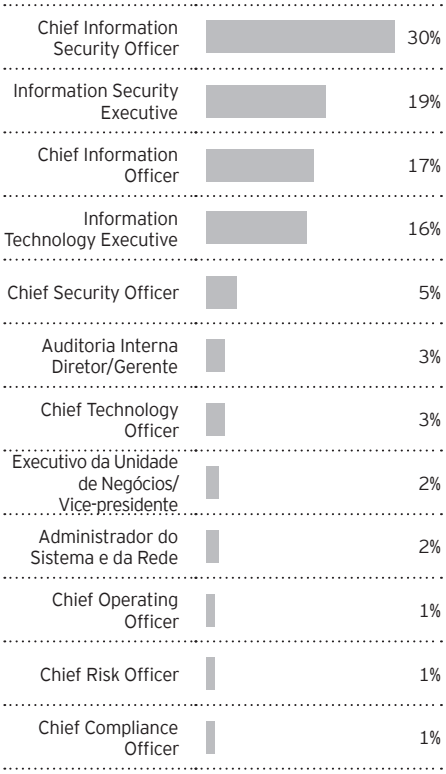
Menos de 10 milhões	5%
De 10 milhões a 25 milhões	5%
De 25 milhões a 50 milhões	4%
De 50 milhões a 100 milhões	6%
De 100 milhões a 250 milhões	9%
De 250 milhões a 500 milhões	9%
De 500 milhões a 1 bilhão	11%
De 1 bilhão a 2 bilhões	10%
De 2 bilhões a 3 bilhões	7%
De 3 bilhões a 4 bilhões	4%
De 4 bilhões a 5 bilhões	3%
De 5 bilhões a 7,5 bilhões	4%
De 7,5 bilhões a 10 bilhões	3%
De 10 bilhões a 15 bilhões	3%
De 15 bilhões a 20 bilhões	2%
De 20 bilhões a 50 bilhões	4%
Mais de 50 bilhões	3%
Governo e organizações sem fins lucrativos	6%
Não aplicável	4%

Respondentes por setor de atividade

Respondentes por número de funcionários



Respondentes por posição na empresa



Você gostaria de saber mais?

Insights sobre governança, risco e compliance é uma série de relatórios sobre liderança focados em TI e outros riscos empresariais e nos diversos desafios e oportunidades relacionados. Essas publicações sobre o tema foram concebidas para ajudá-lo a entender melhor o assunto e proporcionar insights valiosos sobre a nossa perspectiva. Visite nosso site www.ey.com/GRCinsights e conheça a nossa série Insights sobre governança, risco e compliance.

Informações sobre as ameaças cibernéticas - como se antecipar ao crime cibernético

www.ey.com/CTI

SOC gerenciado - Centro de Segurança Avançada da EY: segurança cibernética de alto nível trabalhando para você

http://www.ey.com/managedSOC

Conquistando a resiliência no ecossistema cibernético

www.ey.com/cyberecosystem

Centros de Operações de Segurança - ajudando você a se antecipar ao crime cibernético

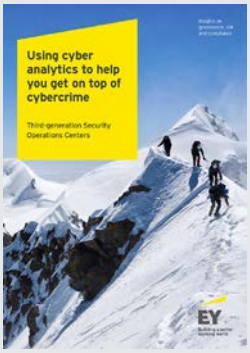
www.ey.com/SOC

Antecipe-se ao crime cibernético: Pesquisa Global da EY sobre Segurança de Informação 2014

www.ey.com/GISS2014

A Segurança Cibernética e a Internet das Coisas

www.ey.com/IoT



Usando a analítica cibernética para obter informações atualizadas sobre o crime cibernético: Centro de Operações de Segurança de Terceira Geração

www.ey.com/3SOC

Programa de Gestão Cibernética: identificando os caminhos para se antecipar ao crime cibernético

www.ey.com/CPM

Gestão de resposta às violações cibernéticas - Violações acontecem. Você está preparado?

www.ey.com/cyberBRM

Se você sofresse um ataque cibernético, você perceberia?

Para a EY Advisory, um mundo de negócios melhor significa solucionar os grandes e complexos problemas do setor, capitalizar as oportunidades e concretizar resultados que ajudem a crescer, otimizar e proteger os negócios dos nossos clientes. Formamos um ecossistema global de consultores, profissionais do setor e alianças com parceiros com um único objetivo em mente - você.

Acreditamos que a única forma de estar à frente dos criminosos cibernéticos e se defender deles é prever seus ataques. Focando em você, conseguimos formular as melhores perguntas sobre as suas operações, prioridades e vulnerabilidades.
E trabalhamos juntos para criar respostas mais inovadoras que o ajudarão a implementar as soluções de que necessita. Vamos ajudá-lo a obter resultados melhores e mais duradouros, da estratégia à execução.

Acreditamos que, quando as organizações gerenciam melhor a segurança cibernética, o mundo funciona melhor.

Quanto melhor a pergunta. Melhor a resposta. Melhor o mundo de negócios.

Sobre a EY

A EY é líder global em serviços de Auditoria, Impostos, Transações Corporativas e Consultoria. Nossos insights e os serviços de qualidade que prestamos ajudam a criar confiança nos mercados de capitais e nas economias ao redor do mundo. Desenvolvemos líderes excepcionais que trabalham em equipe para cumprir nossos compromissos perante todas as partes interessadas. Com isso, desempenhamos papel fundamental na construção de um mundo de negócios melhor para nossas pessoas, nossos clientes e nossas comunidades.

No Brasil, a EY é a mais completa empresa de Auditoria, Impostos, Transações Corporativas e Consultoria, com 5.000 profissionais que dão suporte e atendimento a mais de 3.400 clientes de pequeno, médio e grande portes.

A EY Brasil é Apoiadora Oficial dos Jogos Olímpicos e Paralímpicos Rio 2016 e fornecedora exclusiva de serviços de Consultoria para o Comitê Organizador. O alinhamento dos valores do Movimento Olímpico com os da EY foi decisivo nessa iniciativa.

EY refere-se à organização global e pode referir-se também a uma ou mais firmas-membro da Ernst & Young Global Limited (EYG), cada uma das quais é uma entidade legal independente. A Ernst & Young Global Limited, companhia privada constituída no Reino Unido e limitada por garantia, não presta serviços a clientes. Para mais informações sobre nossa organização, visite ey.com.br.

© 2016 Ernst & Young Global Limited.
Todos os direitos reservados

Esta é uma publicação do Departamento de Marca, Marketing e Comunicação. A reprodução deste conteúdo, na totalidade ou em parte, é permitida desde que citada a fonte.

www.ey.com.br

facebook | EYBrasil
twitter | EY_Brasil
linkedin | ernstandyoung
app | ey.com.br/eyinsights

Nossos líderes na área de Riscos são:

Líder global de Riscos		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Líderes de Risco por área		
Américas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Ásia-Pacífico		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japão		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp

Nossos líderes em Segurança da Informação são:

Líder global de Segurança da Informação		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Líderes das áreas de Segurança da Informação		
Américas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
EMEIA		
Scott Gelber	+44 207 951 6930	sgelber@uk.ey.com
Ásia-Pacífico		
Paul O'Rourke	+65 8691 8635	paul.o'rourke@sg.ey.com
Japão		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp

Nossos contatos de Segurança da Informação no Brasil são:

Sócios de Segurança da Informação		
Sergio Kogan	+55 11 2573 3395	sergio.kogan@br.ey.com
Demetrio Carrión	+55 21 3263 7038	demetrio.carrion@br.ey.com

APOIADOR OFICIAL