Kroll

RELATÓRIO GLOBAL DE FRAUDE E RISCO

Construindo Resiliência em um Mundo Volátil

EDIÇÃO ANUAL **2016/17**

Resumo da Pesquisa

Introdução

Há uma década, o Relatório Global de Fraudes da Kroll avalia o ambiente atual de fraudes e compartilha as conclusões de entrevistas realizadas no mundo inteiro, com executivos de alto-escalão de diversos setores. Na pesquisa deste ano, a Kroll expandiu o âmbito de sua investigação para incluir uma gama mais ampla de riscos enfrentados pela comunidade empresarial. O Relatório Global de Fraude e Risco da Kroll inclui agora, além de tendências relacionadas à incidência de fraudes, parâmetros para riscos cibernéticos e de segurança física.

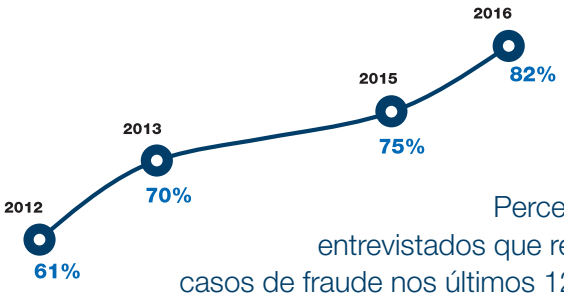
Os resultados da pesquisa deste ano refletem um ambiente de negócios repleto de riscos de crescente complexidade, autores e canais diversos, assim como a adoção de políticas e procedimentos de mitigação de risco para fortalecer as defesas internas. Alguns destaques principais da pesquisa serão apresentados a seguir.

1 Alta incidência e repercussões generalizadas

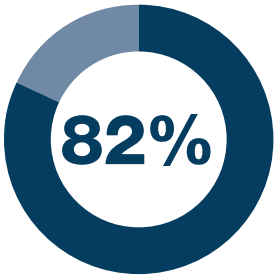
Incidência

FRAUDE

De acordo com a pesquisa deste ano, a incidência de fraudes mantém sua tendência de crescimento acentuado. No total, 82% dos executivos entrevistados relataram pelo menos um caso de fraude no ano passado, acima dos 75% relatados em 2015. Isso confirma a tendência de crescimento divulgada em Relatórios de Fraude anteriores da Kroll, que apresentaram uma incidência de fraudes de 61% em 2012 e de 70% em 2013.



Percentual de entrevistados que relataram casos de fraude nos últimos 12 meses



dos entrevistados relataram pelo menos um incidente de fraude

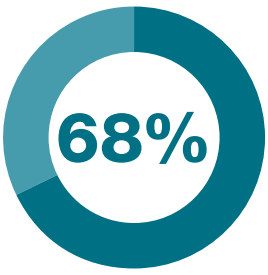
CIBERSEGURANÇA

85% dos entrevistados disseram que sua empresa sofreu ciberataque, roubo, perda ou ataque envolvendo seus dados nos últimos 12 meses.

dos entrevistados disseram que sua empresa sofreu um ciberataque ou perda, roubo e ataque a informações

SEGURANÇA

Mais de dois terços (68%) dos entrevistados relataram pelo menos um incidente de segurança no último ano.



dos entrevistados relataram um incidente de segurança

Repercussões

A pesquisa mostra que um incidente de fraude, cibersegurança ou segurança tem repercussões amplas para os funcionários e clientes de uma empresa, assim como para sua receita e reputação.

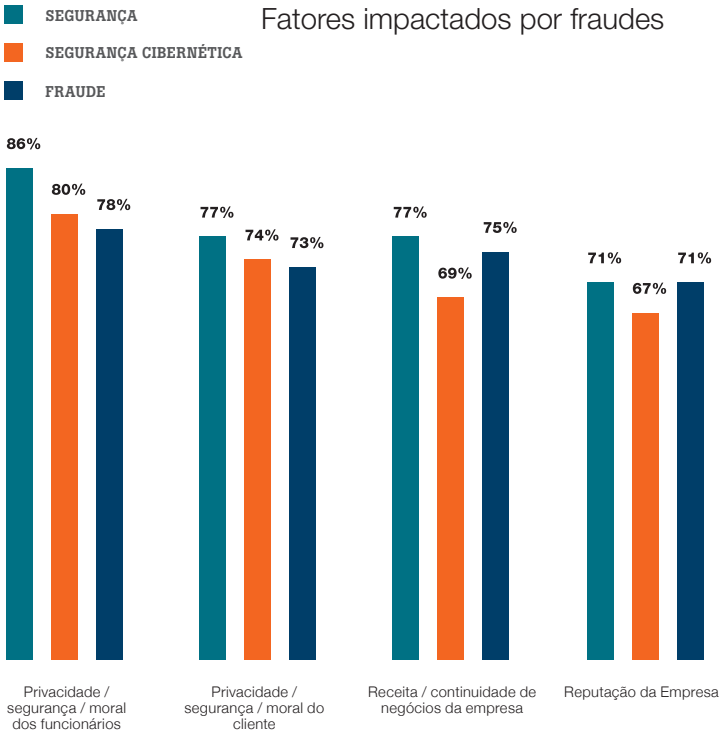
- A maior repercussão foi o impacto sobre os funcionários: 86% dos entrevistados que relataram um incidente de segurança disseram que a privacidade, segurança ou moral dos seus funcionários foi afetada. Esse nível de impacto foi relatado por 80% dos entrevistados que citaram pelo menos um ciberataque e por 78% dos que citaram pelo menos um incidente de fraude.

- Enquanto o número global de incidentes de segurança é menor do que o número de incidentes de fraude ou ciberataques, o impacto é maior. Além do impacto sobre os funcionários, 77% dos que relataram pelo menos um incidente de segurança declararam que seus clientes e suas receitas foram afetados, e 71% afirmaram que a reputação da sua empresa foi impactada.

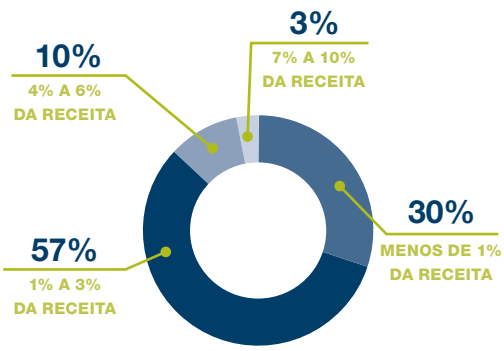
- Entre os entrevistados que sofreram um ciberataque, quase três quartos (74%) observaram que a privacidade, segurança ou satisfação dos seus clientes foi afetada.

- Os entrevistados afirmaram que os casos de fraude causaram danos econômicos significativos. A maioria (57%) dos executivos estimou que os prejuízos relacionados à fraude representam entre 1% e 3% de suas receitas, e uma em cada 10 empresas registrou uma perda entre 4% e 6% das receitas.

Fatores impactados por fraudes



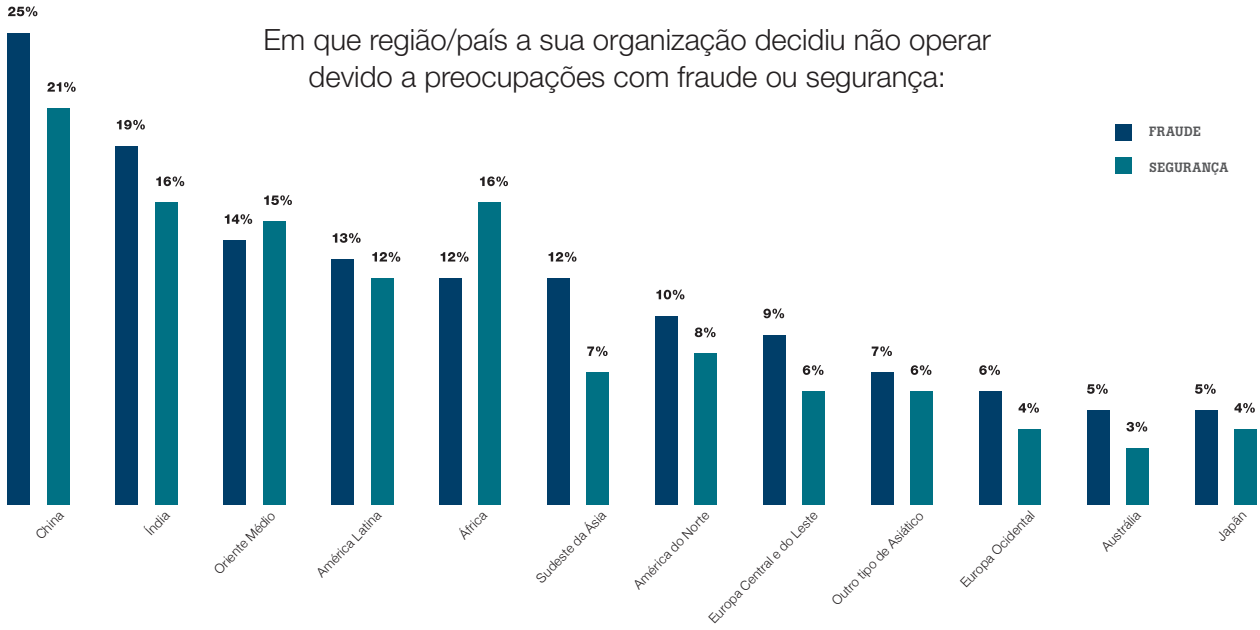
Estimativa de perdas relacionadas à fraude nos últimos 12 meses



Riscos regionais

A globalização de negócios trouxe oportunidades de expansão estratégica, e também uma grande variedade de riscos regionais. De fato, 69% dos executivos disseram que foram aconselhados a não operar em um determinado país ou região no ano passado, porque isso aumentaria sua exposição à fraude. Da mesma forma, 63% dos entrevistados se afastaram de determinadas regiões devido a preocupações com segurança.

As preocupações são mais elevadas em relação a operações localizadas na China e na Índia.



Os entrevistados do setor industrial apresentaram os maiores índices de fraude (89% relataram um incidente no ano passado). Mais da metade dos participantes do setor industrial (51%) considerou a entrada em mercados novos e de maior risco um fator chave para o crescente risco de fraude.

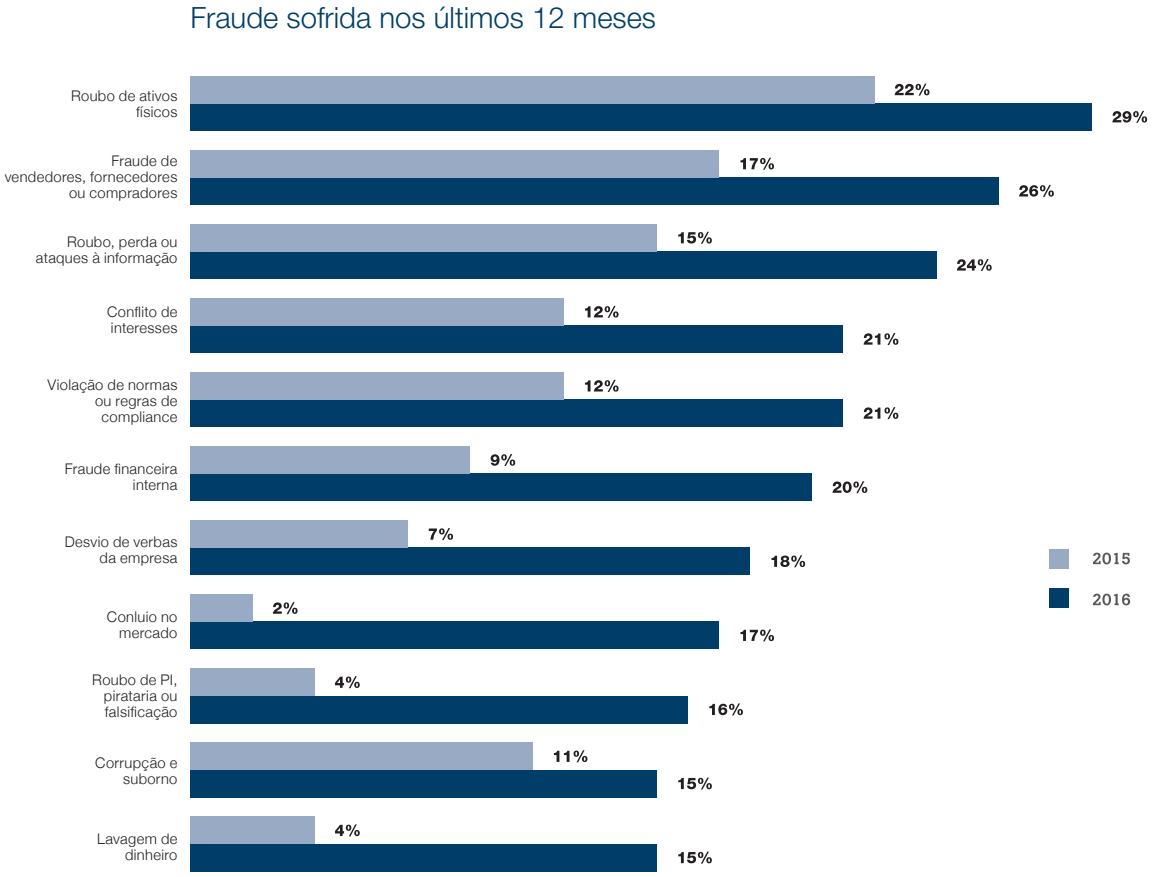
2 A complexidade da ameaça

A grande variedade de incidentes, autores e meios de ataque mostram que o ambiente de gerenciamento de risco corporativo é cada vez mais complexo.

Tipos de incidentes com impacto sobre os negócios

TIPOS DE FRAUDES

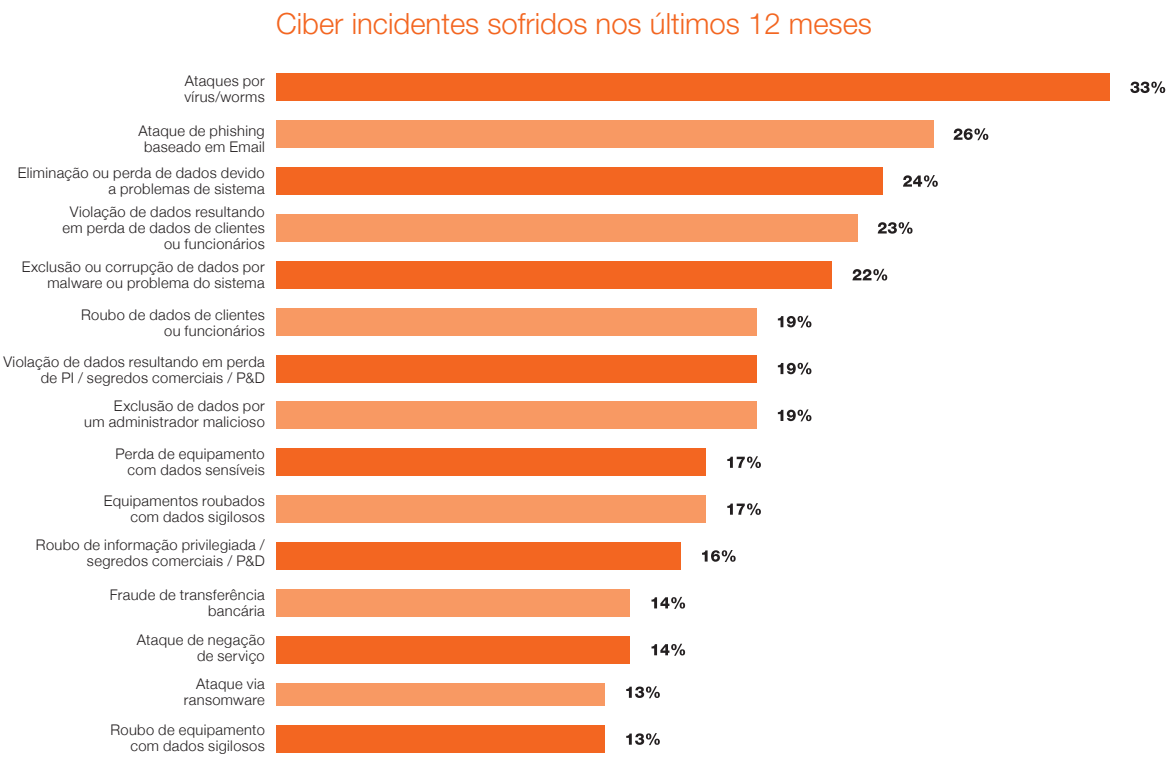
No ano passado, os entrevistados relataram crescimento de todos os tipos de fraude citados na pesquisa de 2015. Além disso, a incidência declarada de cada tipo de fraude atingiu níveis de dois dígitos.



O roubo de ativos físicos ainda foi o tipo de fraude mais comum durante o ano passado, relatado por 29% dos entrevistados, e até 7 pontos percentuais acima dos 22% registrados na última pesquisa. As fraudes cometidas por vendedores, fornecedores ou compradores (26%) e o roubo, perda ou ataques envolvendo informações da empresa (24%) foram citados como o segundo e terceiro tipos de fraude mais comuns, cada um crescendo 9 pontos percentuais comparado com os resultados de 2015.

TIPOS DE CIBERATAQUES

A pesquisa mostra que as empresas passaram por muitos ciberataques com vários níveis de complexidade.



Um terço (33%) dos executivos entrevistados disseram que foram atingidos por um vírus ou *worm*, o tipo mais frequente de ciberataque mencionado no relatório deste ano. O segundo tipo mais frequente de ciberataque, o ataque de *phishing* baseado em e-mail, foi citado por pouco mais de um quarto (26%) de todos os participantes.

Nessa era de Big Data, a pesquisa revelou que muitos dados foram perdidos ou roubados durante ciberataques, que incluem, entre outros, violação de dados, supressão de dados e perda de equipamentos com dados sigilosos.

- **Violação de dados:** Cerca de um quarto (23%) dos entrevistados disseram que a violação de dados resultou na perda de dados de clientes ou funcionários, enquanto 19% mencionaram perda de Propriedade Intelectual (PI), de segredos comerciais e de Pesquisa & Desenvolvimento (P&D).

- **Exclusão de dados:** 24% dos executivos entrevistados mencionaram incidentes de exclusão de dados devido a problemas de sistema, 22% sofreram exclusão ou corrupção de dados como resultado de malware ou problemas de sistema e 19% foram vítimas de eliminação de dados por um insider malicioso.

- **Perda de equipamentos:** 17% informaram que equipamentos com dados sensíveis foram perdidos e 13% relataram que esse tipo de equipamento foi roubado.

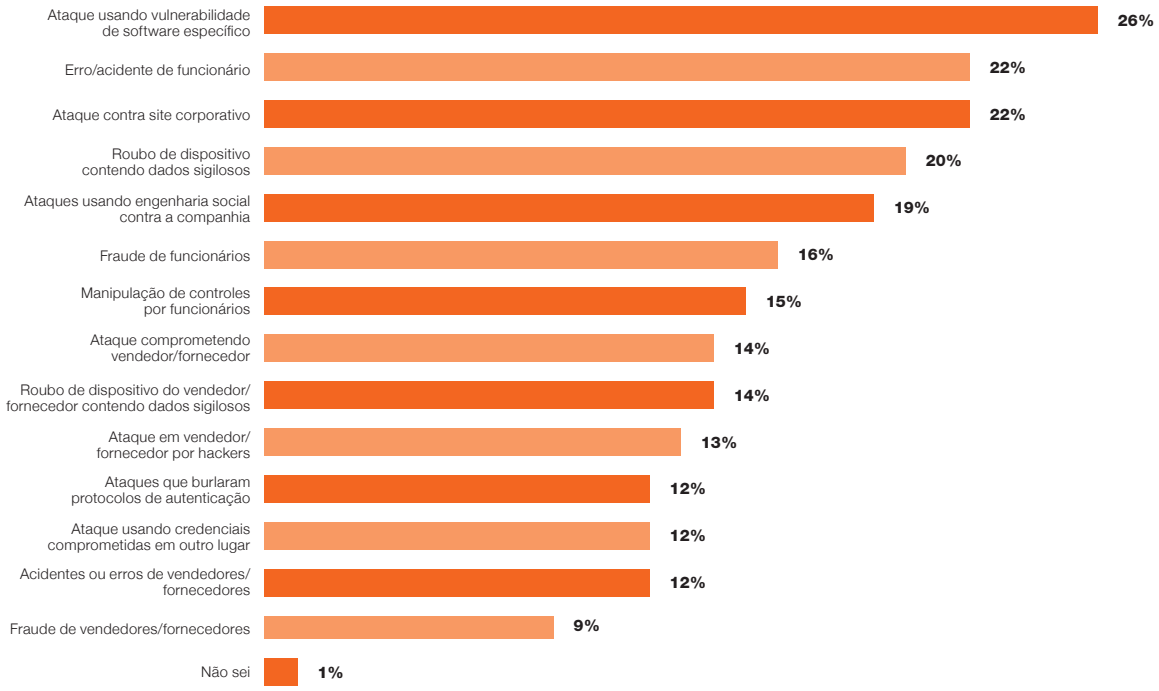
Como ciber incidentes acontecem

A pesquisa também revela que a maioria dos ciberataques envolve mais de um vetor de ataque. Múltiplos vetores de ataque foram identificados - por softwares, sistemas e sites corporativos; por terceiros, em atividades dolosas, ataques contra sistemas ou erro; por erro ou fraude de funcionário; e por roubo de dispositivos.

O principal vetor de ataque relatado pelos entrevistados foi a vulnerabilidade de software, que afetou mais de um quarto dos entrevistados (26%). Erros de funcionários ou acidentes foram relatados por 22% dos entrevistados. E outros 22% também observaram ataques em sites corporativos.

Se sua empresa sofreu um ciberataque, ataque, roubo ou perda de informação nos últimos 12 meses, qual seria a sua descrição do evento?

(Participantes foram instruídos a escolher até três respostas)



Responsáveis

Os resultados revelam que as ameaças geralmente vêm de dentro da empresa. Os funcionários atuais ou antigos foram os principais responsáveis por fraudes, ciberataques e incidentes de segurança nos últimos 12 meses. Mesmo assim, terceiros também foram identificados como autores ativos.

RESPONSÁVEIS POR FRAUDE

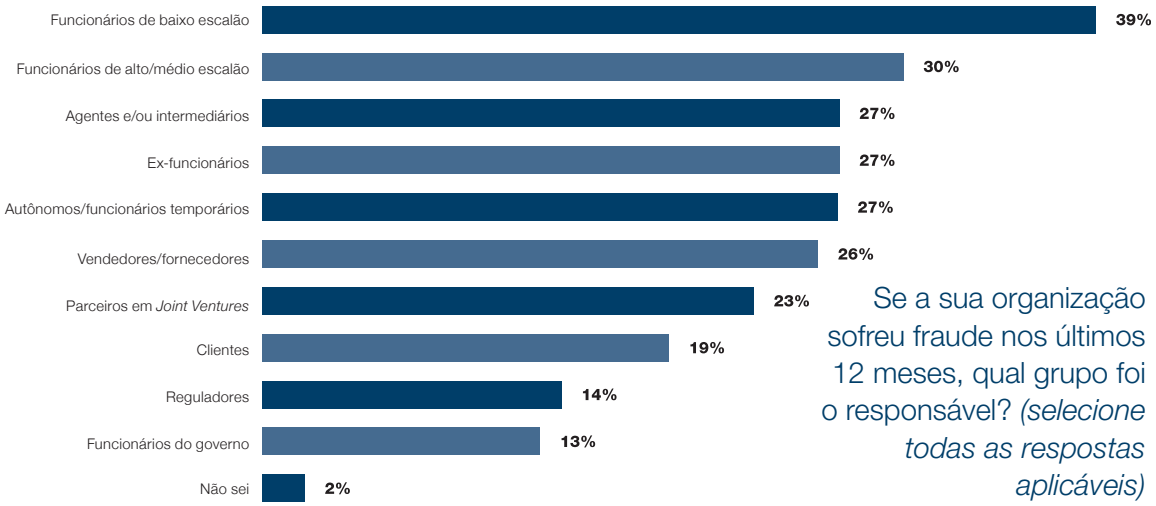
Quase 8 entre cada 10 entrevistados (79%) citou uma das opções a seguir como o principal responsável:

- Funcionários de alto e médio escalão da própria empresa
- Empregado júnior da própria empresa
- Ex-funcionários
- Autônomos e empregados temporários

Refletindo a complexidade dos riscos de fraude, a maioria (60%) dos executivos que relataram incidentes identificou uma combinação de responsáveis que inclui funcionários atuais, ex-funcionários e terceiros, com quase a metade dos casos (49%) envolvendo todos os três grupos. Praticamente quatro em dez entrevistados (39%) que foram vítimas de fraude sinalizaram que ela foi cometida por um empregado de baixo escalão, 30% por gerentes de alto e médio escalão, 27% por ex-funcionários e 27% por autônomos e funcionários temporários. Os agentes e intermediários, que podem ser considerados quase funcionários, também foram citados por 27% dos respondentes.

Os insiders são citados como os principais responsáveis por fraudes, mas eles também são identificados como os mais propensos a descobri-las. Quase metade (44%) dos entrevistados disse que recentemente descobriu uma fraude por meio de sistema de denúncias e 39% a detectaram por meio de auditoria interna.

Responsáveis por fraude

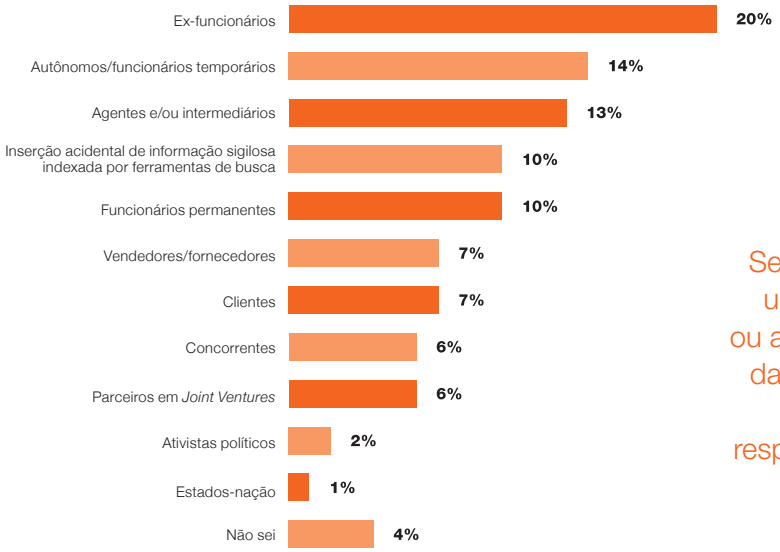


Se a sua organização sofreu fraude nos últimos 12 meses, qual grupo foi o responsável? *(selecione todas as respostas aplicáveis)*

AUTORES DE CIBER INCIDENTES

Em geral, 44% dos entrevistados reportaram que os *insiders* foram os principais responsáveis por um ciber incidente, citando ex-funcionários (20%), autônomos e funcionários temporários (14%) e funcionários permanentes (10%). Ao considerar como quase funcionários os agentes e intermediários, apontados como autores por 13% dos participantes, os *insiders* passam a representar a maioria, ou 57% dos responsáveis. Por outro lado, um em cada três entrevistados (29%) identificou atores externos como os principais responsáveis.

Autores de ataques cibernéticos ou roubo, perda e ataque envolvendo informações



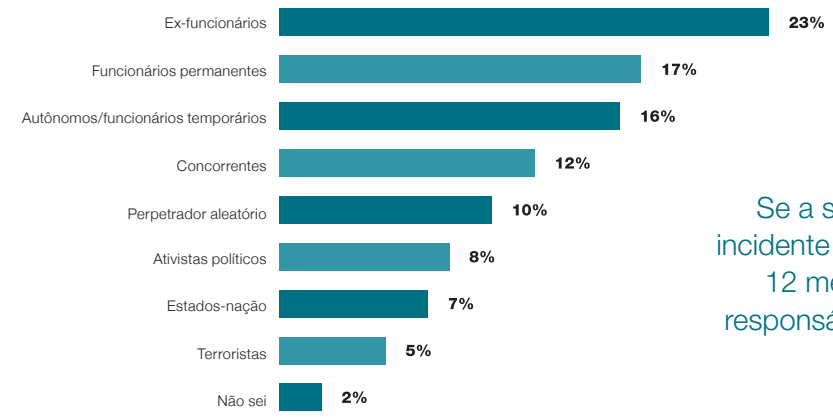
Se a sua organização passou por um ciberataque ou perda, roubo ou ataque envolvendo informações da companhia durante os últimos 12 meses, quem foi o principal responsável? *(escolha uma opção)*

RESPONSÁVEIS POR INCIDENTES DE SEGURANÇA

No total, 56% dos executivos entrevistados disseram que os *insiders* são os principais responsáveis por incidentes de segurança, citando ex-funcionários (23%), funcionários permanentes (17%) e autônomos e funcionários temporários (16%).

Curiosamente, em termos de autores externos, mais de um em dez (12%) dentre os entrevistados apontaram os concorrentes como grupo chave e 10% apontaram autores aleatórios. Em conjunto, os ativistas políticos, estados-nação e terroristas representam 20% das respostas.

Autores de incidentes de segurança



Se a sua organização sofreu um incidente de segurança nos últimos 12 meses, quem era o principal responsável? *(escolha uma opção)*

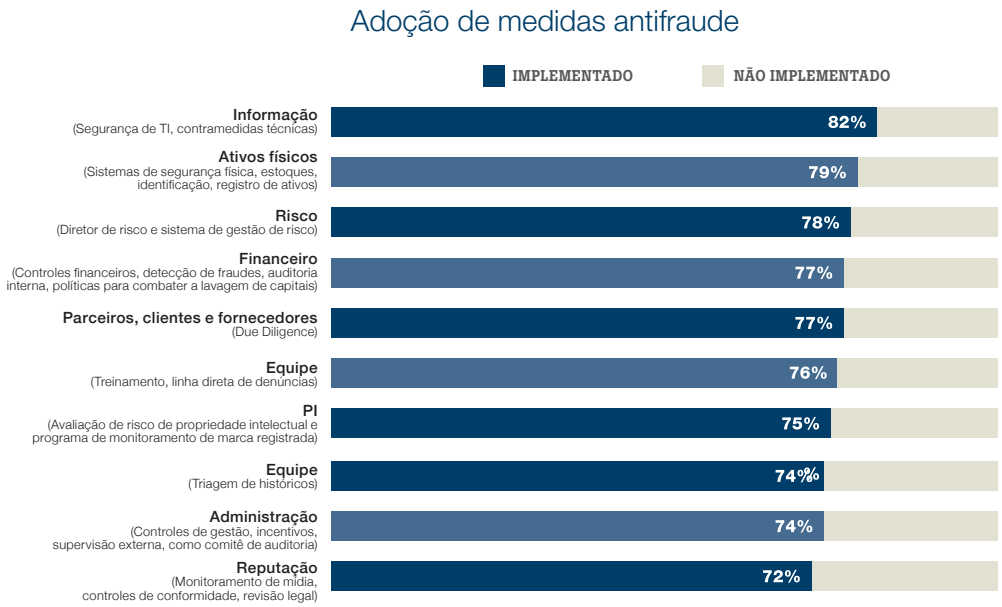
3 Construindo defesas

Diante do alto nível de risco empresarial, custos significativos e impacto generalizado sobre as partes interessadas e a reputação corporativa, as empresas adotaram muitas medidas para reduzir o risco de fraudes, incidentes cibernéticos e de segurança. Contudo, ainda é necessário fazer mais para construir e manter uma defesa robusta.

A seguir, apresentamos um resumo das medidas que muitas empresas já adotaram - frequentemente com planos de expandi-las.

Medidas adotadas para mitigação de riscos

MEDIDAS PARA REDUZIR O RISCO DE FRAUDE

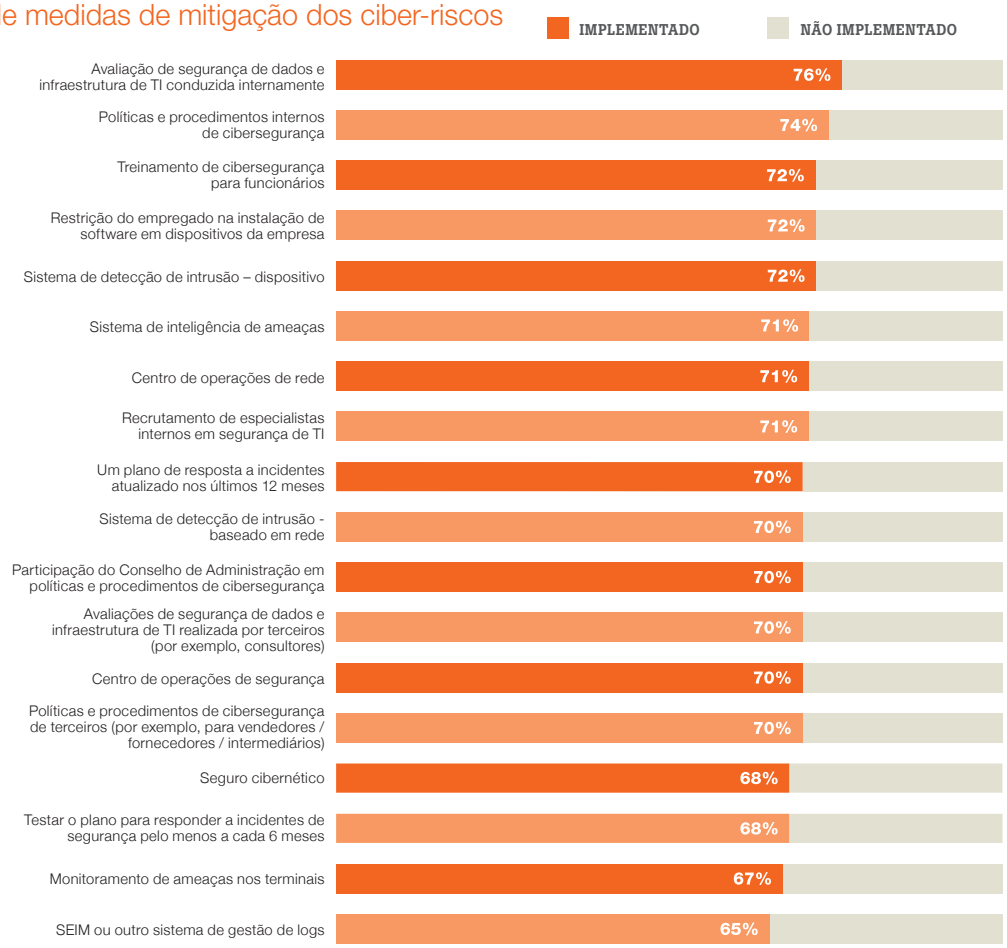


A medida mais popularmente implementada para combater a fraude - mencionada por 82% dos executivos pesquisados - foca na proteção de informações, como segurança de TI e contramedidas técnicas. Por outro lado, é preocupante constatar que quase um quinto dos entrevistados (18%) não adotou esse tipo de proteção. Como observado anteriormente neste relatório, o tipo de fraude mais frequente foi o roubo de ativos físicos ou estoques (29% dos executivos pesquisados); por esse motivo, a segunda medida antifraude mais usada está focada na proteção de ativos, como a utilização de sistemas de segurança física e de identificação. Curiosamente, a terceira medida mais popular foi a nomeação de um diretor de risco e a instalação de um sistema formal de gerenciamento de riscos. Logo em seguida está a implementação de controles financeiros (77%), que possui o mesmo percentual que o *due diligence* em terceiros.

O grande volume de dados internos mantido pelas empresas pode ser muito valioso na luta contra a fraude. Por exemplo, ferramentas de análise de dados em conjunto com análises de especialistas frequentemente levantam importantes alertas e identificam anomalias durante investigações envolvendo suborno e corrupção.

MEDIDAS DE MITIGAÇÃO DO RISCO CIBERNÉTICO

Adoção de medidas de mitigação dos ciber-riscos



Os entrevistados revelaram que a medida mais comum para mitigação do risco cibernético foi a realização de avaliações internas de segurança de dados e infraestrutura de TI, citadas por 76% dos executivos pesquisados. Observamos que 70% dos respondentes também citou a contratação de um terceiro/consultor para avaliar a segurança de dados e infraestrutura de TI. Quase três quartos (74%) dos participantes dizem que sua empresa implementou políticas e procedimentos internos de cibersegurança.

Conforme discutido anteriormente, os *insiders* (funcionários permanentes, temporários/autônomos e ex-funcionários) são responsáveis por 44% dos ciber incidentes, motivando a adoção de treinamentos e políticas internas: 72% introduziram treinamento em cibersegurança para seus funcionários e igual percentual aplicou restrições para a instalação de software em dispositivos da empresa.

Métodos de detecção também são populares, com sistemas de detecção de intrusão, sistemas de inteligência para ameaças e centros de operações de rede próximos no ranking.

85% dos entrevistados reportaram ciber incidentes nos últimos 12 meses e, por isso, gera preocupação o fato de que apenas 70% disseram que suas empresas mantêm um plano para responder a incidentes de segurança da informação atualizado nos últimos 12 meses, e apenas 68% testam seu plano de resposta a cada seis meses.

Notamos que 70% dos participantes do estudo dizem que sua diretoria está envolvida em políticas e procedimentos de cibersegurança, um número que reflete a importância das questões de governança cibernética.

Mapa de Risco Global

CANADÁ

FRAUDE	88%
CIBER	85%
SEGURANÇA	78%

Maior contato com o público via canais digitais é o principal fator de aumento do risco de fraude (citado por 54% dos entrevistados)

93% Acreditam que a exposição à fraude aumentou

REINO UNIDO

FRAUDE	90%
Ciber	92%
SEGURANÇA	82%

O alto índice de rotatividade de funcionários é o principal fator de aumento do risco de fraude (citado por 47% dos entrevistados)

92% Acreditam que a exposição à fraude aumentou

ESTADOS UNIDOS

FRAUDE	80%
CIBER	88%
SEGURANÇA	58%

A complexidade da infraestrutura deTI é o principal fator de aumento do risco de fraude (citado por 50% dos entrevistados)

94% Acreditam que a exposição à fraude aumentou

MÉXICO

FRAUDE	82%
CIBER	82%
SEGURANÇA	48%

Aumento de terceirização e offshoring é o principal fator no aumento do risco de fraude (citado por 45% dos entrevistados)

94% Acreditam que a exposição à fraude aumentou

COLÔMBIA

FRAUDE	95%
CIBER	95%
SEGURANÇA	62%

A entrada em mercados novos e de maior risco e a complexidade da infraestrutura de TI são os principais fatores para aumento do risco de fraude (citado por 29% dos entrevistados)

100% Acreditam que a exposição à fraude aumentou

BRASIL

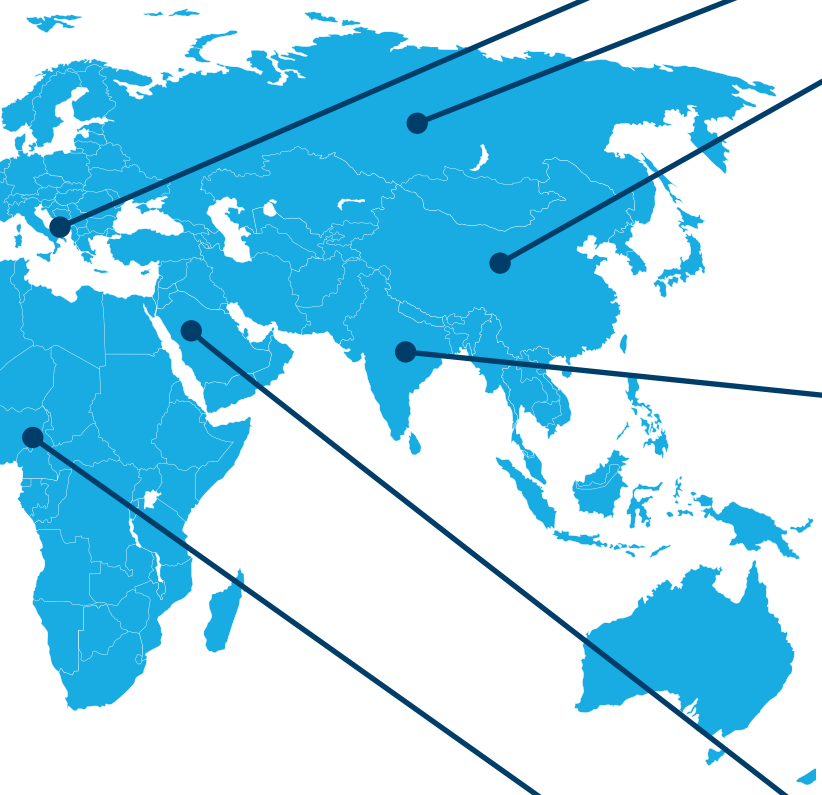
FRAUDE	68%
CIBER	76%
SEGURANÇA	53%

A entrada em mercados novos e de maior risco e a complexidade da infraestrutura de TI são os principais fatores de aumento do risco de fraude (citado por 29% dos entrevistados)

94% Acreditam que a exposição à fraude aumentou

Base: 545 executivos que influenciam ou são responsáveis por estratégias para combater risco e fraude em suas empresas

Fonte: Relatório produzido pela Forrester Consulting a pedido da Kroll, Agosto de 2016



ITÁLIA

FRAUDE	77%
CIBER	79%
SEGURANÇA	68%

91% Acreditam que a exposição à fraude aumentou

A entrada em mercados novos e de maior risco é o principal fator de aumento do risco de fraude (citado por 36% dos entrevistados)

RÚSSIA

FRAUDE	82%
CIBER	82%
SEGURANÇA	59%

85% Acreditam que a exposição à fraude aumentou

O alto índice de rotatividade de funcionários é o principal fator de aumento do risco de fraude (citado por 31% dos entrevistados)

CHINA

FRAUDE	86%
CIBER	86%
SEGURANÇA	75%

92% Acreditam que a exposição à fraude aumentou

O alto índice de rotatividade de funcionários é o principal fator de aumento do risco de fraude (citado por 55% dos entrevistados)

ÍNDIA

FRAUDE	68%
CIBER	73%
SEGURANÇA	72%

78% Acreditam que a exposição à fraude aumentou

A entrada em mercados novos e de maior risco é o principal fator de aumento do risco de fraude (citado por 45% dos entrevistados)

ÁFRICA SUBSAARIANA

FRAUDE	89%
CIBER	91%
SEGURANÇA	74%

93% Acreditam que a exposição à fraude aumentou

Maior contato com o público via canais digitais é o principal fator de aumento do risco de fraude (citado por 33% dos entrevistados)

ORIENTE MÉDIO

FRAUDE	88%
CIBER	90%
SEGURANÇA	82%

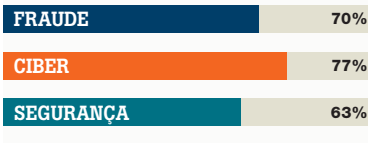
94% Acreditam que a exposição à fraude aumentou

A complexidade da infraestrutura de TI e a falta de orçamento/recursos para a infraestrutura de compliance são os principais fatores que aumentam o risco de fraude (citado por 34% dos entrevistados)

Mapa de Risco da Indústria

O mapa mostra o percentual de participantes de cada grupo industrial cujas empresas sofreram com fraude, incidentes cibernéticos ou de segurança nos últimos 12 meses.

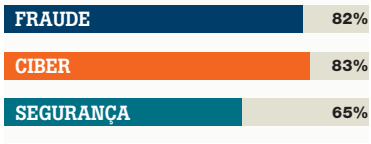
CONSTRUÇÃO, ENGENHARIA E INFRAESTRUTURA



O alto índice de rotatividade de funcionários é o principal fator de aumento do risco de fraude (citado por 40% dos entrevistados)

86%
Acreditam que a exposição à fraude aumentou

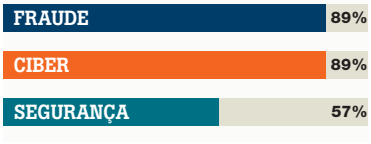
BENS DE CONSUMO



A entrada em mercados novos e de maior risco é o principal fator de aumento do risco de fraude (citado por 40% dos entrevistados)

92%
Acreditam que a exposição à fraude aumentou

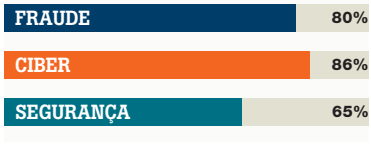
SERVIÇOS FINANCEIROS



A entrada em mercados novos e de maior risco é o principal fator de aumento do risco de fraude (citado por 34% dos entrevistados)

91%
Acreditam que a exposição à fraude aumentou

SERVIÇOS DE SAÚDE, FARMACÊUTICAS E BIOTECNOLÓGICOS



O alto índice de rotatividade de funcionários é o principal fator de aumento do risco de fraude (citado por 41% dos entrevistados)

88%
Acreditam que a exposição à fraude aumentou

MANUFATURA

A entrada em mercados novos e de maior risco é o principal fator de aumento do risco de fraude (citado por 51% dos entrevistados)

96%
Acreditam que a exposição à fraude aumentou

VAREJO, COMÉRCIO E DISTRIBUIDORAS

Maior contato com o público via canais digitais é o principal fator de aumento do risco de fraude (citado por 33% dos entrevistados)

87%
Acreditam que a exposição à fraude aumentou

RECURSOS NATURAIS

O alto índice de rotatividade de funcionários é o principal fator de aumento do risco de fraude (citado por 40% dos entrevistados)

92%
Acreditam que a exposição à fraude aumentou

TRANSPORTE, LAZER E TURISMO

O alto índice de rotatividade de funcionários é o principal fator de aumento do risco de fraude (citado por 43% dos entrevistados)

96%
Acreditam que a exposição à fraude aumentou

SERVIÇOS PROFISSIONAIS

O alto índice de rotatividade de funcionários é o principal fator de aumento do risco de fraude (citado por 47% dos entrevistados)

96%
Acreditam que a exposição à fraude aumentou

TECNOLOGIA, MÍDIA E TELECOMUNICAÇÕES

A complexidade da infraestrutura TI é o principal fator de aumento do risco de fraude (citado por 39% dos entrevistados)

86%
Acreditam que a exposição à fraude aumentou

Base: 545 executivos que influenciam ou são responsáveis por estratégias para combater risco e fraude em suas empresas

Fonte: Relatório produzido pela Forrester Consulting a pedido da Kroll, Agosto de 2016

4 Visão geral do Brasil

A partir de entrevistas com executivos sêniores brasileiros, atuantes em diversos setores da economia, o relatório apresenta resultados que, à primeira vista, podem surpreender no comparativo com o cenário global e com o ano anterior da pesquisa (2015).

Isso porque a detecção de fraudes no Brasil, segundo os respondentes do país, é menor do que a aferida no resto do mundo, ainda que a percepção de exposição à fraude em 2016 tenha aumentado, na visão de 94% dos respondentes brasileiros (em 2015, este número era de 80%).

Se por aqui as ocorrências de fraude no último ano levam à marca de 68%, o índice global é de 82% - uma diferença considerável de 14 pontos percentuais. O mesmo acontece com os eventos de segurança cibernética e segurança física, que também apresentam números abaixo da média global.

Em comparação com o ano anterior, o número de fraudes sofridas pelos respondentes brasileiros em 2016 foi reduzido em 7% - ainda que o total de fraudes reportadas para 'roubo de ativos físicos ou estoque' e 'fraude relacionada a compras, vendedores ou fornecedores' tenha aumentado de um ano para outro.

Nossa análise permite concluir que a desproporção entre os resultados brasileiro e global pode estar associada a um agravamento na deficiência de controles internos, possivelmente resultante da redução de investimentos associada à crise econômica. Corrobora esta hipótese o fato de que, na pesquisa de 2015, havia intenção abaixo da média global de implementar defesas antifraude.

Este cenário é preocupante na atual conjuntura do país, tendo em vista a importância crescente dada pela legislação, por autoridades e reguladores, a medidas antifraude e anti-risco.

É importante lembrar que os perpetradores continuam inovando em suas formas de atuação. A ameaça de risco nunca pode ser completamente eliminada e os impactos adversos não podem ser subestimados, sejam eles financeiros ou reputacionais.

RELATÓRIO DO BRASIL

Principais respostas dadas pelos entrevistados

Fraudes

68 — Percentual de respondentes afetados por fraude nos últimos 12 meses

▼ 9% pontos abaixo de 2015

▼ 14% pontos abaixo da média global de 82%

			média global
TIPOS MAIS COMUNS DE FRAUDE	Roubo de ativos físicos ou de estoque	**24%**	29%
	Roubo, ataque ou perda de informações *(ex., roubo de dados)*	**21%**	24%
	Fraude cometida por vendedores, fornecedores ou na aquisição	**21%**	26%
PRINCIPAIS RESPONSÁVEIS	Ex-funcionários	**43%**	27%
	Autônomos/funcionários temporários	**26%**	27%
	Funcionários de baixo escalão	**22%**	39%
	Vendedores/fornecedores*(ex., fornecedor de tecnologia ou serviços para sua empresa)*	**17%**	26%
	Agentes e/ou intermediários *(ex., um terceiro trabalhando em nome da sua empresa)*	**17%**	27%
	Parceiros em Joint Ventures *(ex., parceiro que fornece manufatura ou outra função comercial, ou um franqueado)*	**17%**	23%
	Clientes	**17%**	19%
MEDIDAS ANTIFRAUDE MAIS COMUNS *Percentual de respondentes que implementaram medidas antifraude*	Ativos *(sistemas de segurança física, estoques, marcação, registro de ativos)*	**88%**	79%
	Informação *(Segurança da informação, contramedidas técnicas)*	**88%**	82%
	Gestão *(controles de gestão, incentivos, supervisão externa, como comitê de auditoria)*	**85%**	74%
PRINCIPAIS MEIOS DE DESCOBERTA	Por meio de auditoria externa	**43%**	36%

Segurança cibernética

76 — Percentual de respondentes que sofreram um incidente cibernético nos últimos 12 meses

▼ 9% pontos abaixo da média global de 85%

			média global
TIPOS MAIS COMUNS DE INCIDENTES CIBERNÉTICOS	Ataques por vírus/worm	**41%**	33%
	Violação de dados resultando em perda de dados de clientes ou funcionários	**29%**	23%
	Eliminação ou perda de dados devido a problemas do sistema	**21%**	24%
PRINCIPAIS RESPONSÁVEIS	Ex-funcionários	**38%**	20%
PRINCIPAIS ALVOS	Registros de clientes	**46%**	51%
	Registros de funcionários	**42%**	40%
	Identidade da empresa/empregado	**42%**	36%
CONTATO MAIS COMUM APÓS UM INCIDENTE CIBERNÉTICO	Webhosting/provedor de site	**23%**	9%

Segurança

53 — Percentual de respondentes que sofreram um incidente de segurança nos últimos 12 meses

▼ 15% pontos abaixo da média global de 68%

			média global
TIPOS MAIS COMUNS DE INCIDENTES DE SEGURANÇA	Roubo ou perda de IP	**32%**	38%
	Risco ambiental *(Incluindo danos causados por desastres naturais como furacões, tornados, inundações, terremotos, etc.)*	**18%**	27%
	Risco geográfico e político *(ex., operação em áreas de conflito)*	**12%**	22%
PRINCIPAIS RESPONSÁVEIS	Ex-funcionários	**39%**	23%
RESPONDENTES SÃO MAIS SUSCETÍVEIS A SE SENTIR ALTAMENTE VULNERÁVEIS AOS SEGUINTES RISCOS DE SEGURANÇA	Roubo ou perda de IP	**21%**	19%
	Violência no local de trabalho	**18%**	27%
	Risco geográfico e político *(ex., operação em áreas de conflito)*	**15%**	12%
	Risco ambiental *(Incluindo danos causados por desastres naturais como furacões, tornados, inundações, terremotos, etc.)*	**15%**	20%

Menor número de fraudes no Brasil revela deficiência de controles internos

Por Glen Harloff e Fernanda Barroso

A edição atual do Relatório Global de Fraude & Risco 2016/17 aponta o crescimento da incidência de fraudes em todo o mundo. Os registros vêm aumentando ano a ano, vindo de 61% em 2012, para 70% em 2013, 75% em 2015, até chegar ao ápice de 82% no levantamento recente.

O recorte nacional, contudo, surpreende ao ir na contramão dessa tendência. Ao lado de Itália e Índia, o Brasil aparece abaixo da média global: 68% dos respondentes brasileiros relataram ter sofrido algum tipo de fraude em 2016. Seria o Brasil um oásis de segurança empresarial ou um país em que as fraudes são pouco detectadas?

A segunda hipótese é certamente a mais provável e pode decorrer de uma deficiência relevante de controles internos, fundamentada em antigos padrões culturais e de governança. Mesmo com um exercício recente de amadurecimento, as empresas ainda atribuem pouca importância ao Compliance e, consequentemente, demoram mais para detectar erros e fraudes do que países onde programas de conformidade são melhor estruturados.

A pesquisa realizada pela Kroll aponta que, para os respondentes brasileiros, o roubo ou desvio de inventário é o tipo mais frequente de fraude (24%), seguido por roubo ou perda de informação (21%), fraude de fornecedores ou no departamento de compras (21%) e conflitos de interesse (18%).

Chama atenção o fato de o maior inimigo responsável pelas fraudes estar dentro de casa: dentre as diversas partes que simultaneamente participaram das fraudes reportadas, 57% são funcionários, 43% são ex-funcionários e 26% são temporários. Ainda assim, o Background Screening (pesquisa reputacional, de conflitos de interesse e da experiência profissional de funcionários) não está entre as principais medidas a serem expandidas ou implementadas pelos respondentes brasileiros.

Em relação à segurança cibernética, os respondentes do Brasil também registraram índices inferiores de detecção de fraude em relação ao resto do mundo: 76% contra 85%, respectivamente. Aspectos regulatórios podem explicar esta diferença – enquanto no Brasil a Lei de Crimes Cibernéticos entrou em vigor em 2013, nos Estados Unidos, a primeira legislação sobre o tema foi sancionada há mais de 30 anos.

Entre os tipos de ataque cibernético mais comuns para os respondentes brasileiros estão infestação por vírus/ worm (41%), violação de dados de clientes ou funcionários (29%) e deleção ou perda de dados por conta de problemas sistêmicos (21%). O fato de informações de clientes poderem ser comprometidas por potenciais invasões cibernéticas é bastante preocupante e pode afetar de forma definitiva a reputação de empresas.

Os dados colhidos no Brasil, em comparação a outros países, evidenciam a necessidade de transformação dos padrões locais de governança e controles internos. Vale ressaltar que, apesar dos escândalos de corrupção no Brasil, o país não está entre as principais regiões evitadas para negócios, de acordo com os respondentes internacionais – China e Índia ocupam os primeiros lugares da lista. Para manter este cenário, portanto, é importante que as empresas implementem metodologias de prevenção à fraude, mudando o quadro de atuação reativa e gerando maior transparência para os shareholders.

Glen E. Harloff

Glen E. Harloff é Diretor Executivo da América Latina, Caribe e Brasil, especialista em Investigaçoes Financeiras, de lavagem de dinheiro e rastreamento de ativos.

Fernanda Barroso

Fernanda Barroso é Diretora Executiva Associada do escritório de São Paulo/ Brasil, especialista em Investigações Financeiras.

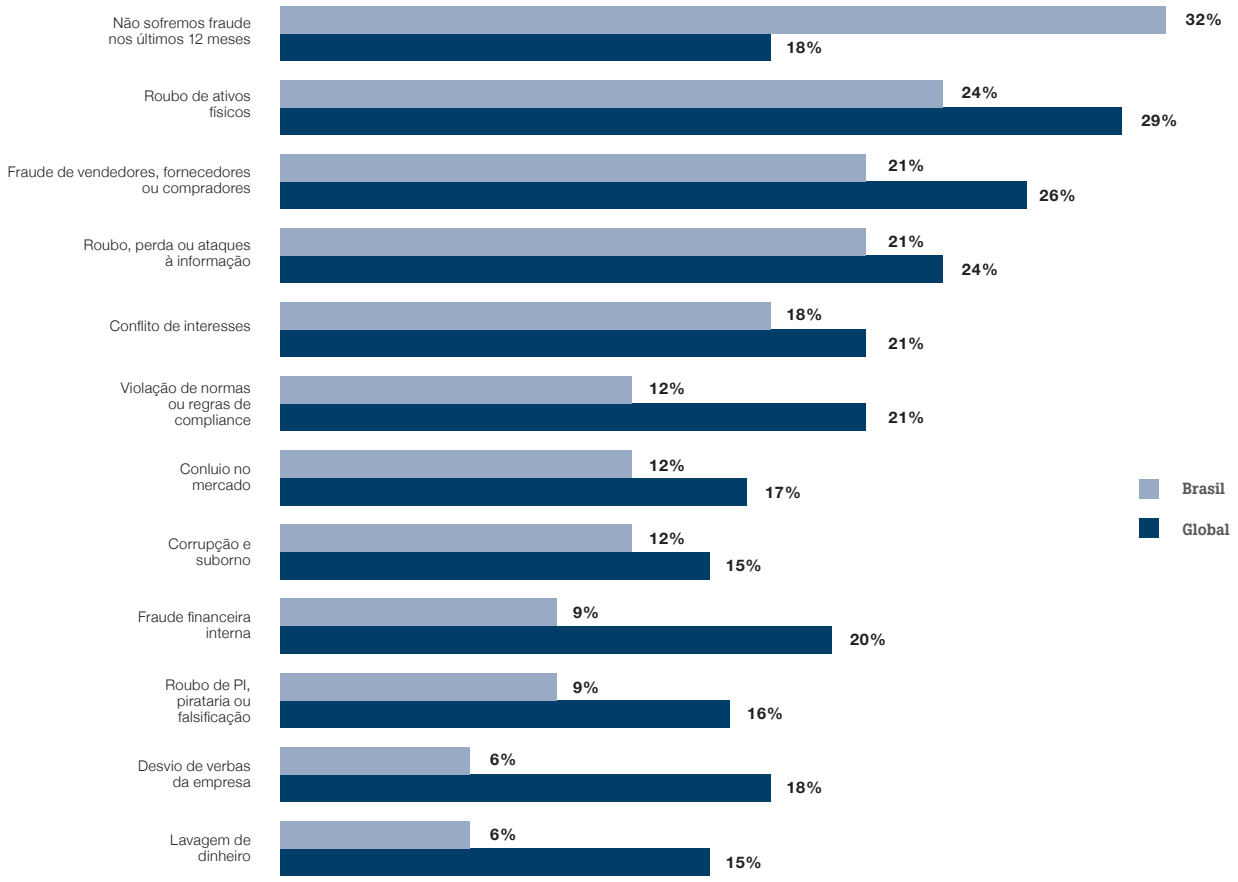
Incidência

FRAUDE

No Brasil, em 2016, 68% dos respondentes disseram ter sofrido algum tipo de fraude. As mais comuns seriam o 'roubo de ativos físicos' (24%), o 'roubo, perda ou ataques à informação' (21%) e a 'fraude de vendedores, fornecedores ou compradores ' (21%). Os três principais tipos de fraude são os mesmos globalmente e no Brasil; no entanto, as médias globais indicam maior incidência de fraudes lá fora do que por aqui. Nota-se especialmente, quando comparada ao Brasil, maior detecção global de fraudes complexas, como, por exemplo, 'fraude financeira interna', 'desvio de verbas da empresa', 'lavagem de dinheiro', 'conluio no mercado' e 'corrupção e suborno'.

É importante destacar que mais de um terço dos respondentes brasileiros (32%) afirmou não ter detectado fraude no último ano, enquanto globalmente este número é de apenas 18%, o que pode indicar deficiência na detecção de eventos de risco.

Fraudes mais sofridas nos últimos 12 meses

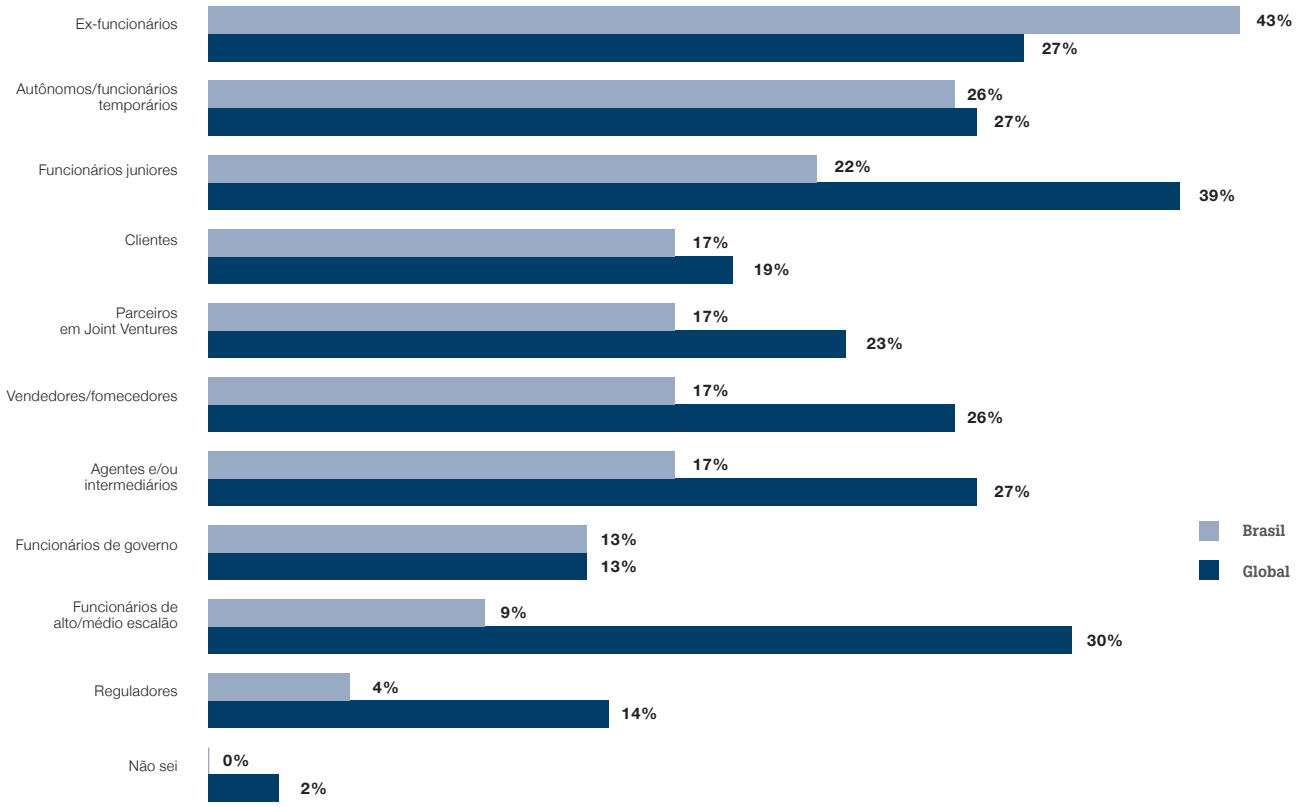


RESPONSÁVEIS

Em geral, o perigo está ou já esteve dentro de casa. Por aqui, as primeiras colocações no ranking de autoria de irregularidades nas empresas cabem a 'ex-funcionários' (43%), 'autônomos e funcionários temporários' (26%) e 'funcionários juniores' (22%). Se somados os 'funcionários juniores' com os 'funcionários de alto e médio escalão' e os 'autônomos e funcionários temporários', o total de funcionários responsáveis pelas irregularidades cresceria para 57%, colocando-os na primeira colocação entre os perpetradores. Nota-se que 13% dos respondentes citaram 'agentes governamentais' e 4%, 'reguladores', o que pode indicar prática de corrupção.

Globalmente, os principais responsáveis por fraudes também são funcionários e ex-funcionários; no entanto, seguindo a lista de perpetradores, 'agentes e intermediários', 'vendedores e fornecedores' e 'parceiros em *joint ventures*' foram detectados como tendo maior participação nas fraudes sofridas, quando comparado às respostas do Brasil. Isso leva à dúvida: as empresas brasileiras estão escolhendo bem seus parceiros de negócios ou a efetividade dos controles internos é falha?

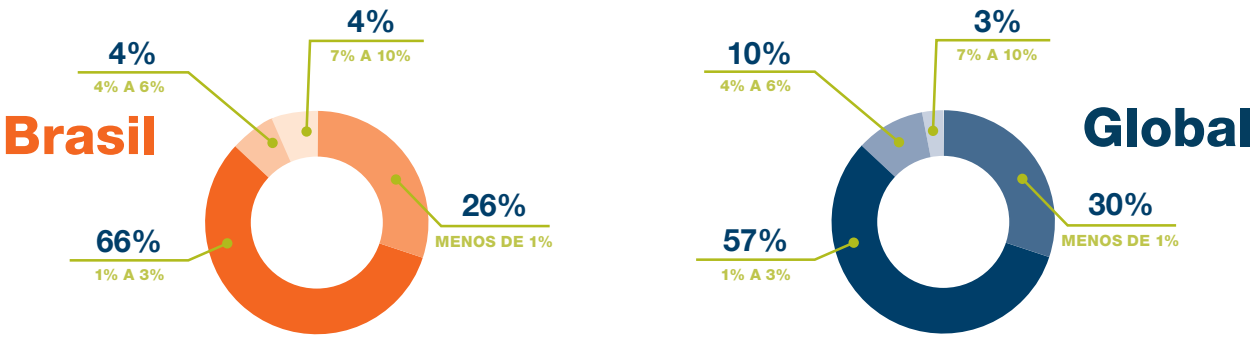
Principais responsáveis por fraudes



ESTIMATIVA DE PERDAS

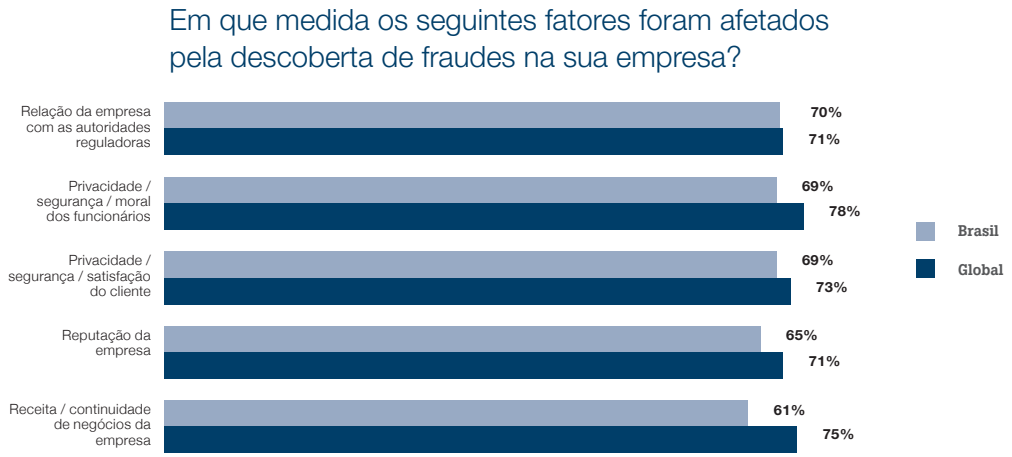
As perdas em decorrência de fraudes aferidas no Brasil, de acordo com os respondentes locais, estão em equivalência com as perdas no resto do mundo. A maioria dos respondentes (66%) estima prejuízos financeiros entre 1% e 3%.

Estimativa de perdas relacionadas a fraude nos últimos 12 meses



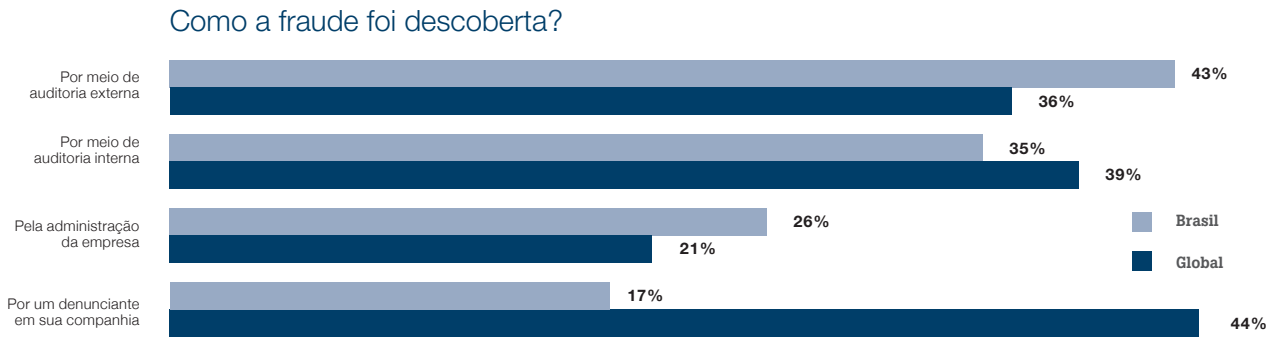
FATORES IMPACTADOS POR FRAUDES

A repercussão da fraude não fica limitada apenas ao caixa. Os respondentes indicaram que a descoberta da fraude teve alto ou algum impacto em fatores determinantes para a gestão do negócio e o ambiente organizacional, como, a 'relação da empresa com autoridades reguladoras' (70%), a 'privacidade, segurança e moral dos funcionários' (69%) e a 'privacidade, segurança e satisfação dos clientes' (69%). No contexto global, nota-se que a percepção de impacto é maior. Além disso, a 'receita e continuidade de negócios da empresa' sofre abalo maior do que a 'relação da empresa com autoridades reguladoras', quando comparada ao Brasil.



CANAIS DE DESCOBERTA DA FRAUDE

A análise dos meios em que a fraude foi descoberta no Brasil chama atenção pela diferença com os resultados globais. Enquanto o *whistleblower* (denunciante) é o mais citado globalmente, no Brasil ele ocupa a última colocação entre os canais indicados pelos respondentes para a detecção do evento. A auditoria externa foi citada como principal meio de descoberta da fraude, o que causa estranheza por não ser este o papel essencial dos auditores independentes. O baixo uso de canais de denúncia pode ser um dos fatores responsáveis pela baixa detecção de fraudes.



Denúncias no Brasil ainda enfrentam barreiras culturais

Por Ian Cook

Ian Cook

Ian Cook é Diretor Senior do escritório do Brasil, especializado em Compliance.

As empresas brasileiras têm amadurecido em termos de gestão e segurança da informação, mas ainda esbarram em limitações culturais relevantes. A maior delas talvez seja a dificuldade de implementar medidas preventivas de médio e longo prazo, capazes de deter vazamentos de informações, fraudes, perdas financeiras e consequentes danos à reputação e imagem.

Esse desafio é ainda maior quando se espera a colaboração de funcionários, colaboradores temporários e parceiros. Afinal, na cultura brasileira ainda é muito comum a repulsa pela figura do *whistleblower* (denunciante), que é facilmente associada à imagem de traidor, mesmo quando está a favor da ética e contra a perpetuação de crimes. Esse estigma cultural é uma barreira e tanto para a consolidação de um canal eficiente de denúncia, atualmente a principal ferramenta de detecção de fraude no mundo.

Conforme mostra o Relatório Global de Fraude & Risco 2016/17, 44% das fraudes identificadas pelo consolidado de respondentes globais foram reveladas por whistleblowers, enquanto no Brasil, denunciantes respondem por apenas 17% das descobertas, sendo o canal menos citado.

Para que esse canal dê certo, as empresas devem estar cientes de que é necessário criar condições favoráveis ao denunciante. Além de medidas jurídicas de proteção, é importante garantir que suas revelações sejam mantidas em anonimato ou em caráter confidencial. Também é necessário demonstrar na prática que toda acusação com bases reais será, de fato, investigada, bem como toda conduta imprópria, punida.

Um estímulo relevante é que, na esteira da Operação Lava Jato, a opinião pública tem cobrado cada vez mais *accountability* e transparência das empresas públicas e privadas. Isso ocorre em consonância a iniciativas jurídicas que buscam coibir ilegalidades e fraudes, como a Lei Anticorrupção (12.846/2013), que institucionaliza a figura do *whistleblower* em seu artigo 7º.

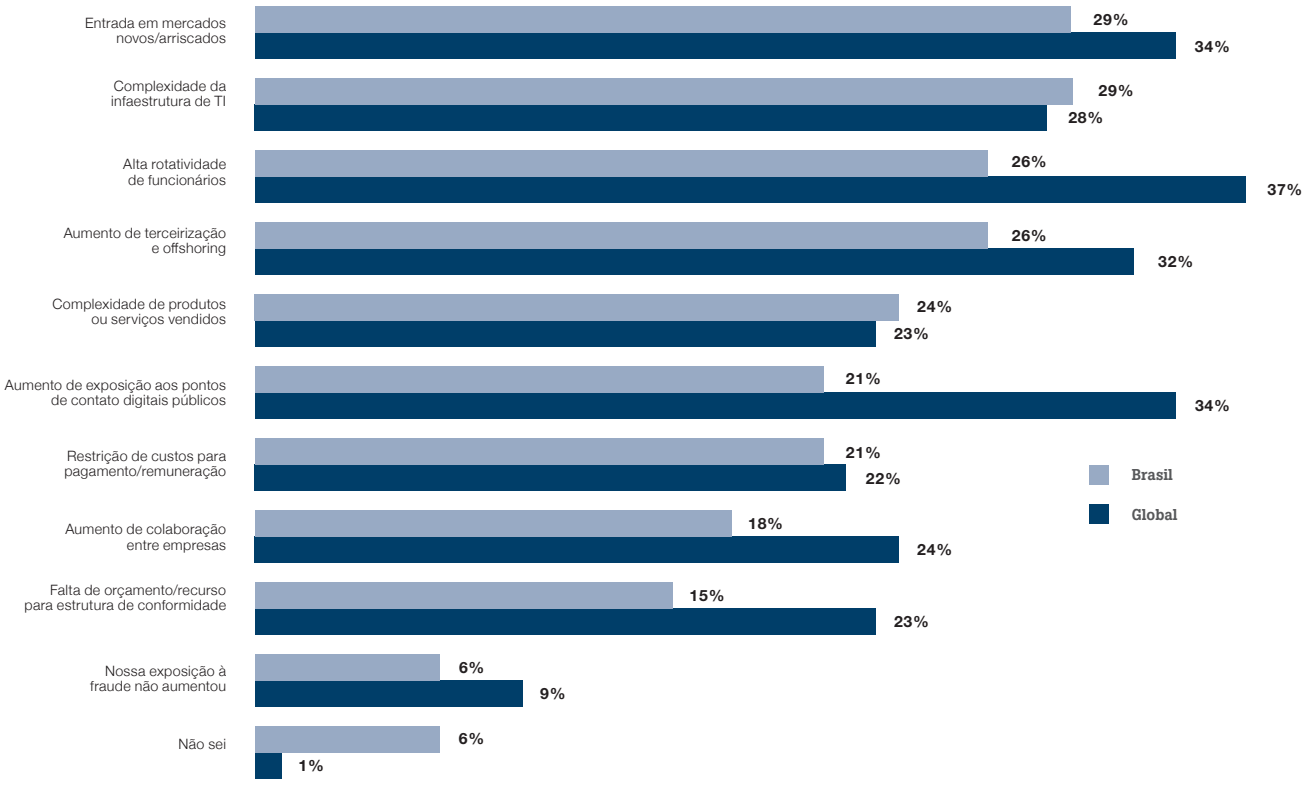
O incentivo à cultura de proteção ao denunciante é vital aos objetivos de empresas de qualquer setor ou segmento, sendo altamente recomendável como boa prática. É a partir de informações coletadas em um canal de denúncia que se permite exercer um trabalho pleno de investigação: entrevistar pessoas, cruzar dados, realizar pesquisas em registros públicos e arquivos corporativos, rastrear ativos, fazer investigações financeiras e perícia contábil.

Vale salientar que ferramentas tecnológicas têm pouca efetividade na prevenção a fraudes quando não há uma cultura corporativa que a respalde. Deste modo, a participação da direção da empresa, de cima pra baixo, é necessária para alavancar a conduta requerida, as políticas e controles internos e, consequentemente, o amadurecimento das práticas de denúncia.

CRESCIMENTO DA EXPOSIÇÃO À FRAUDE

De acordo com 94% dos respondentes brasileiros, houve aumento da exposição à fraude no último ano, contra 80% em 2015, o que indica potencial tendência de crescimento. A 'entrada em mercados novos ou arriscados' (29%) e a 'complexidade da infraestrutura de TI' (29%) são os principais fatores que aumentaram a exposição a fraudes no Brasil. A 'alta rotatividade de funcionários' e o 'aumento de terceirização e *offshoring'* vêm em seguida no ranking, ambos com 26%. Estes fatores abrangem a maioria dos itens principais indicados globalmente, exceto por 'aumento de exposição aos pontos de contato digitais públicos', que ocupa a segunda posição no ranking global, mas não está entre os cinco fatores mais relevantes para os respondentes brasileiros.

Fatores que aumentaram a exposição à fraude



MEDIDAS A ADOTAR PARA MITIGAÇÃO DE RISCO

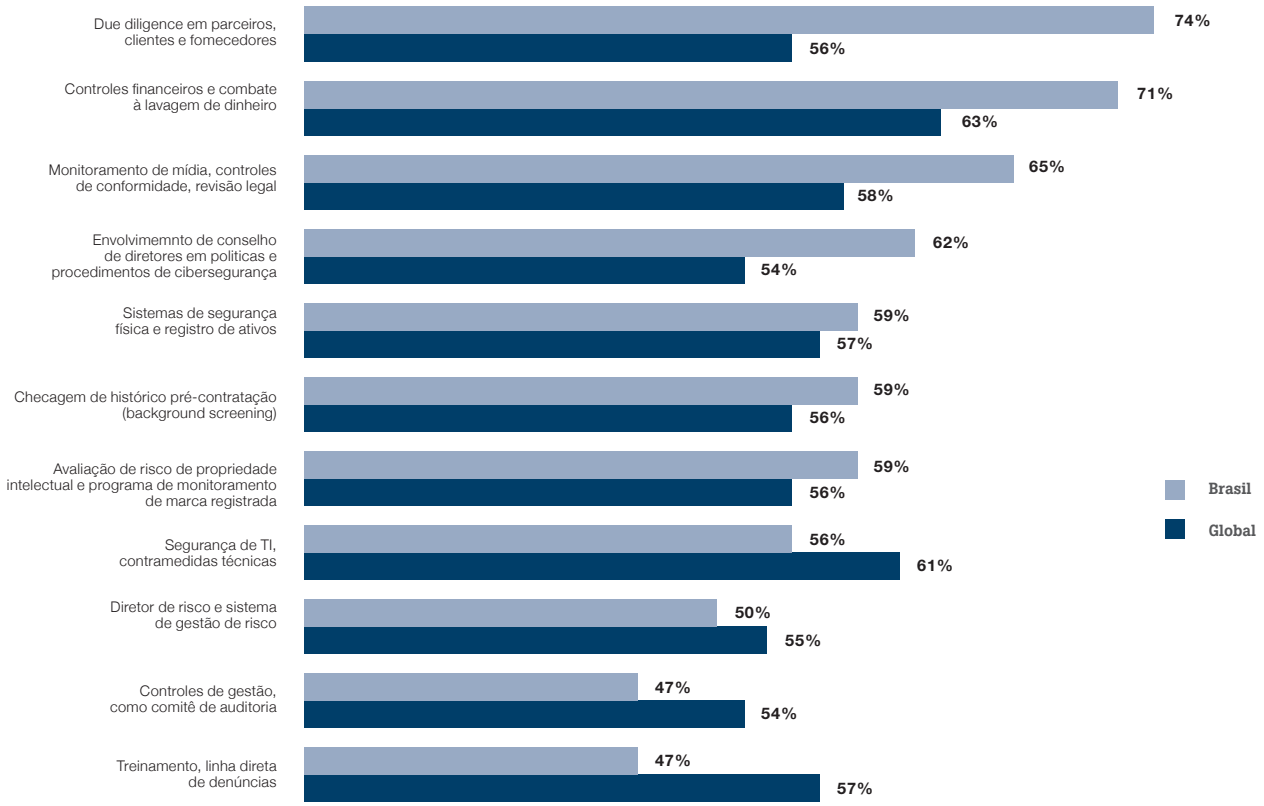
Quanto a medidas antifraude em implementação ou a serem implementadas nos próximos 12 meses, a maioria dos respondentes demonstra prioridade em '*due diligence* em parceiros, clientes e fornecedores' (74%), 'controles financeiros e combate à lavagem de dinheiro' (71%) e 'monitoramento de mídia, controles de conformidade e revisão legal' (65%).

Considerando que as medidas antifraude a serem implementadas devem minimizar as vulnerabilidades das empresas, nota-se que não estão sendo priorizadas medidas para defendê-las dos principais tipos de fraude detectados em 2016 – exceto no caso de '*due diligence* em parceiros, clientes e fornecedores', que pode ajudar a reduzir as 'fraudes de vendedores, fornecedores e compradores'.

As medidas que poderiam minimizar as 'fraudes de roubo de ativos físicos' e 'roubo, perda ou ataque à informação' – respectivamente, 'sistemas de segurança física e registro de ativos' e 'segurança de TI, contramedidas técnicas' – não foram citadas pelos respondentes como prioridade de implementação. Mesmo que estas duas medidas estejam entre as mais implementadas pelas empresas respondentes, é importante lembrar que a defesa contra riscos deve estar em constante evolução, para acompanhar o avanço da atuação dos perpetradores.

Também chama a atenção o fato de a 'checagem de histórico pré-contratação (*background screening*)' não estar entre as prioridades, tendo em vista que os grupos de funcionários e ex-funcionários são os maiores responsáveis pelas fraudes e, ainda, que a alta rotatividade de funcionários está entre os principais itens que aumentam a exposição à fraude. Nota-se também que a 'linha direta de denúncias' está em último lugar na lista de prioridades de implantação, apesar de, pelos resultados globais, ser o meio mais eficiente de detecção de fraude.

Medidas a serem adotadas no próximo ano



Novas regras incentivam *due diligence* de fornecedores, parceiros e *background screening* de funcionários

Por Carlos Lopes

Muito aconteceu desde que o Brasil começou a dar importância a problemas reputacionais e prejuízos financeiros advindos da corrupção. Ainda há um longo caminho a avançar, porém algumas mudanças na legislação brasileira já apontam para uma seleção natural em curso entre as corporações públicas e privadas atuantes no país. Quem não se adequar às melhores práticas e regulações está passível de sofrer punições severas e danos irreparáveis a reputação, competitividade e valor de mercado.

Sancionada em 2013, a Lei Anticorrupção (12.846/2013) marcou o início de uma nova etapa na cultura empresarial brasileira. Sob o risco de responder civil, administrativa e objetivamente pelas ações indevidas de funcionários e parceiros, as empresas foram levadas a perceber a importância de se estabelecer um programa eficaz de Compliance.

Outro dispositivo mais recente, a Lei 13.303, sancionada em junho de 2016, também impõe novas regras às empresas estatais e às sociedades de economia mista. Em uma corrida contra o relógio, essas empresas devem estabelecer, num prazo de 24 meses, uma série de mecanismos de transparência e governança, como códigos de conduta, comitês, testes de integridade e medidas de transparência.

Nesse contexto, os serviços de Due Diligence de parceiros/ fornecedores e de Background Screening de (potenciais) funcionários tornam-se aliados importantes para empresas privadas e estatais, independente do seu segmento. Em 2016, a Kroll registrou um aumento de 44% nos serviços de diligência prévia no Brasil, comparado ao ano anterior, principalmente no setor de infraestrutura, alavancado pelo crescimento dos investimentos advindos de empresas estrangeiras.

Não por acaso, 74% dos respondentes brasileiros entrevistados para o Relatório Global de Fraude & Risco 2016/17 planejam implementar e expandir programas de Due Diligence para parceiros, clientes e fornecedores, sendo esta a principal medida a ser adotada pelas empresas pesquisadas.

Ao regular a adoção de medidas preventivas, essas leis trazem benefícios para toda a economia brasileira, uma vez que estabelecem novos padrões de transparência, semelhantes aos adotados nos Estados Unidos, com a Foreign Corrupt Practices Act (FCPA), e no Reino Unido, com o UK Bribery Act (UKBA). Dessa forma, esses novos dispositivos legais colocam o país na direção certa para atingir um novo patamar de competitividade global e, sob a ótica cultural, as empresas aos poucos começam a perceber que a gestão de riscos é um investimento indispensável para evitar prejuízos reais.

Carlos Lopes

Carlos Lopes é Diretor do escritório do Brasil, especializado em Due Diligence.

Incidências

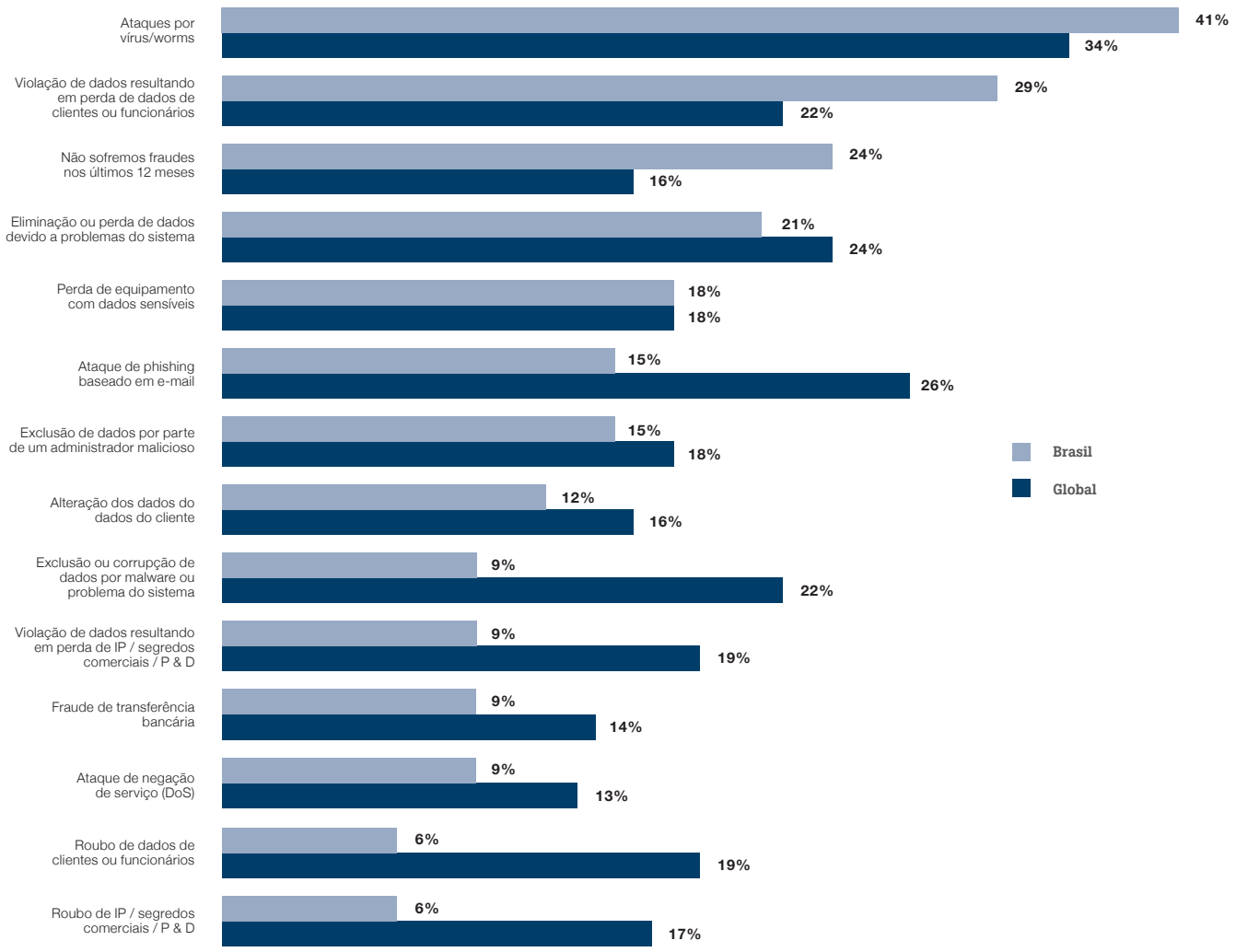
SEGURANÇA CIBERNÉTICA

Assim como ocorre na percepção geral de fraudes, os executivos brasileiros também relataram uma incidência expressivamente menor de ciberataques no último ano, em comparação à média global. Enquanto no Brasil 76% sinalizaram ao menos um evento, no resto do mundo essa avaliação sobe para 85%.

Os tipos mais comuns de ciberataques identificados pelos respondentes brasileiros advêm de 'vírus/*worm*' (41%), seguido de 'violação de dados resultando em perda de registros de clientes ou funcionários' (29%) e de 'eliminação ou perda de dados devido a problemas do sistema' (21%). Estes fatores abrangem a maioria dos itens principais indicados globalmente, exceto por 'ataque de *phishing* baseado em email', que ocupa a segunda posição no ranking global.

Quase um quarto dos respondentes brasileiros (24%) afirmou não ter detectado fraude no último ano, enquanto globalmente este número é de 16%.

Ciber incidentes sofridos nos últimos 12 meses



Fragilidade das empresas mascara número de ciberataques no Brasil

Por Fernando Carbone

Fernando Carbone

Fernando Carbone é Diretor Sênior do escritório do Brasil, especialista em Segurança Cibernética.

No último ano, as corporações brasileiras aumentaram os investimentos em segurança cibernética e implementaram ferramentas tecnológicas modernas para combater ataques; no entanto, essa tendência ainda segue aquém do crescimento e da sofisticação das ameaças perpetradas por vírus e malwares (softwares maliciosos, que podem corromper sistemas ou roubar informações). Como resultado, em vez de detectar ataques com rapidez, as empresas costumam enfrentar os incidentes cibernéticos tardiamente, o que pode aumentar as perdas financeiras e os riscos reputacionais.

Por este motivo, os resultados positivos do Brasil no último Relatório Global de Fraude & Risco 2016/17 devem ser encarados com reservas, de modo a não suscitar uma falsa sensação de segurança.

Alguns aspectos culturais e de governança empresarial ajudam a explicar porque a pesquisa feita com executivos brasileiros demonstrou uma menor incidência de ataques cibernéticos no país (76%), se comparada ao resto do mundo (85%) e a países como Estados Unidos (88%), Reino Unido (92%) e Canadá (85%).

Em primeiro lugar, a legislação brasileira não obriga as empresas a reportarem a autoridades invasões e ataques a bancos de dados e matrizes tecnológicas, assim como ocorre em outros países. Dessa maneira, muitos casos não são comunicados oficialmente ao poder público e deixam de ser contabilizados.

Outra informação relevante para a compreensão dos resultados da pesquisa diz respeito à demora em identificar uma invasão com potencial nocivo. Isso porque a ameaça pode persistir instalada por um longo período de tempo, de forma imperceptível e atuante – característica que pode estar relacionada ao fato de, no Brasil, os ciberataques ocorrerem majoritariamente (38%) com a participação direta de ex-funcionários. A proporção representa quase o dobro da global.

Tal panorama favorece a não detecção de ameaças que visam obter e explorar financeiramente informações sensíveis a partir de ataques a clientes, funcionários e fornecedores. Para perpetrar fraudes como o golpe do boleto de pagamento, por exemplo, os invasores distribuem, a partir de IPs anônimos, uma variedade de vírus por meio de phishing e worm attacks, que correspondem a 41% dos incidentes cibernéticos detectados pelos respondentes brasileiros, índice 8% acima do global.

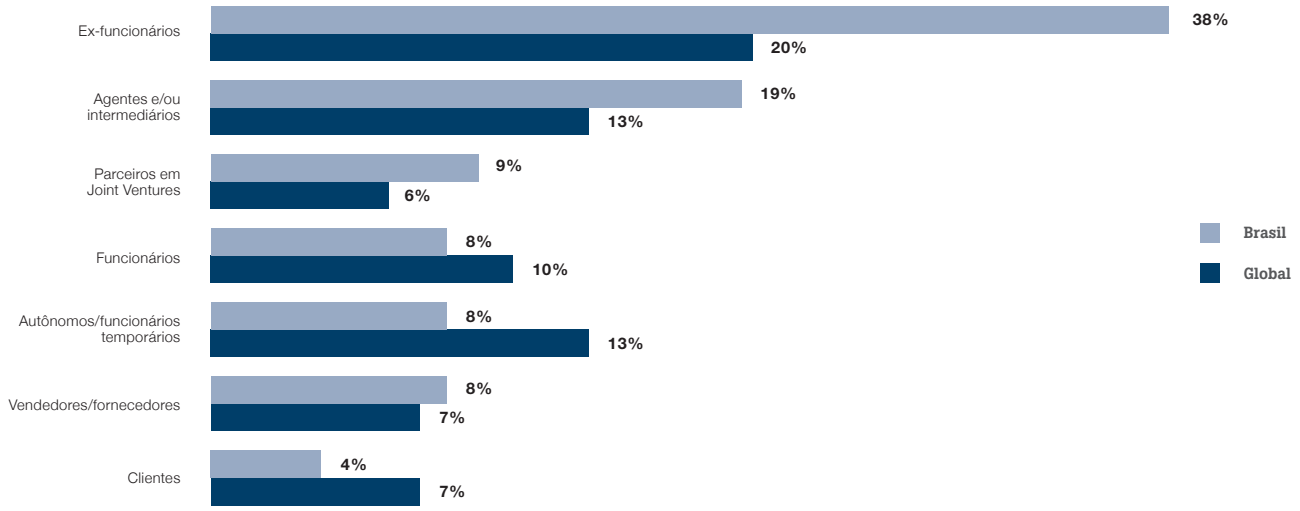
Outro método comum e nocivo atualmente atende pelo nome de ransomware – uma série de códigos maliciosos que tornam os dados contidos em um equipamento inacessíveis, geralmente por meio de criptografia. Para reestabelecer o acesso aos arquivos, as empresas são extorquidas e obrigadas a pagar um valor estabelecido pelo sequestrador, geralmente com bitcoins.

É impossível criar uma solução única e definitiva contra as ameaças. Qualquer empresa, independente de sua dimensão e a qual setor pertença, está suscetível a sofrer algum tipo de ataque em determinado momento. No entanto, há uma série de medidas preventivas, processos e ferramentas que podem ser aliados extremamente valiosos na rápida detecção e remediação de ameaças. Em vista disso, é aconselhável às empresas e aos investidores recorrerem à ferramenta de Cyber Due Diligence, que permitirá um conhecimento amplo sobre os riscos, fragilidades e possibilidades tecnológicas, de forma a construir uma estrutura menos suscetível a perdas financeiras, materiais, intelectuais e de imagem.

RESPONSÁVEIS

Os principais autores de ciberataques são, segundo os respondentes brasileiros, ex-funcionários (38%) e agentes ou intermediários (19%).

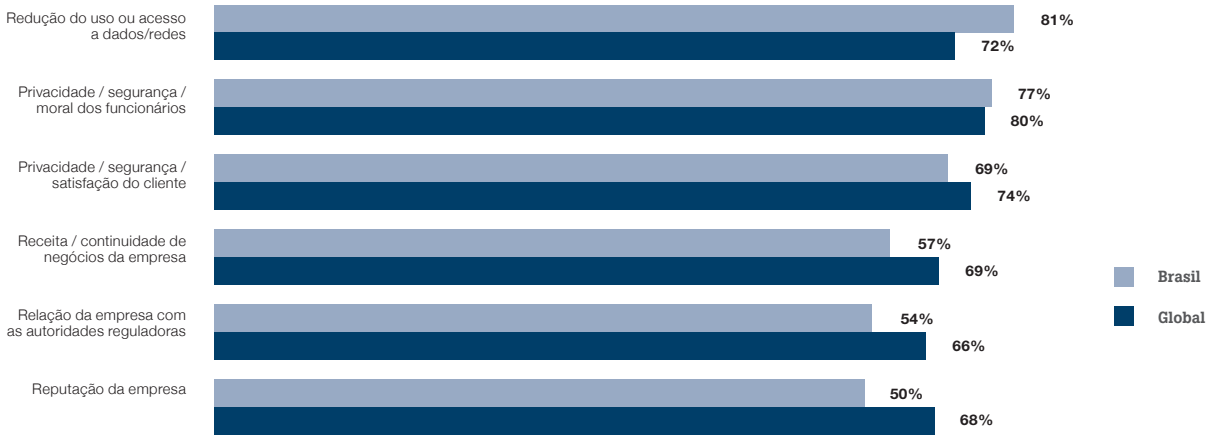
Responsáveis por ciberataques



FATORES IMPACTADOS POR CIBERATAQUES

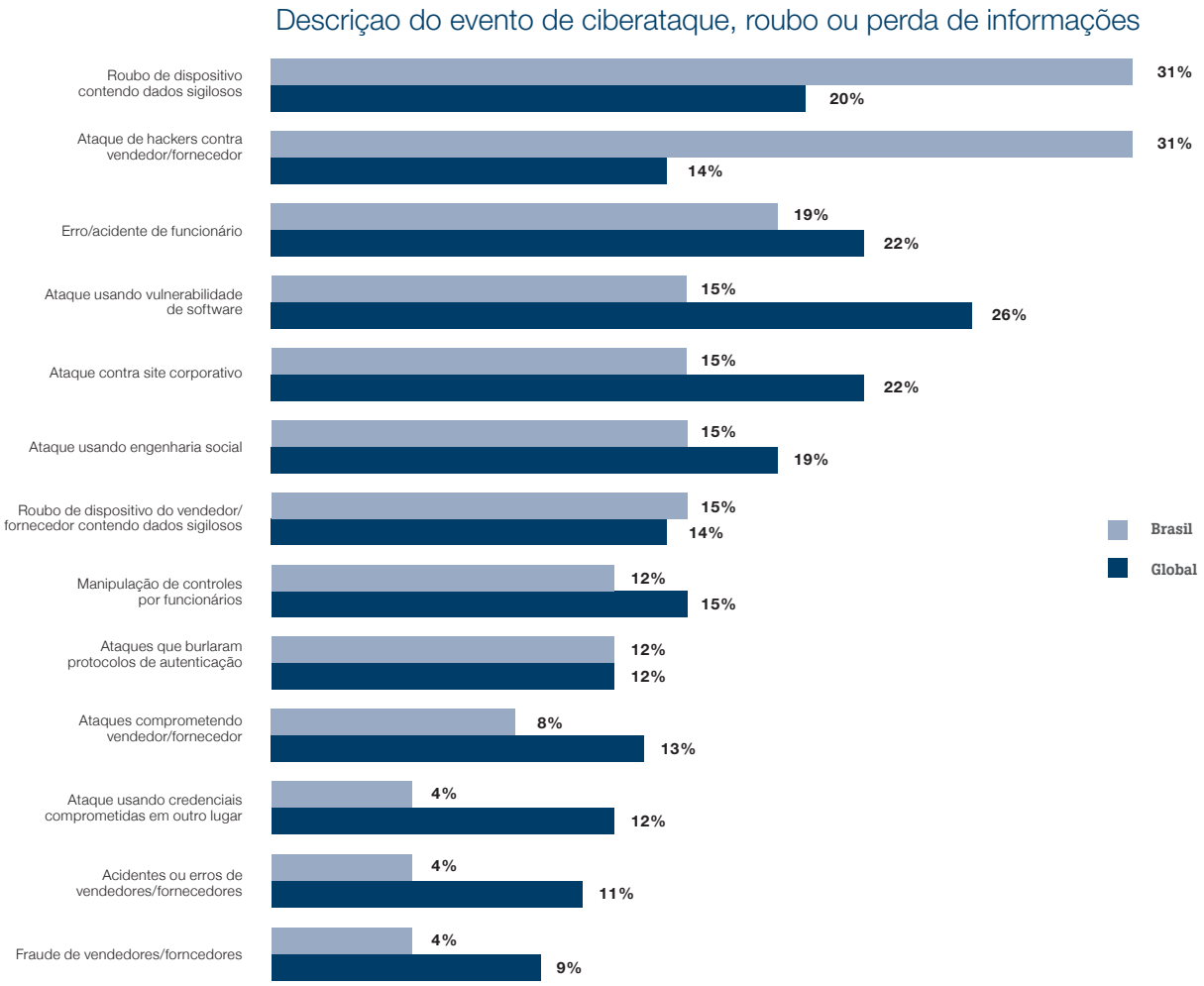
Uma vez descoberto, o ciberincidente, tanto aqui como lá fora, impacta diretamente a 'redução do uso ou acesso a dados, redes', a 'privacidade, segurança e moral dos funcionários' e a 'privacidade, segurança e satisfação do cliente'.

Em que medida os seguintes fatores foram afetados por ciberataques na sua empresa?



DESCRIÇÃO DO CIBERATAQUE

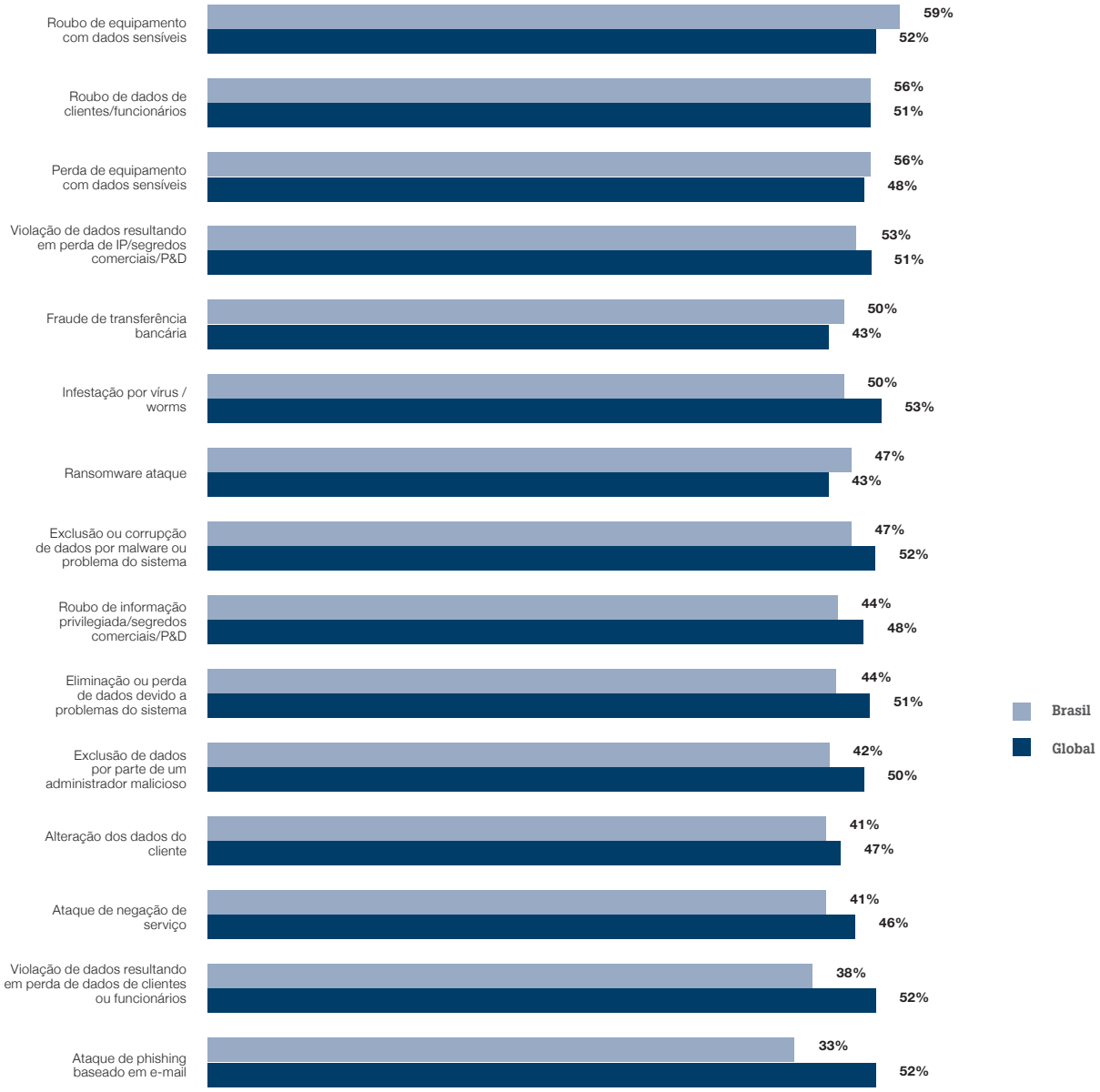
Embora um funcionário ou ex-funcionário possa agir como peça-chave para o acesso a informações privilegiadas (nem sempre de modo intencional), o 'ataque de hackers contra vendedor ou fornecedor' e o 'roubo de dispositivo contendo dados sigilosos' foram os eventos que mais comprometeram a segurança cibernética no país.



FATORES DE VULNERABILIDADE

Os principais fatores de vulnerabilidade no Brasil, segundo os respondentes brasileiros, são o 'roubo de equipamento com dados sensíveis', o 'roubo de dados de clientes ou funcionários' e a 'perda de equipamento com dados sensíveis'. Globalmente, mais vulnerabilidades são apontadas como relevantes, como 'exclusão ou corrupção de dados por *malware* ou problema do sistema', 'violação de dados resultando em perda de dados de clientes e funcionários', e 'ataque de *phishing* baseado em email'. Isso deixa a dúvida: será que as empresas brasileiras estão de fato cientes das suas vulnerabilidades?

Quão vulnerável você acredita que sua empresa está a cada um dos seguintes tipos de ciberataque, perda e roubo de informações hoje?

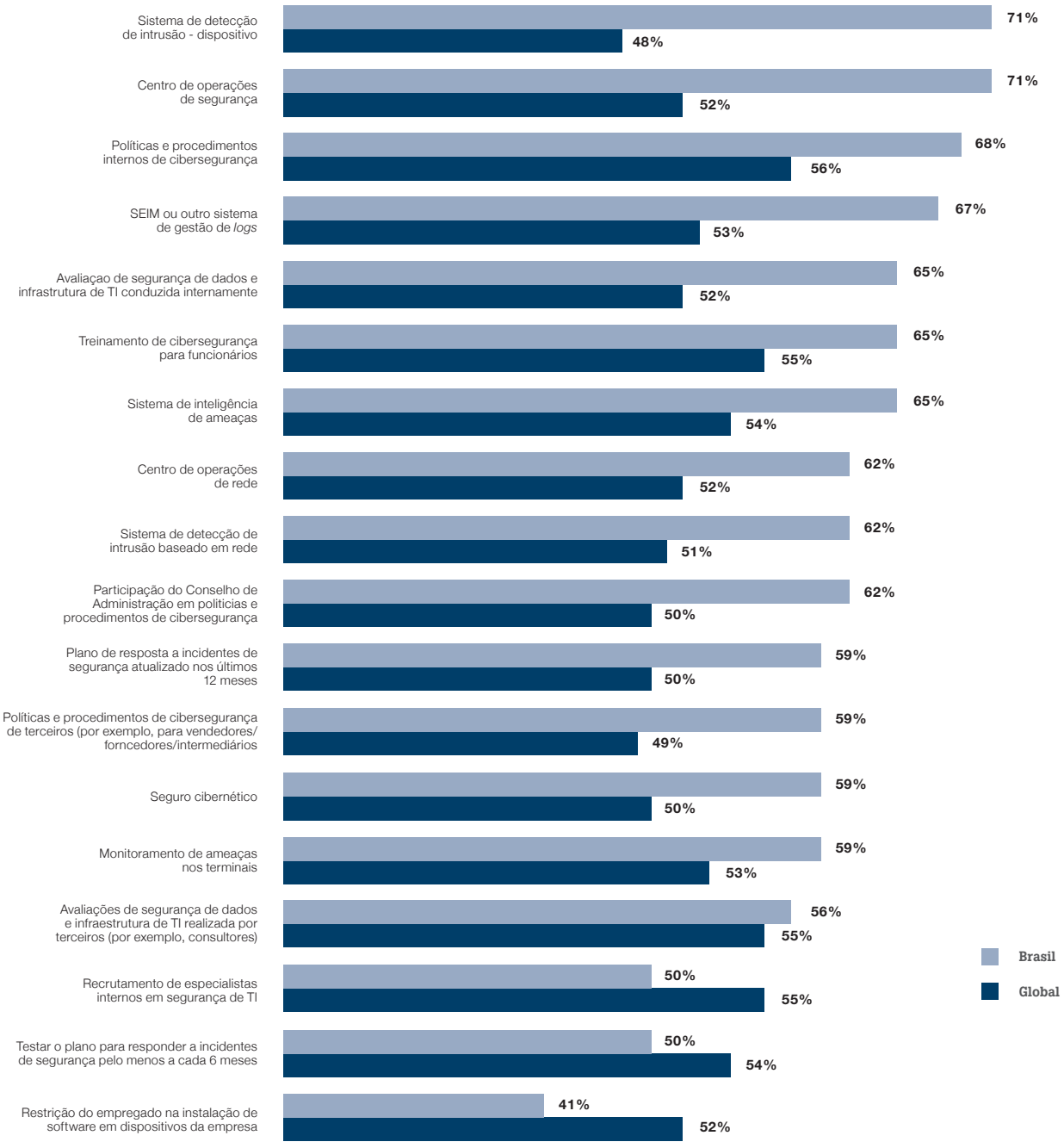


MEDIDAS A ADOTAR PARA MITIGAÇÃO DE RISCO

Uma vez corrompidos, os dados e informações sigilosas podem ser usados de diversas formas para fins de extorsão, falsidade ideológica e como moeda de troca no mercado negro, com consequências que vão muito além do prejuízo

financeiro. Para enfrentar essa ameaça com maior eficiência, as medidas prioritárias para expansão ou a serem implementadas nos próximos 12 meses são a instalação de 'centro de operações de segurança' e de 'sistema para detecção de intrusão - dispositivo', ambas com 71% de indicações, seguidas por 'políticas e procedimentos internos de ciber segurança' (68%). Considerando que as medidas antifraude a serem implementadas devem minimizar as vulnerabilidades das empresas, nota-se que não estão sendo priorizadas medidas para defendê-las dos principais tipos de ataque cibernético detectados em 2016. As medidas que poderiam minimizar os ataques de 'violação de dados resultando em perda de dados de clientes ou funcionários' e 'eliminação ou perda de dados devido a problemas do sistema' – sistema de inteligência de ameaças e sistema de detecção de intrusão, por exemplo – não foram citadas pelos respondentes como prioridade de implementação.

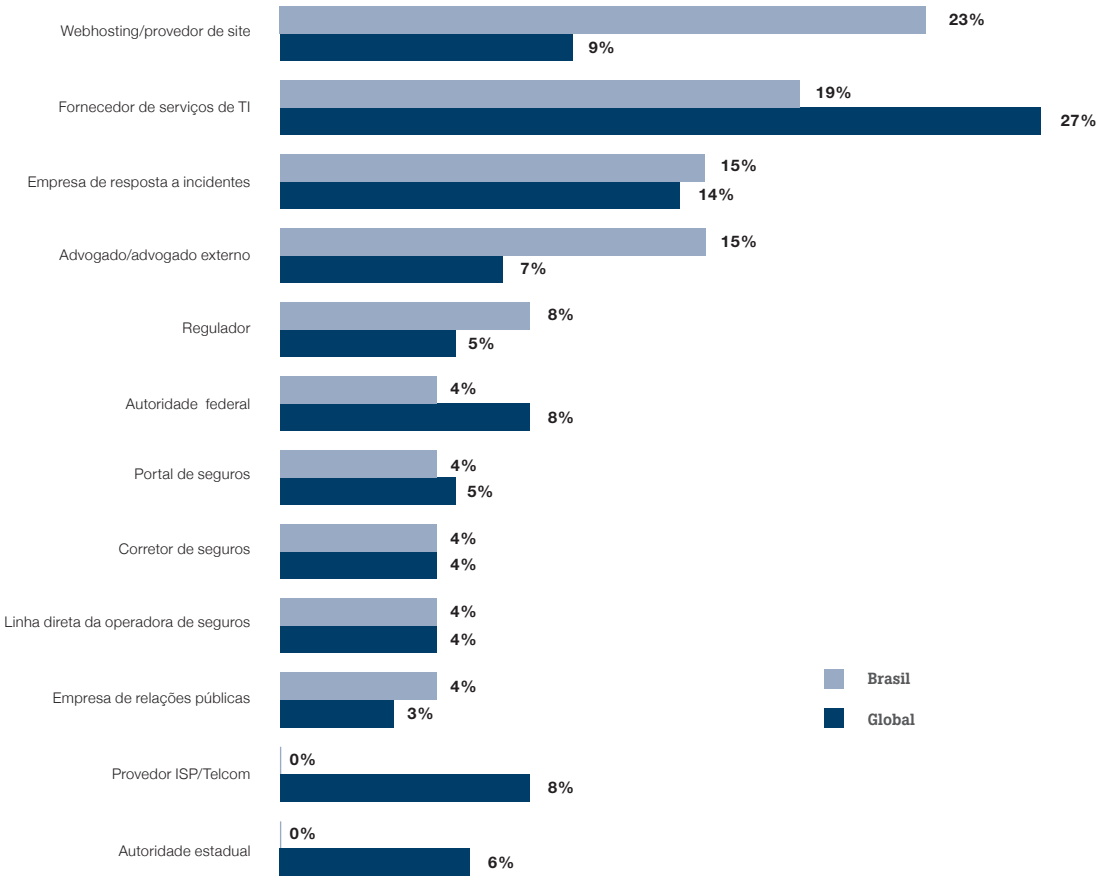
Medidas a serem implementadas no próximo ano



SUPORTE PÓS INCIDENTE

Por fim, como suporte pós-incidente, o primeiro contato mais comum para os respondentes brasileiros é com o provedor do site corporativo, prática em 23% das empresas. Já globalmente, é ao provedor de serviços de TI que os respondentes costumam recorrer em primeiro lugar.

Parte contatada após ciber incidente



Kroll

Rua Gomes de Carvalho, 1507, 7° andar, Vila Olímpia
São Paulo – SP, 04547-005 Brasil
+55 11 3897.0900

kroll.com