MARSH | Microsoft

INSIGHTS | SETEMBRO 2019

2019 Global Cyber Risk Perception Survey

MARSH & McLENNAN COMPANIES

INSIGHTS | SETEMBRO 2019

2019 Global Cyber Risk Perception Survey

CONTEÚDO

Introdução

A tecnologia está transformando drasticamente os ambientes de negócios a nível global, com avanços contínuos em áreas que vão desde inteligência artificial e Internet das Coisas (IoT) até a responsabilidade sobre dados e blockchain. A velocidade com que as tecnologias digitais evoluem e rompem com os modelos tradicionais de negócios segue aumentando. Enquanto isso, os riscos cibernéticos parecem evoluir ainda mais rápido.

O risco cibernético passou de roubo de dados e a preocupação com privacidade a esquemas mais sofisticados que podem alterar empresas, indústrias, cadeias de suprimento e nações, custando milhões de dólares à economia nos mais diversos setores. A dura realidade que as organizações devem enfrentar é que o ciberrisco pode ser mitigado, administrado e recuperado, mas não pode ser eliminado.

O Global Cyber Risk Perception Survey Marsh-Microsoft 2019 investiga as percepções de ciberriscos e gestão de riscos em empresas de todo o mundo, especialmente nesse contexto de um ambiente de negócios em rápida transformação.

A análise inclui dados relacionados à pesquisa realizada em 2017 e publicada em 2018. Nossos resultados se baseiam em cinco conceitos importantes que destacam o âmbito do risco cibernético no cenário empresarial atual:

1. Na América Latina, a preocupação das empresas com os ciberriscos e a confiança em suas próprias capacidades de gerir os riscos cibernéticos aumentaram, em comparação com 2017.

2. Tanto a nível mundial quanto na América Latina, as empresas dão maior prioridade a tecnologia e prevenção que dedicação de tempo, recursos e atividades necessárias para construir uma ciberresiliência.

3. Apesar de pouco mais de 1/3 dos respondentes afirmarem que o ciberrisco não seja um empecilho para a adoção de novas tecnologias, 29% responderam que acreditam altamente que o risco esteja associado a essas tecnologias.

4. A digitalização das cadeias de suprimentos traz benefícios, mas muitas empresas não avaliam completamente a questão da interdependência entre seus papeis e responsabilidades dentro da cadeia de suprimentos, principalmente as grandes corporações.

5. Existe uma incerteza sobre o valor tanto da legislação estatal como das normas da própria indústria acerca de cibersegurança. A maioria das empresas considera que ambas têm uma efetividade limitada. Ainda assim, existe um forte desejo por uma liderança governamental e o apoio para combater as ciberameaças nacionais.

O Global Cyber Risk Perception Survey 2019 revela sinais animadores de uma melhora na percepção e gestão de riscos cibernéticos nas organizações. O ciberrisco é, agora, uma prioridade na pauta de riscos corporativos e podemos ver uma mudança positiva na adoção de uma gestão de riscos cibernéticos mais rigorosa e integral em diferentes áreas. No entanto, várias organizações continuam empenhando-se, como podem, para articular, abordar e agir sobre o risco cibernético dentro de sua estrutura geral de riscos corporativos, mesmo quando a maré de mudanças tecnológicas traz preocupações novas e imprevistas sobre o ciberrisco.

Esperamos que este estudo ajude sua empresa a visualizar um panorama em constante evolução do risco cibernético. Incentivamos a todas as empresas a desenvolver ciberresilência, abordando o risco cibernético como uma ameaça crítica que, com vigilância e aplicação das melhores práticas, pode ser gerido com confiança. Finalmente, agradecemos aos nossos clientes e, em geral, àqueles que compartilharam seus pontos de vista sobre este tema de grande importância.

Destaques do estudo

O Global Cyber Risk Perception Survey Marsh-Microsoft 2019 analisa como as empresas lidam com a ameaça crescente do ciberrisco, particularmente dentro de um ambiente de negócios altamente dinâmico, com transformações nos âmbitos de inovação tecnológica e interdependência. Os resultados mostram uma melhora, em comparação com 2017, em várias áreas relacionadas com a sensibilidade e as tácticas para abordar o tema de riscos cibernéticos.

Prioridade e confiança

O risco cibernético se fortaleceu como uma prioridade das empresas da América Latina. Os resultados mostram que a confiança das organizações em sua capacidade para gerir o ciberrisco aumentou, na contramão do restante do mundo, onde esta percepção diminuiu.

- 73% dos respondentes na América Latina classificaram o risco cibernético como uma das cinco principais preocupações para sua empresa, contra 47% em 2017.
- O nível de confiança das empresas latino-americanas em sua própria capacidade para enfrentar o risco cibernético também aumentou em comparação com 2017, em cada uma das três áreas críticas de ciberresiliência.
  - De 16% para 22%, para compreender e avaliar riscos cyber.
  - De 12% para 20%, para prevenir ameaças cibernéticas.
  - De 7% para 18%, para responder e recuperar-se de incidentes cibernéticos.

Nova tecnologia

A inovação tecnológica é vital para a maioria das empresas. Mas isso inclui ainda mais complexidade ao ambiente tecnológico de uma organização, como o ciberrisco.

- 34% mencionaram que o risco cibernético quase nunca é um empecilho para a adoção de novas tecnologias (55% consideram que sejam de alto risco).
- 45% consideram que os benefícios das novas tecnologias superam os potenciais riscos para o negócio.
- 75% avaliam os riscos cibernéticos antes de adotarem efetivamente novas tecnologias.

Cadeia de suprimentos

A crescente interdependência e digitalização das cadeias de suprimentos resultam em um maior risco cibernético para todas as partes. Porém, muitas empresas não se percebem como ameaças dentro da própria cadeia de suprimentos e, muitas vezes, pensam estarem expostas aos riscos por causa de seus fornecedores.

- 37% das empresas brasileiras percebem os riscos de sua cadeia de suprimentos.
- Apenas 21% pensam que sua própria organização representa risco à sua cadeia de suprimentos, no Brasil.
- Globalmente, os entrevistados foram mais propensos a estabelecer padrões mais altos em suas organizações para suas próprias ações de gerenciamento de riscos cibernéticos do que para com seus fornecedores.

Papel do governo

As empresas brasileiras veem uma efetividade limitada das regulamentações governamentais no que diz respeito ao risco cibernético - com exceção do que é feito em relação aos ciberataques ao Estado.

- No Brasil:
  - 35% acreditam que leis e regulamentações ajudam a melhorar o posicionamento da empresa em cibersegurança.
  - 44% se dizem muito preocupadas com ciberataques ao Estado.
  - 44% defendem que governo deve fazer mais para proteger as empresas de ciberataques.

Cultura de cibersegurança e resiliência

Muitas empresas estão focando seus investimentos de cibersegurança em ferramentas de proteção, deixando outras áreas de gestão de riscos que criam resiliência cibernética desprotegidas, como a avaliação e transferência de riscos, assim como os planos de resposta a incidentes.

- 88% dos respondentes da América Latina dizem que o setor de tecnologia/segurança da informação é o principal responsável pela gestão dos riscos cibernéticos, seguidos por 57% que têm os setores de planejamento estratégico/operações/RH como responsáveis e, em terceiro lugar, liderança executiva/conselho administrativo (53%).
- Na América Latina, a figura do gerente de riscos, como peça-chave na gestão de ciberriscos, passou de 17% em 2017 para 46% em 2019.
- 70% dos respondentes brasileiros pretendem investir em tecnologia de cibersegurança nos próximos 3 anos.
- 68% disseram que um ataque cibernético em sua empresa seria o principal propulsor para aumentar investimentos na gestão de ciberriscos, no Brasil.
- 41% das empresas brasileiras afirmam que a adoção de novas tecnologias é responsável por mais investimento em riscos cibernético.
- 33% das empresas latino-americanas disseram usar métodos quantitativos para avaliar sua exposição ao risco, um aumento de 8% em relação a 2017.
- Dos respondentes brasileiros, 65% esperam investir mais nos próximos anos em capacitação de pessoal para lidar com riscos cibernéticos.

Seguro Cyber

A cobertura do seguro cyber está em expansão para enfrentar as ameaças em evolução, o que inclui mudanças também nas apólices.

- 29% das empresas participantes, na América Latina, possuem seguro cyber, enquanto a média global é de 47%.
- Empresas de grande porte (+ US$ 1 bilhão de receita) representam 40% dentre os que possuem seguro cyber e empresas com receita inferior a US$ 100 milhões, 22%.
- 52% das empresas latino-americanas consideram que o seguro cibernético cobre todas ou grande parte de suas necessidades. Entretanto, 39% declaram não saber se o seguro é uma ferramenta eficaz de proteção.
- 75% das empresas que possuem seguro cyber confiam que suas apólices cobrirão o custo de um eventual incidente cibernético.

Risco cibernético: maior prioridade e maior confiança

Cada vez mais as empresas veem os ciberriscos como uma prioridade. No Brasil e na América Latina, ao contrário do que acontece ao redor do mundo, a confiança na sua gestão do risco cibernético aumentou.

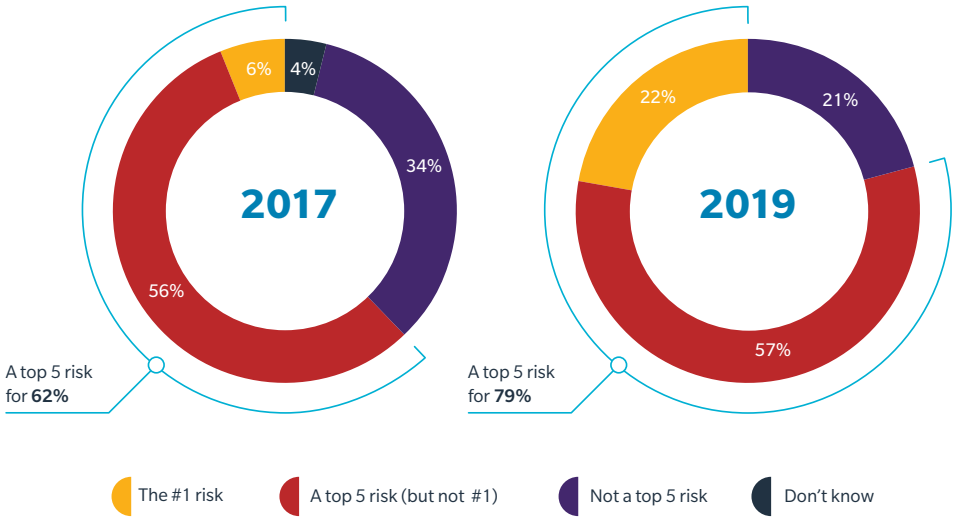
Aumenta a consciência sobre o risco cibernético

Impulsionados pela frequência e gravidade de incidentes como o NotPetya de 2017, a preocupação com os riscos e ameaças cibernéticas se ampliaram significativamente entre as principais prioridades das empresas latinas em 2019 (gráfico 1). 73% dos entrevistados classificaram o ciberrisco como uma das cinco principais preocupações. No Brasil, 57% colocam os riscos cibernéticos no Top 5 de preocupação.

FIGURE 1

Cyber risk has climbed sharply among organizations' risk priorities.

Q. Of the following business threats, please rank the top 5 that are the biggest concerns to your organization (cyber-attacks/cyber threats shown).



Base: All answering; n=1312 (2017); n=1512 (2019)

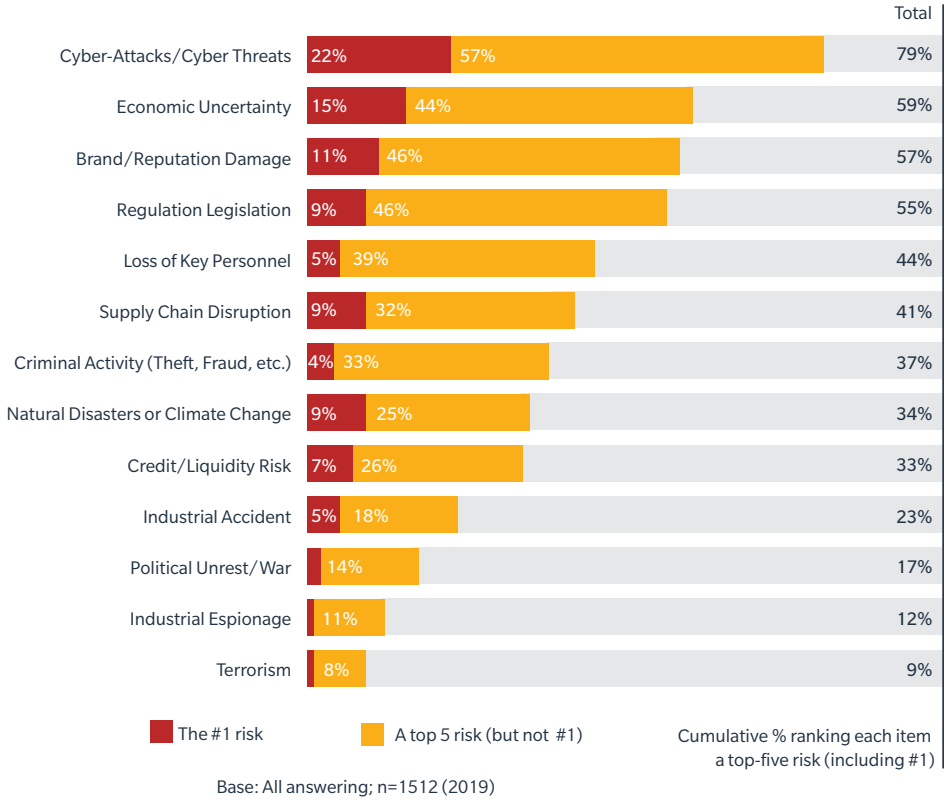
Em 2019, mais entrevistados classificaram o risco cibernético como uma de suas principais preocupações em comparação com outro importante risco comercial (gráfico 2). A incerteza econômica ficou em segundo lugar no Top 5, com 59%.

Esses resultados sugerem um aumento evidente da importância do risco cibernético e se correlacionam fortemente com outros estudos recentes. Por exemplo, o Relatório de Risco Global de 2019 do Fórum Econômico Mundial (FEM) classificou o roubo de dados e os ataques cibernéticos entre os cinco riscos mais frequentes.

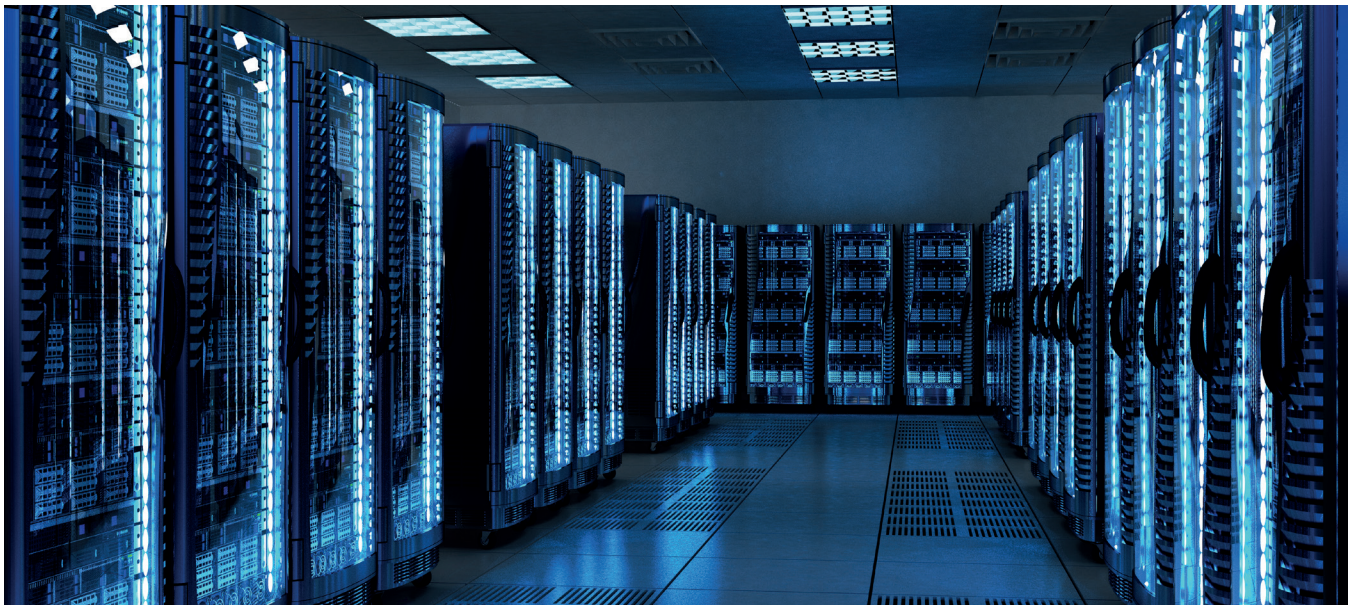
FIGURE 2

Cyber risks outrank all other risks by a wide margin.

Q. Of the following business threats, please rank the top 5 that are the biggest concerns to your organization.



Base: All answering; n=1512 (2019)



A confiança em ciberresiliência aumentou

A pesquisa deste ano constatou um aumento da confiança na resiliência cibernética para que as empresas:

1. Compreendam, avaliem e meçam os possíveis ciberriscos
   Observando o tipo, a probabilidade e o impacto econômico potencial das exposições às quais uma empresa está suscetível pelo uso de dados e tecnologias.

2. Sejam capazes de reduzir a probabilidade de ciberataques ou prevenir danos
   Compreendendo uma combinação de proteções técnicas e não-técnicas.

3. Administrem, recuperem e respondam a incidentes cibernéticos
   Planos de contingência claros e bem ensaiados e recursos disponíveis facilmente para minimizar as consequências negativas e o tempo para recuperação de um incidente.

Em conjunto, estas áreas apresentam uma média geral da capacidade de recuperação de uma empresa: para superar um ciberataque, aplicar uma gama de práticas de planificação, avaliação, prevenção, mitigação e resposta para gestão do risco, além do retorno ao normal das operações com tempo de inatividade e perdas mínimos. Eles se alinham à amplamente utilizada Estrutura de Cibersegurança do Instituto Nacional de Padrões e Tecnologia (NIST) para detectar, impedir, responder e recuperar.

Em 2019, 40% disseram confiar amplamente na sua capacidade atual de gerir os próprios riscos cibernéticos no Brasil. Já na América Latina, o aumento mais significativo foi relacionado à confiança no gerenciamento, resposta e recuperação de um incidente cibernético, de 7% para 18%, em relação a 2017.

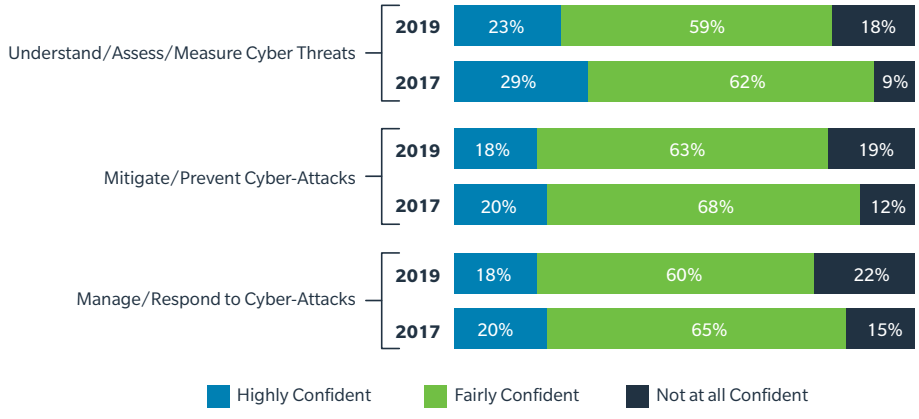
No entanto, apesar desse aumento positivo na confiança das empresas, quase 30% ainda não confiam nos três pilares da resiliência cibernética.

That lack of confidence may stem in part from the relatively small effect organizations are seeing from ever-increasing investments in cybersecurity technology — products and services aimed at preventing or mitigating cyber-attacks. The cybersecurity market is forecast to surpass $124 billion in 2019, but despite soaring cybersecurity spending, the annual cost of cybercrime in 2019 is estimated at $1 trillion.

As organizações podem se sentir frustradas ou confusas quando o aumento do investimento em mitigação de riscos cibernéticos não se correlaciona diretamente com melhores resultados, como costuma acontecer em outras áreas de investimento empresarial e melhoria de desempenho.

FIGURE 3

Confidence in cyber resilience measures slipped from 2017 to 2019.



Base: All answering, excluding "don't know" responses; n=1312 (2017); n=1457 (2019)

A governança cibernética ainda é delegada ao setor de TI

Embora o risco cibernético esteja entre as prioridades das organizações, a governança e a propriedade geralmente não se alinham com essa classificação. Frequentemente, aqueles que deveriam se concentrar na segurança cibernética, não são encarregados disso: as áreas de segurança e sistemas de informação ainda são vistas como as principais responsáveis pelo gerenciamento de riscos cibernéticos.

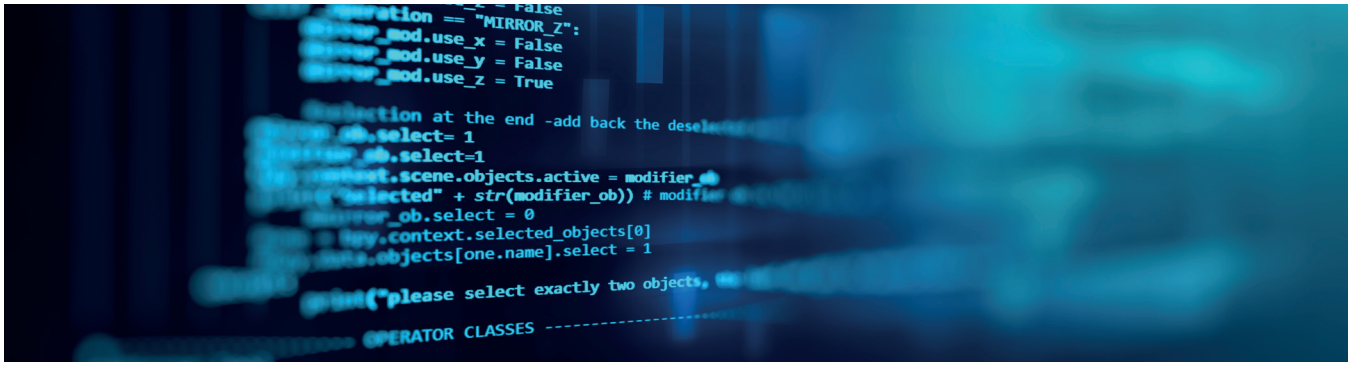
Nas empresas latino-americanas, verificou-se um aumento da predominância do setor com essa responsabilidade nos últimos 2 anos: quase 9 em cada 10 (gráfico 4): o crescimento foi de 28% em relação a 2017. A função de risk manager passou de 17% (2017) para 46% (2019). Esse aumento indica uma tendência clara e positiva sobre um maior posicionamento dos administradores de riscos.

FIGURE 4

IT staff continue to be the main owners of cyber risk management at most firms.

Q: Please rank the three functions which are the main owners or drivers of cyber risk management in your organization.

% Identifying each function as one of the main owners/drivers of cyber risk management
Base: All answering in 2017 and 2019; n=1514 (2019); n=1312 (2017)



46%

A figura do risk manager cresceu como principal responsável pelo gerenciamento de riscos cibernéticos, de 17% para 46%

A tendência de colocar TI, conselho administrativo e risk manager como os principais responsáveis pelos ciberriscos é um sinal positivo de que as pessoas certas estão comandando este assunto. Mas o fato de o TI ser indicado como o líder quase duas vezes mais que os risk managers aponta para uma visão contínua e errônea do risco cibernético como um problema tecnológico, em vez de um risco comercial crítico que merece uma abordagem de gerenciamento estratégico.

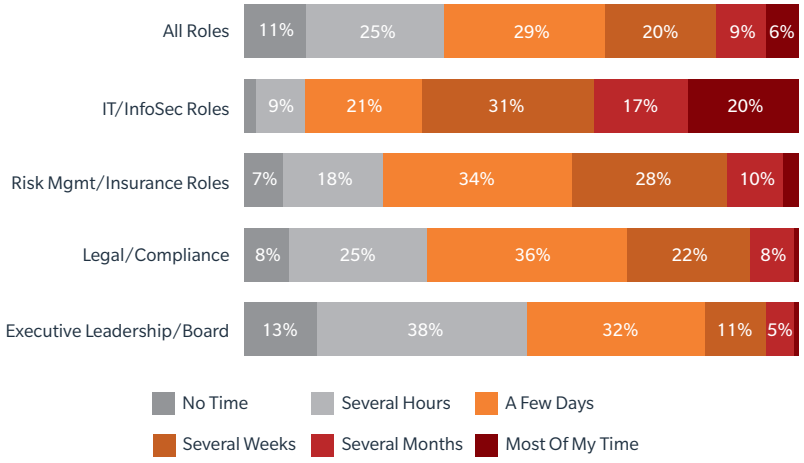
The collective ranking of IT, boards, and risk managers as the primary owners of cyber risk management is a positive sign that the right stakeholders are leading the way. But the fact that IT is named as a primary owner nearly twice as often as risk management points to a continuing, mistaken view of cyber risk as primarily a technology issue, rather than a critical business risk that merits a strategic enterprise risk management approach.

The question of who leads cyber risk management is just one area in which there is dissonance between an organization's perceptions and actions. Despite the high level of strategic concern organizations say they have for cyber risks, not all internal "risk governors" give the issue the attention it deserves (see Figure 5). Only 17% of executive leaders/board members spent more than a few days over the past year focusing on cyber risk issues. Even among IT respondents, 30% said they spent only a few days or less. This

FIGURE 5

Key decision makers are not spending much time on cyber risk management.

Q: Over the past 12 months, approximately how much of your total professional time has been spent on cyber risk and/or cybersecurity?



% Reporting time spent on cyber risk/cyber security issues by each role
Base: All answering; n=1422 (All roles, 2019)

low allocation of time is concerning given that these two constituencies are ranked among the top three organizational owners of cyber risk management.

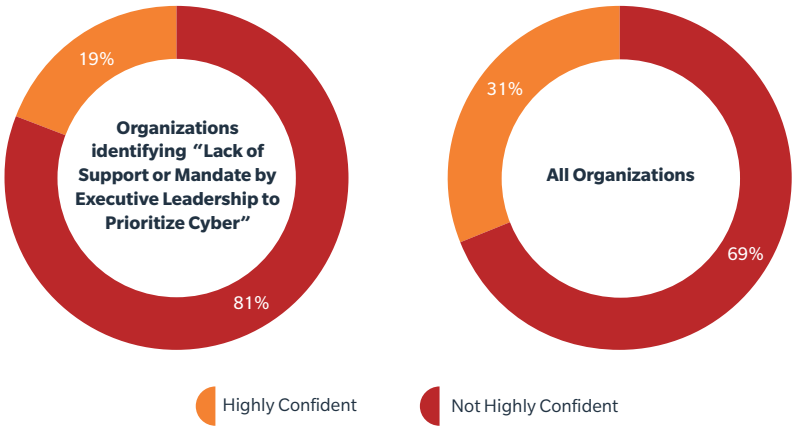
The importance of senior leadership driving the cyber risk agenda is underscored by the confidence gap in overall cyber resilience as reported by those who lack such leadership (see Figure 6). Only 19% of organizations without a senior-level mandate to prioritize cyber risk were highly confident in any of the three areas of cyber resilience, compared to 31% of all respondents.

Despite wide acknowledgement of cyber risk as a top priority, too few organizations currently take actions to create a strong cybersecurity "culture" with appropriate standards for governance, prioritization, management focus, and ownership. This places them at a disadvantage both in building cyber resilience and in confronting the increasing cyber challenges of a changing technology and supply chain environment.

FIGURE 6

Confidence in cyber resilience is very low where senior leaders don't prioritize cyber risk management.

Q: Which of the following do you consider major challenges or barriers to effective cyber risk management for your organization?



"High Confidence Score" - % selecting "Highly Confident" in any of the three areas of cyber resilience
Base: All answering; n=1517 (2019)

Novas tecnologias aumentam a exposição aos ciberriscos

As empresas estão abraçando a inovação tecnológica e a maioria não vê o risco cibernético como uma barreira. Mas a avaliação do risco cibernético das novas tecnologias não é tão rigorosa e contínua como deveria ser.

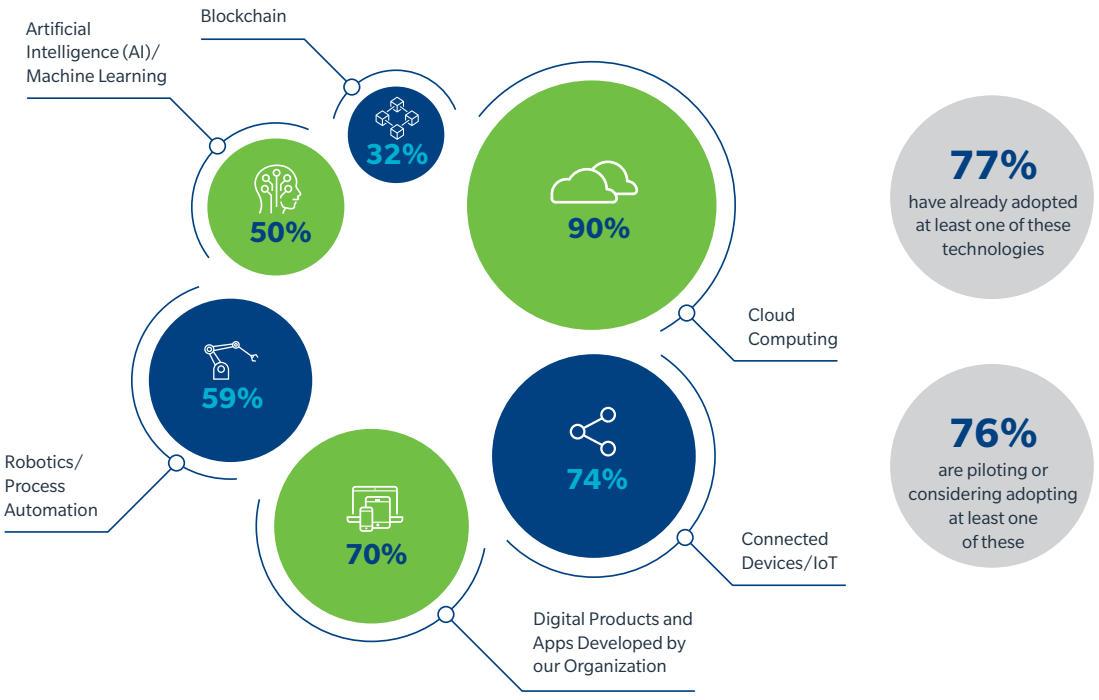
Estima-se que em 2025 a quantidade de dispositivos conectados à internet seja de 75 bilhões. A medida que o mundo se utiliza da Internet das Coisas (IoT), aumenta a quantidade e variedade de dados digitais armazenados, processados e compartilhados pelas empresas. Setores tradicionais da indústria manufatureira esperam que cerca de 50% dos produtos desenvolvidos sejam "inteligentes" ou "conectados" de alguma maneira até 2020, o que resultaria em novas fontes de receita em serviços baseados em dados.

More than three-quarters of 2019 survey respondents cited at least one innovative operational technology — including cloud computing, proprietary digital products, and connected devices/IoT — that they have adopted or are actively considering (see Figure 7).

FIGURE 7

Most organizations are considering or using a range of new technologies.

Q: For each of the following technologies, please indicate which consideration or usage scenario best applies to your organisation



% of organizations that have adopted or are piloting/considering each technology
Base: All answering, excluding don't know responses: n=588-773 (2019)

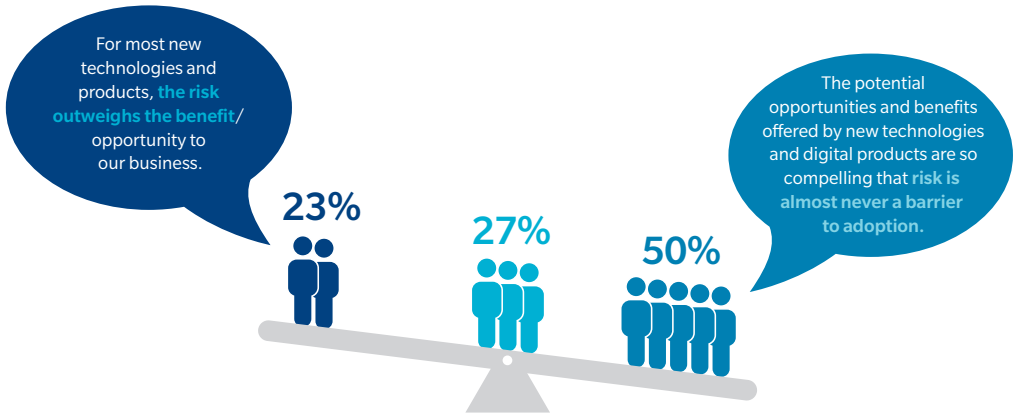
Os desafios para a segurança podem ser percebidos cada vez que uma nova tecnologia passa a fazer parte da infraestrutura corporativa, representando uma nova e adicional preocupação ao marco tecnológico. Riscos e exposições oferecidos pelas novas tecnologias devem pesar diante dos possíveis efeitos transformadores do negócio e a tolerância ao risco varia de acordo com a indústria e a própria empresa. Um terço dos entrevistados respondeu que o ciberrisco quase nunca é um empecilho à adoção de novas tecnologias (gráfico 8).

A preferência por promover a transformação digital prevalece, apesar dos possíveis riscos à segurança. Apesar disso, 29% dos entrevistados mencionaram que a maioria das novas tecnologias apresenta riscos que superam os possíveis benefícios e oportunidades. Essa tendência ocorreu principalmente em pequenas empresas (aquelas com faturamento anual inferior a US$ 100 milhões), independentemente do setor.

FIGURE 8

The potential benefits of new technologies are generally seen to outweigh the potential risks.

Q: For each of the following pairs of statements, please indicate which most strongly reflects your organization's attitude.



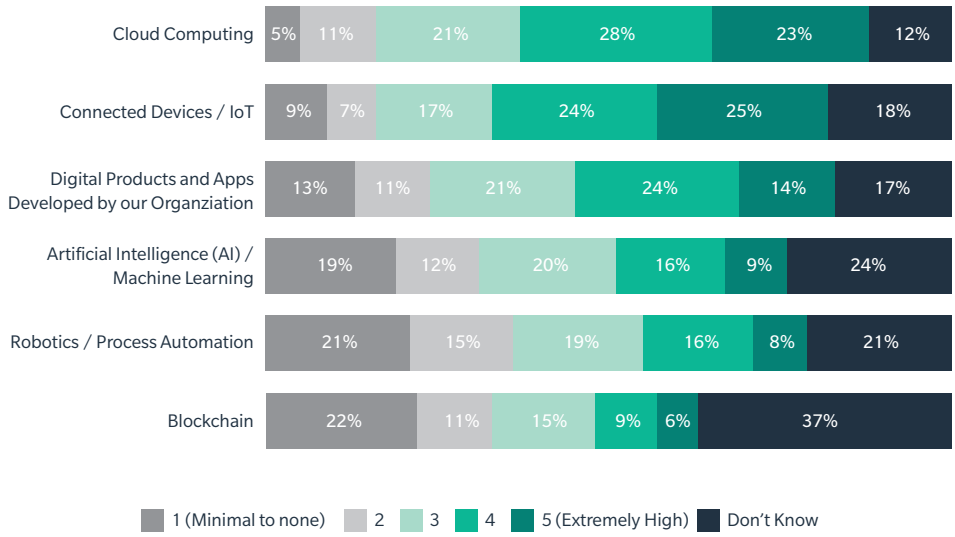
% of organizations agreeing with each of the statements (presented to respondents as a trade off)
Base: All answering; n=852 (2019)

Apesar da predisposição para novas e emergentes tecnologias, há incerteza sobre o nível de risco associado a essas tecnologias (ver figura 9). Com relação ao nível de risco cibernético associado, o armazenamento em nuvem teve a menor quantidade de respostas relacionadas à opção "não sei" (10%), enquanto que blockchain obteve a maior (34%). No caso de novos produtos ou aplicativos digitais em desenvolvimento, as opiniões foram divididas igualmente: aqueles que perceberam um alto nível de risco e aqueles que viram um nível mais baixo. O nível mais alto de incerteza foi relacionado às novas tecnologias blockchain (34%) e inteligência artificial (20%).

FIGURE 9

Many business decision-makers are uncertain about the degree of risk posed by new business technologies.

Q: Please rate the level of perceived cyber risk associated with each technology, on a 5 point scale.



Base: All answering for each technology: varies from n= 892 to n=900 (2019)

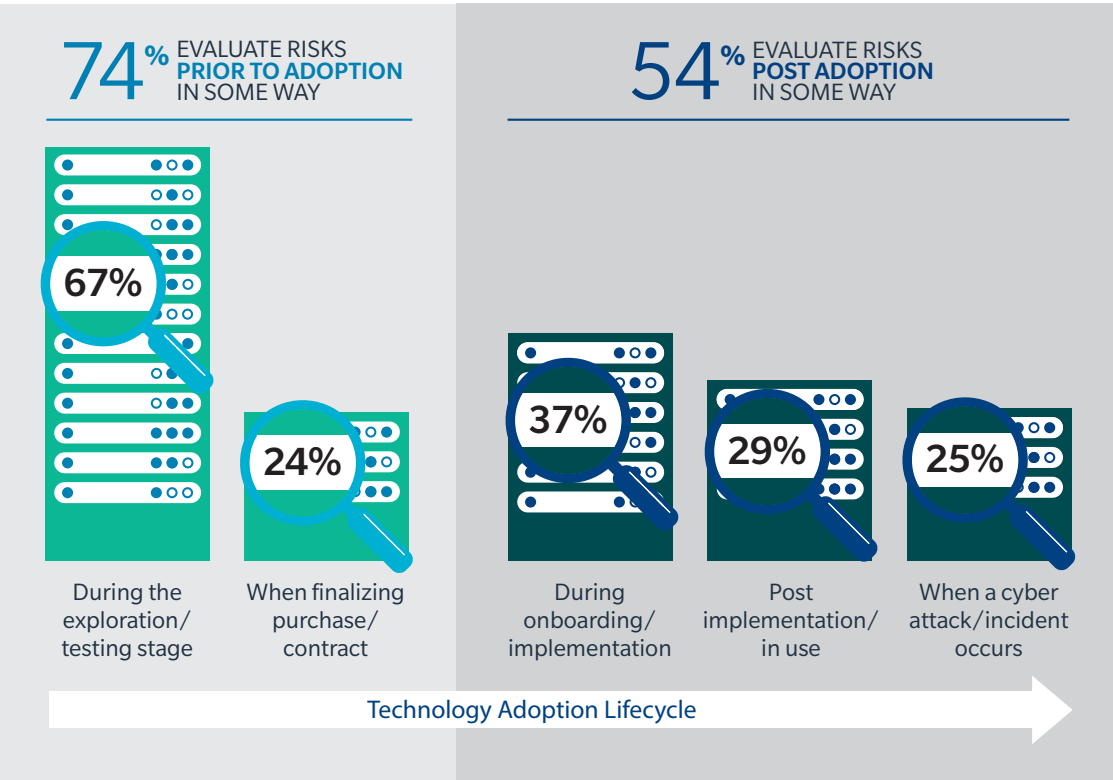
Entre os entrevistados, a consideração do risco cibernético acontece, com muita frequência, como um evento que ocorre em um momento específico (geralmente, em um estágio de exploração e teste inicial), em vez de uma avaliação contínua em vários estágios de implementação (gráfico 10).

Apenas 37% das empresas na América Latina examinam os riscos potenciais de uma nova tecnologia antes e depois da adoção. Somente 5% mencionaram a avaliação do risco cibernético em cada estágio do ciclo de vida da tecnologia.

FIGURE 10

Cyber risk most commonly evaluated during the exploration/testing stage of technology adoption.

Q: When adopting and implementing new technologies, such as those you have just identified, at which of the following stages is cyber risk typically evaluated in your organization?



Only **36%** evaluated risks both prior to and after adoption.

Just **5%** evaluate risks at all possible stages of the lifecycle.

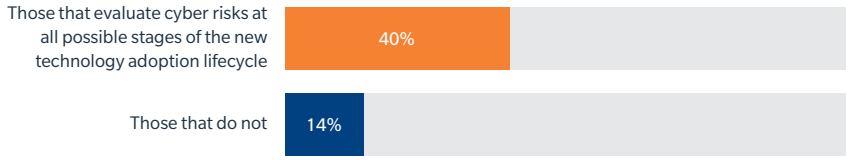
11% don't evaluate at all.

Base: All answering, excluding don't know: n=696 (2019)

O seleto grupo de empresas que avaliam riscos cibernéticos continuamente ao longo da implementação de novas tecnologias confiam mais em seus próprios recursos para gerenciar ou responder a ataques cibernéticos (gráfico 11).

FIGURE 11

Organizations that continuously evaluate new technology cyber risk are more confident in their overall cybersecurity.



% reporting high confidence in ability to manage or respond to a cyber attack
Base: All answering both Q9 & Q24: n=696 (2019)

As empresas que testam os riscos da tecnologia em vários estágios de implementação podem se sentir melhor informadas porque a avaliação contínua dos riscos fornece visibilidade em tempo real dos riscos e vulnerabilidades emergentes. Preparadas com o conhecimento oportuno de possíveis fraquezas ou exposições de segurança, elas estão prontas para implementar melhorias rapidamente e desenvolver planos de contingência para gerenciar os riscos envolvidos nesses sistemas.

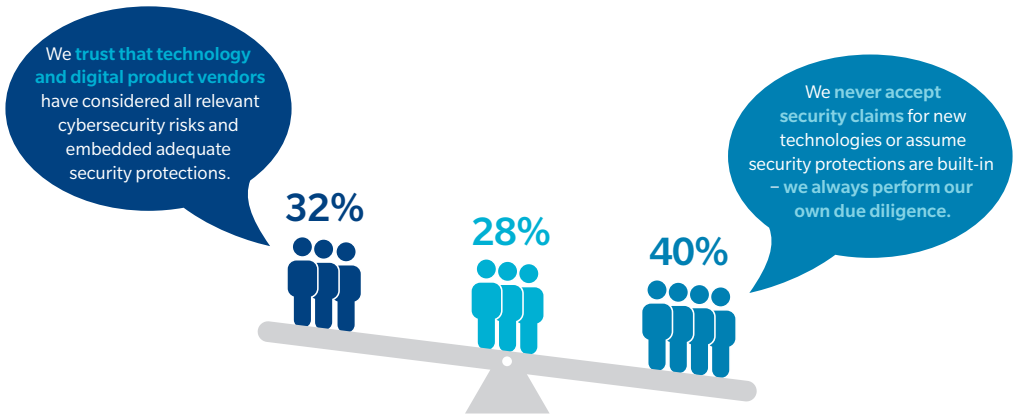
A avaliação de riscos cibernéticos de novas tecnologias está intimamente associada à confiança que as organizações têm, ou não, nos fornecedores que as fornecem. As tecnologias inovadoras não representam necessariamente novos riscos cibernéticos para as organizações que as adotam. Algumas tecnologias podem adicionar novos riscos se não tiverem sido implementadas de acordo com os padrões de segurança ideais, mas em muitos casos, a segurança é integrada a partir da criação da tecnologia ou dispositivo.

45% das empresas na América Latina assumem que os fornecedores de tecnologia consideraram todos os riscos cibernéticos relevantes e que nenhuma verificação adicional é necessária. Apenas 27% disseram que "sempre realizam seu próprio procedimento" para verificar se as necessidades de segurança e as proteções integradas que os fornecedores de novas tecnologias estão completas (gráfico 12).

FIGURE 12

One third of organizations assume technology vendors have considered all relevant cyber risks.

Q: For each of the following pairs of statements, please indicate which most strongly reflects your organization's attitude.



% of organizations agreeing with each of the statements (presented to respondents as a trade off)
Base: All answering: n=830 (2019)

Cada empresa depende de um certo nível de confiança em seus relacionamentos com seus fornecedores e contratados. No entanto, dada a importância de plataformas e serviços tecnológicos para ativos e operações centrais, uma posição rigorosa de confiança e verificação deve ser assumida para ajudar a garantir a validade e adequação das proteções prometidas por terceiros. Essa maior vigilância é especialmente importante quando novos processos digitais são inerentes aos modelos de negócios das empresas.

37%

das empresas brasileiras percebem os riscos de sua cadeia de suprimentos

Risco na cadeia de suprimentos: rumo a uma responsabilidade social tecnológica

Nas cadeias de suprimentos digitais cada vez mais interdependentes, o risco cibernético deve ser uma responsabilidade coletiva.

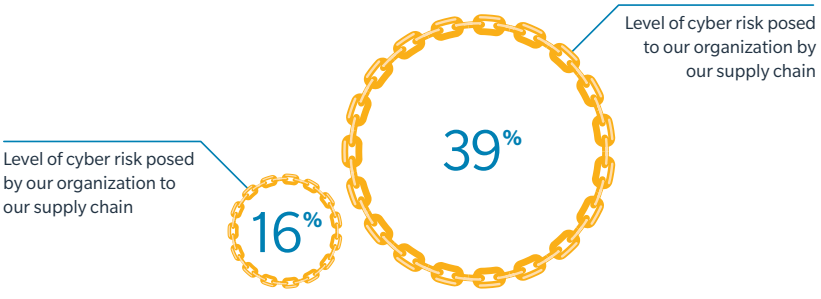
Em um mundo de cadeias de suprimentos hiperconectadas, há uma necessidade crítica de confiança entre parceiros. A falta de confiança pode levar ao prejuízo do desempenho e da inovação dos negócios. Toda organização precisa entender, confiar e desempenhar um papel de igual importância na segurança dos componentes e softwares de suas cadeias de suprimentos digitais. O conceito de "responsabilidade social tecnológica" (o conhecimento e o reconhecimento de cada organização de seu papel e obrigações de segurança cibernética na cadeia de suprimentos) está na agenda de muitos líderes do setor.

No entanto, embora muitas organizações reconheçam os riscos potenciais que seus parceiros da cadeia de suprimentos podem representar para si, a maioria não vê. Há uma discrepância notável na visão de muitas organizações em relação ao ciberrisco: maior para os parceiros em comparação com o nível de risco que sua organização representa para eles.

FIGURE 13

Many organizations are more attuned to the risks they face from their supply chains than the risks they themselves pose.

Q: What level of cyber risk is posed to your organization by its supply chain/third parties? And the reverse: what level of cyber risk does your organization pose to its supply chain/third parties?

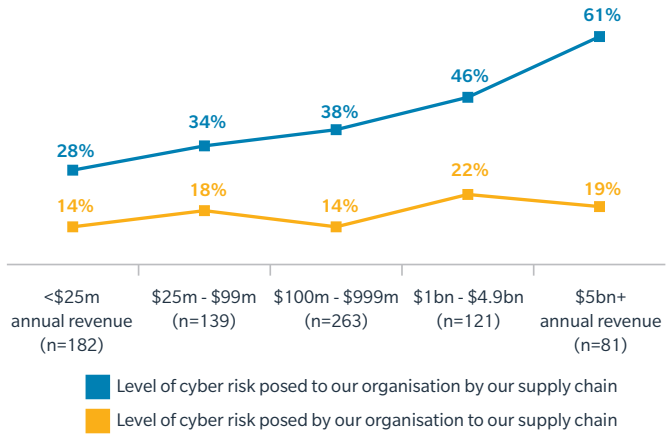


% regarding each risk as "somewhat" or "very high"
Base: All answering: n=786 (2019)

FIGURE 14

Larger organizations are more likely to perceive risks from their supply chains than to recognize risks they themselves pose.

Q: What level of cyber risk is posed to your organization by its supply chain / third parties? And the reverse: what level of cyber risk does your organization pose to it's supply chain / third parties?



% regarding each risk as "somewhat" or "very high"
Base: All answering (2019): Base varies as indicated.

Cerca de 1 em cada 3 entrevistados considera que a cadeia de suprimentos representa um risco para sua organização (gráfico 13). Enquanto que eles acreditam que há duas vezes mais chances de estarem vulneráveis aos riscos de seus parceiros do que em suas próprias cadeias de suprimentos. Esse padrão apareceu em todos os setores e regiões geográficas.

Moreover, the largest organizations exhibited the largest dissonance on this topic. Among the smallest firms, 28% stated that they faced high risks from their supply chain, while half of that said they posed risks to it (see Figure 14). This gap increased markedly with revenue size, with 61% of companies of $5 billion revenues or more saying they faced high risks from their supply chain and only 19% saying they posed a risk to it.

This is a perception gap that many organizations, especially large ones, need to address in order to effectively protect their supply chain ecosystem — embracing their own technological social responsibilities.

Apenas 21% *pensam que sua própria organização representa risco à sua cadeia de suprimentos*

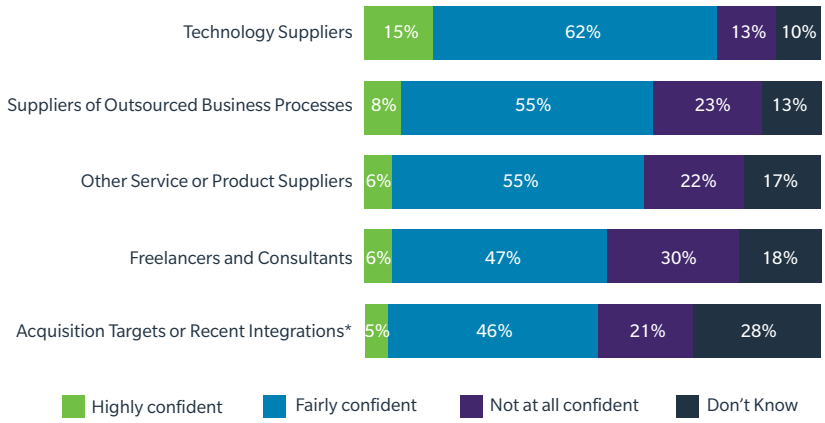
Em geral, **25%** *das empresas na América Latina disseram não confiar nem um pouco em sua capacidade de impedir ameaças cibernéticas de pelo menos um de seus parceiros*

A desconexão pode ser gerada pela baixa confiança das organizações em suas habilidades para prevenir ou mitigar os riscos cibernéticos derivados de seus stakeholders. A porcentagem de organizações que disseram ter "alta confiança" na mitigação das ameaças cibernéticas de seus parceiros da cadeia de suprimentos variou entre 8% e 19%, dependendo do tipo de fornecedor (gráfico 15). No geral, 25% disseram que "não confiavam em nada" em sua capacidade de impedir ameaças cibernéticas de pelo menos um de terceiros.

FIGURE 15

Few organizations are highly confident in their ability to manage cyber risk from third parties.

Q: How confident are you in your organization's ability to prevent / mitigate cyber risk from the following?



% of organizations reporting different levels of confidence
Base: All answering; n=878 (2019); *Results for this option only shown for businesses with US$1bn+ revenues (n=215)

Midsize firms tended to report the strongest levels of confidence in managing suppliers of various types. For example, 71% of firms with between $100 million and $1 billion in annual revenue stated that they were "fairly" or "highly confident" in their ability to mitigate risks arising from outsourced business process providers, compared with 60% in all other size categories. This may suggest that midsize firms are small enough to know their supply chain partners' risks, yet large enough to have the resources to adequately assess them.

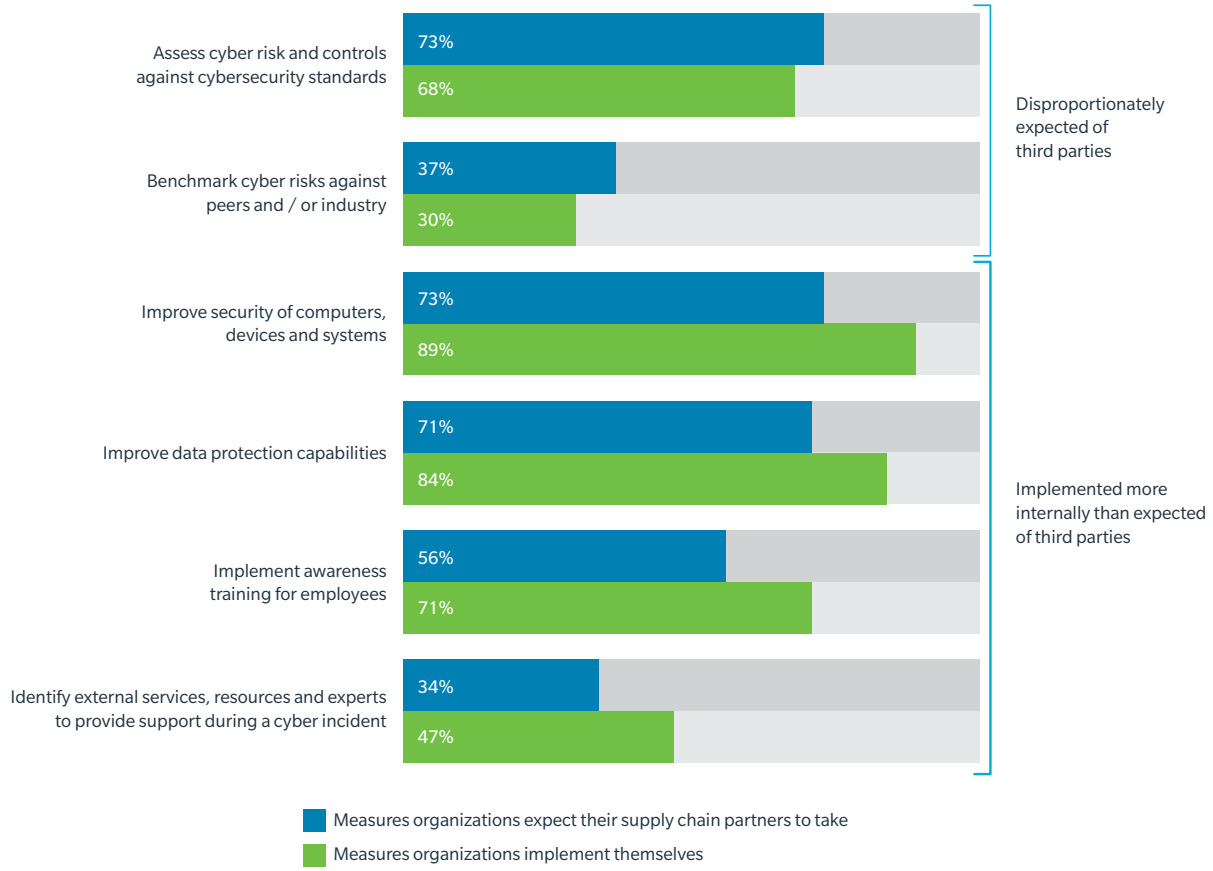
Há também uma disparidade entre medidas e padrões de cibersegurança que as organizações aplicam a si mesmas, em comparação com o que elas esperam dos fornecedores (gráfico 16). Em geral, os entrevistados tinham maior probabilidade de estabelecer um nível mais alto para as medidas de gerenciamento de riscos cibernéticos de sua própria organização do que para seus fornecedores.

56% das organizações disseram esperar que os fornecedores de suas cadeias de suprimentos digitais implementem treinamento de conscientização para seus funcionários. No entanto, 66% disseram que sua organização implementou esse requisito por si só. Tais disparidades podem levar as organizações a pensar que seus fornecedores estão menos preparados para gerenciar riscos cibernéticos do que eles, o que diminui a confiança da empresa em sua cadeia de suprimentos.

FIGURE 16

There is a disparity between what measures organizations expect of themselves versus what they expect from third parties.

Q: What cybersecurity measures do you expect your supply chain partners / thirds parties to take? Please indicate whether your organization has taken the specific actions listed below.



Base: All answering both questions: n=706 (2019)

Opiniões divididas sobre o papel do governo

As empresas veem uma eficácia limitada da regulamentação governamental para ajudar a gerenciar o risco cibernético, mas estão ansiosas por receber ajuda com desafios cibernéticos que não podem resolver sozinhas.

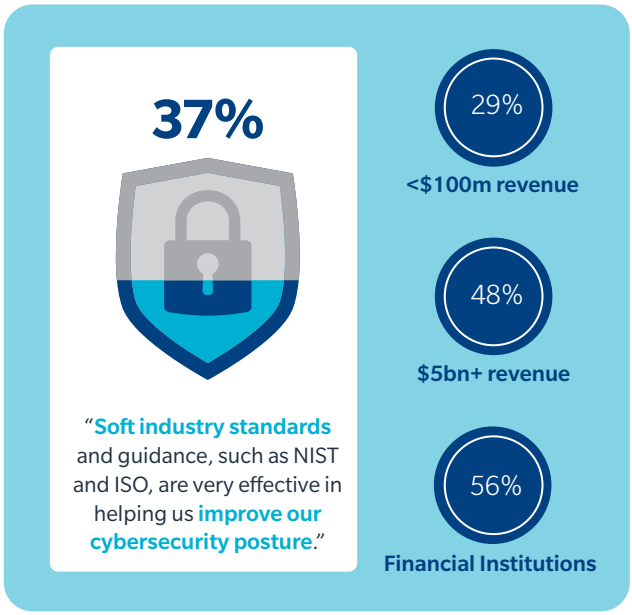
Nos últimos anos, os reguladores globais adotaram inúmeras medidas para tornar as empresas e os executivos mais diretamente responsáveis por garantir uma segurança cibernética eficaz e manter os dados dos clientes em segurança. Muitos desses regulamentos e estruturas legais exigem um maior grau de transparência das organizações em todos os níveis de suas atividades de gerenciamento de dados e na preparação para o gerenciamento de riscos cibernéticos. O crescimento de tais leis e regulamentos complementa um conjunto de padrões bem estabelecidos para computadores e cibersegurança das autoridades do setor, como o NIST e a Organização Internacional para Padronização (ISO).

A maioria dos entrevistados disse que as leis e os regulamentos governamentais são menos eficazes para ajudá-los a melhorar sua postura de segurança cibernética em comparação com os padrões e orientações "suaves" do setor (gráfico 17). Mesmo assim, poucos entrevistados acreditam que a regulamentação ou orientação do setor seja muito eficaz para ajudar a melhorar a conduta de suas empresas com relação aos ciberriscos.

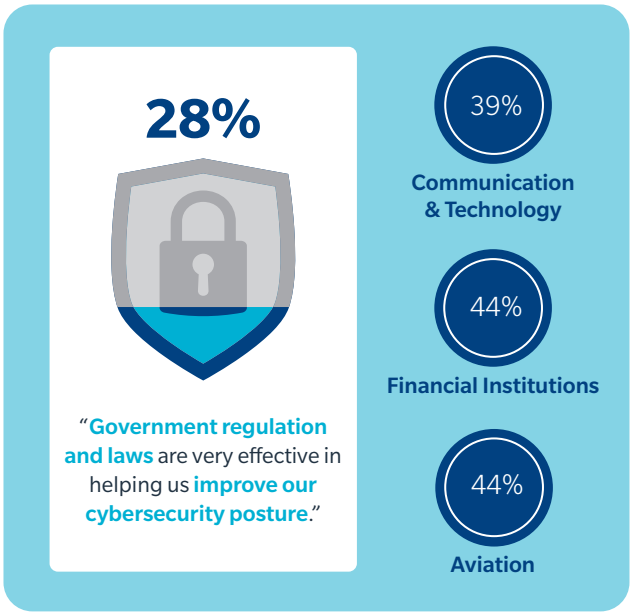
FIGURE 17

Fewer than half of businesses globally regard government regulations or industry standards as being effective in improving cybersecurity.

Q: For each of the following pairs of statements, please indicate which choice most closely reflects your organization's views.



Base: All answering: n=822 (2019)



Base: All answering: n=828 (2019)

Industry guidance and standards, such as NIST and ISO, appear to be best appreciated by the largest, best-resourced companies. Only 29% of organizations with revenues of under $100 million revenue see these as being effective, compared to nearly half (48%) of companies with annual revenues over $5 billion. Notably, 41% of organizations that carry out rigorous economic quantification of their cyber risks viewed NIST and ISO-type standards as being very effective.

Barely a quarter of respondent organizations identified government regulations and laws as being very effective in improving cybersecurity. This held across all major regions, despite considerable variance in local laws and regulation. However, highly regulated industries, such as aviation, financial institutions, and communications, were more likely to see value in government regulation of cyber risk.

The major area of difference in the attitude toward cyber regulation related to cyber-attacks by nation-state actors (see Figure 18). In this context, a majority (54%) of respondents said they are highly concerned about the impact of nation-state cyber-attacks. This percentage rises to 60% to 70% for the largest organizations and those engaged in critical national infrastructure, such as financial institutions, aviation, communications, and energy firms. Of companies with under $100 million annual revenue, 49% registered “high concern”.

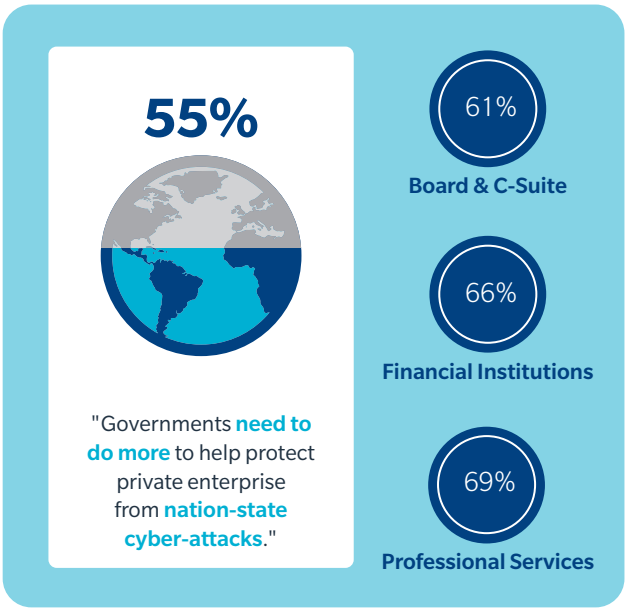
Consistent with that view, 55% of organizations said there is a need for governments to do more to protect private enterprise from nation-state cyber-attacks. This call-for-action resounds consistently across regions, with the highest positive response among financial institutions and professional services organizations. Such calls for government assistance were most often voiced by executive leadership. These results show that while firms generally prefer a non-prescriptive approach to managing their cyber security and cyber risk affairs, nation-state activity is a clear exception.

FIGURE 18

Organizations looking to government for help addressing nation-state cyber-attacks.

Q: For each of the following pairs of statements, please indicate which choice most closely reflects your organization’s views.

Base: All answering: n=825 (2019)



Base: All answering: n=821 (2019)

O investimento cibernético se concentra na prevenção e não na resiliência

O gerenciamento eficaz de riscos cibernéticos requer uma expressão quantitativa de risco. Embora mais empresas latino-americanas meçam seus riscos cibernéticos economicamente em comparação com dois anos atrás, ainda há um longo caminho para todas as organizações adotarem essa prática e aplicarem essa medida quantificada para conduzir decisões sólidas de investimento em ciberriscos.

Os investimentos em tecnologia de cibersegurança estão aumentando rapidamente e excedendo em muito os gastos com seguros cyber. Estima-se que o mercado global de seguros cibernéticos, medido pelos prêmios emitidos brutos, esteja abaixo de US$ 8.000 milhões até 2020 (gráfico 19), em comparação com um mercado global de segurança cibernética de US$ 124.000 milhões.

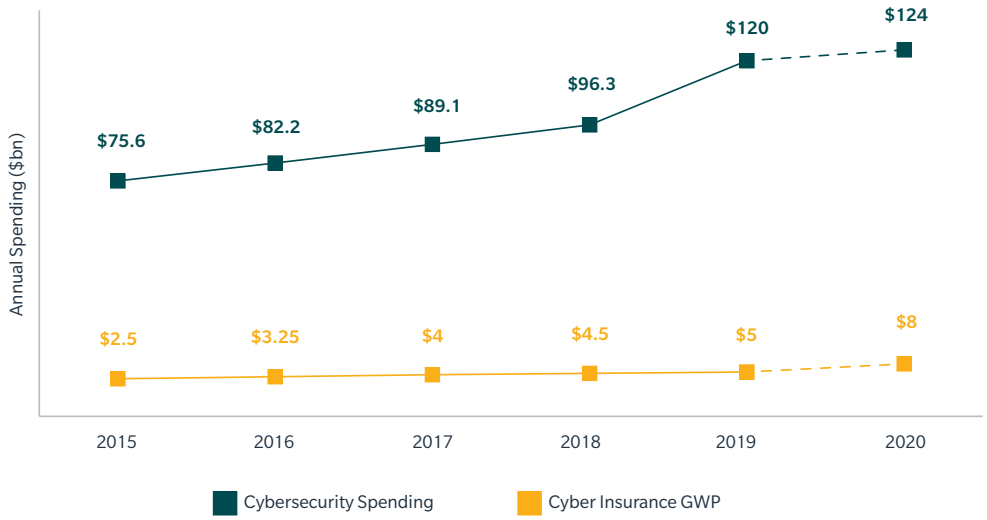
Muitas organizações concentram sua estratégia de gerenciamento de ciberriscos na prevenção, investindo em defesa cibernética com tecnologia de ponta. Enquanto isso, os gastos com outras ferramentas e recursos para gerenciamento de riscos cibernéticos, como seguro cyber ou treinamento em resposta a incidentes, continuam sendo uma fração do orçamento destinado à tecnologia. Isso sugere que muitas organizações continuam acreditando que podem eliminar ou gerenciar seus riscos cibernéticos principalmente por meio da tecnologia e não por uma ampla gama de medidas de planejamento, transferência e resposta.

As melhores práticas não exigem a igualdade de gastos, mas uma estratégia de investimento que, refletindo o perfil de risco e o desejo exclusivos de uma organização, aproveite as funções complementares de tecnologia e seguro para impedir ataques cibernéticos sempre que possível e transferir riscos daqueles que não podem ser evitados. No entanto, a ênfase nos gastos e tecnologia em cibersegurança em detrimento de outras medidas revela que muitas empresas ainda não aceitaram essa verdade.

FIGURE 19

Cybersecurity spending far outpaces cyber insurance spending.

SOURCE: Gartner, Munich Re



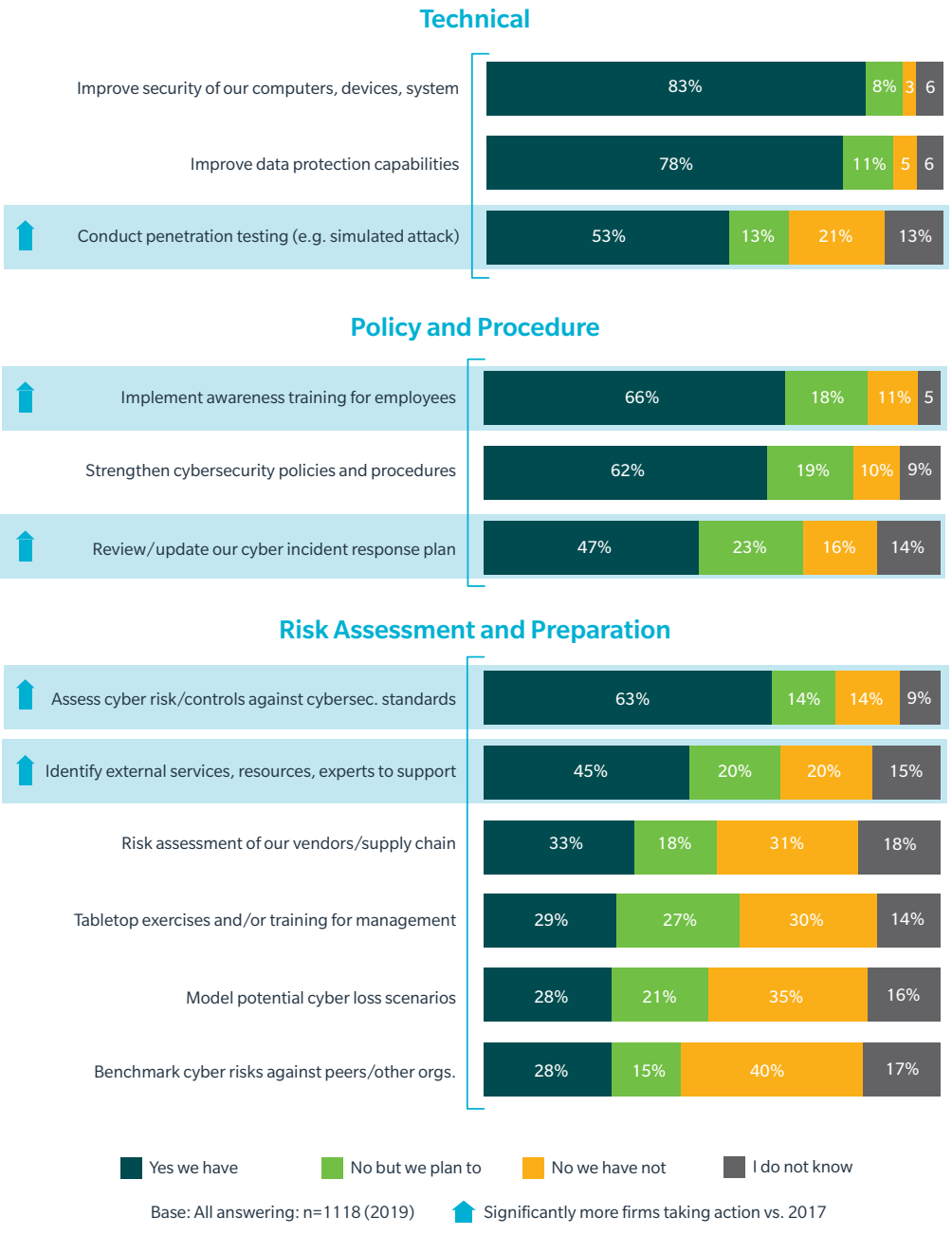
Por exemplo, a maioria dos entrevistados citou uma ou mais melhorias técnicas como ações executadas nos últimos 12 ou 24 meses (gráfico 20). Menos iniciativas são tomadas em áreas como treinamento de funcionários, políticas de segurança cibernética e planos de resposta a incidentes cibernéticos.

Algumas das ações relatadas com menos frequência foram as que estão alinhadas com a avaliação e modelagem de riscos cibernéticos. A quantidade de ações não mudou muito desde 2017. A exceção em relação à avaliação de riscos cibernéticos foi onde os riscos eram principalmente técnicos: 56% disseram que avaliaram seus controles técnicos em relação aos padrões estabelecidos de cibersegurança.

FIGURE 20

Cyber risk resilience actions tend to focus on technical measures.

Q: Please indicate whether your organization has taken the specific actions listed below within the past 12 to 24 months.

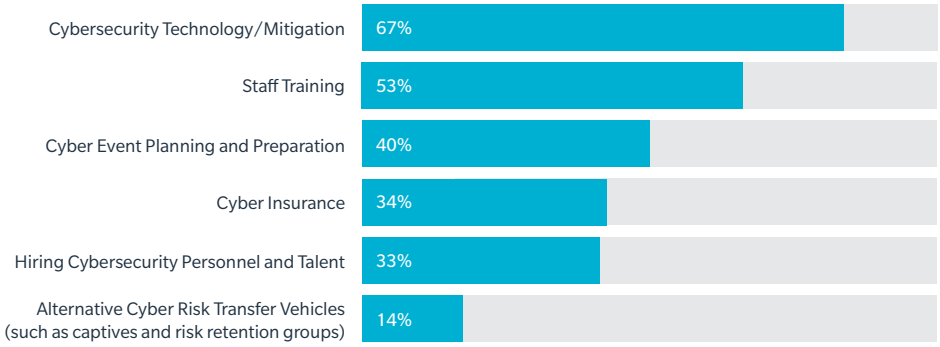


Olhando para o futuro, as tendências parecem estar prontas para continuar. Entre as áreas em que as empresas planejam aumentar os gastos com gerenciamento de riscos nos próximos três anos, mais da metade citou a tecnologia e capacitação de pessoal em segurança cibernética, muito mais do que em todas as outras áreas (gráfico 21).

FIGURE 21

Cybersecurity technology and mitigation top the list of future investment allocations for risk management.

Q: How do you expect your investment allocations in the following areas of risk management to evolve over the next three years?



% expecting to spend some or significantly more on each area
Base: All answering: n=885 (2019)

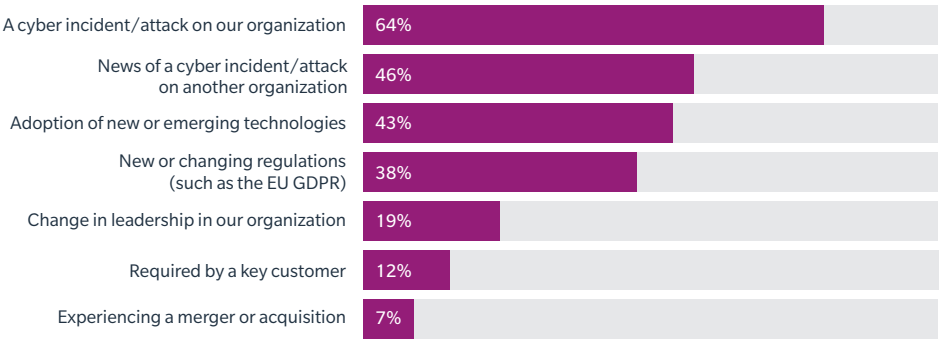
Os gastos com tecnologia continuam aumentando, mas sem um aumento correspondente no uso de estruturas econômicas, como quantificação de ciberriscos, para informar decisões de investimento, medir a eficácia da redução de riscos ou permitir a comparação com outros investimentos de risco corporativo.

De fato, muitas organizações parecem ter uma postura reativa em relação aos riscos cibernéticos: o gatilho mais citado para aumentar o investimento foi um incidente cibernético (gráfico 22). Muito menos comum de acontecer são os líderes das empresas proativamente investirem nisso.

FIGURE 22

Cyber incidents are the main trigger for increases in cyber risk management investments.

Q: Which factor will have the biggest impact on your organization's planned increase in budget allocation for the following areas of cyber risk management?



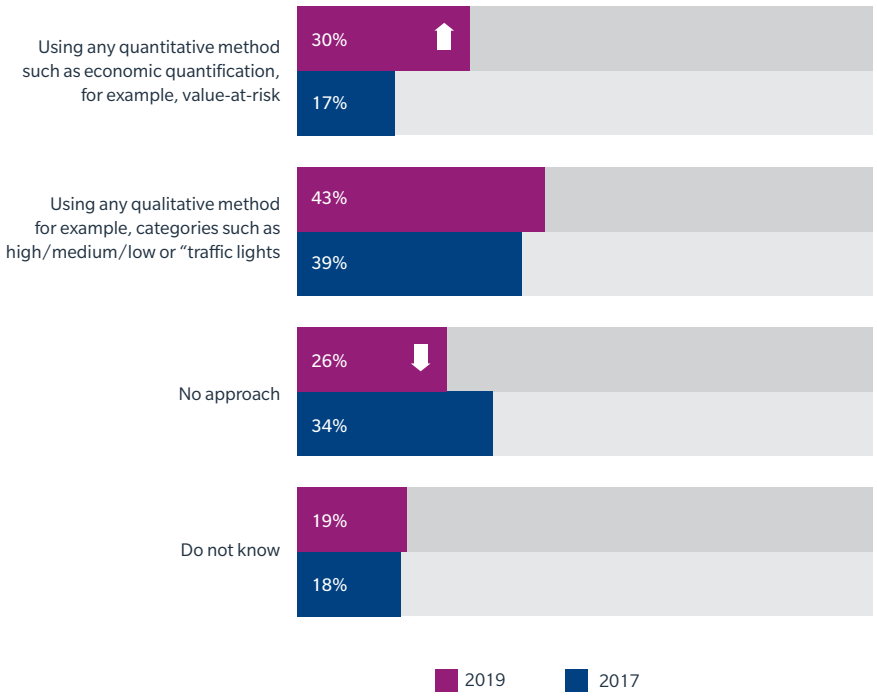
% selecting as a driver for any area of increased cyber risk investment
Base: All answering & stating they plan to invest more, excluding don't know responses: n=615 (2019)

O uso de métodos quantitativos para expressar exposições a riscos cibernéticos está progredindo (gráfico 23). A proporção de organizações latino-americanas que utilizaram esses métodos quadruplicou desde 2017, de 8% para 33%. Houve uma redução simultânea na proporção de entrevistados que disseram não ter uma abordagem para avaliar formal ou sistematicamente sua exposição ao ciberrisco, de 43% para 29%.

FIGURE 23

Quantitative measurement of cyber risk exposure has increased substantially since 2017, but remains low overall.

Q: In general, how does your organization measure or express its cyber risk exposure?



Base: All answering: n=1303 (2019); n=1312 (2017)

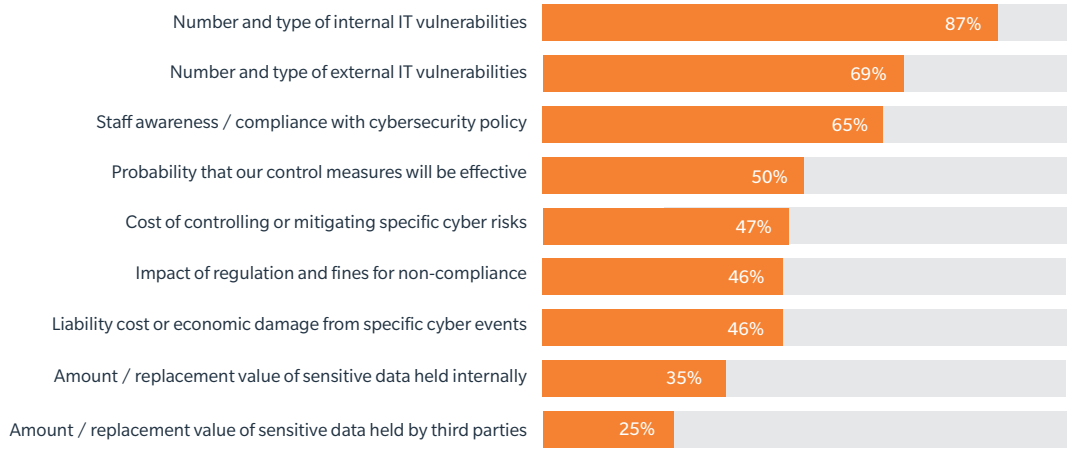
Mesmo assim, a maioria dos entrevistados em 2019 (67%) não expressou quantitativamente suas exposições a riscos cibernéticos ou usou dados quantitativos para orientar as decisões de investimento. Isso pode ser devido à falta de experiência organizacional em relação à quantificação do risco cibernético, à falta de recursos (tempo e dinheiro) ou à probabilidade de muitas empresas continuarem a considerar as ameaças cibernéticas como um problema tecnológico e não econômico. Essa última posição é apoiada pelo fato de que mais do dobro da organização avalia o ciberrisco contando as vulnerabilidades dos sistemas em comparação com as que avaliam custos, multas e perdas em potencial (gráfico 24).

Além de como os riscos cibernéticos são expressos, as áreas consideradas ao realizar avaliações também variaram bastante. As organizações que realizam alguma forma de avaliação de riscos cibernéticos tendem a se concentrar na contagem de vulnerabilidades técnicas, em vez de em custos de reparação ou recuperação, multas ou outras responsabilidades.

FIGURE 24

Risk assessment methods focus on counting technical vulnerabilities, but fail to adequately consider economic aspects of cyber exposure.

Q: Which of the following does your organization consider in its cyber risk assessment/measurement?



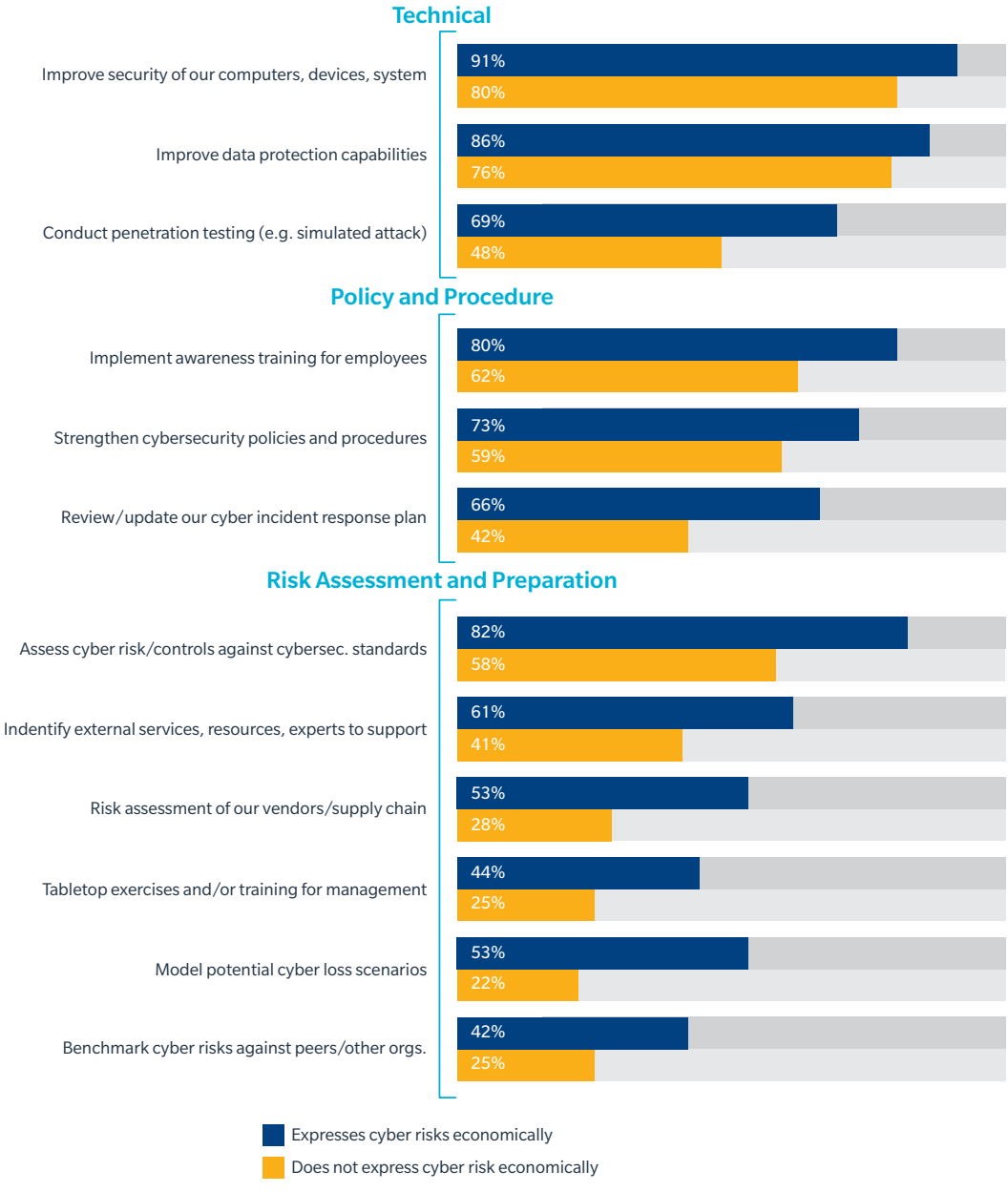
Base: Those with some form of cyber risk assessment method: n=660 (2019)

As organizações que expressam e relatam financeiramente os riscos cibernéticos parecem ter muito mais probabilidade de implementar uma relação maior de atividades de avaliação, planejamento e treinamento que complementam medidas técnicas e são essenciais para o desenvolvimento de resiliência cibernética (gráfico 25). Isso envolve a transferência de riscos, políticas e procedimentos e uma abordagem abrangente da avaliação desses riscos, incluindo de fornecedores e cadeias de suprimentos.

FIGURE 25

Companies conducting economic quantification of cyber risk are more likely to balance technical and non-technical actions.

Q: Please indicate whether your organization has taken the specific actions listed below within the past 12 to 24 months.



Base: All answering: n=1118 (2019)

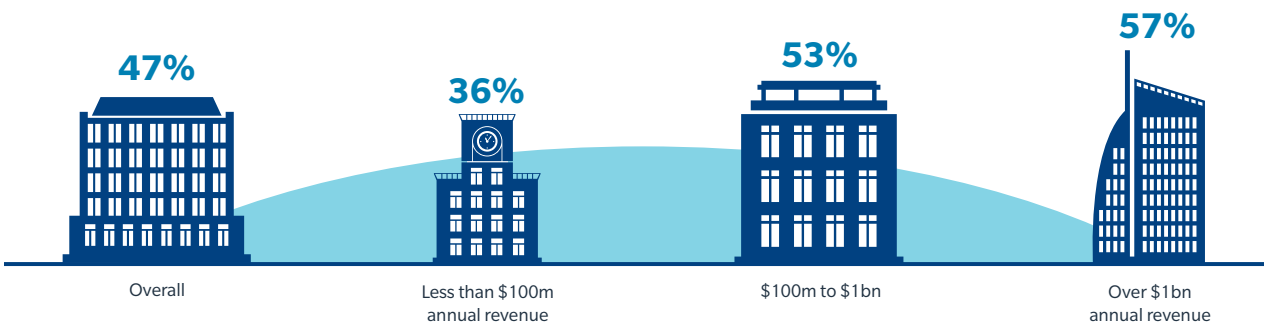
Mas nem todos os riscos cibernéticos podem ser mitigados por meio de tecnologia, política ou processo, especialmente as perdas de baixa frequência, mas de alta gravidade que podem causar danos financeiros e operacionais significativos. Nesses casos, a transferência de risco por meio de seguro ou outros métodos é essencial.

Na América Latina, 29% das empresas dizem que agora têm essa cobertura de seguro (gráfico 26). Por trás dessa imagem, há tendências divergentes em relação ao tamanho da empresa: embora mais de um terço das empresas de médio e grande porte tendam mais a ter seguro cibernético, apenas 22% das pequenas empresas o possuem.

FIGURE 26

Midsize and larger enterprises are more likely to have cyber insurance.

Q: What is your organization's status with regard to cyber insurance?



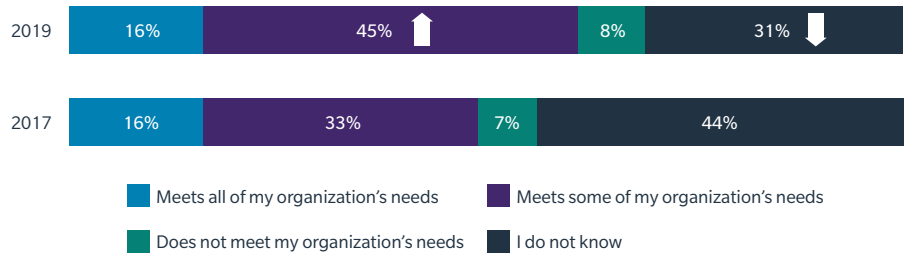
Base: All answering, excluding don't know responses: n=1120 (2019)

Desde 2017, a incerteza em torno da capacidade do seguro cibernético de proteção contra perdas diminuiu. O número de empresas que dizem não saber sobre a disponibilidade do seguro cyber caiu de 42% em 2017 para 39% em 2019 (gráfico 27). A proporção de organizações que afirmam que o seguro cibernético atende a algumas necessidades organizacionais aumentou de 29% em 2017 para 40% em 2019. O desafio para as seguradoras no futuro é aumentar a percepção dos compradores de que o seguro cyber pode atender adequadamente, uma vez que esse número permaneceu constante em 12%.

FIGURE 27

Uncertainty in the ability of cyber insurance to meet an organization's needs declined signifcantly over the past two years.

Q: Please finish this sentence by selecting one of the options below: The cyber insurance available in today's market...



Base: All answering; n=1307 (2019); n=1120 (2017)

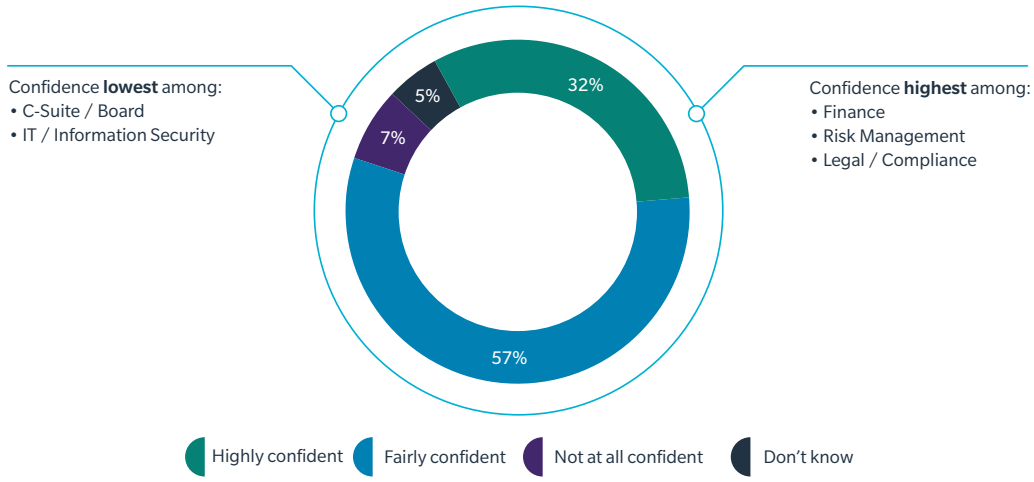
Esse nível moderado de certeza se reflete nas percepções sobre a capacidade de resposta de políticas cibernéticas organizacionais específicas. Um quinto das empresas pesquisadas demonstrou grande confiança de que seu seguro cobriria os custos associados a um incidente cibernético e mais da metade possuía bastante confiança (gráfico 28).

Only 7% said they were "not at all confident." Confidence in the adequacy of existing insurance programs is higher among those respondents who are likely most familiar with their organization's insurance programs, such as those in risk management, finance, and legal/compliance roles.

FIGURE 28

More than 4/5 of organizations are highly or fairly confident their insurance policies would cover the costs of a cyber event.

Q: How confident are you that the coverages within your organization's insurance program - cyber policies and/or other policies - will respond to costs incurred by your organization in the event of a cyber event?



Base: All with cyber insurance: n=526 (2019)

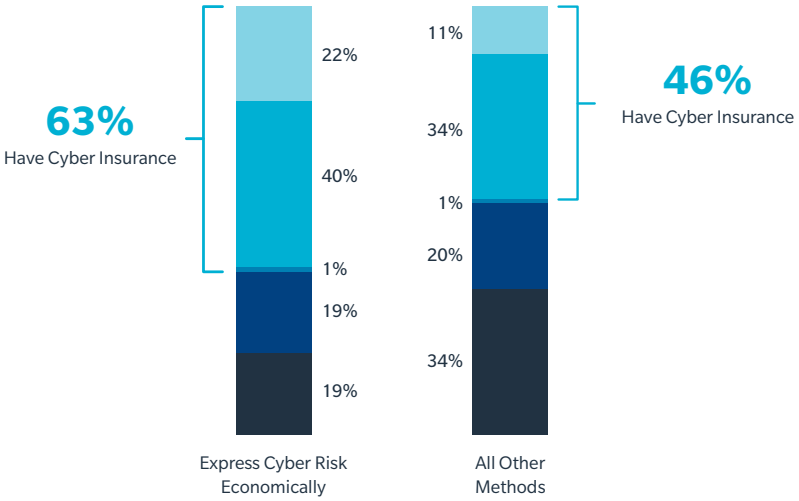
As empresas que usam métodos quantitativos de avaliação de riscos cibernéticos têm maior probabilidade de comprar seguro cyber do que aquelas que usam apenas métodos qualitativos ou nenhum método para avaliar exposições a ciberriscos (gráfico 29).

As empresas que quantificam economicamente suas exposições ao risco cibernético podem estar mais informadas e dispostas a capitalizar o valor do seguro. Consequentemente, quase três vezes a proporção de empresas que expressam o risco planeja expandir a cobertura, em comparação com as que não o fazem.

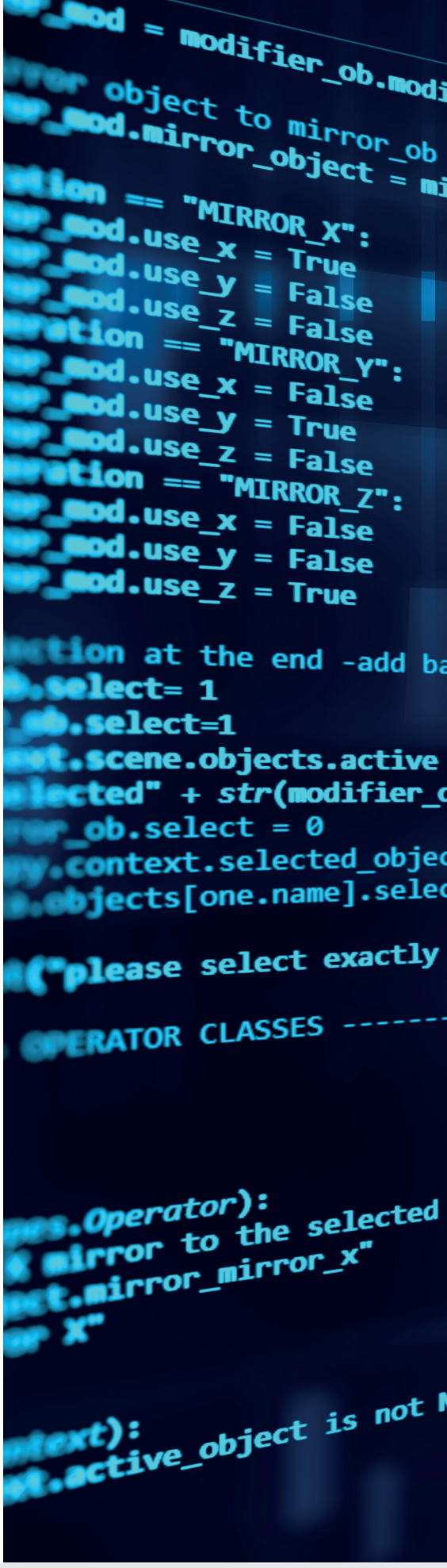
FIGURE 29

Organizations that use economic cyber risk assessment methods are more likely to purchase cyber insurance and increase current coverages.

Q: What is your organization's status with regard to cyber insurance?



Base: All answering, excluding dont know responses: n = 1120 (2019)



Conclusão

À medida que os riscos cibernéticos se tornam cada vez mais complexos e desafiadores, percebe-se que as empresas, lenta mas seguramente, estão começando a implementar as melhores práticas de gerenciamento ciberrisco. Quase todas as organizações pesquisadas reconhecem a magnitude do risco cibernético: muitas estão mudando aspectos de sua abordagem para enfrentar a ameaça e a maioria está fazendo um bom trabalho na segurança cibernética tradicional (proteção do perímetro).

As organizações mais experientes estão desenvolvendo resiliência cibernética por meio de estratégias mais abrangentes e equilibradas para gerenciar os riscos, em vez de se concentrarem apenas na prevenção. Essas abordagens mais complexas explicam a necessidade de desenvolver recursos para entender, avaliar e quantificar os riscos cibernéticos em primeiro lugar, além de adicionar as ferramentas e os recursos para responder e recuperar-se de incidentes cibernéticos quando eles ocorrem.

No entanto, a pesquisa deste ano mostra que permanece uma lacuna considerável entre a localização do risco cibernético na agenda corporativa e o nível geral de maturidade organizacional no gerenciamento de riscos. Muitas empresas em todo o mundo poderiam se beneficiar se aplicassem os princípios do gerenciamento estratégico de riscos à sua abordagem de ciberrisco, apoiadas por mais experiência, recursos e atenção dos membros da gerência à medida que desenvolvem resiliência cibernética.

Na era da Internet das Coisas (IoT), com cadeias de suprimentos digitalmente dependentes e tecnologia inovadora, as práticas e mentalidades de ontem não são suficientes e podem realmente inibir a inovação. Otimizar a segurança do "castelo" (a organização de mente fechada) para a comunidade em geral é mais difícil, mas inevitável. É fundamental uma mudança do foco exclusivo na segurança comercial para assumir a responsabilidade pela segurança em toda a cadeia de suprimentos.

Na prática, o estudo deste ano aponta para uma série de melhores práticas empregadas pelas empresas com maior resiliência cibernética e que todas as empresas devem considerar a adoção de:

- Criação de uma cultura de segurança cibernética organizacional forte, com padrões claros e compartilhados de governança, responsabilidade, recursos e ações.
- Quantificação do risco cibernético para tomar decisões de alocação de capital melhor embasadas, permitindo a medição do desempenho e enquadramento do risco nos mesmos termos econômicos que outros riscos comerciais.
- Avaliação das implicações do ciberrisco trazido pelas novas tecnologias como um processo contínuo e prospectivo ao longo de seu ciclo de vida.
- Gerenciamento do risco da cadeia de suprimentos como um problema coletivo, reconhecendo a necessidade de padrões de confiança e segurança compartilhados em toda a rede, incluindo o impacto cibernético da organização em seus parceiros.
- Procura e apoio a parcerias público-privadas em torno de problemas críticos de risco cibernético que possam fornecer proteções mais fortes e padrões básicos de boas práticas para todos.

Com o aumento da confiança organizacional na capacidade de gerenciar riscos cibernéticos, mais empresas reconhecem claramente a natureza crítica da ameaça e começam a buscar e adotar as melhores práticas. O gerenciamento eficaz de riscos cibernéticos requer uma abordagem abrangente que utilize avaliação, medição, mitigação, transferência e planejamento de riscos, e o programa ideal dependerá do perfil de risco exclusivo e da tolerância de cada empresa. Mesmo assim, essas recomendações abordam muitos dos aspectos comuns e mais urgentes do risco cibernético que as organizações enfrentam atualmente e devem ser vistas como sinais no caminho para a construção da verdadeira resiliência cibernética.

Metodologia

Este relatório é baseado em descobertas da 2019 Marsh Microsoft Global Cyber Risk Perception Survey, administrada entre fevereiro e março de 2019.

No geral, 1.500 líderes de empresas participaram da pesquisa globalmente, representando uma série de funções-chave, incluindo gerenciamento de riscos, tecnologia / segurança da informação, finanças, jurídico / compliance, diretores executivos e conselhos de administração.

Dados demográficos da pesquisa

Geografia

Onde os mais de 1.500 participantes da pesquisa estão	
América Latina e Caribe	35%
Europa	35%
EUA e Canadá	22%
Ásia e Pacífico	6%
Oriente Médio e África	2%

Receita

Receita anual total das organizações dos entrevistados, em US$	
Mais de $ 5 bilhões	10%
$1 bilhão - $ 5 bilhões	15%
$ 250 milhões - $ 1 bilhão	17%
$ 100 milhões - $ 250 milhões	14%
$ 25 milhões - $ 100 milhões	21%
Menos de $ 25 milhões	23%

Indústrias

Setores da indústria principais nos quais as empresas operam	
Manufatura/Automotora	16%
Varejo/Atacado	11%
Instituições Financeiras	9%
Energy/Power	8%
Health Care/Life Science	7%
Transportes/Ferrovias/Marine	6%
Comunicações, Mídia and Tecnologia	5%
Professional Services	5%
Real Estate	4%
Chemical	4%
Infraestrutura	4%
Educação	4%
Entidades Públicas/Nonprofit	4%
Mineração/Metais/Minerais	2%
Aviação/Aerospace	1%

SOBRE A MARSH

Marsh é a principal corretora de seguros e consultora de riscos do mundo. Com mais de 35.000 colaboradores operando em mais de 130 países, a Marsh atende clientes comerciais e individuais com soluções de risco orientadas a dados e serviços de consultoria. A Marsh é uma subsidiária integral da Marsh & McLennan Companies (NYSE: MMC), empresa líder global de serviços profissionais nas áreas de risco, estratégia e pessoas. Com receita anual superior a US$ 15 bilhões e 75.000 colaboradores em todo o mundo, a MMC ajuda os clientes a navegar em um ambiente cada vez mais dinâmico e complexo por meio de quatro empresas líderes de mercado: Marsh, Guy Carpenter, Mercer e Oliver Wyman. Siga a Marsh no Twitter @MarshGlobal, LinkedIn, Facebook e YouTube, ou assine *BRINK*.

SOBRE A MICROSOFT

A Microsoft (Nasdaq "MSFT" @microsoft) permite a transformação digital para a era de nuvem com vantagem inteligente. Sua missão é capacitar todas as pessoas e organizações do planeta para alcançar mais. A equipe de Diplomacia Digital da Microsoft, que fez parceria com Marsh neste estudo, combina conhecimento técnico e perspicácia em políticas públicas para desenvolver políticas que melhoram a segurança e a estabilidade do ciberespaço e possibilitam a transformação digital das sociedades em todo o mundo.

RECONHECIMENTOS

Marsh e Microsoft agradecem à B2B International por sua ajuda na criação, análise e relatório dos resultados desta pesquisa. A B2B International é a principal empresa de pesquisa de mercado business-to-business do mundo. É especializada no desenvolvimento de pesquisas de mercado personalizadas e programas de insight para algumas das principais marcas da indústria, financeiras e de tecnologia do mundo. A B2B International conta com 600 das 1.500 maiores empresas entre seus clientes. A B2B International faz parte da gyro, a agência criativa b2b dedicada à Dentsu Aegis Network.

Para mais informações sobre as soluções de gerenciamento de riscos cibernéticos da Marsh, acesse marsh.com.br ou entre em contato com seu representante Marsh Brasil:
Marta Schuh (líder de riscos cibernéticos)
+55 11 998 857 118
marta_schuh@jltbrasil.com

Para saber mais sobre as ofertas de segurança da Microsoft, visite www.microsoft.com/security.