SOPHOS
Cybersecurity delivered.

O Estado do Ransomware 2022

Resultados de uma pesquisa independente com 5.600 profissionais de TI em organizações de médio porte em 31 países.

Documento técnico Sophos. Abril, 2022

Introdução

Este estudo anual encomendado pela Sophos sobre as experiências reais com ransomwares enfrentadas por profissionais de TI que trabalham na linha de frente revelou um ambiente de ataque muito mais desafiador quando somado à carga operacional e financeira que o acompanha e em que o ransomware coloca suas vítimas. Ele também coloca em evidência a relação entre ransomwares e seguros de proteção digital, e o papel desempenhado pelo sistema de seguro no direcionamento das mudanças na defesa cibernética.

Sobre a pesquisa

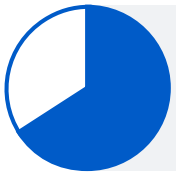
A Sophos contratou uma agência de pesquisa de opinião, a Vanson Bourne, para realizar um estudo independente com 5.600 profissionais de TI em organizações de médio porte (de 100 a 5.000 funcionários) em 31 países. A pesquisa ocorreu durante os meses de janeiro e fevereiro de 2022, e os entrevistados foram solicitados a responder às questões com base na experiência que tiveram no ano anterior.

Os ataques estão crescendo e sua complexidade e impacto estão aumentando

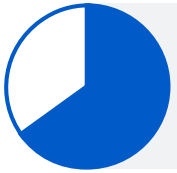
66% das organizações foram atingidas por ransomwares no ano passado, superior aos 37% em 2020. Trata-se de um aumento de 78% no decorrer de um ano, demonstrando que os adversários estão consideravelmente mais capazes de executar ataques que crescem em significância. Isso muito provavelmente também reflete o sucesso crescente do modelo Ransomware como Serviço, que amplia significativamente o alcance de um ransomware ao reduzir o nível de aptidão necessário para lançar um ataque. Observação: ser atingido por um ransomware é definido com um ou mais dispositivos impactados por um ataque, mas não necessariamente criptografados.

Os adversários também estão tendo mais sucesso na criptografia de dados durante os ataques. Em 2021, os invasores conseguiram criptografar dados em 65% dos ataques, um aumento em relação ao índice de 54% de criptografia registrado em 2020. Contudo, houve uma redução de 7% para 4% no percentual de vítimas que passaram por um ataque apenas de extorsão, em que os dados não foram criptografados, mas que a organização ficou sob a ameaça de ter seus dados expostos.

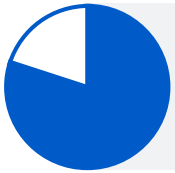
O aumento do sucesso dos ataques de ransomware dá-se em parte à expansão das fronteiras que norteiam o perímetro da ameaça: no último ano, 57% registraram um aumento no volume de ataques cibernéticos em geral, 59% perceberam o aumento na complexidade dos ataques e 53% disseram que o impacto dos ataques aumentou. 72% observaram um aumento em pelo menos uma dessas áreas.



66%
atingidos por ransomwares no ano passado



65%
ataques que resultaram em dados criptografados



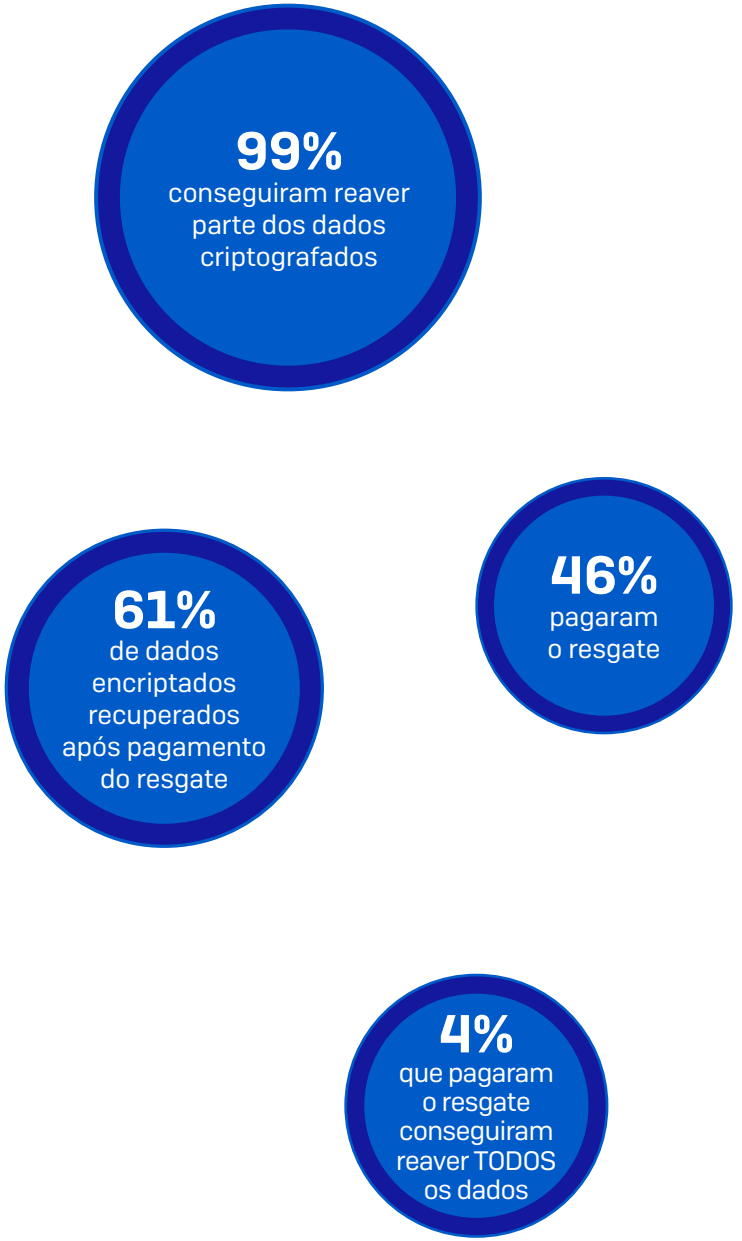
72%
sentiram um aumento em volume/ impacto de ataques cibernéticos

As organizações estão melhorando na restauração de dados após um ataque

Com a maior predominância de ransomwares, as organizações melhoraram na forma como tratam as repercussões após um ataque. Quase todas as organizações atingidas por ransomwares no ano passado (99%), hoje já conseguem recuperar parte dos dados criptografados, um ligeiro aumento em relação aos 96% do ano anterior.

Backups são o método mais utilizado para recuperar dados, usados por 73% das organizações cujos dados foram criptografados. Ao mesmo tempo, 46% disseram ter pago o resgate para restaurar os dados. Esses números refletem o fato de que muitas organizações usam diferentes abordagens de restauração para maximizar a rapidez e a eficiência com que conseguem voltar ao trabalho. No geral, quase metade (44%) dos entrevistados de organizações cujos dados foram criptografados usaram vários métodos para restaurar esses dados.

Ainda que pagando o resgate você quase sempre consiga reaver parte dos dados, a porcentagem de dados restaurados após o pagamento diminuiu. Em média, as organizações que realizaram o pagamento recuperaram apenas 61% dos dados, uma queda em comparação aos 65% em 2020. Comparativamente, em 2021, apenas 4% das que pagaram o resgate conseguiram reaver TODOS os seus dados, inferior aos 8% de 2020.



Os pagamentos de resgate aumentaram

Dos entrevistados cujas organizações pagaram o resgate, 965 compartilham de um mesmo montante, revelando que a média no pagamento de resgate aumentou consideravelmente no último ano.

No ano passado, a proporção de vítimas que pagaram resgates de US$ 1 milhão ou mais quase triplicou, de 4% em 2020 para 11% em 2021. Paralelamente, o percentual que pagou menos de US$ 10.000 caiu de um em cada três (34%), em 2020, para um em cada cinco (21%), em 2021.

No geral, o pagamento médio de resgate chegou a US$ 812.360, um aumento de 4,8 da média de 2020 de US$ 170 mil (baseado em 282 entrevistados). Ainda que essa somatória seja influenciada por 15 pagamentos acima da casa dos oito dígitos, fica claro que os resgastes estão mostrando uma tendência de ultrapassar o teto. Existe uma considerável variação na indústria, com adversários que sacam somas maiores daqueles que consideram mais aptos a pagar:

- os MAIS ALTOS pagamentos médios de resgate foram US$ 2,04 milhões em manufatura e produção (n=38) e US$ 2,03 milhões em energia, petróleo/gás e serviços de utilidade (n=91)
- os MAIS BAIXOS pagamentos médios de resgate foram US$ 197 mil em saúde (n=83) e US$ 214 mil em governo local/estadual (n=20)

Na Itália, onde o pagamento de extorsão é ilegal – o que significa que as organizações não podem, por lei, pagar o resgate, 43% daquelas que tiveram seus dados criptografados admitiram que suas organizações pagaram (n=76). A pesquisa mostra que as barreiras do legislativo apenas não são suficientemente eficazes para interromper os pagamentos de resgate.

3x
aumento na proporção de quem pagou resgastes de US$ 1 milhão ou mais

21%
pagaram resgates abaixo de US$ 10.000

$812360
pagamento médio de resgate (excluindo exceções)

MANUFATURA, SERVIÇOS DE UTILIDADE
pagamento médio de resgate mais alto (US$ 2 milhões)

SAÚDE
pagamento médio de resgate mais baixo (US$ 197 mil)

Os ransomwares têm um grande impacto comercial e operacional

Os valores dos resgates são apenas parte da história, e o impacto do ransomware é muito mais amplo do que apenas entre dispositivos e bancos de dados criptografados. 90% daqueles que foram atingidos por ransomware no último ano disseram que o ataque mais significativo impactou sua capacidade de operação. Além disso, entre as organizações do setor privado, 86% disseram que perderam negócios/receita.

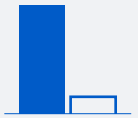
No geral, o custo médio para uma organização retificar o impacto do ataque de ransomware mais recente em 2021 foi US$ 1,4 milhão. Essa queda bem-vinda de US$ 1,85 milhão em 2020 reflete que, provavelmente, como ransomwares se tornaram mais prevalentes, o dano reputacional de um ataque diminuiu. Paralelamente, as seguradoras estão mais aptas a orientar as vítimas com rapidez e eficácia no processo de resposta a incidentes, reduzindo o custo do reparo.

Vale notar que, em muitos dos casos em que o resgate foi pago, a seguradora pagou a conta, não a vítima. Falaremos sobre isso mais adiante e em mais detalhes.

Em média, as organizações que sofreram ataques no último ano levaram um mês para se recuperar do ataque mais significativo – um período muito longo para a maioria das empresas. A maior demora na recuperação foi observada no ensino superior e governo central/federal, em que cerca de duas em cada cinco instituições levaram mais de um mês para se restabelecer. Em contrapartida, os setores mais rápidos foram os de manufatura e produção (10% levaram mais de um mês) e serviços financeiros (12% levaram mais de um mês), provavelmente resultado dos altos índices de planejamento e preparo em recuperação.

Além disso, algumas organizações continuam a depositar as esperanças em defesas ineficientes. Dos entrevistados cujas organizações não foram atingidas por ransomware no último ano, e que não esperam ser atingidos no futuro, 72% baseiam suas opiniões em abordagens que não impedem que as organizações sejam atacadas: 57% citaram backups e 37% citaram seguro de proteção digital como motivos pelos quais não anteveem um ataque, com alguns selecionando as duas respostas. Enquanto esses elementos ajudam na recuperação de um ataque, eles não impedem que ele aconteça.

90%
o ataque de ransomware impactou sua capacidade de operação



86%
o ataque de ransomware causou perda de negócios/receita

US$ 1,4 milhão
custo médio para reparar um ataque

UM MÊS
tempo médio para se recuperar de um ataque

72%
depositam as esperanças em abordagens que não impedem o ataque

As organizações não são capazes de usar seus orçamentos e recursos de maneira eficiente para deter os ransomwares

A pesquisa revelou que simplesmente alocar pessoas e dinheiro para resolver o problema não ajuda a solucioná-lo. O que você precisa é investir na tecnologia certa e adquirir as habilidades e o know-how para utilizá-la com eficiência. Sem isso, o seu retorno de investimento é baixo.

64% dos que foram atingidos por ransomware no último ano disseram ter um orçamento para segurança cibernética maior do que precisam, enquanto outros 24% disseram ter o valor certo de orçamento. De modo semelhante, 65% das vítimas de ransomware disseram ter mais pessoal para segurança cibernética do que precisam, e 23% disseram ter o número certo de pessoal. Essas descobertas sugerem que muitas organizações estão tendo dificuldades para implantar seus recursos com eficiência frente ao aumento desenfreado em volume e complexidade dos ataques.

Os resultados também indicam que as organizações talvez não tenham se dado conta de que não têm as aptidões certas para parar as técnicas de ataque mais recentes: 58% dos que foram atingidos por ransomware descrevem suas organizações como as mais atentas nas revisões de log para identificar indícios ou atividades suspeitas, e 56% disseram ser as mais bem equipadas com metodologias/ferramentas contra os ataques mais recentes.

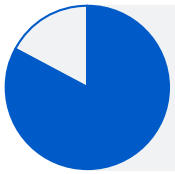
Por outro lado, entre as organizações que não foram atingidas por um ransomware no ano anterior, e que não previram um futuro ataque, o motivo principal por trás de tamanha confiança foi terem uma equipe de segurança de TI treinada ou um centro de operações de segurança (SOC) capaz de bloquear os ataques.

O ransomware direciona a cobertura do seguro de proteção digital

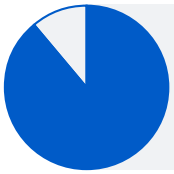
A cada cinco organizações de médio porte, mais de quatro têm seguro de proteção digital contra ransomware. Contudo, enquanto 83% dos entrevistados dizem que suas organizações têm seguro de proteção digital que dá cobertura na eventualidade de serem atingidos por ransomware, 34% dizem que há exclusões/exceções em suas apólices. Energia, petróleo/gás e serviços de utilidade são os mais propensos a ter cobertura (89%), seguidos de perto pelo varejo (88%). A adoção do seguro de proteção digital aumenta proporcionalmente ao tamanho da organização, com 88% das organizações com entre 3.001 e 5.000 funcionários cobertas em comparação a 73% das com entre 100 e 250 funcionários.

As organizações atingidas por ransomware no ano passado estão muito mais propensas a ter um seguro de proteção digital do que aquelas que não foram vítimas de um ataque. Entre as que foram atingidas, 89% tinham seguro de proteção digital em comparação aos 70% das que não foram atingidas. A causa e o efeito não estão muito claros aqui. É possível que a experiência com um incidente de ransomware tenha levado várias organizações a fazer um seguro de proteção digital para ajudar a mitigar o impacto de ataques futuros. Alternativamente, os adversários podem estar direcionando seus ataques a organizações que não têm cobertura de seguro para aumentar as chances de receber o pagamento do resgate. Outra opção seria a de que algumas organizações fizeram um seguro de proteção digital para amortecer os pontos fracos em suas defesas. A realidade mais provável é que seja uma combinação das três possibilidades.

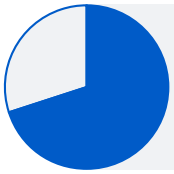
A cobertura do seguro de proteção digital cai para 61% entre os que não foram atingidos e que não esperam passar por um ataque. Considerando-se que muitos nesse grupo estão depositando suas esperanças em abordagens que não bloqueiam o ransomware, a falta de cobertura os deixa completamente suscetíveis aos custos de um possível incidente.



83%
têm seguro de proteção digital contra ransomware



89%
atingidos por ransomware têm seguro de proteção digital



70%
não atingidos por ransomware têm seguro de proteção digital

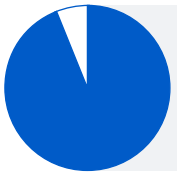
O seguro de proteção digital está levando a melhorias nas defesas cibernéticas

94% daqueles com seguro de proteção digital disseram que o processo para garantir a cobertura mudou bastante no decorrer do último ano.

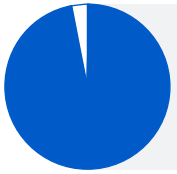
- 54% dizem que o nível de segurança cibernética de que precisam para se qualificarem ficou muito alto
- 47% dizem que as apólices agora estão mais complexas
- 40% dizem que há menos empresas que oferecem seguro de proteção digital
- 37% dizem que o processo demora mais
- 34% dizem que é mais caro

Dado que a maior disparada nos preços de seguro de proteção digital tenha começado no segundo ou terceiro trimestre de 2021, é bastante provável que muitos dos entrevistados não tenham passado pelo impacto dessa mudança na época da pesquisa.

Conforme o mercado de seguro de proteção digital fica mais rígido e se torna mais desafiador garantir a cobertura, 97% das organizações que têm seguro de proteção digital fizeram alterações em suas defesas cibernéticas para melhorar suas posições no mercado de seguros de proteção digital. 64% implementaram novas tecnologias/serviços, 56% aumentaram o índice de treinamento dos funcionários/atividades educativas, e 52% mudaram seus processos/comportamentos.



94%
acharam difícil garantir
a cobertura do seguro
de proteção digital no ano passado



97%
que têm seguro de proteção digital fizeram alterações
em suas defesas para melhorar suas posições
no mercado de seguros de proteção digital

O seguro de proteção digital paga a maioria de todos os sinistros por ransomware

É tranquilizador para aqueles que têm a cobertura do seguro de proteção digital saber que 98% dos atingidos por ransomware, e que tinham um seguro de proteção digital que cobria ransomwares, disseram que a apólice pagou no ataque mais significativo – uma subida em relação aos 95% em 2019. Em alguns países, esse valor chegou aos 100% no índice de pagamento: Suíça (n=52), México (n=131), Suécia (n=68), Bélgica (n=66), Polônia (n=75), Turquia (n=51), Emirados Árabes (n=49), Índia (n=218) e Singapura (n=91).

Analisando o que o seguro de proteção digital pagou, a pesquisa revela um aumento no pagamento dos custos de limpeza e uma queda nos pagamentos de resgate pelas seguradoras. 77% dos entrevistados disseram que suas seguradoras pagaram pelos custos de limpeza, ou seja, os custos incorridos para restabelecer as atividades da organização – uma subida frente aos 67% em 2019. Comparativamente, 40% disseram que a seguradora pagou o resgate, valor abaixo dos 44% em 2019.

Contudo, o índice de pagamentos de resgate realizados varia consideravelmente de um setor para outro. Os mais altos índices, de acordo com a pesquisa, foram em ensino fundamental (educação básica/média) (53%), governo local/estadual (49%) e saúde (47%); e os mais baixos em manufatura e produção (30%) e serviços financeiros (32%). É interessante observar que os setores com o mais baixo índice de pagamento também são aqueles capazes de se recuperar mais rapidamente de um incidente, enfatizando a importância de ter um plano de recuperação de desastres e estar preparado.

Vale lembrar que, embora o seguro de proteção digital o ajude a voltar ao seu estado original, ele não cobre "melhorias", por exemplo, quando você precisa investir em melhores tecnologias e serviços para tratar de um ponto vulnerável que levou ao ataque.

98%
índice de pagamento de sinistros por ransomware

△ Pagamento de custo de limpeza △

67% 2019

77% 2021

▽ Pagamento de resgate ▽

44% 2019

40% 2021

Conclusão

O desafio que as organizações enfrentam com os ransomwares continua a crescer. A proporção de organizações que são diretamente impactadas por ransomwares quase duplicou em 12 meses: de apenas um pouco mais de um terço em 2020 para dois terços em 2021.

Em face a essa quase normalização, as organizações ficaram melhores no tratamento que dispensam às consequências de um ataque: praticamente todas agora recebem de volta parte dos dados criptografados, e quase três quartos são capazes de utilizar backups para restaurar dados.

Ao mesmo tempo, a proporção de dados criptografados restaurados após o pagamento do resgate caiu, em média, para 61%. Apesar disso, a porcentagem de vítimas que pagaram resgates de US$ 1 milhão ou mais quase triplicou.

A pesquisa revelou que simplesmente alocar pessoas e dinheiro para resolver o problema não ajuda a solucioná-lo. O que você precisa é investir na tecnologia certa e adquirir as habilidades e o know-how para utilizá-la com eficiência. As organizações deveriam buscar parceiros especializados que possam ajudar a melhorar o retorno de seus investimentos em segurança cibernética e elevar suas defesas.

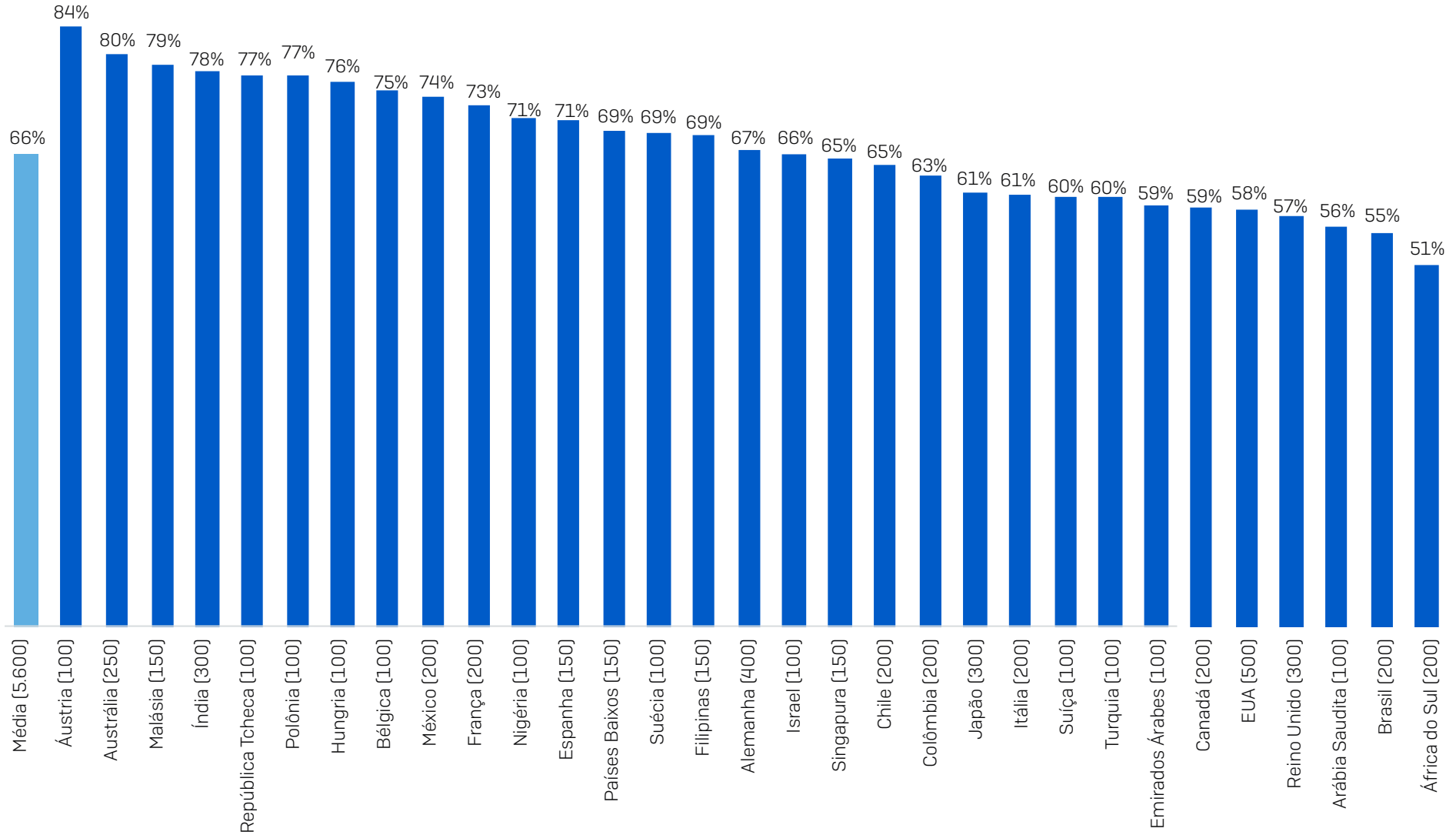
A maioria das organizações opta por reduzir o risco financeiro associado fazendo um seguro de proteção digital. Para elas, é tranquilizador saber que a seguradora pagará parte dos custos em quase todos os sinistros. Contudo, está ficando mais difícil para as organizações garantir a cobertura, o que as leva a fazer alterações em suas defesas cibernéticas para melhorar suas posições no mercado de seguros de proteção digital.

Não importa se você quer ou não garantir a cobertura do seu seguro, otimizar segurança cibernética é imperativo para todas as organizações. Nossas cinco dicas mais importantes:

- Assegure defesas de alta qualidade em todos os pontos do seu ambiente. Revise seus controles de segurança e confirme que continuam a atender às suas necessidades.
- Busque ameaças de maneira proativa de modo a ser capaz de deter os adversários antes que eles lancem seus ataques – se você não tem tempo nem pessoal interno, terceirize a tarefa para um especialista em MDR.
- Reforce o seu ambiente procurando e eliminando as lacunas na segurança: dispositivos sem patches, máquinas sem proteção, portas RDP abertas etc. A Detecção e Resposta Estendidas (XDR) é ideal para essa finalidade.
- Prepare-se para o pior. Saiba o que fazer na eventualidade de um incidente cibernético e quem você precisa contatar.
- Faça backups e pratique a restauração. Seu objetivo é voltar às atividades rapidamente, com um tempo mínimo de interrupção.

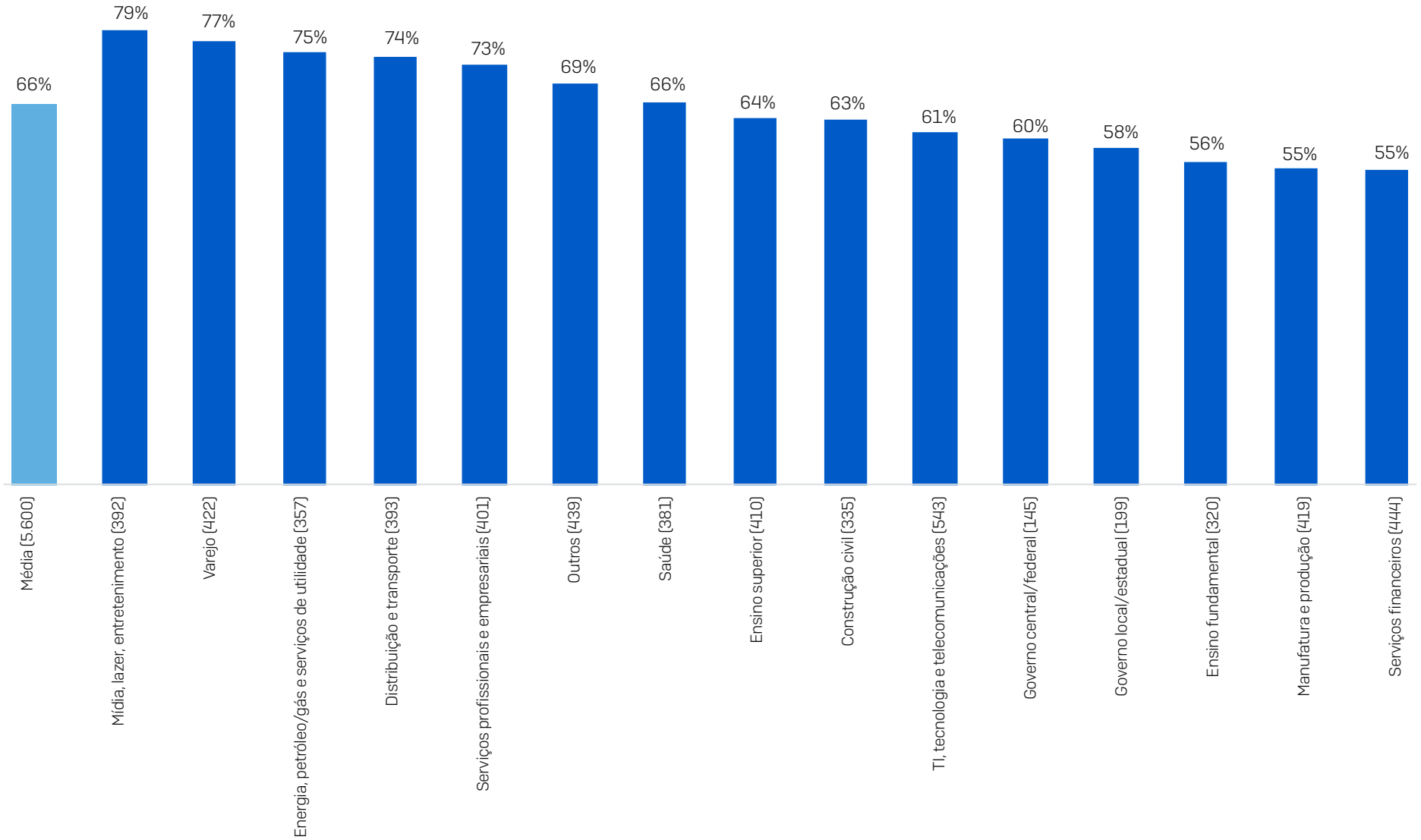
Para obter informações detalhadas sobre grupos individuais de ransomwares, consulte o centro de inteligência da Sophos sobre ameaças de ransomware.

Porcentagem de organizações atingidas por ransomware no ano passado



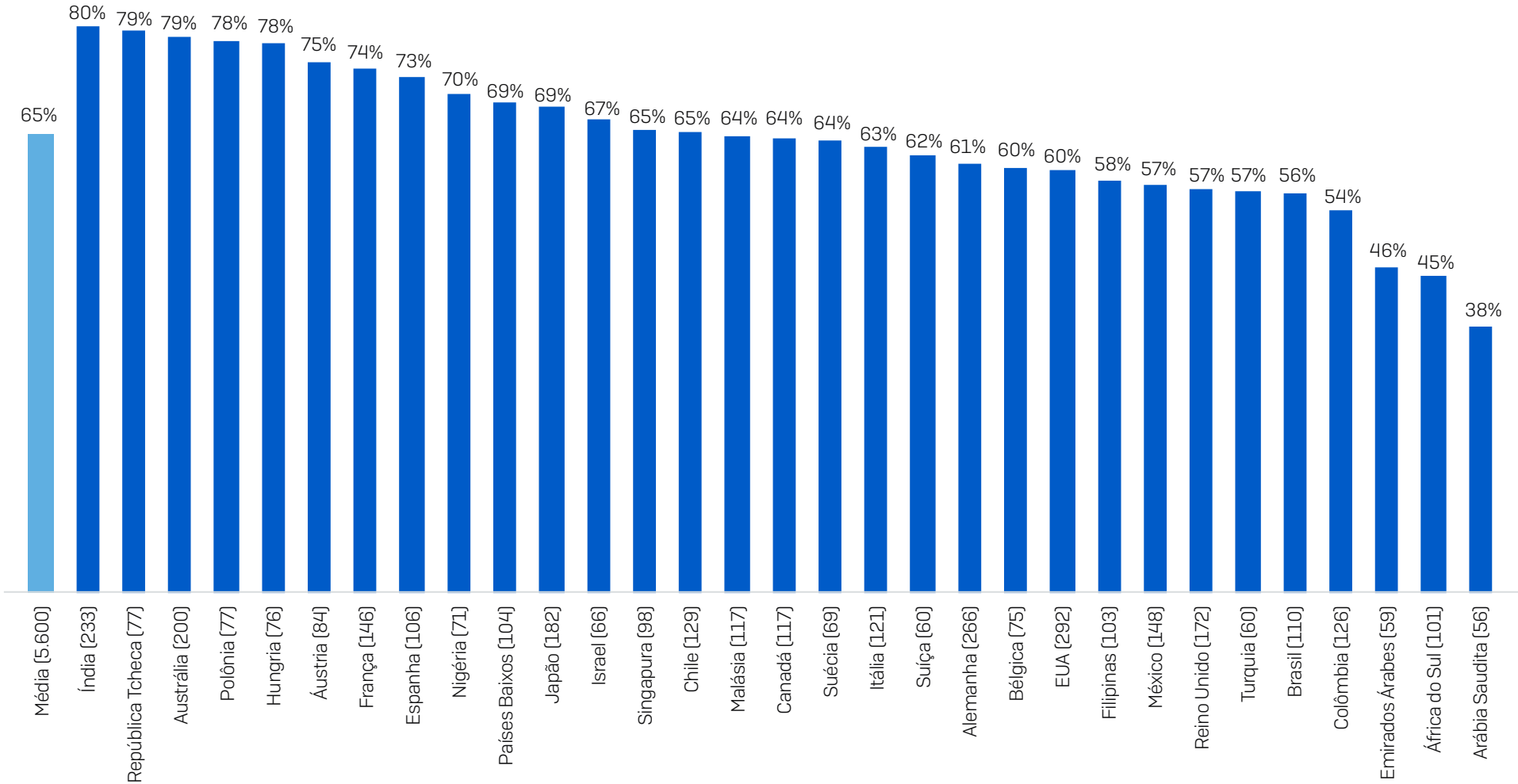
Sua organização foi atingida por ransomware neste último ano? (n=5.600): Sim

Porcentagem de organizações atingidas por ransomware no ano passado



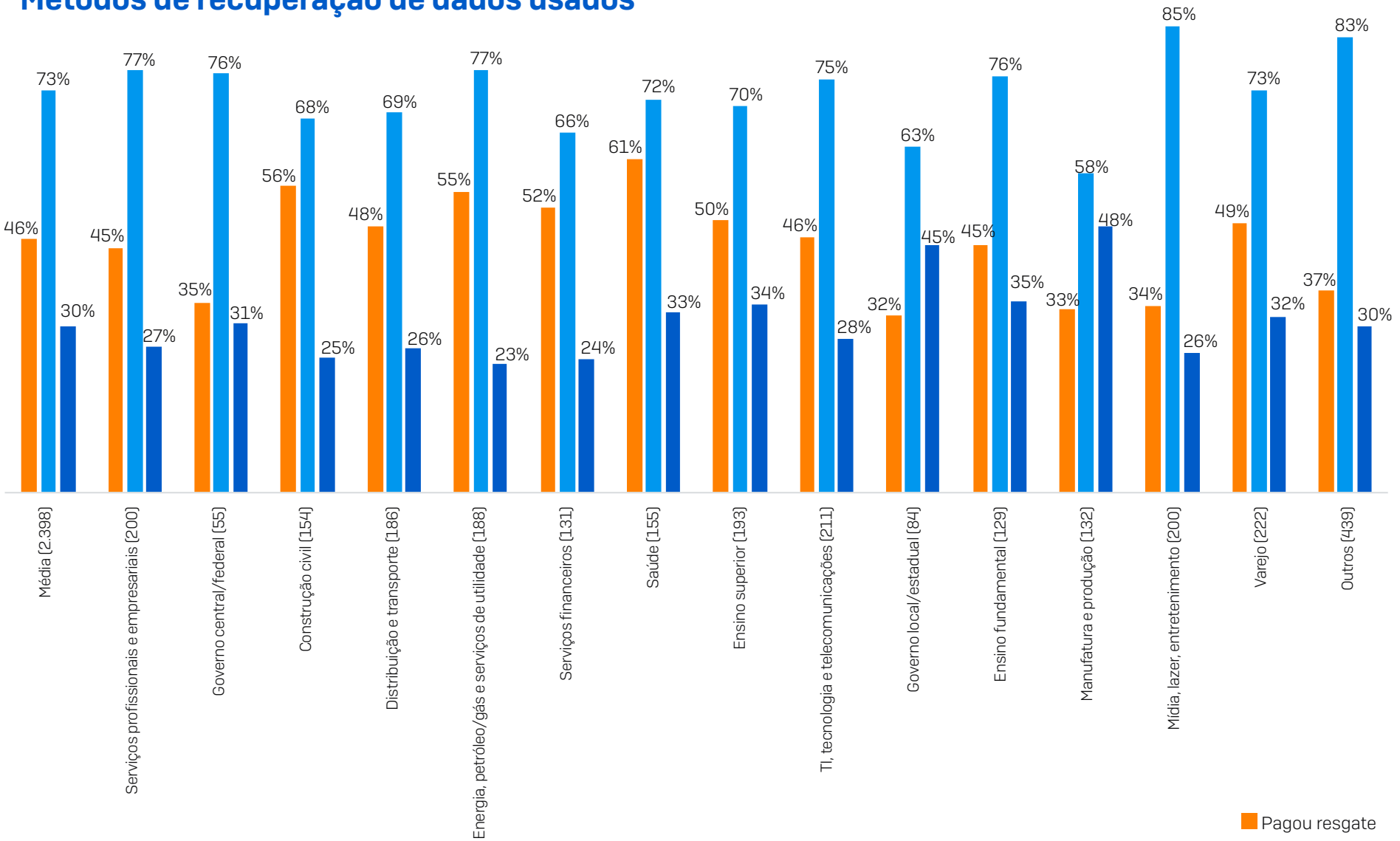
Sua organização foi atingida por ransomware neste último ano? (n=5.600): Sim

Índice de criptografia em ataques de ransomware



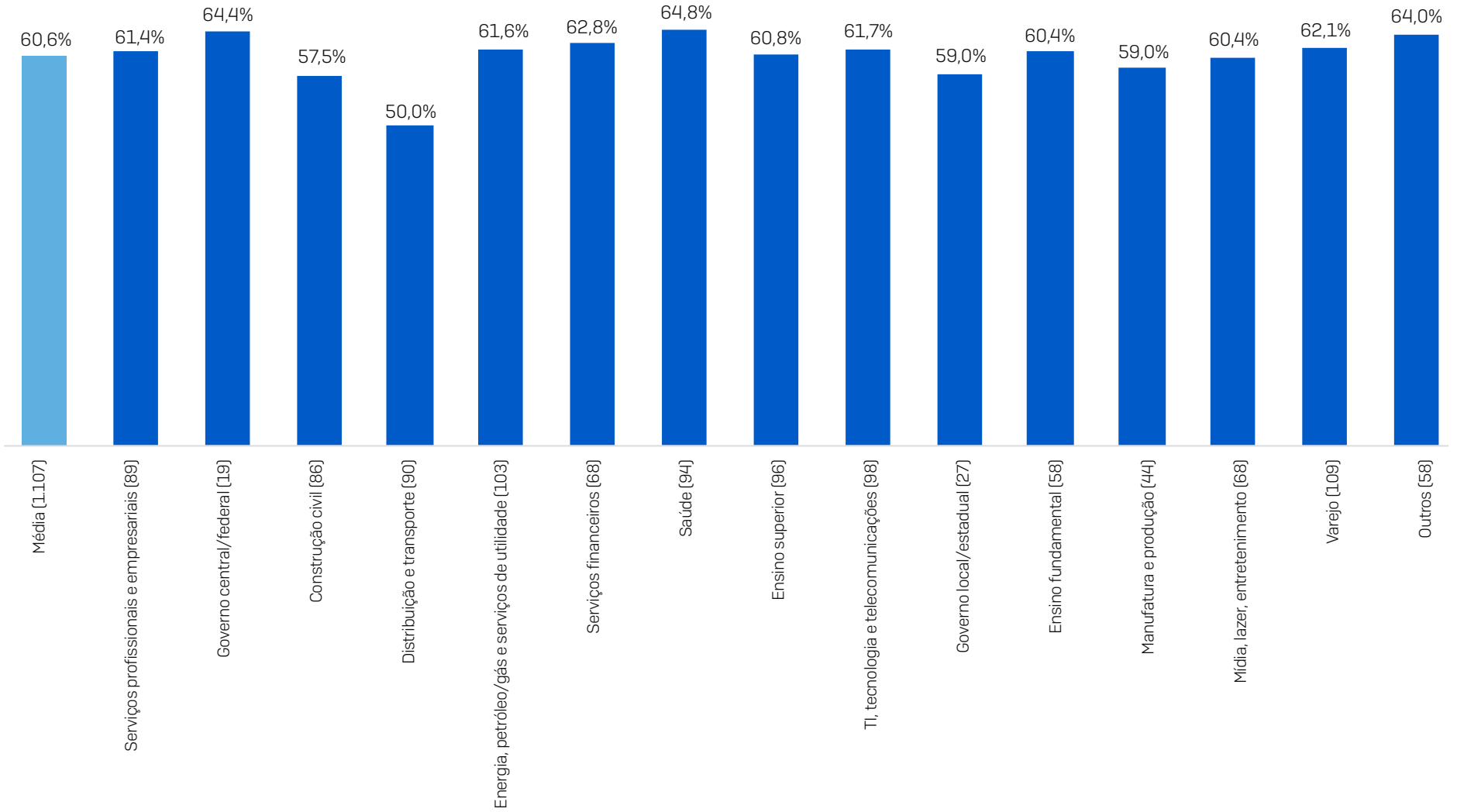
Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização nos ataques de ransomware mais significativos? (n=3.702 organizações atingidas por ransomwares no ano passado): Sim

Métodos de recuperação de dados usados



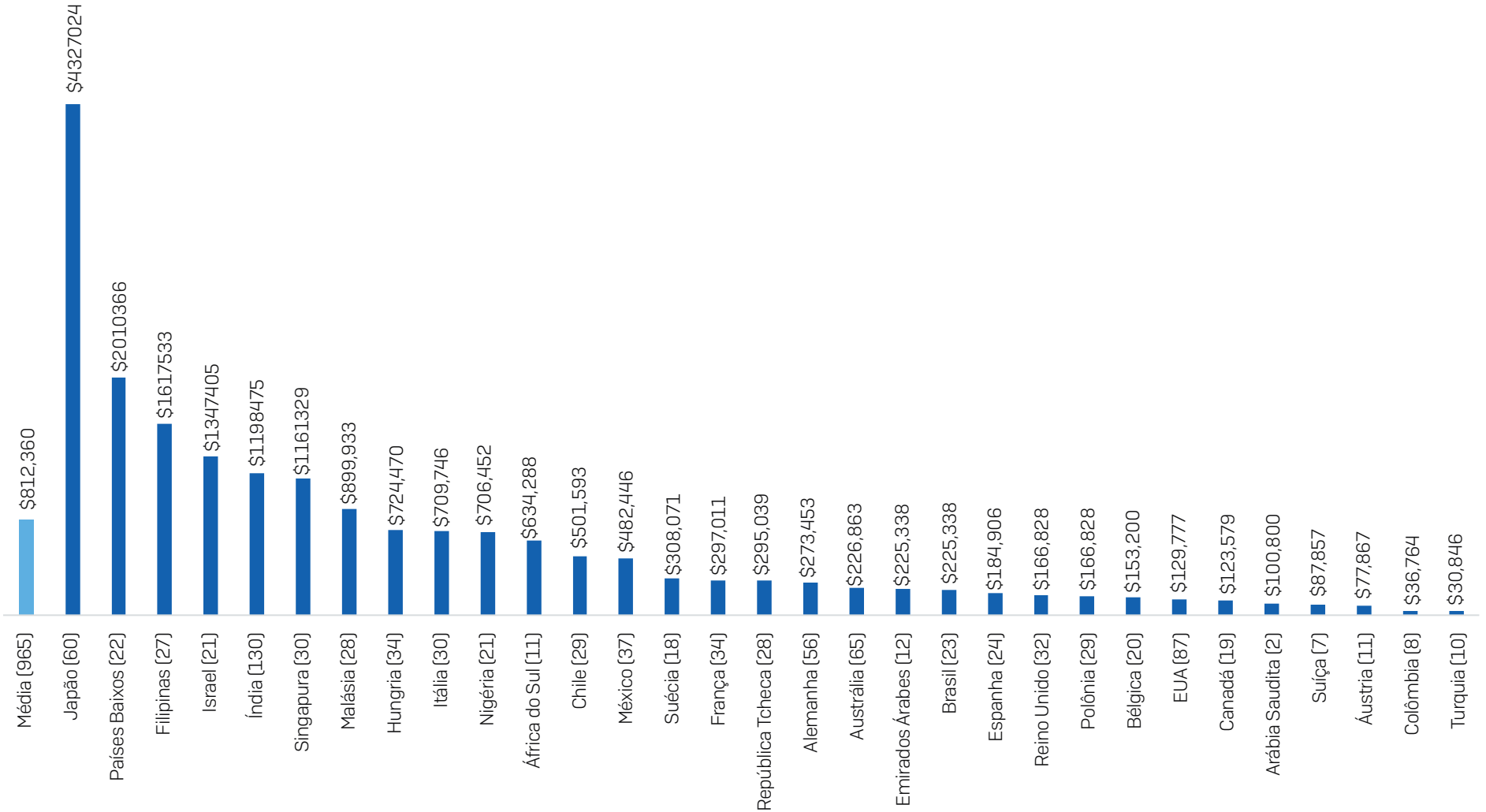
Sua organização conseguiu reaver dados capturados no ataque de ransomware mais significativo? (n=2.398 organizações tiveram dados criptografados): Sim, pagamos o resgate e recuperamos os dados; Sim, usamos backups para restaurar os dados; Sim, usamos outros meios para reaver nossos dados.

Porcentagem de dados recuperados após pagar o resgate



Quantos dos dados da sua organização vocês conseguiram reaver no ataque de ransomware mais significativo?
(n=1.107 organizações que pagaram o resgate e conseguiram reaver os dados)

Pagamentos médios de resgate por país



Qual foi o resgate que a sua organização pagou no ataque de ransomware mais significativo? US$. Número de base no gráfico. Excluindo respostas "Não sei" e exceções.

N. B. Para países com número de base baixo, os resultados devem ser considerados indicativos.

Custo médio da organização para retificar o ataque (milhões de US$)

País	2021	2020	Mudança ano a ano
Média (3.702)	$1,40	$1,85	-24%
Austrália (200)	$1,01	$1,84	-45%
Áustria (84)	$0,81	$7,75	-90%
Bélgica (75)	$3,71	$4,75	-22%
Brasil (110)	$0,69	$0,82	-16%
Canadá (117)	$0,65	$1,92	-66%
Chile (129)	$1,58	$0,73	116%
Colômbia (126)	$0,50	$1,26	-60%
República Tcheca (77)	$2,58	$0,37	589%
França (146)	$2,03	$1,11	83%
Alemanha (266)	$1,73	$1,17	48%
Hungria (76)	$1,51	n/d	n/d
Índia (233)	$2,81	$3,38	-17%
Israel (66)	$1,41	$0,57	148%
Itália (121)	$1,65	$0,68	141%
Japão (182)	$0,96	$1,61	-40%
Malásia (118)	$1,22	$0,77	58%

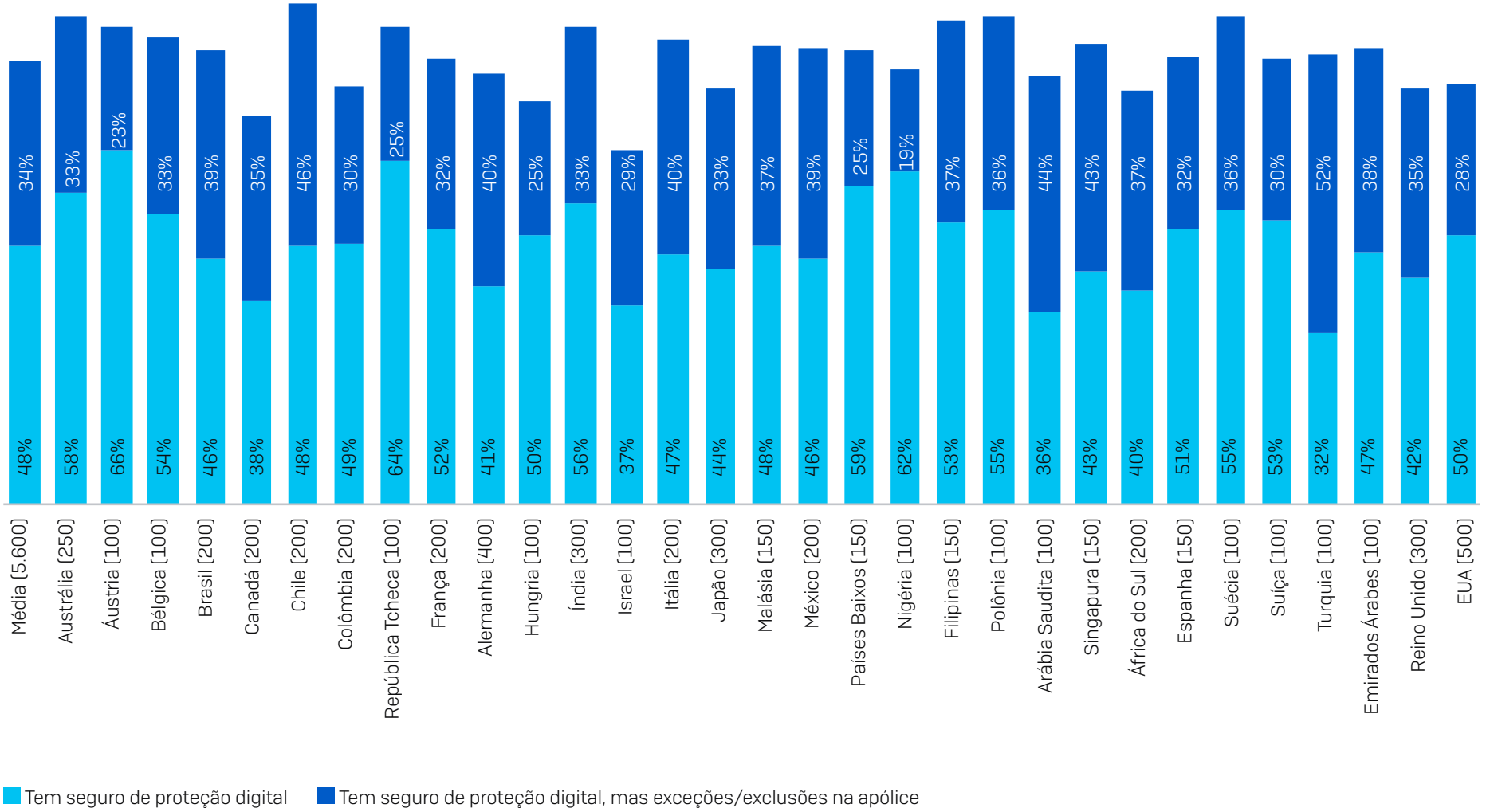
País	2021	2020	Mudança ano a ano
México (148)	$0,88	$2,03	-57%
Países Baixos (104)	$0,98	$2,71	-64%
Nigéria (71)	$3,43	$0,46	644%
Filipinas (103)	$1,34	$0,82	63%
Polônia (77)	$1,78	n/d	n/d
Arábia Saudita (56)	$0,65	$0,21	212%
Singapura (98)	$1,91	$3,46	-45%
África do Sul (101)	$0,71	n/d	n/d
Espanha (106)	$0,75	$0,60	25%
Suécia (69)	$0,75	$1,40	-46%
Suíça (60)	$1,64	$1,43	15%
Turquia (60)	$0,37	$0,58	-36%
Emirados Árabes (59)	$1,26	$0,52	144%
Reino Unido (172)	$1,08	$1,96	-45%
EUA (292)	$1,08	$2,09	-49%

N.B. Números de base se aplicam apenas a dados de 2021.

N.B. Valores em milhões de US$

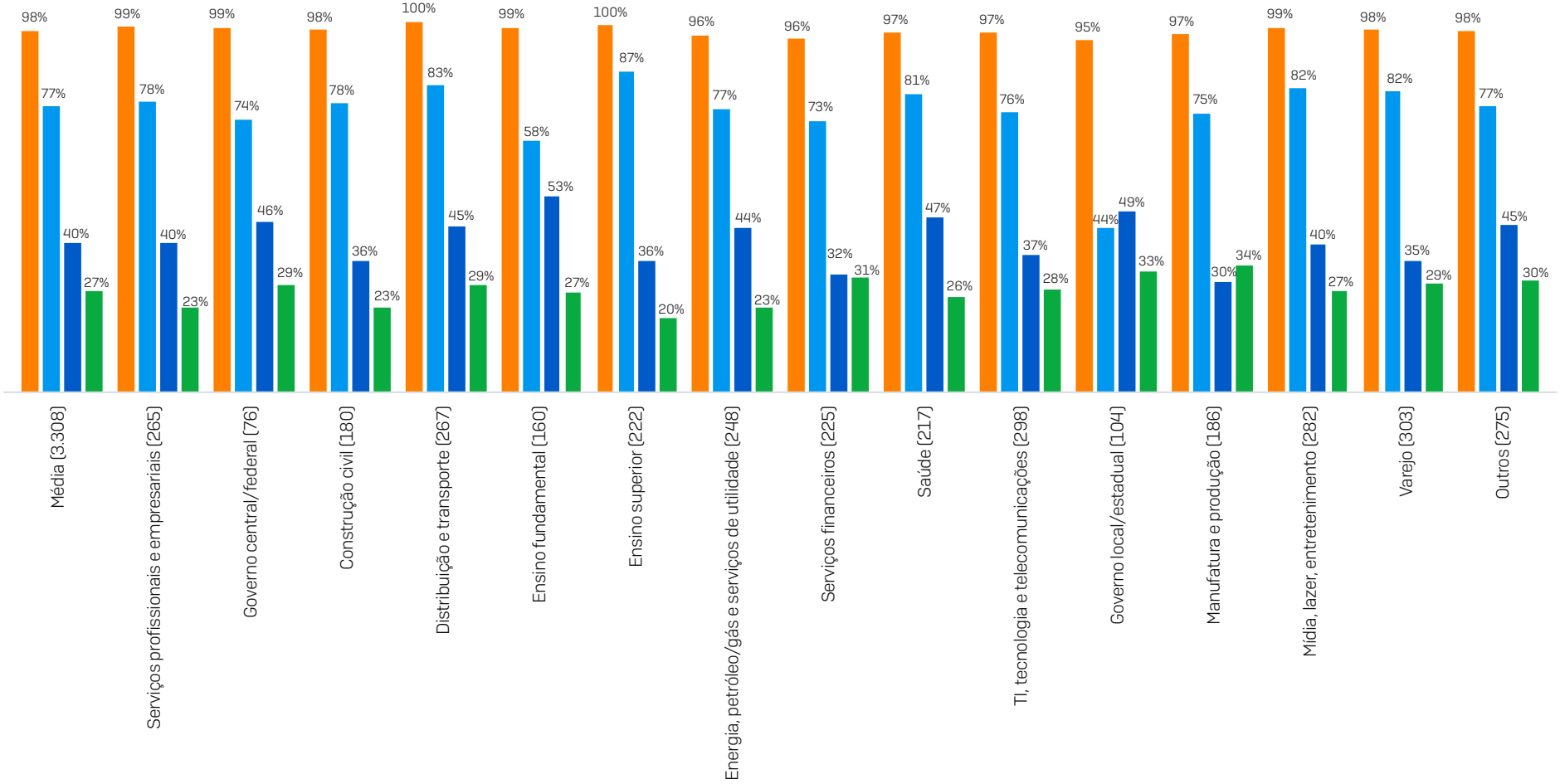
Qual foi o custo aproximado para a sua organização retificar o impacto do mais recente ataque de ransomware (considerando-se período de inatividade, tempo de pessoal, custo dos equipamentos, custo da rede, perda de oportunidades, resgate pago, etc.)? (n=3.702 organizações que foram atingidas por ransomware no ano anterior)

Porcentagem de organizações com cobertura de seguro de proteção digital



Sua organização tem seguro de proteção digital com cobertura contra ataques de ransomware? (n=5.600). Sim; Sim, mas há exceções/exclusões em nossa apólice

Índice de pagamento de seguro de proteção digital



O seguro de proteção digital pagou de modo a cobrir os custos associados ao ataque de ransomware mais significativo que a sua organização enfrentou? (n=3.308 organizações que foram atingidas por ransomware no ano anterior e que tinham seguro de proteção digital que cobria ransomware.) Sim, pagou pelos custos de limpeza (por exemplo, os custos para recolocar a organização em atividade); Sim, pagou o resgate; Sim, pagou outros custos (por exemplo, custos com inatividade, perda de oportunidades)

- Seguro pagou
- Seguro pagou custos de limpeza
- Seguro pagou o resgate
- Seguro pagou outros custos

Saiba mais sobre ransomware e como a Sophos pode ajudar a defender a sua organização.

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2022-04-04 (WP-NP)

SOPHOS