PREPARADAS OU EXPOSTAS AO RISCO:

COHESITY

A lacuna da resiliência cibernética na saúde

Os ataques cibernéticos não são mais eventos isolados, mas uma característica constante do nosso mundo digital. Cada dia traz um novo lembrete de que as empresas de serviços de saúde de todo o mundo são cada vez mais visadas. Nenhuma empresa está imune, e o aumento da frequência e da sofisticação das ameaças levou a um pico em ataques cibernéticos materiais que causam danos mensuráveis em termos financeiros, operacionais e de reputação.

UMA PESQUISA GLOBAL COM QUASE 400 TOMADORES DE DECISÕES DE TI E OPERAÇÕES DE SEGURANÇA NA ÁREA DE SAÚDE REVELA A REALIDADE.

85%
das empresas de saúde sofreram um ataque cibernético material

66%
foram atacadas nos últimos 12 meses

1 EM CADA 3
foi atacada várias vezes

OS PREJUÍZOS SÃO MUITOS E OS **CUSTOS SE ACUMULAM RAPIDAMENTE**

92% perderam receita

59% perderam pacientes ou clientes

80% das organizações de saúde publicamente listadas relataram uma revisão das orientações financeiras

97% enfrentaram consequências regulatórias ou legais

94% pagaram resgate nos últimos 12 meses

MESMO DIANTE DAS PROVAS, MUITAS EMPRESAS DE SAÚDE SUPERESTIMAM SUA RESILIÊNCIA.

49%
delas têm confiança total em sua estratégia de resiliência cibernética

A MAIORIA AINDA PRIORIZA A PREVENÇÃO E A DETECÇÃO, EM VEZ DAS FUNÇÕES DE RESPOSTA E RECUPERAÇÃO, IGUALMENTE CRUCIAIS.

Ordem baseada na estrutura de segurança cibernética NIST. O tamanho da caixa mostra a proporção de investimentos em resiliência cibernética, em ordem decrescente.

#2	#1	#3	#4	#5
Identificar	Proteger	Detectar	Responder	Recuperar

A CONFIANÇA E OS PADRÕES DE GASTOS **CONTAM SÓ UMA PARTE DA HISTÓRIA**

A verdadeira resiliência depende das práticas e recursos de apoio. Quando avaliadas conforme critérios do mundo real, apenas 2% das empresas de saúde demonstram maturidade em cinco áreas essenciais: **proteção de dados, recuperação de dados, detecção e investigação de ameaças, resiliência de aplicativos e otimização do risco de dados.**

O reconhecimento da necessidade de aprimorar a resiliência está impulsionando a próxima evolução, com o poder da automação e da IA. Conforme as ameaças se tornam mais rápidas e complexas, a automação é essencial para acelerar a detecção, simplificar a resposta e fortalecer a recuperação.

61%

dizem que a melhoria da automação na detecção, resposta e recuperação é uma das lições mais importantes aprendidas após o ataque cibernético

37%

acreditam que a IA terá um papel central na detecção e resposta a ameaças, incluindo a tomada de algumas decisões autônomas

99%

planejam usar a IA para dar suporte às operações de segurança dos dados até 2026

VOCÊ ESTÁ PREPARADO PARA O RISCO?

- **Faça download do relatório de resiliência cibernética do setor de saúde para ver detalhes sobre as descobertas.**
- **Agende um workshop de resiliência contra ransomware.**
- Obtenha nosso e-book "**5 passos para a resiliência cibernética**" e comece a avançar sua maturidade hoje.

A Vanson Bourne entrevistou 3.200 líderes de TI e Segurança nas regiões da América do Norte, Ásia-Pacífico, Europa e América Latina, representando empresas com 1.000 ou mais funcionários em 2025. Os entrevistados incluíam 371 participantes de empresas do setor de saúde.

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
6200030-001-BR 4-2026