

## **HEALTHCARE'S INFLATION PROBLEM:**

# RISING BREACH COSTS



<u>Report</u> that lists healthcare as the industry with the highest breach costs of all sectors for the 12th year in a row.

\$10.1M

average cost of a breach for healthcare organizations (up from \$9.23 in 2021)



average cost of ransomware attack, not including the ransom itself

average cost savings if an Incident Response Plan and tabletop testing are in place

19%

of organizations studied have had more than one data breach

45% of breaches were cloud-based

sector for breach costs

277 days

of breaches were the result of ransomware attacks

19%

12 consecutive years number of years that healthcare as been ranked the highest

compromised credentials

average number of days to detect and contain a breach (down from 287 days in 2021)

#### Healthcare dominates the highest 60% of organizations in the study said they breach cost sector at \$10.1m per increased the price of their products and breach; the next closest are Financial

The United States has the highest

average breach cost of any country at

Middle East (7.46m) and Canada (\$5.6m)

\$9.44m per breach; the next closest are the

Breach detection and escalation costs (\$2.62m) surpassed lost business costs (\$1.42m) for the first time in six years

services as a result of the data breach; which

doesn't bode well for a healthcare industry

working to lower operational costs



### impacted Security skills shortage

Business continuity Insurance protection

Artificial Intelligence (AI)

DevSecOps approach

Employee training

Formation of IR team

platform implementation

Extensive use of encryption

Extensive tests of the IR plan

**INCIDENT RESPONSE** 

reviews, and more

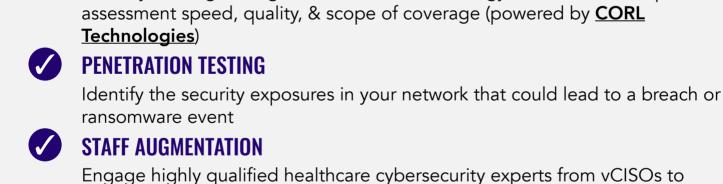
**CLOUD SECURITY SERVICES** 

- Participation in threat sharing Identity & access management

Lost or stolen devices

Third-party involvement





security projects

**SECURITY CERTIFICATIONS** 

maturity of your security controls

HIPAA COMPLIANCE HIPAA risk analysis and assessments, OCR preparation and response, policy and

HITRUST CSF and SOC 2 Type II certifications to drive and demonstrate

Meditology's services and technical testing are very valuable to our organization because they help us proactively protect our network, show us where we might potentially be vulnerable, and outline the steps required to fix it. It's a hefty price for a critical access hospital, but "you get what you pay for" and we don't want to

skimp. We have high expectations and a high level of trust which speaks to

staff-level team members that can hit the ground running to tackle your critical

WHAT OUR CLIENTS ARE SAYING

procedure development, and more SECURITY & PRIVACY RISK ASSESSMENTS Comprehensive risk assessments based on industry standards including HITRUST, NIST CsF, HIPAA, and more

#### We don't currently have the internal capacity to support all of our cybersecurity objectives. We are a huge organization, and tons of practices go live all the time -

Meditology's ability. We respect them and they've done a good job.

Where we sit now, the wins we've had and the ability to demonstrate value have been absolute home runs - 5 out of 5 rating. If I could give a 10 rating, I would. We would not be where we are today without this relationship. Meditology brings the brainpower to solve problems and provides us with a system, giving us a great starting point versus us creating from scratch.

so our partnership with Meditology is very valuable. Compared to other vendors I've worked with, Meditology is extremely responsive and flexible in scheduling and

always follows up. The cost of our team not having to do this has been great.

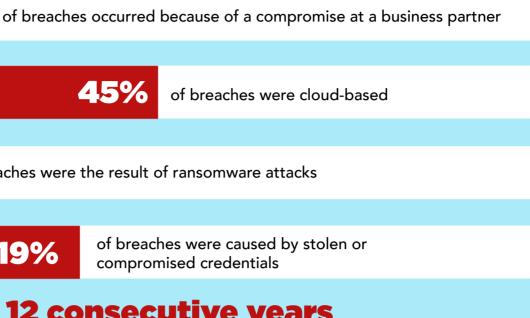
Manager for a regional healthcare provider in Colorado

cybersecurity program and keep rising breach costs in check.

MEDITOLOGY

Meditology is the healthcare industry's preeminent cybersecurity consulting firm and certification body. Our extensive knowledge of the healthcare ecosystem uniquely positions us to address the cybersecurity challenges presented by today's intense threat landscape.









credentials (19%), phishing (16%), cloud misconfiguration (15%), and third-party software/vendor (13%)

**TOP 5 KEY FACTORS** 

The top initial attack vectors for

**breaches** included compromised







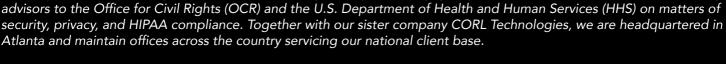


CIO & CISO for a private, non-profit community hospital in Vermont



Contact our team for more information and guidance to support your

We are proud to serve many of healthcare's most respected providers, payors, and business associates; and to act as expert



info@meditologyservices.com

**MEDITOLOGYSERVICES.COM**