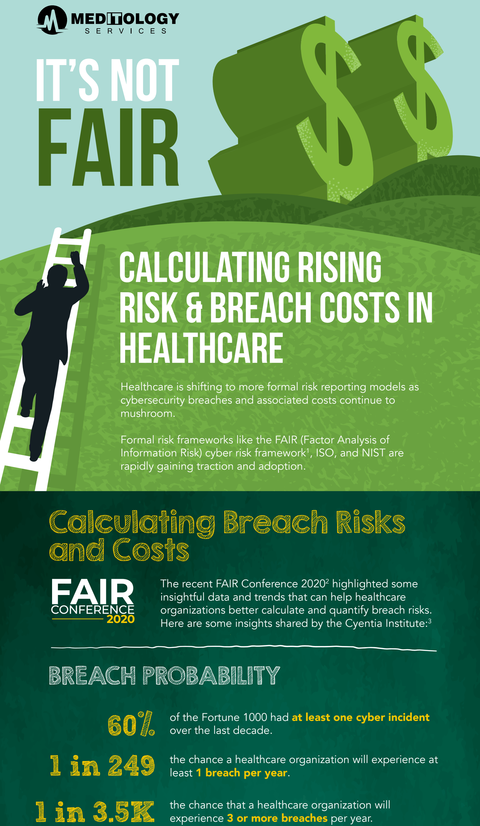
MEDITOLOGY SERVICES

IT'S NOT FAIR



CALCULATING RISING RISK & BREACH COSTS IN HEALTHCARE

Healthcare is shifting to more formal risk reporting models as cybersecurity breaches and associated costs continue to mushroom.

Formal risk frameworks like the FAIR (Factor Analysis of Information Risk) cyber risk framework[1], ISO, and NIST are rapidly gaining traction and adoption.

Calculating Breach Risks and Costs

FAIR CONFERENCE 2020

The recent FAIR Conference 2020[2] highlighted some insightful data and trends that can help healthcare organizations better calculate and quantify breach risks. Here are some insights shared by the Cyentia Institute:[3]

BREACH PROBABILITY

60% of the Fortune 1000 had **at least one cyber incident** over the last decade.

1 in 249 the chance a healthcare organization will experience at least **1 breach per year**.

1 in 3.5K the chance that a healthcare organization will experience **3 or more breaches** per year.

1 in 19K the chance that a healthcare organization will experience **10 or more breaches** per year.

BREACH COSTS

$200K **primary breach cost** per incident

10% of breaches fall into the **"large breach" category**

$19M primary breach cost for each **large breach**

$24M secondary loss cost for **incident response** activities per large breach

$21M secondary loss cost for **known fines and judgments** per large breach

$68M secondary loss cost for **productivity losses** per large breach

VULNERABILITY MANAGEMENT

66% of known global vulnerabilities **are not present** in most organizations

29% of known global vulnerabilities **are present** in most organizations, but are not actively exploited

5% of known global vulnerabilities **are present** and exploited in most organizations

51% of organizations are **actively reducing** their amount of high-risk vulnerabilities over time

16% of organizations are **just able to keep up** with patching new high-risk vulnerabilities

33% of organizations are **falling behind** with patching high-risk vulnerabilities and are accruing a backlog of "vulnerability debt"

ENTERPRISE RISK REPORTING TRENDS & PUBLICATIONS

FAIR & HITRUST Integration

The FAIR Institute announced a partnership with the HITRUST Alliance to integrate the FAIR framework with the HITRUST CSF to enable analysis for decision support[4]

Multi-Party Incidents

A recent report from Cyentia and RiskRecon notes the escalating trend of "multi-party cyber incidents" and the ripple effect in breach costs that traverse from Covered Entities to downstream business associates and vice-versa[5]

Healthcare Risk Reporting Best Practices

Meditology recently published guidance on designing effective enterprise risk reporting programs for healthcare entities[6]

[1] https://www.fairinstitute.org/
[2] https://www.fairinstitute.org/virtual-faircon-2020
[3] https://www.cyentia.com/ & https://www.cyentia.com/iris/
[4] https://www.fairinstitute.org/blog/fair-institute-and-hitrust-plan-integration-of-fair-standard-and-hitrust-csf
[5] https://https://library.cyentia.com/report/report_003839.html
[6] https://www.meditologyservices.com/enterprise-risk-reporting-the-healthcare-cisos-achilles-heel/

MEDITOLOGY'S RISK MANAGEMENT SERVICES

Meditology offers advisory and managed services to support enterprise risk reporting and management for healthcare entities including:

Enterprise Risk Reporting Managed Services for Healthcare — LEARN MORE

HIPAA Risk Assessments (HITRUST & NIST) — LEARN MORE

HITRUST CSF Certifications — LEARN MORE

Meditology is a top-ranked healthcare security and privacy firm servicing healthcare entities of all shapes and sizes. We were designated the #1 Best in KLAS firm for 2019 and 2020 for healthcare cybersecurity advisory services. Meditology also serves as the HIPAA expert witness firm for OCR and supports hundreds of healthcare entities coast-to-coast for the security, privacy, and compliance programs.

MEDITOLOGY SERVICES
info@meditologyservices.com
MEDITOLOGYSERVICES.COM