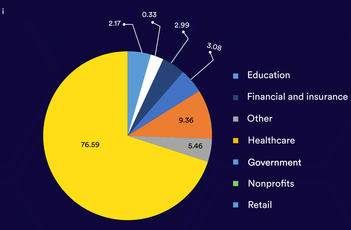
QUALITEST™

The Challenge and Future of Cyber Security for Healthcare

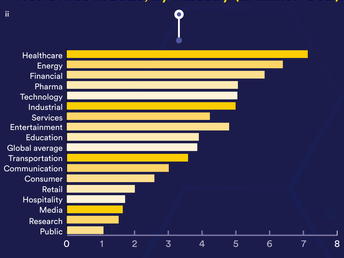
Among all industries, healthcare is suffering the most data breaches.

% Data Breaches by Sector 2015-2019.



Healthcare is also suffering the biggest cost of data breaches.

Average Cost of Data Breaches Worldwide in 2020, by Industry (in million USD).



Healthcare companies do not like to pay for cyber security.

$65 billion

Spent on cyber security from 2017 to 2021. But it's not enough.

% IT budget spent on cyber security

Up to 15%

Other sectors e.g. financial.

Healthcare 4–7%

From 2020 to 2025, the healthcare cyber security industry will continue to swell...

15%

Healthcare cyber security growth year on year.

$125 billion

Spending over this 5-year timespan.

Driven by key factors

- Remote patient monitoring
- Wearable medical devices
- Artificial intelligence
- Legacy technology
- Aging population

As a result, healthcare is a prime target for ransomware attacks.

1. Increased dependency results in higher requirements for availability and integrity of devices and services.

2. Increased amounts of data results in more complex confidentiality challenges. Healthcare is a prime target for ransomware attacks.

Cyber security testing needs to be integrated into your development lifecycle.

Plan and design
Assessing key risks, risk appetite and developing a holistic plan to address people, processes, and technology requirements.

Implementation and integration
Integrating a risk-based approach plan into the existing development environment and processes.

Maintenance
Ensuring ongoing maintenance of integrated frameworks.

Read more at:
qualitestgroup.com/cyber

QUALITEST™

Source: Privacy Rights Clearinghouse
Source: IBM Ponemon Institute