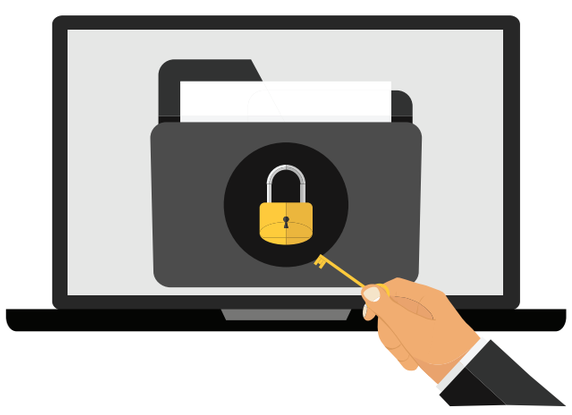
10 Security Stats Every Healthcare CIO Should Know

Healthcare continues to be a lucrative target for hackers with weaponized ransomware, misconfigured cloud storage buckets, and increasingly sophisticated phishing emails. More than 93% of healthcare organizations have experienced a data breach over the past three years.[1]



Healthcare cybersecurity breaches cost more than any other industry at $7.13 million.[2]

87%

87% of healthcare IT security leaders say they don't have the personnel to achieve a more effective security posture.[3]

560

At least 560 U.S. healthcare facilities were impacted by ransomware attacks in 2020.[4]

50%

Ransomware attacks account for almost half of healthcare data breaches.[5]

50x

Personal health information is 50 times more valuable on the black market than financial information.[6]

Phishing scams and other forms of email fraud are the most common point of information compromise in healthcare.[7]

91%

91% of cyberattacks begin with spear-phishing emails, which are commonly used to infect health-care providers with ransomware.[8]

45%

Healthcare industry cyberattacks increased by 45% in 2020.[9]

98%

98% of IoT devices are unencrypted and unsecured, exposing confidential data on healthcare networks.[10]

Yesterday was too late, but today is better than tomorrow to improve your security posture.
Talk to a TPx specialist to see how we can help.

Learn more at tpx.com/healthcare

TPx®

[1] Herjavec Group [2] IBM [3] Keeper Security Report [4] Emsisoft report [5] Tenable Research 2020 Threat Landscape Retrospective Report [6] Cisco/Cybersecurity Ventures Cybersecurity Almanac [7] 2019 HIMSS Cybersecurity Survey [8] Cybersecurity Ventures Report [9] 2020 Checkpoint report [10] Unit 42 report