

2025 SensCy SMO Cybersecurity Readiness Report

This infographic gives you a quick snapshot of our 2025 Cybersecurity Readiness Report. We've pulled the most eye-opening data to show where SMOs—small and medium-sized organizations—stand today, and what they need to do to stay protected.

The bottom line—Cyber threats are real, but taking the right steps can make all the difference.



Built on the trusted NIST framework, SensCy gives SMOs clear, actionable steps to strengthen cybersecurity. The SensCy Score-like a credit score for cyberhealth—makes it easy to measure and improve security.



SMOs Are at Risk.

Cyber threats aren't just a possibility—they're an inevitability. Without proper defenses, SMOs face financial loss, operational disruption, and reputational damage. Taking action now can mean the difference between business continuity and catastrophe.

< 20%

have dedicated cybersecurity resources

> have no cybersecurity budget

believe they are too small for an attack

of cyberattacks are targeted to SMOs

Report Findings

SensCy conducted hundreds of cyber assessments with SMOs across the U.S. That data reveals that:



Do not follow baseline cybersecurity practices, making them prone to phishing and ransomware attacks.

497

The average initial SensCy Score of SMOs across all sectors (think of this number like a credit score).



The average improvement companies saw in just months by adopting best practices.

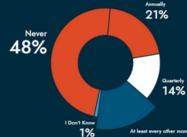
Measuring Cyber Risk & Resilience

The SensCy Score and this report examine cyber risk and resilience through the lens of three core components—People, Process, and Tools—essential for building and maintaining a strong cybersecurity program and culture. Below is a glimpse of the insights you'll find in the full report.



People

88% of cyberattacks stem from human error. Despite this, many SMO-70%— lack structured cybersecurity awareness training programs.



63%

Cybersecurity Awareness Training

Incident Response Plan



Process

A step-by-step incident response plan significantly reduces the downtime and financial impact caused by a cybersecurity incident, yet 66% of SMOs don't have one.



Tools

55% of SMOs never perform internal or external vulnerability scans, and only 17% provide password management tools to their employees.



Be Prepared. Be Protected. Act Now.



Take the first step. Get your SensCy Score.

your free cyberhealth assessment.

Scan the code to schedule



17%

To get your copy of the full report, click **here**.