UncommonX

How a Risk Score Helps Improve an Organization's Security Posture

by Ryan Pisoni, Senior Vice President of Development, UncommonX

Technology has exploded in the last 25 years and providing security in this space is an ever-evolving target. In today's landscape it's not uncommon for security practitioners to ask of their organization "Are we protected?" or "Are we doing enough?" Identifying risk in an organization is a challenging task and many companies do not know where to start. One way is to determine your security posture by compiling a risk score, including how you rank in relation to your competitors.

Standards such as NIST's Cybersecurity Framework were created to help entities manage its risk posture by way of best practice. This is a voluntary framework to help measure an organization across multiple control categories. The standard itself can also take considerable effort to manage. At Uncommon, we have taken much of the guesswork out of NIST alignment for technical controls.

Using our proprietary risk assessment system, we effectively measure a company's security posture and alignment to the technical controls of the NIST Cybersecurity Framework — specifically, identify, detect, protect, respond, and recover. At a high level, UncommonX identifies gaps in an organization's technical controls. The technical control gaps, coupled with observed data in network assets and data ingestion, are used to formulate a security posture, or risk score, that aligns with the NIST standard.

An organization's standalone risk score is powerful in its own merit and can quickly help a security practitioner understand where its organization stands. However, at UncommonX, we have taken this approach one step further using our Relative Risk Rating (R3) system. The R3 system is designed to compare risk scores among industry peers.

For example, a financial institution may have an overall score in the 85th percentile with no immediate gaps in technical controls. Another financial institution may have a score in the 95th percentile with no immediate gaps in the technical controls. However, the scores may differ based on tool coverage, observed security vulnerabilities, and other deterministic factors that modify the risk scoring.

The R3 system will show an organization how it compares to peers in its industry and make recommendations to help improve its security posture. This becomes a relative measure of risk between cohorts designed to highlight gaps among peers and provide a path to improve its own risk score and reduce overall risk and threats.

About the author

Ryan Pisani is Senior Vice President of Development for UncommonX. He has spent his career as a driving force in the technology industry, including over 18 years at Motorola Mobility. Currently, he is leading UncommonX's product development team to ensure delivery of the most innovative security solutions at a time when companies need it most.