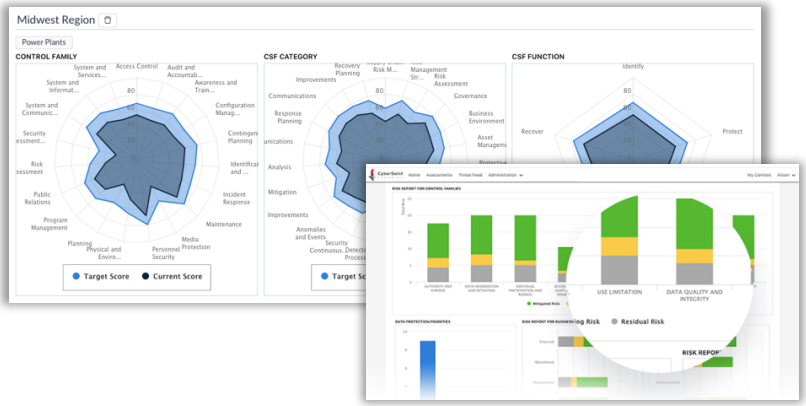
Digitalization, Regulatory Change, and Increasing Cyber Threats Create Urgency for the Energy Sector to Prioritize Cybersecurity

59% of energy companies believe their OT network is likely to be the next cyber-attack target. Only 42% rate their readiness as high, and only 31% rate readiness to respond to or contain a breach across IT and OT as high. In the face of growing cyber risk, these numbers have to change.

Even the most effective security leaders in enterprise energy organizations are challenged to assess the efficiency of their cybersecurity program, plan proactive risk mitigation, and communicate their posture across all levels of the organization from the Board of Directors to auditors and asset owners. Next-generation technologies both simplify and accelerate cybersecurity program management, enabling proactive cyber readiness at scale across both IT and OT environments, and augmenting where manual spreadsheets and legacy Governance, Risk and Compliance (GRC) systems fail to meet the needs of the organization.



The **CyberStrong Integrated Risk Management platform** empowers organizations to manage their unique security and risk posture with **Governance Dashboards** that provide real-time **Board and auditor assurance** and visibility across all levels of the organization. The platform's **automated assessment workflow** and real-time **remediation action planning** informs **Security Return on Investment (SROI)** from a scalable, centralized system of reference.

Cybersecurity Posture In Business Context
View posture by region, asset type, plant, or fleet, and instantly drill down from enterprise-wide into business unit or asset-level security

Regulatory Standards
Easily adopt the NIST CSF, NERC-CIP, ISO27001, COBIT or any control set while eliminating duplicate efforts

OT/IT Continuous Compliance
Automate gap analyses and remediation plans based on compliance and risk scores, while decreasing time to baseline by 75%+

CyberStrong enables energy and utility organizations to be proactive about cybersecurity and ready to respond to attacks. Leveraging intuitive metrics, agile automation, and clean dashboards, CISOs and CEOs clearly articulate value to the rest of the C-Suite and Board. When presented clearly, an organization's cybersecurity program becomes a true business function that is ready to respond to threats at scale, while credibly driving security return on investment and supporting business growth.

CYBERSTRONG FOR ENERGY & UTILITIES

Know Your Assets. Accelerate Compliance. Continuously Improve.

Enterprise Energy Business Case Study

BUSINESS CHALLENGE

This Fortune150 Industrial client, one of the top utility companies globally, sought to drive a **continuous and trackable** IT & OT **improvement program** across **enterprise, BUs, geographies, plants and sites**.

Their objectives were to **measure risk and security posture in real-time** and drive secure digital **transformation** via **policy integration** and **improvement**.

PARTNER APPROACH

- **Design** a tailored assessment methodology
- **Develop** prevention, detection, response, and recovery plans
- **Implement** a continuously improving program
- **Monitor and Report on** readiness and cyber posture

IMPACT & RESULTS

ASSESSMENT AUTOMATION

Assessed **cyber risk maturity** by **BU, geographic location, and asset type.**

BOARD REPORTING

Provided **real-time insight** into cybersecurity risk and **return on security investment.**

ENABLED COMPLIANCE

Determined **NIST CSF** and **NERC-CIP** compliance at **~6,000 sites** and **plants.**

CONTINUOUS IMPROVEMENT

Addressed **real-time** critical **vulnerabilities** and mapped controls to **policies**.

DIGITAL TRANSFORMATION AND CLOUD MIGRATION

Accelerated **virtualization** of legacy systems and siloed assets, securely moved programs to the cloud