Data Documentation
Comprehensive Cybersecurity Resilience Factors Assessment Survey for Stakeholders

This dataset contains anonymized quantitative survey data collected as part of a convergent parallel mixed-methods study examining cybersecurity resilience in privately owned and operated critical infrastructure organizations in the United States. The dataset supports the quantitative strand described in Chapter Three (Methods) of the associated research. The dataset includes responses from 141 organizational stakeholders and examines relationships among governance, internal controls, cybersecurity knowledge and skills, attitudes toward cybersecurity policy, organizational vulnerabilities, and cybersecurity resilience. Data were collected using a structured questionnaire employing five-point Likert-type scales (1 = Strongly Disagree to 5 = Strongly Agree). Missing responses are represented as blank cells. Exploratory Factor Analysis (EFA) was conducted using principal axis factoring with varimax rotation to examine the underlying structure of the instrument. Confirmatory Factor Analysis (CFA) was subsequently performed to validate the factor structure. Model fit was evaluated using standard indices including CFI, TLI, RMSEA, and SRMR. Reliability was assessed using Cronbach's alpha, with all constructs demonstrating acceptable to strong internal consistency. The dataset contains no personally identifiable information or sensitive operational cybersecurity details and has been fully anonymized. It is intended for academic research, policy analysis, and methodological reference and is not designed for operational cybersecurity decision-making or commercial use.