Lower Colorado River Authority

Cybersecurity Framework Success Story

The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improve security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.

Organizational Profile

The Lower Colorado River Authority (LCRA) exists to serve the people of Texas. It's been that way since the state Legislature created the nonprofit public utility organization in 1934. LCRA continues that legacy today by providing a multitude of vital services to customers and communities. Texans depend on LCRA for vital services such as providing a clean and reliable water supply, managing the lower 600 miles of the Colorado River, securing and protecting the water supply for more than 2 million people, and managing floodwaters that otherwise could devastate Austin and other communities. Cities, businesses, industries, agriculture, and the environment all rely on water from the Colorado River. LCRA has been the primary wholesale provider of electricity in Central Texas since 1937.

LCRA sells wholesale electricity to more than 30 retail utilities, including cities and electric cooperatives that serve one of the nation's fastest growing regions. LCRA Transmission Services Corporation is one of the largest transmission providers in Texas, moving power across the state through about 5,300 miles of transmission lines in more than 75 counties. In addition to supporting critical infrastructure for Texas residents, LCRA owns or operates more than 40 parks, recreation areas, and river access sites that provide people with outdoor adventure and access to the Colorado River.

Situation

Prior to implementing the Cybersecurity Framework (CSF), LCRA adopted NIST 800-53 security controls. Due to the diverse nature of the businesses at LCRA, those controls were not universally applicable across business units such as power generation, river operations, and telecommunications. The implemented security controls didn't account for differences between the operations technology (OT) and enterprise information technology (IT) environments. The flexibility of the CSF allowed LCRA to encompass multiple business standards and requirements. It was also evident that implementing controls required taking into account organizational maturity, business needs, and risk appetite. This sort of tailored approach was primarily addressed through ad hoc efforts. The Cybersecurity department would become aware of a security issue and contact the affected business units to solicit compliance with the relevant security control.

Process

- LCRA began conducting system- or departmental-level CSF assessments.
- LCRA uses a risk-based approach to the CSF. The CSF provides a context and a common vocabulary. The tiered method of risk assessment and analysis allows groups within LCRA to determine needed maturity levels; target tiers are decided upon within the business units.
- LCRA's CSF is composed of the following steps:

  - **Step 1: Prioritize and Scope**. LCRA identified its business/mission objectives and high-level organizational priorities. LCRA used those objectives and priorities to make strategic decisions regarding cybersecurity implementations. Further, LCRA adapted the CSF to support different business units, which have varied needs andassociated risk tolerance. Risk tolerances are reflected in a target Implementation Tier. The CSF roadmap was signed-off by LCRA executive leadership.

"As a critical infrastructure provider, LCRA faces the full spectrum of cyber threats. LCRA's adoption of the NIST Cybersecurity Framework enables risk-based business decisions that protect our dams, power plants, electric transmission and telecommunication systems. Successfully securing such diverse businesses requires flexibility and adaptation. The Cybersecurity Framework is the core means for LCRA to establish business objectives, assess risk and establish appropriate security controls."

– Madhava Utagikar, LCRA CISO

Process (Continued)

  - **Step 2: Adjust.** After the scope of the cybersecurity program was determined for the business units, the related systems and assets, regulatory requirements, and overall risk approach were identified. LCRA consulted vulnerability scans as well as penetration tests and audit findings to identify threats and vulnerabilities applicable to those systems and assets.
  - **Step 3: Create a Current Profile**. LCRA developed a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are being achieved. If an outcome has been partially achieved, noting this fact will help support subsequent steps by providing baseline information.
  - **Step 4: Conduct a Risk Assessment**. This assessment is guided by LCRA's overall risk management process or previous risk assessment activities. Stakeholders analyze the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important to identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.
  - **Step 5: Create a Target Profile**. LCRA created a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Subcategories account for unique organizational risks. LCRA also considers influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.
  - **Step 6: Determine, Analyze, and Prioritize Gaps**. LCRA compares the Current Profile and the Target Profile to determine gaps. A prioritized action plan was developed to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. LCRA then determined resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.
  - **Step 7: Implement Action Plan**. LCRA has determined actions to take to address gaps. Its cybersecurity practices are adjusted, as needed, to achieve the Target Profile. LCRA's CSF is dynamic, with an emphasis on continual improvement; as applicable national standards are updated, LCRA modifies its related CSF procedures.

Drivers

- An audit of LCRA's industrial control systems' security controls "determined that policies and procedures are not adequate and effective." In response to the audit, LCRA management committed to forming a cross-functional team to address the audit findings. Senior leaders from LCRA's business units recognized that securing industrial control systems and operational control systems were a high priority and may differ from securing information systems.
- The enterprise level is responsible for cybersecurity across all business units, and LCRA needed a way to secure cybersecurity processes. The CSF allows a cybersecurity program to be organized across the enterprise. At the same time, it allows tie-in of specific requirements applicable to each area.
- The CSF allows a cross-business understanding of what standards apply. For example, the IT environment has applicable NIST controls, but the OT environment uses North American Electric Reliability Corporation (NERC) or Institute of Electrical and Electronics Engineers (IEEE) controls.
- The flexibility of the CSF provides a roadmap and a process for developing truly functional systems that help LCRA secure critical infrastructure for millions of Texans and visitors to the state.

Results and Benefits

- Business leadership, the CISO, and the Cybersecurity department collaborated to identify the applicable standards. It was a business-driven approach to identify applicable cybersecurity standards and risk tolerance. Business units provided input into the content of security controls and signed-off on their final content.
- The CSF architecture provides LCRA the flexibility to give multiple sets ofcontrols that are applicable to the OT and the IT environments. An established baseline of what standards applied to which part of the business allows further maturity of LCRA's CSF.
- The framework enables the various business units to tailor the CSF to meet their needs. As a result, there is a greater level of acceptance to work on cyber matters now that businesses are being held to agreed-upon standards.
- CSF assessments are conducted based on higher-level, nationally recognized NIST standards. Becausste LCRA mapped the different standards used by the organization's various businesses, when an assessment is conducted, the results can be directly tied to the applicable business unit.
- The CSF facilitates the business units' development and ownership of security policies and processes. It aids the transition from a single set of standards to adopting a flexible CSF construct. LCRA umbrella. The flexibility of the CSFmet the needs of diverse businesses. Different regulatory schemes apply to the various businesses under the LCRA umbrella.

What's Next

- LCRA is completing CSF assessments across the enterprise, prioritizing assessment focus areas by system criticality. The assessment results are returned to system owners, which support cybersecurity risk-informed business decisions.
- Assessment results will also be used as an input for an internally developed Cybersecurity Risk Quantification Tool. The tool aims to create a data-driven management instrument that informs cyber risk decisions, performance, and activity. It uses CSF assessment results to represent effectiveness of security controls in the environment and yields numerical representation of cybersecurity risk at the system- and organizational-levels.
- LCRA is implementing a Cybersecurity Risk Register that will support the overall Cybersecurity Risk Management Program. CSF assessment results are one of the sources that will be used to populate the risk register. The Cybersecurity Governance, Risk and Compliance team will assign risk ownership, identify risk response actions, track status towards completion of the actions, and generate metrics to measure success of the program.

Contact Information & Resources

LCRA Website:
LCRA.org

LCRA Contact:
Contact.LCRA@LCRA.ORG

NIST Cybersecurity Framework Website:
https://www.nist.gov/cyberframework

NIST Contact:
cyberframework@nist.gov