Entergy’s Cybersecurity Management Overview

Entergy has adopted and implemented a “Three Lines of Defense” model to facilitate a systematic approach to govern and oversee security risk management and control by defining first, second and third line roles, duties and accountabilities. In this model, Entergy streamlines security into a single centralized governance program by unifying physical and cybersecurity risk management through the same risk lens to gain the enterprise's visibility of all security risks.

The first line of defense is comprised of business units performing operational functions, including the Chief Information Security Office, and is responsible for identification and management of security and reliability risks directly through design, implementation and execution of control activities.

The second line of defense is comprised of the Chief Security Officer and Chief Security Office who perform and support security and reliability risk management and govern and oversee the execution of security and reliability controls by the first line of defense. Ownership of specific security operations may migrate from a business unit in the first line of defense to the second line of defense, as determined to be appropriate by the Chief Security Office. The Chief Ethics and Compliance Officer reports to the Executive Vice President and General Counsel and works with the CSO to ensure that requirements of external security-related regulations are addressed and, where applicable, translated into business policies.

The third line of defense, which includes Internal Audit, independent third parties and certain regulatory constructs like the North American Electric Reliability Corporation’s Reliability Standards and the U.S. Nuclear Regulatory Commission’s Cyber Security Rule, provides assurance of selective actions taken by the first and second lines of defense to Entergy’s senior management and board of directors.

As we expand and automate our utility infrastructure, our coordinated “three lines of defense” risk management model has evolved to ensure that adequate protections and controls are in place and are being monitored to secure our part of North America’s electric grid, protect sensitive information and maintain secure business operations. We manage physical and cybersecurity threats as an enterprise risk that includes close coordination and information sharing with our federal, state and local partners. Cyber and physical security risks and security program performance are regularly reviewed by senior corporate executives and the audit committee of our board of directors. We consider ourselves stewards of customer, employee and vendor information that we collect, maintain and use. We must ensure data privacy through a comprehensive data governance program and adequate data security controls.

To prevent cyber incidents, we maintain access-management controls, including a layered multi-factor authentication process for network and system access, and a defense-in-depth security ecosystem that includes advanced threat detection from independent third parties and federal agencies, security logging and monitoring, and independent third-party penetration and vulnerability assessments. Relevant employees and contractors must complete cybersecurity trainings periodically to heighten security and threat awareness, promote best practices, and meet regulatory requirements. Additional multi-layered prevention and detection processes and technologies to mitigate and minimize the effects of cybersecurity risks include email security, continuous monitoring, vulnerability scanning, anti-virus and anti-malware software, backups and recovery strategy, network segregation, third-party security, and information protection.

Entergy has incorporated certain cyber-specific response protocols and procedures into our Incident Management System framework for responding to emergency incidents. This includes the Entergy Incident Response Team Plan, which outlines Entergy's procedures, steps and responsibilities for preparing for, detecting, containing and recovering from an incident. The plan details the roles and responsibilities of Entergy's officers who would be engaged in such a response to an emergency incident, including key questions to be addressed, critical decision points and sources of key information to support decision-making. Senior management and the Emergency Incident Response Team periodically review and drill on the plan.

As cybersecurity risks continue to evolve with multiple threat vectors, Entergy maintains a comprehensive security strategy to keep current with the changing threats. To inform this effort, we utilize the National Institute of Standards and Technology Cybersecurity Framework, which consists of standards, guidelines and best practices to manage cybersecurity risk across the enterprise. A risk-based approach is used to direct security initiatives to the most significant risks and provide the most value in terms of risk reduction and protection. Entergy uses a vendor risk management program to assess and monitor security risks that arise from third-party vendors. In addition, we utilize technology and threat intelligence services to assess and continuously monitor the cybersecurity risk of key vendors, as identified through the vendor risk management program.

We engage with local, state and federal law enforcement agencies on initiatives to share threat information and participate in a wide range of industry collaborations and classified briefings on cybersecurity. These partnerships include:

- Utilities United Against Scams, a consortium of electric, gas and water utilities dedicated to combating utility scams by providing a forum to share data and best practices and working together to implement initiatives to inform and protect customers.
- Electricity Information Sharing and Analysis Center, a provider of security services to North American electric utilities.
- U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response programs.
- Federal Bureau of Investigation Domestic Security Alliance Council, a strategic partnership between the FBI and U.S. private industry that enhances communication and promotes the timely and effective exchange of security and intelligence information.
- Electricity Subsector Coordinating Council, a primary security communications channel provider for the electricity subsector and a resource to assist with incident preparedness.
- National Security Agency Cybersecurity Collaboration Center, a program which provides cybersecurity support to entities that provide services to the U.S. Department of Defense.