Entergy's Cybersecurity Management Overview

Entergy has adopted and implemented a "Three Lines of Defense" model to provide a systematic approach to govern and oversee security risk management and control by defining 1st, 2nd, and 3rd line roles, duties, and accountabilities. In this model, Entergy streamlines security into a single centralized governance program under Entergy's Chief Security Officer (CSO) by unifying physical and cyber security risk management through the same risk lens to gain the enterprise's visibility of all security risks.

The First Line of Defense: *Operations and Business Units* - Line management is responsible for identifying and managing risk directly (i.e., through the design and execution of controls to respond to risk). The first line consists of a corporate "hub" supporting operations and business unit "spokes" responsible for the management and execution of the security program and complying with the security policies. Business units such as Distribution, Transmission, Power Generation, Information Technology, and Information Security make up the first line.
The Second Line of Defense: *Management Assurance and Risk Management* - Responsible for ongoing monitoring of the design and operation of controls in the first line of defense and providing advice and facilitating risk management activities. The CSO organization falls within the second line. It is responsible for setting policies, monitoring, and reporting the security program being executed by the first line, and providing some support activities that may not be entirely independent of the first line. The Chief Compliance Officer reports to the Executive VP & General Counsel, monitors the external security-related regulations, and works with the CSO to ensure these requirements are translated into business policies.
The Third Line of Defense: *Independent Assurance* - Responsible for assuring senior management and the board over both the first- and second-line's efforts. This line includes internal audit, external audit, and regulatory constructs, such as the North American Electric Reliability Corporation (NERC) Reliability Standards, Nuclear Regulatory Commission (NRC) Cyber Rule, Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), and Health Insurance Portability and Accountability Act (HIPAA).

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 have implemented modern access-management controls, including a layered multi-factor authentication process for network and system access and a

defense-in-depth security ecosystem includes advanced threat detection from independent third parties and federal partners, security logging and monitoring, and routine independent third-party penetration and vulnerability assessments. All employees must complete computer-based cybersecurity training modules throughout the year to heighten security and threat awareness, promote best practices, and meet regulatory requirements. Additionally, employees are subject to disciplinary measures for security policy violations and repeat responses to Entergy's simulated phishing campaigns. A formalized corporate incident response plan is documented and tested, exercised annually, and continuously improved based on lessons learned should an event materialize within the enterprise. The response plan outlines Entergy's procedures, steps, and responsibilities for preparing for, detecting, containing, and recovering from an event.

Since the cyber-threat landscape continues to evolve with multiple threat vectors, Entergy maintains a comprehensive security strategy to keep pace with the changing threat landscape. To inform this effort, a blend of internal and independent third parties perform continuous and annual assessments, vulnerability and penetration tests, SOC 2 analysis, and audits on Entergy's key information security program elements, technology functions, and critical vendors. As new threats emerge, investments are made to improve enterprise security technology capabilities. A risk-based methodology is in place to ensure security initiatives address the most significant risks and provide the most value in terms of risk reduction and protection.

Entergy evaluates risk to prevent or limit the impact or consequences of a security attack. A robust suite of multi-layered prevention and detection processes and technologies mitigate and minimize the effects of these risks. These include, among others:

- **Training and Awareness** - Simulated phishing assessments and general cyber and physical security awareness provided for employees and contractors
- **Email Security** - Email scanning and filtering; Internet blocking; Suspicious email reporting mechanisms.
- **Access Control** - Multi-factor authentication and physical access controls protecting against unauthorized external access
- **Continuous Monitoring** - 24x7 advanced persistent threat and physical security protection, monitoring, and alerting
- **Vulnerability Scanning** - Regular vulnerability scanning on Internet Facing Devices to limit the attack
- **Virus and Malware** - Antivirus and anti-malware software blocking unauthorized software
- **Backup and Recovery** - Comprehensive daily backup and recovery strategy for critical systems and critical data
- **Network Segregation** - Business and operational networks segregated
- **Third-Party Security** - Program mitigating risk of security attacks targeting industry supply chains

- **Information Protection** - Process and technology protecting storage and transmission of highly sensitive data on-premise or in the cloud

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.
- Department of Energy Cybersecurity Risk Information Sharing Program.
- 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, and
- American Gas Association Natural Gas Security Committee.