AN ENERGY COMPANY LOOKS TO SHAPE THE FUTURE BY REINFORCING ITS ROOTS

A Powerhouse with a Purpose

Southern Company (NYSE: SO) is America's premier energy company. The Atlanta-based conglomerate contains numerous subsidiaries, offering electric utilities in four states and distributing natural gas in seven. Through its unified efforts, the Southern Company family produces 46,000 MW of generating capacity and 1,500 billion cubic feet of combined natural gas consumption and throughput volume – effectively serving nine million customers.

Commitment runs deep in the Southern Company family. The enterprise is dedicated to supporting its customers, communities, employees and shareholders long-term. With guiding principles of honesty, integrity and fairness, the company approaches every day as a critical step towards achieving its mission of *providing clean, safe, reliable and affordable energy.*

Beyond the Bottom Line

With a rich history in research and development (R&D), Southern Company has set its sights on inventing America's energy future. The enterprise is innovating across many fields, including 21st Century coal, natural gas, carbon-free nuclear, sustainable energy and cyber security. This robust portfolio illustrates the enterprise's commitment to leading the industry in R&D, and it demonstrates its belief that its mission can only be carried out by solving the energy problems of today and tomorrow.

> A recent quote from Tom Fanning, CEO Southern Company, really impacted me: "Energy innovation represents an enormous advantage for Southern Company. Our efforts have simple goals: to preserve fuel flexibility and increase the value of energy to our customers." It strikes at the core reason for implementing the technology that is easy to forget, the goal of improving our lives.
>
> **Paul Hurley**
> **CEO, Securicon, LLC**
> **Information Security Solutions**

In recent years, Southern has partnered with the federal government for R&D initiatives that have furthered the cyber security goals of both the government and Southern Company itself. One example is the 2009 Smart Grid Investment Grant Program (SGIG) from the Department of Energy (DOE), which offered financial assistance to projects intended to accelerate the modernization of America's grid infrastructure. Southern's participation in the SGIG program led to the instantiation of a Power Delivery Cyber Security Program (CSP) responsible for governing and implementing a risk-based strategy to identify, protect, detect, respond and recover from cyber threats.

Preparing for Tomorrow

To shape the future of operational technology (OT) cyber security, Southern must develop cyber security solutions that address the unique challenges faced in their OT environments. Currently, the nation's power system consists of both legacy and next-generation technologies. This includes devices that may be 30-50 years old, contain no cyber security controls and utilize proprietary communication protocols and applications. In contrast, new technologies may incorporate modern information technology (IT) devices with commercially-available applications and communication protocols.

One of the ways Southern Company's Power Delivery CSP addressed these challenges, was to create a Systems and Communication Protection (SCP) initiative to protect and segment Power Delivery systems and communications across all applicable Southern Company networks.

The SCP Project aims to tackle three primary challenges:

1. **AVAILABILITY:** Increasing the resilience of operations to ensure business continuity;

2. **INTEGRITY:** Ensuring safe operation of the grid by validating that control traffic originates only from authorized sources; and

3. **CONFIDENTIALITY**: Encrypting sensitive and control traffic traversing Southern Company's networks.

A Partner in Success

For more than 15 years, Southern Company has partnered with Securicon to support its security needs. Securicon has expertly assisted the enterprise in a variety of security endeavors, from performing assessments and testing to developing recommendations and designs. When the company initiated the SCP Project, it selected Securicon to partner with to secure the OT environment.

Securicon's experienced team members know that security is a collaborative effort. Instead of forcing policies or procedures upon its clients, Securicon's engineering professionals create an environment where trust and partnership engender success.

Securicon met with each of Southern Company's four electric operating companies and other key stakeholders to determine requirements, concerns, scheduling conflicts and compliance deadlines. Together, the teams identified risks which Securicon leveraged to craft and design an engineering plan to implement Southern's new security tools and procedures.

> Working with companies who are proactive in implementing new cyber protection methods and technologies, such as Southern Company, is extremely rewarding. We've had the privilege of helping Southern Company realize their vision of growing and maturing their cyber security program for the past fifteen years, and we are excited to envision the partnership for the next fifteen years.
>
> **Paul Hurley**
> **CEO, Securicon, LLC**
> **Information Security Solutions**

Thriving in a Tumultuous Environment

Southern Company's engineers worked diligently with Securicon's team to answer the SCP Project's challenges. They collectively identified and remediated issues that arose during design and implementation, and they executed solutions to ensure that Southern Company's power delivery systems were positioned to adopt emerging security architectures and technologies.

To specifically enhance availability, integrity, and confidentiality, Securicon assisted Southern Company in developing standardized architectures, policies and procedures to implement the following:

- **Leveraging an innovative Palo Alto Networks platform to give Southern Company precise control over its network traffic.** The centralized platform presents Southern Company with heightened visibility into network communication, helping the company troubleshoot performance issues and protect itself from unknown threats.

- **Employing a user-based access model to help protect OT systems with the addition of a distributed, multi-factor authentication strategy.** The new authentication process uses pre-configured hierarchies and policies to enforce a specific level of authentication on each resource, guaranteeing that data and OT are always in the right hands.

- **Reducing the attack surface of ICS systems by the implementation of a standard zoning model.** Securicon employed best-practice zoning strategies to interconnect ICS and business networks, logically segmenting systems and securing access for business partners.

- **Protecting the confidentiality and integrity of industrial control system traffic by establishing encrypted VPN tunnels between control system networks, allowing Southern Company to manage and operate the electric grid securely.**

A Stronger Foundation to Forge Ahead

The improvements and enhancements that were executed during the SCP Project improved the overall reliability and performance of Southern Company's power delivery systems. The collaborative effort strengthened the company's data defenses and secured control of OT. Southern was provided with the tools and processes it needs to protect its critical communication paths and operations proactively to continue providing clean, safe, reliable and affordable energy for years to come.

Southern Company and Securicon have also committed to continuously innovating solutions to secure the OT environment. The constantly-evolving technology landscape, coupled with evolving threats, has increased the complexity of addressing cyber security risks looking ahead. Smart grid technologies, distributed energy resources and other emerging and potentially-disruptive technologies – like those proliferating via the Industrial Internet of Things (IoT) - must be secured as they are introduced into grid operations.

The teams look to continue their relationship as they tackle these challenges and strive to shape the future of OT cyber security.