

The Security Executive Council (SEC) Solution Innovation Partner (SIP) program evolved as a means for practitioners to choose a trustworthy risk mitigation provider with confidence when there is a myriad of options in the marketplace. Proven Solution Innovation Practice Case Studies help evaluate performance claims and differentiate solution providers for business outcomes including risk mitigation, return on investment, and security assurance.

This Solution Innovation Practice Case Study offers a proven process approach for mitigating risk(s) that could result in injury or impairment of people, assets, critical processes, products and/or brand reputation. This proof point examines representative risk issues, mitigations and result outcomes as validated by the Security Executive Council and the end-user.

The following case study demonstrates a unique design approach for a utility company based in the southern United States. The project objective involves the modernization of localized access control and video technology to an integrated enterprise solution with identity management, and a completely redesigned and expanded corporate security operations center (SOC).

Context and Background:

- The company is an electric and gas utility company with over 115 locations ranging from the Gulf of Mexico to the Canadian border. The covered critical facilities include main headquarters, two regional headquarters, electrical substations, natural gas terminals and distribution controls, service support locations, and field sales offices.
- The existing legacy access control system was outdated, lacked modern functionality, and no longer expandable or supported by the manufacturer.
- Video and alarm systems were a mixture of analog and digital systems which required significant maintenance and manual operational workarounds to support continuing operations and performance continuity.
- The existing Security Operations Center (SOC) was cramped, dated and unsuitable for full forward-looking enterprise risk mitigation support.

Risk Issues and Mitigation Opportunities:

- A highly significant security event occurred on company property and inoperable security technology failed to prevent access and capture event video.
- Access control and alarm system failures at critical infrastructure locations required costly 24/7 on-site security and/or law enforcement presence, without incident verification.
- Conducting people and asset protection monitoring in the SOC which was congruent with cultural expectations was hampered by large number of disparate and independent systems, unreliability of technical systems, and maintenance management concerns.
- Inefficiencies in unintegrated access control processes, systems reporting, support for internal and regulatory audits.

Solution Requirements:

- Uniform video solution and integrated access control over all sites that align with company culture expectations.
- Improvements in access control provisioning for access assignments, retraction of access, and audit support for both internal and NERC CIP-compliant inspections.
- Upgraded and expanded SOC with visibility to all company locations.
- Provisions for system expansion in support of projected large acquisition.
- Solution designed to address non-regulated sites as the primary purpose.

Delivered:

- Automated access control integrity assurance and efficiency with measurable labor cost avoidance.
- Daily manual video camera verification replaced by automated self-diagnostics and exception report.
- Video alarm verification eliminated multiple dispatches of personnel and posting guards at remote locations.
- Integrated, Enterprise access control, video, alarm, and intercom solution technologies that aligned with company culture and duty of care expectations.
- Standard design and deployment strategies to maximize installation efficiency, economies of scale, and streamlined maintenance.
- Identity management system to coalesce authority and responsibility for access control permissions with the owners of areas needing protection.
- Project Sequencing and Management support.
- Design Narrative utilized for expectation confirmation and refinement. Addressed project functionality critical to client and security mission, areas of interest with objectives to be accomplished in each area, design strategy, responsibility matrix addressing all project stages from design through operations and maintenance, project risks and assumptions, deployment cost expectation, and deployment schedule expectation.
- Engineering design drawing and specification package.
- Met cost and schedule commitments for project deployment and ongoing maintenance.
- SOC design layout and operations overview proved conducive for verifiable alarm-triggered video assessment.
- Lessons learned on the process shared with client for continuous improvement.
- Achieved data normalization for access authorizations during conversion from legacy system to new system.
- Provided access control authorization structure to support role-base assignment in areas where the company culture would support.
- Qualified integrators to support installation and maintenance with reliable results.



SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Solution Innovation Case Study: Generating and Delivering System Design for Operational Excellence and Cost-Effective Return on Investment

Outcome and Benefits of Service Including ROI:

- Increased enterprise security process governance for access authorization management.
- Significant improvement in security systems integrity and leadership confidence in value delivered by security.
- SOC achieves visibility of all camera views and system alarms across the enterprise, with capacity for expansion and crisis management.
- Standardization of equipment, installation practices, and software configurations to improve system management efficiency and reduce support cost overruns.
- Access authorization shifted to space owners who are also able to self-audit persons with access to their areas. This improves integrity of the process, reduces duplication of process, and allows security personnel to focus on system efficiencies and exceptions rather than continuously manage common daily practice.
- Increase in people and property incident detection, response, and forensic investigation.
- Reduction in contract security and law enforcement expenses incurred due to out-of-service security equipment.
- Installation of optical turnstiles have greatly reduced tailgating and improved accuracy of on-site staff count.
- The organization's senior leadership confidence that an event will be detected moved from 5 out of 10 to 8.5 out of 10.

SIP Process

This process was overseen by a Council Faculty member with 20+ years of experience in developing and leading people and asset protection programs as trusted security advisor for global and multinational organizations. **End-user authenticated in November of 2020.**

Note: The Security Executive Council's Solution Innovation case study represent a snapshot in time to demonstrate a solution to a specific organization's issue. End-user diligence, trial and measurement are strongly recommended for any contemplated risk mitigation activity.

A General Comparison of Competition

	Butchko, Inc.	Other Small Suppliers	Other Large Suppliers
Project Focus	<ul style="list-style-type: none"> Customer Mission Operations Compatibility Technology Design 	Technology Design	Technology Design
Staffing Strategy	Core Team Stays with Project Through Completion	Core Team Stays with Project Through Completion	Often Fill Projects with Junior Staff, and Little Senior Staff Involvement
Engineering, Computer Science, Business Expertise	Bachelor & Master's Degrees	Limited & Varies	Varies
Risk Assessment & Master Planning Expertise	<ul style="list-style-type: none"> Converged (IT, Physical, OT) Strategic & Tactical Analysis Recommendations with Context and Management Justification bSMART® Process/Software (Patent Pending) 	<ul style="list-style-type: none"> Basic or Assessor-Subjective Recommendation List Physical or Cyber only 	<ul style="list-style-type: none"> Basic or Assessor-Subjective Recommendation List Physical or Cyber only
Special Weapons and Tactics / Explosives Expertise	Federal Critical Sites & US Army	No	No
Master Planning & Strategy - Operations & Technology	Global Projects, Enterprise Scope	Limited	Yes
Systems Design	<ul style="list-style-type: none"> Enterprise-Level, Integrated Systems, Converged Cyber/Physical 	Mostly Project-Level	<ul style="list-style-type: none"> Enterprise-Level Integrated Systems
Program Management / Project Management	Formal Training & PMP Certified	Informal Training	Varies
Multi-Lingual	Spanish, French, Arabic	Uncommon	Uncommon, Varies
Global Project Experience	Project & Enterprise Level	Uncommon	Common
IT / Cyber Expertise – Design / Assessment / Strategy	Yes	Uncommon	Varies
Physical Security Systems Design Expertise	Yes	Common	Common