Following the exercise, Booz Allen led comprehensive after-action analysis reviewing the universe of exercise communications to identify trends, gaps, and areas for improvement. In partnership with NERC, Booz Allen identified key findings and recommendations that will be shared with the entire sector, leading to improvements in physical and cybersecurity plans, programs, and responder skill. As the electric reliability organization, NERC is subject to oversight by the Federal Energy Regulatory Commission and governmental authorities in Canada.

Pacific Gas and Electric Company (PG&E) Grid Security Exercise Support

PG&E, one of the largest utilities in North America, partnered with Booz Allen to conduct its first enterprise-wide cyber and physical security exercise. By participating in NERC’s GridEx II sector-wide event, PG&E was able to stress-test both its internal response capabilities and external coordination protocols. As lead support for NERC’s GridEx II, Booz Allen was uniquely positioned to partner with PG&E on participant recruitment, scenario customization, policy review, and exercise conduct.

Scenario development required the coordination of utility functional areas including electric transmission, energy procurement, gas operations, information technology (IT), human resources, and physical security. Booz Allen ensured that the scenario remained consistent with NERC’s baseline while also promoting a coordinated response within PG&E. To position the utility for success, Booz Allen conducted a comprehensive review of response doctrine and developed playbooks to reinforce incident response best practices during the exercise. The firm also conducted senior-level tabletop exercises to train PG&E staff in advance of GridEx II.

During exercise conduct, Booz Allen established a PG&E-specific control cell on-site that monitored internal exercise play, facilitated communications, and recorded critical interactions for further review.

PG&E successfully piloted activation of its Incident Command System in a cyber event and coordinated response activities across its vast enterprise. Following the exercise, the firm led a detailed after-action review that included interviews, player submissions, and communications. A visualization capability was applied to PG&E exercise interactions to identify key communications trends, gaps, and response timing. Booz Allen developed an independent after-action report that highlighted strengths, areas for improvement, and potential corrective actions. PG&E was recognized as one of the most active participating utilities during GridEx II and is allocating resources for future GridEx events.

About Booz Allen Hamilton

Booz Allen Hamilton has been at the forefront of strategy and technology consulting for 100 years. The firm provides services primarily to the US government, and to major corporations, institutions, and not-for-profit organizations. Booz Allen offers clients deep functional knowledge spanning consulting, analytics, mission operations, technology, and engineering. In 2014, Booz Allen celebrates its 100th anniversary year. To learn more, visit www.boozallen.com.

For more information, contact

David Cronin
Principal
cronin_david@bah.com
617-835-3314

Stephen Brevig
Senior Associate
brevig_stephen@bah.com
919-475-4364

John Foti
Senior Associate
foti_john@bah.com
703-902-5865

David London
Lead Associate
london_david@bah.com
703-377-7459

www.boozallen.com
Cybersecurity Strategic Simulations for Utilities

The nation’s critical infrastructure, and the evolving cyber attacks that threaten it, require the attention of key decision makers. Cyber events can have far-reaching implications on physical and information technology assets that could threaten grid reliability. This threat landscape necessitates the establishment and validation of cybersecurity thresholds, response options, and information-sharing mechanisms. Cybersecurity strategic simulations are an effective tool for assessing preparedness and identifying areas for improvement, absent the consequences of an actual cybersecurity incident. Participants can validate policies, plans, processes, procedures, and capabilities that enable preparation, prevention, response, recovery, and continuity of operations. The controlled environment allows participants to safely explore real-world situations, resulting in improved communication, coordination, and the identification of any gaps in existing response plans.

Cybersecurity Simulations Tailored for the Utility Industry’s Threat Landscape

Booz Allen Hamilton is an industry leader in the design and execution of successful cybersecurity strategic simulations. We use our proven approach to design and execute strategic simulations for utilities, resulting in actionable lessons learned for industry participants. Staff experienced in both the unique nature of cyber incidents and simulation design guide clients in establishing objectives, designing the scenario, executing the simulation, and delivering an after-action report. Our belief in the fundamental value of simulations and commitment to the success of our clients takes a tangible form—sustained dedication to the design, execution, and reporting of a simulation with world-class cybersecurity professionals, augmented by subject matter experts in cyber policy and practice.

Emergency Preparedness and Incident Response Simulation Capabilities

Discussion-Based: Discussion-based simulations like tabletop exercises allow key personnel to review simulated scenarios in an informal setting. They can be used to assess plans, policies, and procedures in a consequence-free environment. Unlike operational training events, discussion-based simulations can provide an interactive environment for clarifying cyber containment measures, identifying business-level interdependencies, and validating escalation triggers. Discussion-based exercises are conducted by seasoned Booz Allen facilitators and are supported by a technically credible scenario and accompanying materials that are customized to replicate the client environment.

Functional/Full-Scale: Functional/Full-Scale simulations are a more hands-on training experience that enable geographically distributed participation. They are generally more resource and planning intensive than their discussion-based counterpart and enable organizations to practically exercise tactical response activities. Utilities participating in Functional/Full-Scale simulations can exercise real-time information sharing, forensic analysis, and external reporting through conventional channels and workspaces. Functional/Full-Scale simulations are scalable and can involve a larger number of participants, functional areas, and external partners. These simulations generally occur over multiple days and can be conducted with participants located across multiple areas. Booz Allen supports these simulations with comprehensive scenario development, policy review, and exercise control capabilities.

Cyber strategic simulations allow electricity industry organizations to:

• Test incident response plans and procedures
• Identify reporting thresholds and critical infrastructure protection (CIP) requirements
• Understand corporate and operational network dependencies
• Build a common understanding of system constraints
• Identify elements of a resilience action plan
• Define actionable next steps and generate the urgency to address them

We understand that the value of conducting a simulation extends well beyond successful exercise execution—it is defined by the lessons learned and the momentum achieved to tackle urgent security challenges.

Proven Track Record

Booz Allen is renowned across the federal government and within the utilities sector for our strategic simulation and cyber expertise. Our work improving the nation’s cybersecurity includes engagements with large-scale public-private partnerships, Fortune 500 companies, and long-term engagements with civil government and defense agencies, and the intelligence community. In 2013, Booz Allen successfully demonstrated its ability to deliver both a large scale sector-wide exercise along with parallel utility-specific simulation support.

North American Electric Reliability Corporation’s (NERC) GridEx II

NERC is a not-for-profit entity whose mission is to ensure the reliability of the bulk power system in North America. Booz Allen was initially engaged to design and execute GridEx 2011, a sector-wide exercise to test the current readiness of the electric industry to respond to a cybersecurity incident. After the success of GridEx 2011, Booz Allen was selected to lead the delivery of GridEx II, which expanded on the first GridEx model. On November 13-14, 2013, more than 230 organizations and 2,000 participants engaged in GridEx II, making it the largest sector-specific cyber exercise ever conducted.

Throughout the two-day exercise, utilities coordinated internal response measures and shared information with government agencies and law enforcement in response to a coordinated cyber/physical attack on the grid. While no actual systems were compromised, the realistic scenario enabled a broad spectrum of players to engage in crisis response measures and enterprise-wide coordination. Existing command, control, and communication plans and tools were stress-tested, then evaluated for readiness at the local, regional, and national level. In parallel, Booz Allen hosted an executive tabletop exercise with industry chief executive officers (CEO) and senior government officials that tackled major policy challenges encountered during an attack on the grid.

Booz Allen marshaled resources and expertise from across the firm to provide end-to-end support for the engagement. Partnering with NERC, Booz Allen leveraged its extensive relationships with industry and government to exceed NERC’s recruitment goals by 150 percent. The firm applied an adaptive scenario development framework that established a core scenario foundation and enabled entity-specific customization. This promoted continuity across the broad participant set, while encouraging utilities to tailor elements for their local environment. Our understanding of both the federal and industry-specific cybersecurity threat and policy environment was applied during outreach, scenario design, and after-action phases. Booz Allen also provided all logistical and exercise control resources to register participants, monitor exercise play, maintain situational awareness, and capture critical findings.