B | RILEY Advisory Services

COMPLIANCE, RISK & RESILIENCE:

CYBERSECURITY THREATS TO INDUSTRIAL OPERATIONS

Operational risk results from the cybersecurity vulnerability of the industrial control systems (ICS) that manage automated industrial functions. B. Riley Advisory Services understands that cyberattacks on the operating technology of the transportation, mining, process manufacturing, hospital, and utility sectors can result in direct and consequential damage — to process safety and continuity, public safety, and physical assets — and can create cascading business interruption as well as casualty and liability risk. Though conventionally seen as a low-probability "air-gapped" risk, the potential for consequential impact from a security failure of embedded and process control systems makes it important to more effectively understand these risks. Devices that comprise the industrial internet of things (IIOT) are increasingly digital, connected and potentially targeted by sophisticated nation-state hackers.

UNIQUE RISK IN OPERATING TECHNOLOGY

Industrial control systems monitor and control processes that are often overlooked as potential cyberattack vectors because they have deeper layers than supervisory control and data acquisition (SCADA) displays. ICS include intelligent, electronic devices used for controlling manufacturing and equipment, programmable logic controllers and monitors, sensors, valves, motors, and device status indicators. These are critical to the safe operation of industrial and utility systems, and critical infrastructure. Industry attention to their susceptibility has often not kept pace with either the threat from determined hostile parties with sufficient intent and skill to perpetrate attacks on industrial control systems, or with the threat of an accidental or malicious employee action. These threats have the potential to disrupt systems for extended periods and precipitate significant public safety and economic crises.

SERVICES

The Compliance, Risk & Resilience practice at B. Riley Advisory Services has developed a unique mix of technical and operating insight into how threat actors (hostile nation-states, terrorist organizations, and hacktivist groups) can compromise industrial controls that operate and manage industrial processes — at the process level, the control component level, the human-machine interface level, and the SCADA system level. We help companies map their at-risk industrial component configurations and provide analysis and synthesis of the critical interfaces between operating technology and information technology. We can perform risk and asset downtime impact assessments, and develop practical policy recommendations. The goal is to enable cybersecurity experts and operating engineers to begin to correlate conventional information security anomalies with process controls events that may impact how effectively (and how safely) industrial processes operate.

We are retained to:

- Perform field-level discovery and assessments of digital ICS components that may have replaced their analog predecessors through normal procurement, comparing the as-drawn configuration against the as-installed Operational Technology (OT) environment, so management obtains an empirical picture of addressable device risk.
- Recommend remediation steps that work for both Information Technology (IT) and OT staffs.
- Recommend ICS cybersecurity scenario updates to incident response, business continuity, and crisis management plans.
- Develop and facilitate tabletop exercises and help address senior management questions about ICS cybersecurity risk.

REPRESENTATIVE ENGAGEMENTS

ICS Cybersecurity Risk Assessment for a Public Transportation Agency

We were selected via competitive bid to assess the risks to the buses, telecommunications towers, and operations and maintenance facilities, from the industrial control systems that manage physical operations. We reviewed the agency's incident response, crisis communications, emergency management, and business continuity plans considering potential ICS cybersecurity incident scenarios, and developed a framework for the specification, acquisition, and management of ICS components. The engagement concluded with a tabletop exercise to rehearse the agency's response capabilities.

Cyber Threat Assessment

We assessed the exposure of a large regional gas utility's physical transmission and distribution assets to cyber threats, developed an impact analysis of the loss of key operating components, and recommended a vulnerability remediation plan.

SCADA System Cyber Risk Assessment

We developed a SCADA-relevant IT disaster recovery roadmap for a major California water utility, including a risk assessment, gap analysis, remediation options, costs and timeframes.

THE B. RILEY DIFFERENCE

We bring a cohesive view of how disparate departments — operations, engineering, IT, safety and emergency management, compliance, crisis management, and risk management — can begin to speak the same language about control systems cyber risk, train company staff, and provide technical, operating, and crisis communications insight. We help raise the level of awareness in the C-suite and boardroom about this insidious operating risk. It is our view that awareness of ICS cyber risk should be elevated by companies well above the limited focus on compliance with those industry regulatory regimes that may not have kept pace with the offensive tradecraft used by threat actors. Industrial cyber risk is increasingly worth the consideration of senior management and the board.

PRACTICE LEADER

Duane Lohn
dlohn@brileyfin.com
(602) 321-9818

Corey Gooch
cgooch@brileyfin.com
(312) 925-8550

ABOUT THE FIRM

ABOUT B. RILEY ADVISORY SERVICES

B. Riley Advisory Services provides specialty advisory services and solutions to complex business problems and board-level agenda items. Our team applies a unique mix of skill sets to address top-level, non-typical business challenges, such as developing compliance and risk systems for organizations, planning and executing a major acquisition or divestiture, pursuing a fraud investigation or corporate litigation, or managing through a business crisis or bankruptcy. In addition, we are a leading provider of valuation and appraisal services for asset-based lending applications.

Our team works with lenders, law firms, government entities, private equity sponsors and companies of all types. Our Advisory Services are a unique mix of Compliance, Risk & Resilience Services, Valuation and Appraisal Services, Restructuring and Turnaround Management, Operations Management Services, Forensic Accounting and Litigation Support and Transaction Support Services including Due Diligence and Quality of Earnings Reviews. B. Riley Advisory Services is a combination of the firms formerly known as GlassRatner Advisory & Capital Group and Great American Group.

ABOUT B. RILEY FINANCIAL (“B. RILEY”)

B. Riley Financial, Inc. (NASDAQ: RILY) companies provide tailored financial solutions to meet the strategic, operational, financial advisory and capital needs of its clients through a diverse range of collaborative and complementary business capabilities.

B. Riley's diverse suite of business capabilities goes beyond traditional financial service offerings. By leveraging cross-platform expertise and assets, our business units are uniquely positioned to provide full service, collaborative solutions at every stage of the business life cycle and in all market conditions.