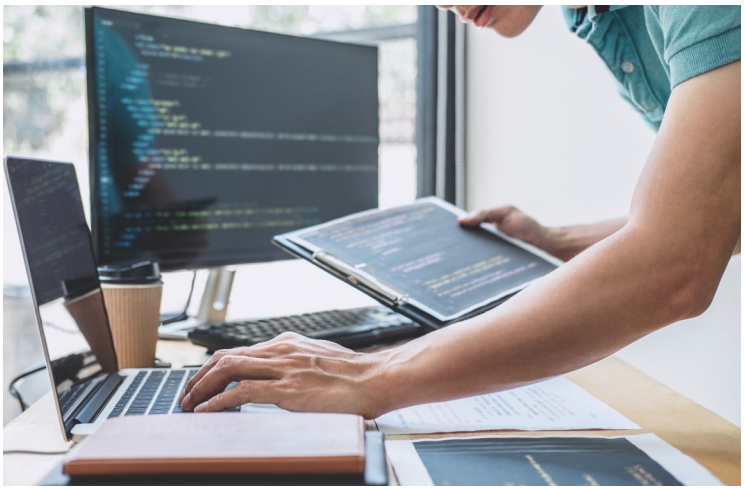
B | RILEY Advisory Services

COMPLIANCE, RISK & RESILIENCE:

23 NYCRR PART 500 & NAIC DERIVATIVE



Cybersecurity rules based on New York State's Part 500 regulation (NYCRR Part 500) and the resulting National Association of Insurance Commissioners (NAIC) Model Law impose challenges to insurers, brokers, and banks doing business in New Yok State whose information security programs may not be sufficiently robust. Part 500 and regulations like South Carolina's Insurance Data Security Act significantly raise the bar. With these regulations cybersecurity is transformed from a technical function into a governance obligation with broadly prescriptive compliance requirements and aggressive timelines.

The Compliance, Risk & Resilience team at B. Riley Advisory Services unpacks the regulatory, technical, and process elements of these rules to help clients appreciate the risks and meet compliance obligations around elements like the breadth of their non-public information, technical controls, and third party provisions.

SERVICES

We conduct compliance assessments and gap analyses, and support compliance implementation around policies and procedures, program governance, risk assessment, technical implementations, and third-party providers. We identify qualified CISOs and senior security staff. We are experienced in software security, encryption, threat detection, access control/ authentication, and continuous risk-based monitoring strategy. Our data governance experts provide insights into data retention and destruction requirements, and our resilience professionals help upgrade business continuity planning (BCP), disaster recovery (DR), cyber incident response, and crisis management plans. We assess and coach third-party service providers to meet minimum security requirements and help make compliance relevant and understandable to top management.

Our team has dissected 23 NYCRR Part 500 and its derivatives from the governance, risk, regulatory, implementation, technical, and supply chain perspectives. We help clients understand the unique challenges of these risk-based cybersecurity rules that are structured around continuous process improvement and linked to operational complexity and periodic risk assessments. We advise about the optimal order in which each provision should be addressed based on the interdependencies among them that can define the degree of difficulty, order, and elapsed time-to-implementation.

Our team has cross-walked these cybersecurity rules with National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) frameworks, the HIPAA Privacy and Security rule, and other regulations to illuminate similarities, avoid duplication of effort, and create cyber programs that meet all regulatory obligations. Governance is key to implementing cybersecurity programs that become successfully inculcated in our clients' operational fabric.

How senior management defines non-public information and what partners constitute third-party information service providers are keys to success. Organization, skill thresholds, threat awareness and review, as well as reporting systems all matter in these rules.

Senior management and the board must now come to recognize effective cybersecurity as a sober governance issue that may create personal liability and increase regulatory enforcement risk. We understand how to help technical, security and compliance executives articulate to leadership the imperatives of cybersecurity hygiene and compliance, and the regulatory optics of making a good-faith effort. We are embedded in our clients' security operations, and in assessing, advising, validating, and implementing programs. We help clients cross the certification finish line with confidence.

REPRESENTATIVE ENGAGEMENTS

23 NYCRR Part 500 Gap Analysis and Compliance Assessment
We field-assessed over 50 Part 500 covered entities controlled by a holding company, as well as its central IT department and the corporate functions that create and manage non-public information (NPI) on the information systems (IS) defined in the regulation. We mapped results to ISO 27001 and NIST Cybersecurity Framework and provided an element-level plan and staff assistance toward 23 NYCRR Part 500 compliance within a multiyear InfoSec maturity road map. We helped the client develop its policies, procedures, and controls to support its cybersecurity program.

Part 500 Risk Assessment for Specialty Financial Underwriter
We worked under privilege for the client's outside counsel to establish the risk assessment criteria defined in 500.09 for evaluating and categorizing risks, assessing the confidentiality, integrity and availability of NPI resident on in-scope IS, and establishing the requirements for accepting or mitigating identified risks. We facilitated the actual risk assessment using these criteria, and helped the client map the results to their 500.02, 500.03, and 500.07 Part 500 requirements.

Cybersecurity Program Installation for Insurance Spin-off
We were engaged to establish the initial cybersecurity program for a new insurance company. Our Office of the CISO wrote policies and procedures, conducted the risk assessment, developed the BCP, and provided program design and implementation advisory services.

THE B. RILEY DIFFERENCE

Our information security experts bring a unique perspective and know-how from their years of hands-on cybersecurity experience as entrepreneurs, specialists in the corporate environment, and as independent and Big Four consultants. We are industry credentialed and have been CISOs, CIOs, CPOs, industry speakers, faculty and authors, and standards contributors. We work in banking, healthcare, law firms, media, insurance, utilities and energy, industrial control systems, ecommerce, and transportation. Clients value the clarity and transparency we provide into their cybersecurity challenges, maturity aspirations, and compliance posture. We "unpack" complex regulations and laws with practical, goal-oriented compliance processes.

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.