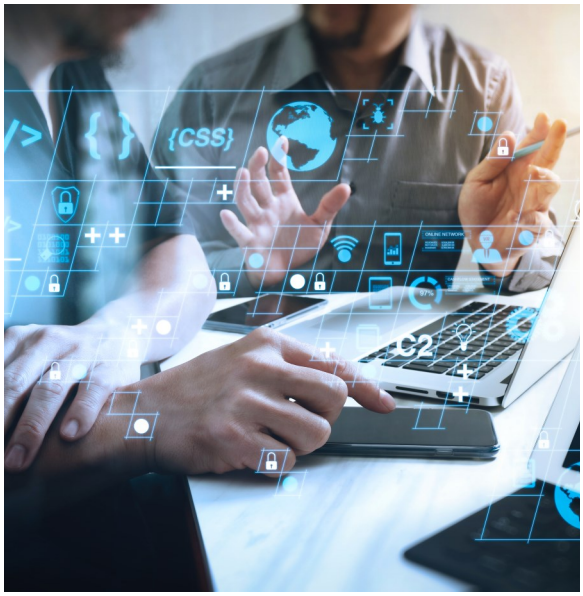
B | RILEY Advisory Services

COMPLIANCE, RISK & RESILIENCE:

INTERIM MANAGEMENT

Among the most fundamental cybersecurity risks organizations face everywhere is the global shortage of qualified, experienced security leadership. Insufficient supply of cybersecurity candidates meets a solid demand by organizations whose boards want to address their companies' cyber knowledge deficits and feel more confident in their ability to prevent, detect, respond to, and recover from increasingly consequential cyber incidents and be more confident in their compliance with changing cyber regulations. The shortage is evident from the senior level, such as Chief Information Security Officers (CISOs), and Chief Security Officers (CSOs), to the analyst level. The shortage impacts everyone in the cybersecurity ecosystem – companies, staffing organizations, recruiters and headhunters, consulting firms, government agencies, and not-for-profits. The result is hyper-competition for qualified security personnel with everyone essentially recruiting and poaching from each other.



MARKET DYNAMICS

Forbes predicts the shortfall will to grow to 3.5 million in 2021. For security staff, the problem manifests in an average of one-year terms for millennial security analysts and employment stints for CISOs that average only 18 months, as recruiters keep escalating offers that challenge companies' salary bands. This ironically does a disservice to both organizations and candidates alike because compensation escalation may be unsustainable over the long term.

OUR APPROACH

The Compliance, Risk & Resilience practice at B. Riley Advisory Services created the Office of the CISO to meet client needs for practical, flexible and cost-effective CISO-level services. We are an independent, trusted adviser providing certified, seasoned and hands-on CISOs who:

- Have the technical ability to be immediately impactful
- Understand the role in the broader context of compliance, enterprise risk management, and operational resilience
- Interpret and articulate clients' cybersecurity needs in a management and board context

Interim CISOs are available remotely and onsite - supported by a "bench" of former CISOs and senior cybersecurity specialists. We listen, observe, and test to quickly understand the cybersecurity posture in the context of the business objectives, compliance obligations and risk tolerance. Clients pay a monthly retainer, based on average days they need our CISO each week. We help clients actively identify and vet a permanent CISO to replace us and offer our institutional knowledge for up to 12 months at the end of our engagement. Our team can help with the following:

CURRENT STATE OF THE SECURITY POSTURE

- Collaborate across the organization to operationalize and enforce policies and procedures, establishing senior management as executive sponsor
- Understand the strengths and weaknesses of the organization's as-is security posture, program, and capability
- Review security assessments and assess threats, vulnerabilities and risks, ranking them around criticality
- Analyze the gaps that should be addressed

INFORMATION ASSETS

- Asset inventory and sensitive data discovery
- Data classification
- Understand and assure custodial responsibility and management for asset classes

COMPLIANCE OBLIGATIONS & STATUS

- Identify the mix of regulations, statues and standards to which the organization must adhere, some of which include:
    - 23 New York Codes Rules and Regulations (NYCRR) Part 500
    - Defense Federal Acquisition Regulation Supplement (DFARS) / Cybersecurity Maturity Model Certification (CMMC)
    - Health Insurance Portability and Accountability Act (HIPAA) / Health Information Technology for Economic and Clinical Health Act (HITECH)
    - Payment Card Industry (PCI)
    - General Data Protection Regulation (GDPR)
    - System and Organization Controls (SOC)
    - The Gramm-Leach-Bliley Act (GLBA)
    - Federal Risk and Authorization Management Program (FedRAMP)
    - Federal Financial Institutions Examination Council (FFIEC)
    - National Institute of Standards and Technology (NIST) 800 series
    - International Organization for Standardization (ISO) 270XX series
    - Control Objectives for Information and Related Technology (COBIT)
- Develop compliance roadmap
- Ensure management and board understands requirements, status and enforcement risk

SECURITY STAFFING & ORGINIZATION

- Understand the skills, experience and capabilities of the current information security team
- Identify target team and staffing adjustments to be made internally or outsourced
- Establish and manage staff training and certification program, and ensure members' knowledge of the current organization-relevant threat environment

POLICIES & PROCEDURES

- Review the policies and procedures around all relevant domains
- Edit and re-write policies, adding those missing from the portfolio
- Collaborate across the organization to operationalize and enforce policies and procedures, establishing senior management as executive sponsor

SECURITY TRAINING & AWARENESS

- Establish or upgrade organization-wide information security awareness program
- Enlist employees as “stakeholders” and re-orient them away from being “resisters”
- Enforce mandatory recurring training processes

SECURITY CONTROLS & TECHNICAL IMPLEMENTATIONS

- Regularly perform technical testing penetration tests and system scans to empirically identify and address vulnerabilities
- Establish and implement technical, operational and physical security controls commensurate with identified risks – access control and authentication, end-point monitoring, security information and event management (SIEM), intrusion-detection, data loss prevention (DLP), user monitoring, encryption, etc.

INCIDENT RESPONSE & REPORTING CAPACITY

- Assess current cyber incident response plans and practices
- Develop organization-specific incident response and management plan, with stakeholders and roles established across the entire breach lifecycle
- Ensure that incident response and forensic stand-by agreements are in place
- Facilitate regular tabletop exercises with participation of breach coach, insurance broker and underwriter, communications, legal, etc.

OPERATIONAL RESILIENCE

- Review the current business continuity plan (BCP) and IT Disaster Recovery Plan (DRP) for sufficiency
- Ensure that operational downtime impacts and costs from cyber incidents are accurately identified and quantified, noting critical dependencies and aligning the recovery time objectives (RTO) of Tier 1 applications with the DRP
- Facilitate regular tabletop exercises with participation of risk management, key operating departments and senior management

THIRD PARTIES, PARTNERS & BUSINESS ASSOCIATES

- Assess the current third-party risk management against compliance obligations
- Ensure vendor classes are appropriately identified and suppliers documented
- Execute on-going third-party risk assessment, vulnerability remediation and validation process
- Collaborate with Legal, Procurement and Compliance around purchasing policies and contractual mechanisms for managing third party security requirements

RISK MANAGEMENT

- Coordinate the controls framework and risk management process within the organization’s approach to Enterprise Risk Management
- Interface with the Risk Manager, Internal Audit, Chief Risk Officer, Chief Financial Officer and Legal to align cybersecurity and directors and officers (D&O) insurance coverage that adequately addresses key risks and exposures

GOVERNANCE & REPORTING

- Advise management on optimal reporting lines for the security organization
- Explore how to align issues, risk and incident reporting across all organization obligations
- Regularly report to the board or its risk, security or audit committee on the state of the organization's information risk management posture

REPRESENTATIVE ENGAGEMENTS

Interim CISO for Two Top 10 Insurance Brokers
We were engaged by two, high-growth brokerages to embed an experienced CISO and business continuity expert for 18 months to stabilize their security program, begin staffing, develop policies and procedures, and upgrade their defense-in-depth cybersecurity capabilities.

Virtual CISO for a Specialty Insurer
We were engaged 18 months as virtual CISO for a company recently spun out of a larger parent company, charged with setting up the security function from scratch.

Interim CISO for Manufacturing and Trading
We were engaged as part of a large-scale information security program development project, to embed an interim CISO as an "insider" to our consulting team to accelerate program speed and improve program effectiveness.

CISO Support for a Brokerage
We are engaged to provide CISO level advisory and support service to the CISO in their compliance remediation activities.

THE B. RILEY DIFFERENCE

Our interim CISOs are experienced executives who have been in the industry for years as chief information security officers (CISO) and chief information officers (CIO) - in the defense, financial services, media and other sectors. They bring senior-level, hands-on know-how, are board-ready, and can help clients stand up an information security program effectively. Our job is to replace ourselves and execute a smooth transition to a permanent candidate who takes over from our initial work.

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.