Compliance, Risk & Resilience: NETWORK, WEB & MOBILE APPLICATION SECURITY

Any application development and procurement process that does not include a rigorous security review in the critical path process is fundamentally broken. It exposes organizations to predictable, unnecessary, and avoidable cybersecurity risk, and misaligns the organization with every cybersecurity framework, regulation, and standard.

The Compliance, Risk & Resilience team at B. Riley Advisory Services includes specialists who help clients design security into every application and ensure that applications never leave the development environment for the production environment until they are security-assured.

Security-by-design should be integral to an effective software development life cycle (SDLC) and procurement process, so organizations neither develop nor purchase applications that are not approved by the information security group.

We understand why every accepted information security framework, standard, and regulation includes an SDLC process that elevates security as a determinative factor prior to software release. Our security experts help developers ensure that their web and mobile retail and e-commerce applications are developed, tested, and launched securely.

We help clients design and install an SDLC approach that elevates security to a critical path activity in software development and acquisition, as an instrumental element of the organization’s cybersecurity policy and process management — at the network, web, or mobile application levels and throughout the software acquisition process.

A best practice is for the security team to have veto authority over final production release. Many organizations use applications built by developers who are neither security-trained nor security-capable. Developers sometimes build software that may have the features, functionality, and performance demanded by users, or may be “fit for purpose,” but that may not include effective security.

Procurement departments sometimes release requests for proposals and tenders that include minimal or no cybersecurity requirements for purchased applications or software packages. Ironically, it is at the ideation and conceptualization stage of internally developed software, or at the RFP development stage for externally procured software, that security is most cost-effectively designed or specified into software. Retrofitting security after the fact can break applications, cost more, and cause organizations to miss release deadlines.
SERVICES

We help our clients appreciate the risks to their information systems and the vulnerabilities resident in their information security environments. Our independence enables us to expertly probe client systems — as insiders or external ethical hackers — to understand the vulnerabilities and potential attack vectors, and to help clients understand and close their gaps.

Services include:

• Software development life cycle process and effectiveness assessment
• Secure software development strategy and training
• Network, web, and mobile application security testing
• Software compliance with regulations and best practices
• System and source code scanning and review
• Penetration tests and ethical hacking
• Remediation oversight and validation
• Sensitive data discovery
• Industrial control systems security specifications and procurement

REPRESENTATIVE ENGAGEMENTS

Our team developed a set of specification, procurement, contractual provision, and asset management policies, procedures, and language to ensure security is emphasized in the acquisition of industrial control system components acquired by a major surface transportation agency.

Security Review for Retailer
Our team conducted a deep dive into the e-commerce applications of a global luxury retailer, and reviewed adherence to Payment Card Industry Data Security Standard (PCI-DSS) and adequacy of fraud control processes from stock keeping unit (SKU) selection to checkout. We applied white-box and black-box ethical hacking techniques to rigorously test these defenses and document our findings.

Secure Software Acquisition Findings
Our team conducted a disaster recovery tabletop exercise for a Fortune 10 financial services provider, where we discovered that the company had inconsistent and inadequate security guidelines around its software acquisitions. We provided best practices recommendations to remedy this risk.

THE B. RILEY DIFFERENCE

Our security experts are accomplished engineers and developers who have authored books on security software development and regularly present at industry events. They specialize in network and application security reviews, using ethical hacking to empirically demonstrate for our clients how their live applications may be vulnerable to internal or external compromise. We understand the SDLC process and knows how to develop this discipline and capability in organizations that historically host applications that were improperly security vetted. As part of our business continuity plan and disaster recovery process, we inventory critical applications and help clients ascribe ownership and responsibility for security.

PRACTICE LEADERS

Scott Corzine
scorzine@brileyfin.com
(917) 930-5300

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