CONFIDENTIAL

COLLYMORE CONSULTING

Cybersecurity Risk & Privacy Excellence

Cybersecurity Due Diligence & Insurance Evaluation Proposal

Comprehensive Risk Assessment for Private Equity Portfolio

Prepared for: **Fort Greene Partners**

Attention: **Mr. Nigel W. Jones, Advisor**

Prepared by: **Cylton Collymore, CEO**

Date: **November 4, 2025**

Executive Summary

Collymore Consulting proposes a limited-scope cybersecurity due diligence and insurance-aligned evaluation designed to assess digital risk, privacy posture, and control maturity for Fort Greene Partners' investment portfolio. Our assessment benchmarks controls against NIST Cybersecurity Framework (CSF) and Center for Internet Security (CIS) standards to identify key exposures and insurability gaps that could impact investment valuations and post-acquisition integration.

This engagement leverages our extensive experience with private equity firms and insurance providers to deliver actionable insights that directly inform investment decisions, risk pricing, and cyber insurance procurement strategies. Our contingent fee structure aligns our interests with Fort Greene Partners' success in identifying and mitigating cyber risks.

Scope of Work

Phase 1 – Data Room & Pre-Assessment Review — $10,000

Comprehensive review of existing documentation to establish baseline understanding and identify critical gaps. This phase includes analysis of security policies, architecture diagrams, compliance certifications, incident history, and vendor assessments. Deliverable includes a preliminary risk outline highlighting key areas of concern and documentation gaps requiring further investigation.

Phase 2 – Cyber & Privacy Control Evaluation — $25,000

In-depth evaluation of technical controls, privacy practices, and operational readiness. This phase encompasses: ransomware susceptibility testing, backup/recovery validation (RTO/RPO), identity and access management review including MFA coverage and PAM assessment, data protection and DLP effectiveness, network security and EDR/XDR deployment validation, patch management verification, incident response tabletop simulation, supply chain and fourth-party risk analysis, cloud security posture (CSPM/CASB), and regulatory compliance mapping (GDPR, CCPA, HIPAA). Includes stakeholder interviews and control validation to verify implementation effectiveness.

Phase 3 – Risk Synthesis & Insurance Readiness — $15,000

Consolidation of findings into actionable intelligence for investment decisions. This phase produces: quantitative risk modeling using FAIR

methodology, Monte Carlo breach simulations with financial impact ranges, comprehensive risk scoring matrix with KRIs, detailed mapping to cyber insurance requirements (including ransomware sublimits), remediation cost estimates with confidence intervals, post-acquisition 100-day security roadmap, M&A representations and warranties insurance considerations, and executive presentation with insurability assessment aligned with major carrier requirements (AIG, Chubb, Beazley).

Total Investment: $50,000 (Contingent upon findings and scope adjustments)

Deliverables

Cyber & Privacy Risk Report

50+ page technical assessment with quantified risk ratings, control gaps analysis, FAIR risk quantification, and prioritized remediation roadmap

Executive Summary Deck

15-slide board presentation with financial impact modeling, breach probability scenarios, and investment go/no-go recommendations

Insurance Readiness Scorecard

Detailed mapping to 12 major carriers' underwriting criteria with premium impact analysis and sublimit recommendations

M&A Risk Transfer Analysis

R&W insurance implications, indemnity caps, survival periods, and specific cyber warranty language recommendations

Ransomware Resilience Report

Dedicated assessment of ransomware defenses, backup integrity, recovery capabilities, and incident response readiness

100-Day Security Roadmap

Post-acquisition integration plan with quick wins, critical fixes, and long-term transformation initiatives

Optional Add-On Services

Limited Penetration Testing

Targeted validation of critical vulnerabilities ($15,000)

Cloud Security Audit

Deep-dive into AWS/Azure/GCP configurations ($12,000)

Forensics Readiness Assessment

> Evaluation of incident response and recovery capabilities ($8,000)

Key Assumptions & Terms

- **Advisory Scope:** This engagement provides advisory services only and does not constitute a formal audit, regulatory certification, or legal opinion
- **Media & Entertainment Focus:** For media industry targets, assessment includes content protection systems, digital rights management security, streaming infrastructure resilience, social media security posture, production workflow security, and reputational risk factors affecting cyber insurability
- **Non-Intrusive Assessment:** No intrusive testing or system modifications will be performed unless explicitly authorized in writing
- **Accelerated Timeline:** Three-week timeline assumes immediate data room access, dedicated stakeholder availability, and no significant access delays. Extensions may be required for complex environments
- **Scope Boundaries:** Base fee covers single target entity up to $500M revenue. Additional fees apply for: multiple entities (+$10K each), complex cloud environments (+$8K), regulated industries (+$12K), or global operations (+$15K)
- **Contingent Pricing:** Final fees adjusted based on target complexity. Reduction of up to 20% for simple environments, increase up to 30% for highly complex scenarios
- **Confidentiality:** All findings and materials will be treated as strictly confidential under mutual NDA
- **Resource Access:** Client will provide timely access to required documentation, systems, and personnel. Delays may impact timeline and fees
- **Travel & Expenses:** Reasonable travel expenses billed at cost plus 10% administration fee

- **Deliverable Rights:** Fort Greene Partners receives unlimited use rights to all deliverables for internal purposes and insurance submissions

Engagement Timeline

Phase 1: Data Room Review

Week 1

Documentation analysis, gap identification, preliminary risk assessment

Phase 2: Control Evaluation

Week 2

Technical assessment, stakeholder interviews, control validation

Phase 3: Risk Synthesis

Week 3

Report generation, executive briefing, recommendations delivery

Principal Consultant

CC

Cylton Collymore

MBA, CISSP, CISM – Chief Executive Officer

Mr. Collymore brings over two decades of cybersecurity leadership experience across government, Fortune 500, and private equity sectors. As the former Expert Cybersecurity Examiner for the Federal Reserve Board (Atlanta Fed), he developed and implemented risk assessment frameworks for systemically important financial institutions. His unique perspective combines regulatory expertise with practical implementation experience from leading security transformations at scale.

At the U.S. Department of State, Mr. Collymore architected and led the identity infrastructure supporting critical visa and passport databases, managing security for systems processing over 20 million transactions annually. His tenure at Meta (formerly Facebook) focused on privacy engineering and data protection initiatives, where he designed controls for handling billions of user records while maintaining regulatory compliance across multiple jurisdictions.

Currently, Mr. Collymore advises private equity firms and insurance carriers on cyber maturity assessments, risk quantification, and portfolio company security transformations. His expertise spans NIST CSF implementation, insurance underwriting criteria, M&A due diligence, and post-acquisition integration strategies.

- Former Federal Reserve Examiner
- U.S. State Dept. Identity Systems
- Meta Privacy Engineering Lead
- 20+ Years Security Experience

Insurance Readiness Framework

Our assessment aligns with leading cyber insurance carrier requirements, ensuring Fort Greene Partners' portfolio companies can secure favorable coverage terms. We evaluate against frameworks recognized by major insurers including AIG, Chubb, Hiscox, and Beazley.

Assessment Coverage Areas

Governance	Identity & Access	Data Protection
Incident Response	Network Security	Third-Party Risk
Business Continuity	Compliance Status	Content Security
Reputational Risk	Brand Continuity	Media Liability

Standards Alignment

- **NIST Cybersecurity Framework (CSF):** Complete mapping to all five core functions
- **CIS Controls v8:** Assessment against implementation groups 1-3
- **ISO 27001/27002:** Gap analysis for international compliance requirements
- **SOC 2 Type II:** Readiness assessment for trust service criteria
- **Media & Entertainment Security:** Content protection, DRM, streaming infrastructure, production workflow security

- **FCC/FTC Compliance:** For media/advertising targets requiring regulatory oversight

Why Collymore Consulting

Private Equity Focus: We understand the unique requirements of PE due diligence, including rapid assessments, value creation opportunities, and post-acquisition integration challenges.

Insurance Expertise: Direct experience with cyber insurance underwriters ensures our assessments address the specific criteria that impact premium pricing and coverage terms.

Regulatory Insight: Federal Reserve examination experience provides deep understanding of regulatory expectations and compliance requirements across industries.

Practical Approach: We focus on material risks that impact investment decisions, avoiding unnecessary technical complexity while maintaining thoroughness.

Contingent Structure: Our fee structure demonstrates confidence in our ability to deliver value and aligns our success with yours.

Media & Entertainment Expertise: Experience evaluating high-profile targets where reputational risk, content security, and brand continuity directly impact cyber insurability. We assess not just technical controls, but also the intersection of public perception, stakeholder relationships, and security posture.

Independence & Potential Conflicts

Professional Independence Statement: Collymore Consulting maintains strict independence standards for all due diligence engagements. We have no financial interest, ownership stake, or business relationships with the target entity or its principals.

Conflict Acknowledgment: We acknowledge that Fort Greene Partners may have existing relationships with target company management, board members, or other stakeholders. Any such relationships will be disclosed to Collymore Consulting prior to engagement commencement to ensure our assessment remains objective and unbiased.

Reputational Risk Assessment: For targets in media, entertainment, or high-profile industries, our assessment will include evaluation of reputational risks that may impact cyber insurance underwriting, including but not limited to: brand continuity concerns, social media crisis management capabilities, celebrity/influencer relationship dependencies, and public controversy exposure that could affect security posture or insurability.

Objectivity Commitment: Should any conflicts of interest be identified during the engagement, Collymore Consulting will immediately disclose such conflicts and work with Fort Greene Partners to determine appropriate mitigation measures or engagement termination if necessary.

Next Steps

1. **Review & Discussion:** Schedule a call to review this proposal and address any questions
2. **Scope Refinement:** Adjust assessment focus based on specific portfolio company or acquisition target
3. **Engagement Letter:** Execute formal agreement with detailed terms and conditions
4. **NDA Execution:** Complete mutual non-disclosure agreement for data room access
5. **Kickoff Meeting:** Align stakeholders on timeline, deliverables, and communication protocols

© 2025 Collymore Consulting. All rights reserved. This proposal is confidential and proprietary.
909 Rose Ave, Suite 400, North Bethesda, MD 20852
Contact: Cylton Collymore, CEO | cylton@collymoreconsulting.com