



M&A; CYBER DUE DILIGENCE

DISCOVER. EXPLOIT. DEMONSTRATE.

Adversarial technical assessment designed to uncover exploitable security exposure before it becomes acquisition risk.

LOOK BEYOND THE QUESTIONNAIRE.

LCSG evaluates acquisition targets from an attacker's perspective - identifying externally and technically observable weaknesses that may affect valuation, integration planning, contractual protections or post-close risk.

Technical Due Diligence Through an Adversarial Lens

Traditional cyber due diligence often relies heavily on questionnaires, policy review and representations made by the target organization. Those inputs have value, but they do not necessarily establish what an attacker can actually reach or exploit. LCSG adds a hands-on technical perspective.

ATTACKER PERSPECTIVE

Assess the target as an adversary would, looking for exposed systems, weak controls and exploitable paths rather than relying solely on declared security posture.

TRANSACTION FOCUSED

Prioritize issues that could materially influence transaction risk, valuation, warranties, remediation obligations or integration planning.

EVIDENCE BASED

Where authorized, validate significant weaknesses to distinguish theoretical exposure from practical exploitability.

TIME CONSCIOUS

Focus effort on the attack paths and technical risks most likely to matter within the compressed timelines of a transaction.

The objective is simple: understand the security exposure you may be acquiring.

Security Exposure Across the Acquisition Target

The precise scope depends on transaction stage, authorization, available access and the sensitivity of the acquisition. Testing can begin externally and expand into deeper technical assessment where appropriate.

EXTERNAL ATTACK SURFACE Internet-facing applications, APIs, cloud services, remote access, exposed infrastructure, forgotten systems and other reachable assets.	APPLICATIONS & APIs Authentication, authorization, business logic, data exposure and exploitable implementation weaknesses in critical applications and services.
IDENTITY & ACCESS Authentication architecture, privileged access, federation, token handling and identity weaknesses capable of increasing compromise impact.	CLOUD & INFRASTRUCTURE Externally reachable cloud resources, permissions, service relationships, exposed management interfaces and infrastructure weaknesses.
SENSITIVE DATA EXPOSURE Evidence that customer, employee, intellectual property or other sensitive information may be accessible through exploitable weaknesses.	ATTACK PATHS Combinations of weaknesses that allow an attacker to move from an exposed foothold toward systems, privileges or data of material importance.

Useful Before, During and After Close

Adversarial cyber due diligence can support different decisions at different stages of a transaction. The engagement can be structured around the information and authorization available at each point.

PRE-TRANSACTION

External and authorized technical assessment can identify visible security exposure before deeper access to the target is available.

DILIGENCE

Where access is granted, focused penetration testing can validate controls, investigate high-value systems and establish the significance of identified weaknesses.

DECISION SUPPORT

Material findings can inform valuation discussions, transaction terms, remediation commitments, warranties, insurance considerations and integration planning.

PRE-CLOSE REMEDIATION

Critical exposures can be prioritized for correction before ownership changes or systems become interconnected.

POST-CLOSE VALIDATION

Focused testing can confirm remediation and identify attack paths created by new trust relationships, identity integration or infrastructure connectivity.

INTEGRATION RISK

Technical findings can help prioritize which systems should - or should not - be connected to the acquiring organization's environment.

Acquisition Security Experience That Predates LCSG

LCSG's M&A; Cyber Due Diligence capability draws on founder Mark Litchfield's extensive offensive security and acquisition-assessment experience developed over more than 25 years in the security industry.

MICROSOFT ACQUISITION DUE DILIGENCE EXPERIENCE

While co-founder of NGS Software, Mark Litchfield performed technical cyber due diligence in connection with Microsoft acquisitions. That historical work was conducted through NGS Software - not LCSG - and provides relevant founder experience behind LCSG's present-day M&A; capability.

That background shapes an approach centered on technical reality: determine what is exposed, establish whether it is exploitable, and explain why it matters to the transaction.

Use AI to Move Faster - Not to Replace Judgement

Transaction timelines can be compressed and target environments can be large. LCSG uses AI to accelerate correlation and technical analysis while experienced testers determine which exposures are credible, which paths deserve investigation and which findings are material to the deal.

AI CAN ACCELERATE

- Attack-surface correlation
- Application and API analysis
- Large technical dataset review
- Pattern and anomaly identification
- Research and hypothesis generation

EXPERIENCE DIRECTS

- Materiality and prioritization
- Selection of meaningful attack paths
- Controlled exploit validation
- Transaction-context interpretation
- Communication of technical risk

25+ YEARS OF OFFENSIVE SECURITY EXPERIENCE

AI can increase the amount of information assessed within a transaction window. Experience determines what that information means to the acquisition.

Technical Findings in Transaction Language

The output is designed to support both security teams and transaction decision-makers. Technical depth is preserved, but significant findings are also explained in terms of the exposure they introduce to the deal.

EXECUTIVE RISK SUMMARY A concise view of significant technical exposure, material attack paths and issues that warrant transaction-level attention.	TECHNICAL FINDINGS Detailed evidence of validated weaknesses, affected assets, exploitation conditions and recommended remediation.
ATTACK-PATH ANALYSIS Explanation of how individual weaknesses combine and what an adversary could ultimately access or control.	TRANSACTION CONSIDERATIONS Identification of findings that may warrant pre-close remediation, contractual treatment, additional diligence or integration controls.
REMEDIATION PRIORITIES A prioritized technical action plan separating immediate exposure from issues that can reasonably be addressed after close.	POST-CLOSE ROADMAP Where requested, a focused plan for validation, remediation and secure integration following completion of the transaction.

KNOW THE EXPOSURE BEFORE IT BECOMES YOUR EXPOSURE.



DISCOVER. EXPLOIT. DEMONSTRATE.

Adversarial technical due diligence backed by decades of offensive security experience and historical acquisition-assessment work.

M&A; CYBER DUE DILIGENCE | PENETRATION TESTING | RED TEAM OPERATIONS

VULNERABILITY RESEARCH | GOVERNMENT CYBER CAPABILITIES

LCSG.US

LITCHFIELD CYBER SECURITY GROUP