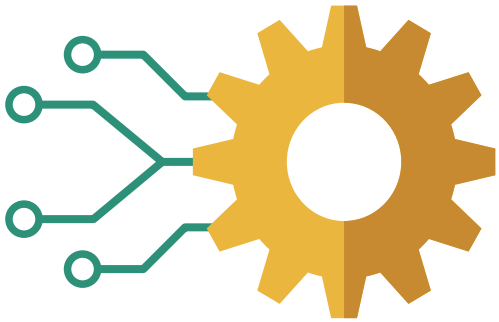
#ForensicPerspectives

Mitigating M&A cyber risk: pre- & post-acquisition due diligence



Robust cybersecurity due diligence on a potential target is imperative in the face of escalating cyber threats and regulatory expectations. Comprehensive pre- and post-acquisition due diligence helps safeguard the buyer's investment by identifying and mitigating information security risks associated with the transaction. This includes defining and implementing minimum standards for an acquisition not immediately integrated.

Why M&A cybersecurity due diligence?

1. Serves as a crucial risk mitigation tool to uncover undisclosed breaches and better assess the time and cost required to bring target up to defined information security standards.
2. Provides leverage in negotiations for purchase price adjustments and additional representations/ warranties by the seller.
3. Identifies ways to reduce insider threats, stemming from potential job security concerns of target's employees.
4. Positions the buyer to capitalize on the Self-Disclosure Compliance Safe Harbor Policy from the U.S. Department of Justice.
5. Reduces regulatory and third-party litigation exposure to the buyer, as well as whistleblower risk.

Representative cyber due diligence work streams pre-acquisition

Work streams	Business reason
Security gap review	Validate information security-related responses to current standard buyer information security questionnaires.
IT asset visibility and security hygiene snapshot	Create inventory of digital assets to understand potential risks of compromise.
Open-source intelligence	Detect and mitigate active threats, vulnerabilities, and reputational risks.
Microsoft Office (email) hygiene review	Reduce risk of a breach incident at target by identifying controls requiring immediate modification through review of security settings.
Dark web intelligence review	Uncover early indicators of cyber-attacks, data breaches, and unauthorized exposure.
External vulnerability scan	Identify potential entry points for cyber attacks proactively.
Active directory review	Detect misconfigurations, unauthorized access, and potential weak points; create work plan to correct immediately upon acquisition.

CRA Charles River Associates

Mitigating M&A cyber risk: pre- & post-acquisition due diligence

Representative cyber due diligence activities post-acquisition

Work streams	Business reason
Ransomware readiness	Examine the company's ability to restore from backups.
Vulnerability/penetration testing	Test system's weaknesses to identify potential cyberattack entry points.
IT security hygiene review	Identify and address security weaknesses, misconfigurations, and vulnerabilities; align with current security best practices.
Compromise discovery	Search for signs of unauthorized access, malware, or other security incidents.
Red team simulation	Test security defenses and incident response capabilities by simulating real-world cyber-attacks and identifying vulnerabilities and weaknesses.
Cloud security review	Assess and enhance the security of data and applications stored in the cloud.
Data inventory and classification	Identify and classify sensitive data to understand the risks associated with potential data breaches.

We invite you to reach out to continue the conversation around ways to reduce information security risk associated with a transaction, and/or other forensic areas of interest, such as fraud, theft of trade secrets, cybercrime, accounting irregularities, export controls and sanctions compliance, anti-bribery and corruption, and anti-money laundering.

About CRA

CRA's award-winning Forensic Services Practice leverages the experience derived from conducting thousands of cyber incident response investigations to help clients proactively reduce business and compliance risk, including cyber risk. Recent accolades include being named CrowdStrike's Americas Engagement Licensing Program *Partner of the Year* and Tanium's Information Security *Innovation Partner of the Year*. Numerous colleagues have been recognized by *Who's Who Legal* and included in *The Consulting Report*'s list of "Top Cybersecurity Consultants."

Contact

Aniket Bhardwaj, GREM, GCIA, GNFA, GCFA | Vice President, Forensic Services
+1-416-323-5574 | abhardwaj@crai.com