Practical Cyber Due Diligence for Investors

Executive Thought Leadership Series
A Practitioner's View
Introduction Paper

Author: Michael J. Loginov

About this Series

Cyber due diligence has become a standard component of mergers, acquisitions and investment decisions. However, many commercially significant cyber risks remain consistently overlooked because traditional diligence approaches were designed for enterprise IT rather than modern digital and industrial businesses.

The CAGI Insights series, Practical Cyber Due Diligence for Investors, is a collection of twelve executive short papers written for investment directors, deal partners, boards and corporate development teams. Each paper focuses on one material issue that influences enterprise value, transaction risk and post-acquisition resilience.

Papers in the Series

1. What Cyber Diligence Misses in Industrial and OT Heavy Targets
2. Why Good Cyber Reports Still Miss Material Deal Risk
3. Cyber Risk That Never Appears in the Data Room
4. The Hidden Cost of Third Party and Supply Chain Trust
5. AI Due Diligence, Beyond the Hype
6. When Cyber Becomes an EBITDA Problem
7. The First 100 Days After Acquisition
8. Operational Resilience as Enterprise Value
9. Ransomware, Recovery and Deal Economics
10. Cyber Warranties That Actually Matter
11. Separating Security Theatre from Material Risk
12. The Future of Cyber Due Diligence in Private Equity

Each paper is designed to be read independently in under fifteen minutes while forming part of a coherent reference series for executives responsible for investment decisions.

The basis of this series

Everything in these papers is a practitioner's view. The observations, judgements and recommendations are drawn from my own work over some thirty years in cybersecurity, across approximately sixteen senior security leadership appointments and more than 140 executive cyber maturity and risk assessments, in industrial, financial, government and sovereign-scale environments.

This is not vendor research and it is not a survey. Where a figure is illustrative it is stated as such. Where an engagement is described it is anonymised or fictionalised, and no client information appears in any paper in this series. Where I rely on an external source or a published framework, it is named so that you can weigh it yourself.

Why that matters

Cyber due diligence is an area where confident general advice is easy to give and hard to act on. These papers take the opposite approach. Each argument comes from having run the estates, commissioned the work or defended the findings in the room, and is offered on that basis rather than as settled industry consensus.

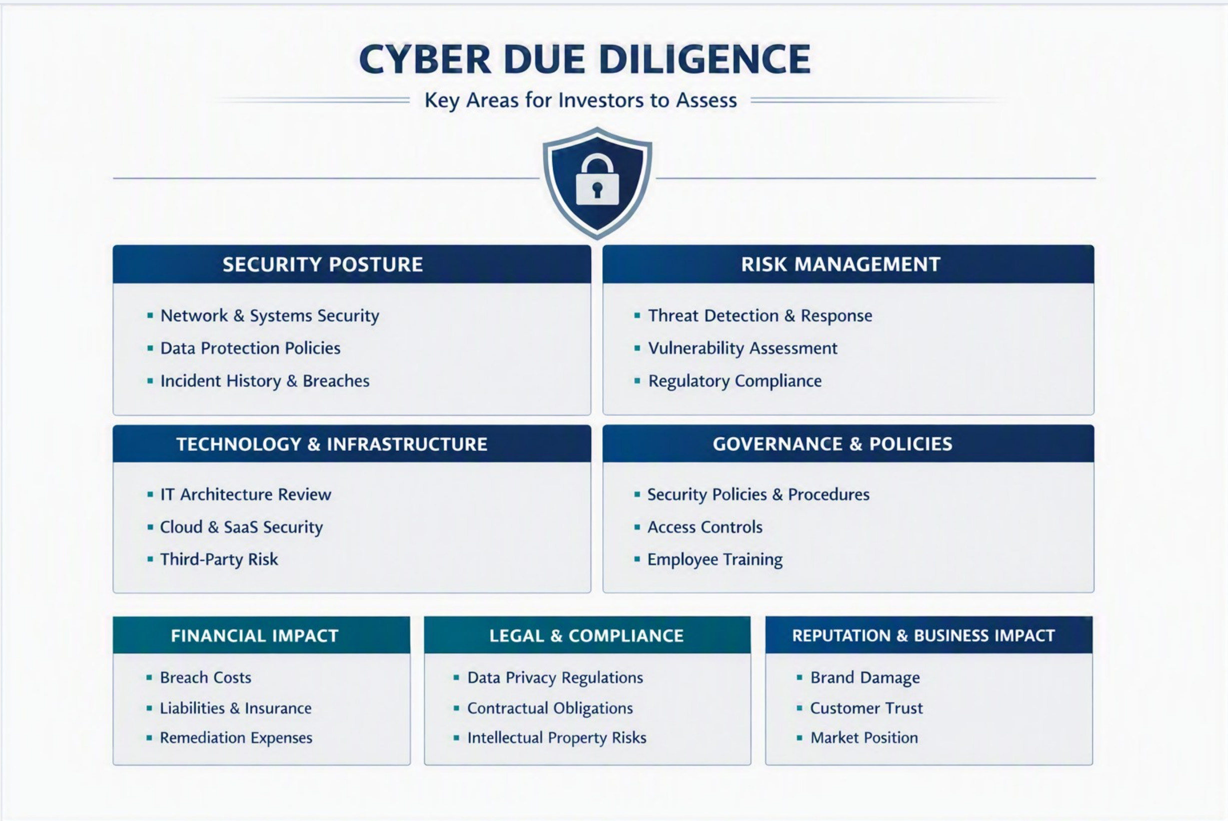

Figure. Cyber due diligence: the areas investors need assessed across the estate.