



Portfolio Cyber Healthcheck

Thomas Murray's Portfolio Cyber Healthcheck is a rapid, cost-effective way of identifying the current cyber security posture of your portfolio companies, including any potentially critical issues. It combines cutting edge technology, expert insight and an efficient managed service with our unparalleled industry data.

Within 2-4 weeks you will have an objective assessment of each of your portfolio companies, benchmarked against each other as well as against their industry peers, with a roadmap highlighting key areas of risk and recommended next steps.

Baseline your portfolio companies' cyber security and identify key risks

Uncover critical risks in your portfolio

The Cyber Healthcheck is the fastest way for a Private Equity firm to identify the companies in their portfolio that are most vulnerable to cyber-attacks. It is the perfect starting point for Private Equity firms looking to take cyber security seriously in an increasingly complex threat landscape.



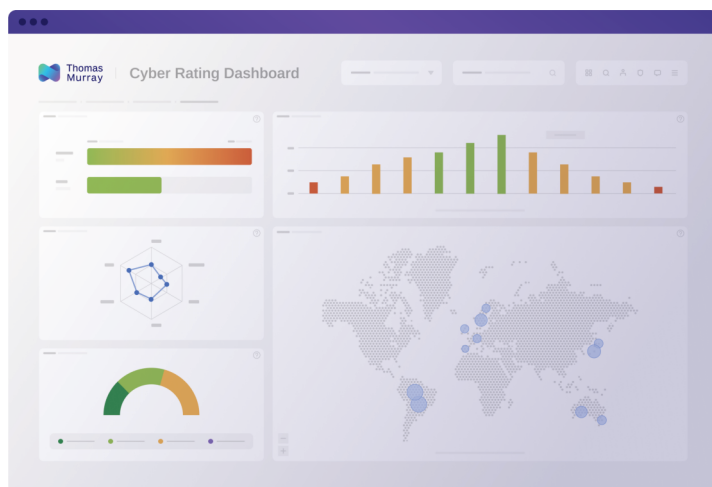
Alternative investment firms
now face more than
200,000 cyber threats daily



Annual losses to the
industry are estimated to
reach **\$100 billion**



Firms taking proactive cyber
security measures recover
from incidents in **7 days**,
compared to **90 days** when
unprepared



Why Thomas Murray?

We specialise in helping our clients reduce their operational and cyber risk exposure. This solution is tailored for small and medium sized alternative investment managers, but is informed by our work with asset owners and allocators – including major Sovereign Wealth Funds (SWFs) – who are increasing their scrutiny of external managers' cyber security.



Key features

01 Internal

Critical Controls

Assess whether the highest-impact security measures are in place



- Short questionnaire to each portfolio company will establish if key protections are in place
- Standardised to ensure a minimum baseline of security across all portfolio companies
- Aligned to cyber insurance and regulatory requirements

02 Perimeter

External Security

See what the hackers' see - an outside-in assessment of each portfolio company



- AI-powered assessment of each portfolio company's internet exposure
- 0-1000 risk rating based on breaches, vulnerabilities and misconfigurations
- Deep, automated analysis by industry-leading Orbit Security platform

03 External

Threat Context





Is this company likely to be targeted by cyber criminals?



- Is there chatter about this company?
- Is this industry being targeted?
- Is this country being targeted?
- What are the common attack methods?
- What mitigations need to be in place?

Portfolio Cyber Risk Report

You will receive:

-  A summary report with a Red, Amber, Green (RAG) assessment of each portfolio company, benchmarked against its industry peers, and a prioritised list of risks that need to be addressed across your portfolio.
-  A tailored report for each portfolio company, summarising its cyber security posture with a list of recommended remediations in priority order.
-  A debrief, in-person or online, with our experts, to present the findings, answer questions, and recommend next steps.
-  Ongoing access to Orbit Security for three months, monitoring the external cyber security posture of your portfolio companies, with weekly updates regarding new breaches and vulnerabilities. Every portfolio can be given their own credentials.



Next steps

Portfolio Cyber Risk Assessment and Monitoring

1

A robust assessment of your Portfolio Companies' cyber security

- Full questionnaire, aligned to industry and regulatory frameworks
- Answers validated and analysed using proprietary methodology
- Reporting includes in-depth remediation roadmap for every PortCo and ongoing engagement
- Ongoing monitoring using Orbit Security
- Demonstrate cyber security to regulators and allocators

Portfolio Company Cyber Improvement Programme

2

Long-term engagement with PortCos to enhance security

- Policy development (e.g. incident response, business continuity)
- Training & awareness (e.g. phishing)
- Vulnerability Scanning
- Penetration Testing
- Incident Response table-top exercises
- Ongoing reporting to PE owners regarding improvements

Due Diligence as a Service (DDaaS)

3

Assess cyber security as part of diligence during acquisitions

- External assessment of prospective acquisitions (without their participation / knowledge)
- Managed cyber due diligence during acquisition – efficient service evidencing current security posture and actions that companies are taking to reduce cyber risk

About Thomas Murray

Thomas Murray is a leading provider of risk and cyber security services to some of the world's largest asset managers, allocators and other financial institutions.

We partner with clients to deliver end-to-end cyber security support across their company and their portfolio, so that they can focus on value creation.

Get in touch

Take the next step in safeguarding your firm and its portfolio companies. Speak to one of our friendly experts today.



Roland Thomas

Director, Cyber Risk

rthomas@thomasmurray.com

+44 (0)20 8057 7187