Beneath the Asset

Out of Sight: The State of Cybersecurity in the Private Equity Industry

Thomas Murray

Risk Intelligence | Due Diligence | Cybersecurity

This study explores the first ever data-driven cybersecurity analysis of 500+ leading players in the Private Equity industry. Thomas Murray's analysts reveal some of the key risks which could impact investors' assets in 2026-27.

29%

of PE firms score below 'good', the normal trigger for escalation

1 in 16

firms are high risk - critical

-21%

the average security deficit of firms with at least one publicly-exposed software vulnerability

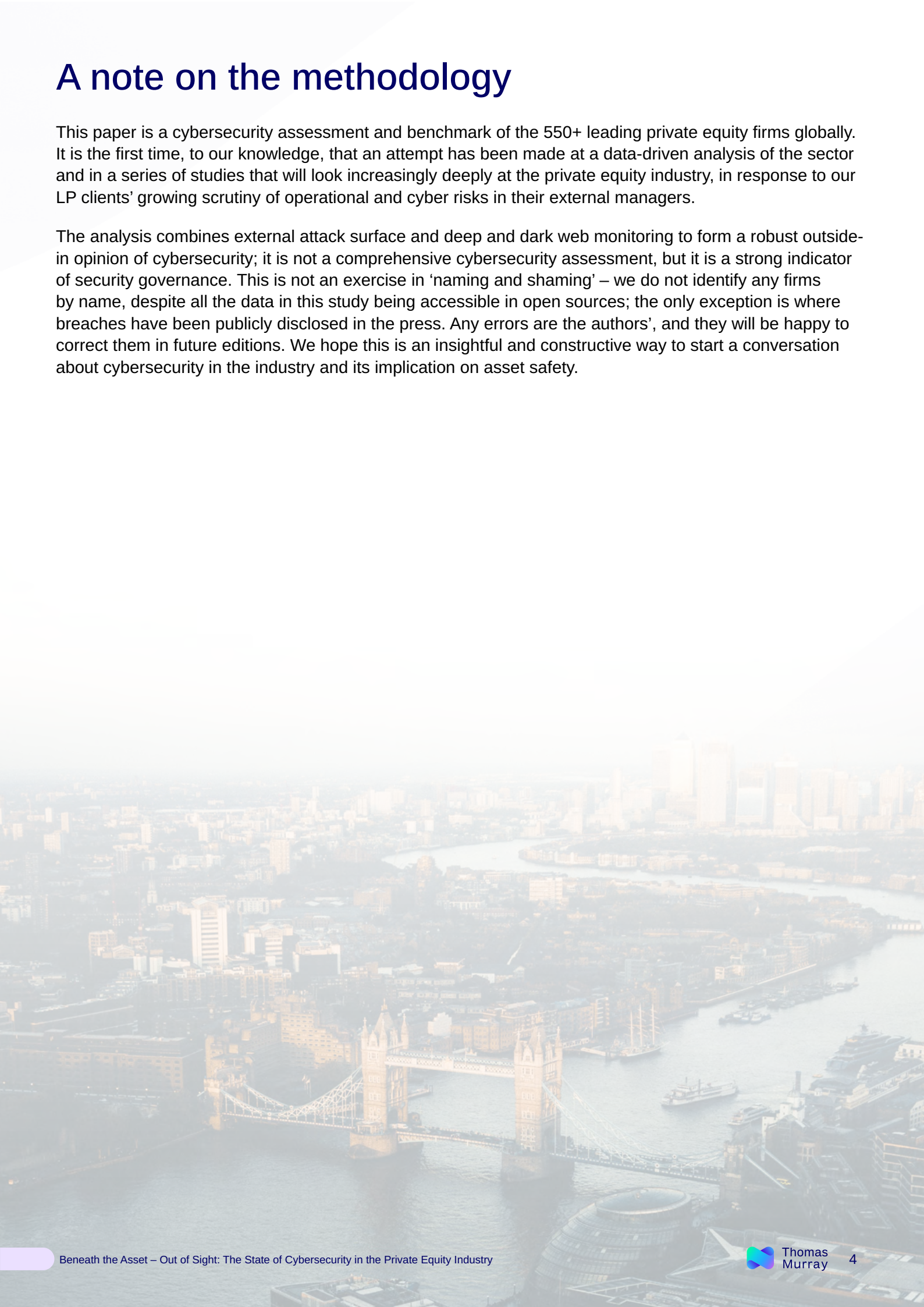
$2.87tn

assets managed by firms with below-expected security

A note on the methodology

This paper is a cybersecurity assessment and benchmark of the 550+ leading private equity firms globally. It is the first time, to our knowledge, that an attempt has been made at a data-driven analysis of the sector and in a series of studies that will look increasingly deeply at the private equity industry, in response to our LP clients' growing scrutiny of operational and cyber risks in their external managers.

The analysis combines external attack surface and deep and dark web monitoring to form a robust outside-in opinion of cybersecurity; it is not a comprehensive cybersecurity assessment, but it is a strong indicator of security governance. This is not an exercise in 'naming and shaming' – we do not identify any firms by name, despite all the data in this study being accessible in open sources; the only exception is where breaches have been publicly disclosed in the press. Any errors are the authors', and they will be happy to correct them in future editions. We hope this is an insightful and constructive way to start a conversation about cybersecurity in the industry and its implication on asset safety.



INTRODUCTION

Size buys protection, but comes with baggage

One myth this study dispels is that size buys cyber maturity. This is often the case, but there are too many exceptions to be complacent. One firm, which we have not named in this study, manages over $150 billion. It is one of the largest and most recognisable names in private equity, the kind an institutional investor would assume is safe by reputation alone. In our cybersecurity index, covering 550+ buyout firms, this one ranks near the very bottom: worse than firms with 1% of its AUM. Its investors almost certainly do not know, because managers' cybersecurity is not yet routinely assessed by LPs. This is the gap we plan to close in 2026-27.

Thomas Murray scored the external cybersecurity of 558 firms, giving each a 0-1000 score based entirely on externally available data, with no access to the firms themselves. The picture is uneven, and the risks are not where most LPs would expect. Nearly three in ten firms (29%) score below the 'good' line: the level below which we advise our clients to escalate. One firm in sixteen sits deep in the tail, scoring below 500/1000, in the kind of exposed position that tends to precede an incident. A single exposed, unpatched vulnerability moves a firm's score more than any other factor we measured. 39% of the very largest firms carry a critical or high-severity dark web finding.

A note on the scale, once: external posture runs 0–1000, in five bands: *very poor* (0–200), *poor* (201–400), *adequate* (401–600), *good* (601–800) and *very good* (801–1000). The line that matters is 601; this is the floor that most of our clients set for their external managers. It is remarkable how many firms fail to meet it, and how few assumptions survive scrutiny. This paper has identified several security trends that LPs should note, but it is also honest about the hypotheses that have not survived investigation.

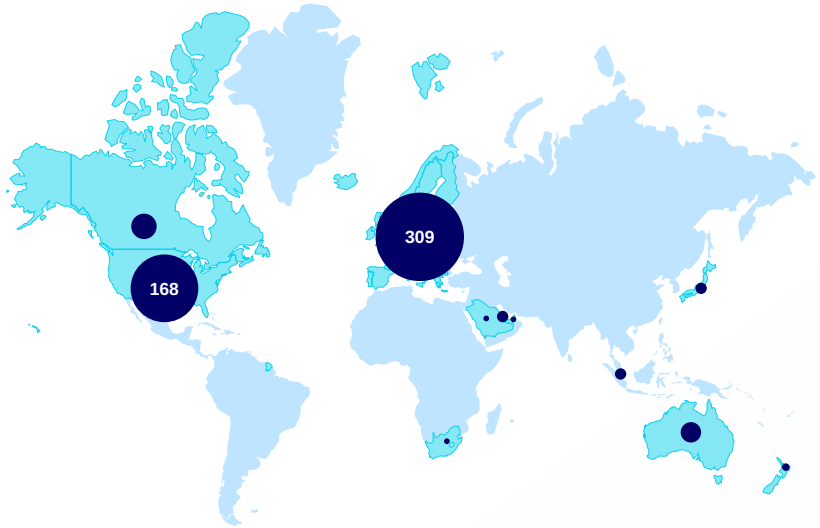


Figure 1. Headquarters of the 558 PE firms analysed. Bubble size = number of firms. The US (168) and UK (102) dominate, with a dense European cluster. Firms have been chosen by AUM, which explains the lack of geographical diversity in this paper; the GCC has a proliferation of early-stage managers, for example, but they do not meet the AUM threshold for our first study.

THE SIZE PARADOX

A firm's size is the single biggest observable driver of cybersecurity posture. Larger firms defend their external perimeter better, but their employees are far more exposed on the dark web. No other trend in this paper is as clearly established. The implication is that large firms have invested heavily in cybersecurity at a technical level, but this investment has not seeped into employee training and culture. In most industries this would be worrying; in private equity it is a tangible risk because of the critical roles played by these employees from deal origination to transaction and value creation.

CASE-STUDY: WHEN THE WORST HAPPENS

Insight Partners: data breach affecting 12,000 staff and LPs

Before the key findings of our study, we wanted to reflect on what is actually at stake. Many in the alternative investment industry downplay the real world impact of a cyber attack on their investments, believing that the risk is insured or otherwise mitigated. But this attitude neglects the impact that a cyber attack can have on cashflow, reputation, regulatory action, investment holding periods and much else besides.

One example is Insight Partners' 2024-25 data breach. In January 2025, the global venture and growth firm Insight Partners, which manages more than $90 billion, disclosed that it had been breached through a sophisticated social engineering attack. The 'unauthorized third-party' accesses Insight information systems, including 'certain fund, management company, and portfolio company information, banking and tax information' as well personal information related to current and former employees, before the incident was contained in January 2025.

In regulatory filings the firm confirmed the breach affected more than 12,000 people.

Insight is not alone: two other well-known venture firms – Advanced Technology Ventures and Sequoia Capital – suffered breaches touching LP data back in 2021. Much more recently, Apollo Global Management disclosed a breach in August 2026.

Why this is a nation-state problem, not just a criminal one

Venture capital and growth equity firms have a different and, we believe, more acute problem than private equity when it comes to cybersecurity. Early-stage companies in IP-rich industries like Bio Tech, Defence Tech or AI often have inadequate legal protection for their IP, and frequently have inadequate security in place. Our study has shown that VCs (and, when we've dug deeper, their portfolio companies) have a weaker perimeter, on average, than their private equity peers. Entrepreneurs and investors in this ecosystem sometimes think they achieve 'defence through obscurity', but this is to misunderstand the value of their companies. Cyber criminals are usually interested in cash, but threat actors are not always mere criminals. Nation states who want the technology or IP and have both the resources and patience to attain them are among the most sophisticated and, for an investor, worrying actors in the cyber threat landscape. The Five Eyes intelligence alliance (UK, US, Australia, Canada, New Zealand) has issued a joint public warning about a sharp rise in state-backed efforts to steal competitive advantage from emerging-technology companies; the UK's domestic security service calls the contest particularly acute in AI, quantum computing and synthetic biology: precisely the categories venture capital exists to fund.

Europe's bet on tech, and the hole in its defence

Mario Draghi's 2024 report on European competitiveness (now the blueprint behind the European Commission's "Competitiveness Compass") identifies a shortage of venture and growth capital as a central reason Europe trails the US and China on innovation, and calls for roughly €800 billion a year in additional investment, and singles out a shortage of venture and growth capital as a key gap. The uncomfortable overlap: Europe's growth strategy depends on channelling far more capital into exactly the category of firm intelligence agencies say is already being targeted; and, on our numbers, the identifiable European venture firms sit below the wider sample on security.

PART ONE | SCALE

Scale buys security, but not safety

The clearest pattern in the data is a steady climb in external security as funds manage more money. The smallest managers (below $1bn AUM) average around 620/1000 in our methodology (*adequate*, but not strong) while the largest funds ($100bn+) average c.715/1000, comfortably inside the good band and about 15% higher than their smaller peers. Put in threshold terms: only around one in eight of the largest firms scores below good, against roughly a third of the smallest. The obvious explanation is that larger firms can afford dedicated security teams, enterprise tooling and mature IT, but this over-simplifies the picture. The divergence could also be explained by a few differences we observe in the way larger and smaller funds manage their IT: in-house vs outsourced. Smaller PE firms almost exclusively, in our experience, rely on IT managed services providers; these MSPs deliver, to different extents, on their core responsibility for IT performance, but security frequently falls between the cracks. PE firms assume their MSP will 'look after' security, and MSPs won't do anything outside of their core remit without being explicitly asked.

This might only account for a small portion of the security gap between large and small firms, but it illustrates that operating model and accountability matters as much as budget when it comes to cybersecurity.

Bigger firms build better walls, and paint a bigger target on their backs.

We looked beyond perimeter security, where bigger firms are more robust, and into the dark web. Here, the data told a different story. The same huge funds that have the most technically robust external attack surface are, by a wide margin, the most exposed on the dark web: 39% of $100bn+ AUM managers carry at least one critical- or high-severity finding such as breached employee credentials, compared with almost none of the smallest firms. This is unsurprising, as older firms with a higher headcount are generally more likely to have experienced a breach, especially via a third party.

Where the best and worst scorers cluster

US and UK firms are over-represented in this study just as they are in the industry. The top scores are therefore almost exclusively from these countries; but two countries perform well relative to their size. Denmark and Canada punch above their weight, both averaging in the good band for perimeter security and among the highest of any well-represented geography. At the other end, PE firms in Japan and Luxembourg performed badly, averaging only adequate; Japan due to genuine weaknesses in firms' external security, and Luxembourg due to the thin digital footprints of funds domiciled in the country.

PART TWO | CONCENTRATION

The $2.87 trillion problem: where the risk actually concentrates

Averages can be reassuring in a way that obscures the real question. But LPs reading this paper are not interested in whether large managers score well on average; rather, they want to know how much of their money sits with firms that are weaker than they should be. The answer is $2.87 trillion, spread across 108 firms: one in five managers in the study.

Some of these are exactly the kind of firm an institutional investor would assume is safe by reputation alone. The seven weakest-scoring firms among those managing $25bn or more illustrate the danger of complacency:

AUM	Attack Surface Score (0-1000)	Band	Worst dark-web finding
$180bn	273	Poor	Moderate
$95bn	463	Adequate	Moderate
$65bn	489	Adequate	Worst Possible
$40bn	501	Adequate	Low
$37bn	429	Adequate	Moderate
$30bn	470	Adequate	Low
$25bn	503	Adequate	Moderate

Table. Large PE firms ($25bn+ AUM) with the weakest independent security scores, identified only by AUM, score and band. Every firm here sits below the 'good' line (601); the weakest is in the 'poor' band.

The weakest firm here scores 273/1000 – in the poor band, close to the floor of the dataset and in the bottom 5% of firms measured – despite managing c.$180bn across c.90 operating companies. Another combines an *adequate*-band score with the single worst dark web exposure finding in our study.

None of this proves an active breach is under way; these are point-in-time hygiene and history scores, not confirmed incidents. But a $180bn firm with an external security posture this weak would not pass a standard vendor risk assessment in the wider financial services industry. Private equity firms are not yet subject to the same scrutiny, but Operational Due Diligence (ODD) teams within the major institutional investors are beginning to take cybersecurity more seriously.

Some LPs invest in domestic or early-stage funds in order to gain exposure to genuinely innovative companies and to support less established firms; they do so with a clear risk appetite and with their eyes open. The story here is quite different. Cyber risk is not contained in the smaller firms alone; a fifth of the market's assets sit with firms that are big enough to invest in security, but appear weak enough to worry about.

PART THREE | THE DANGER BAND

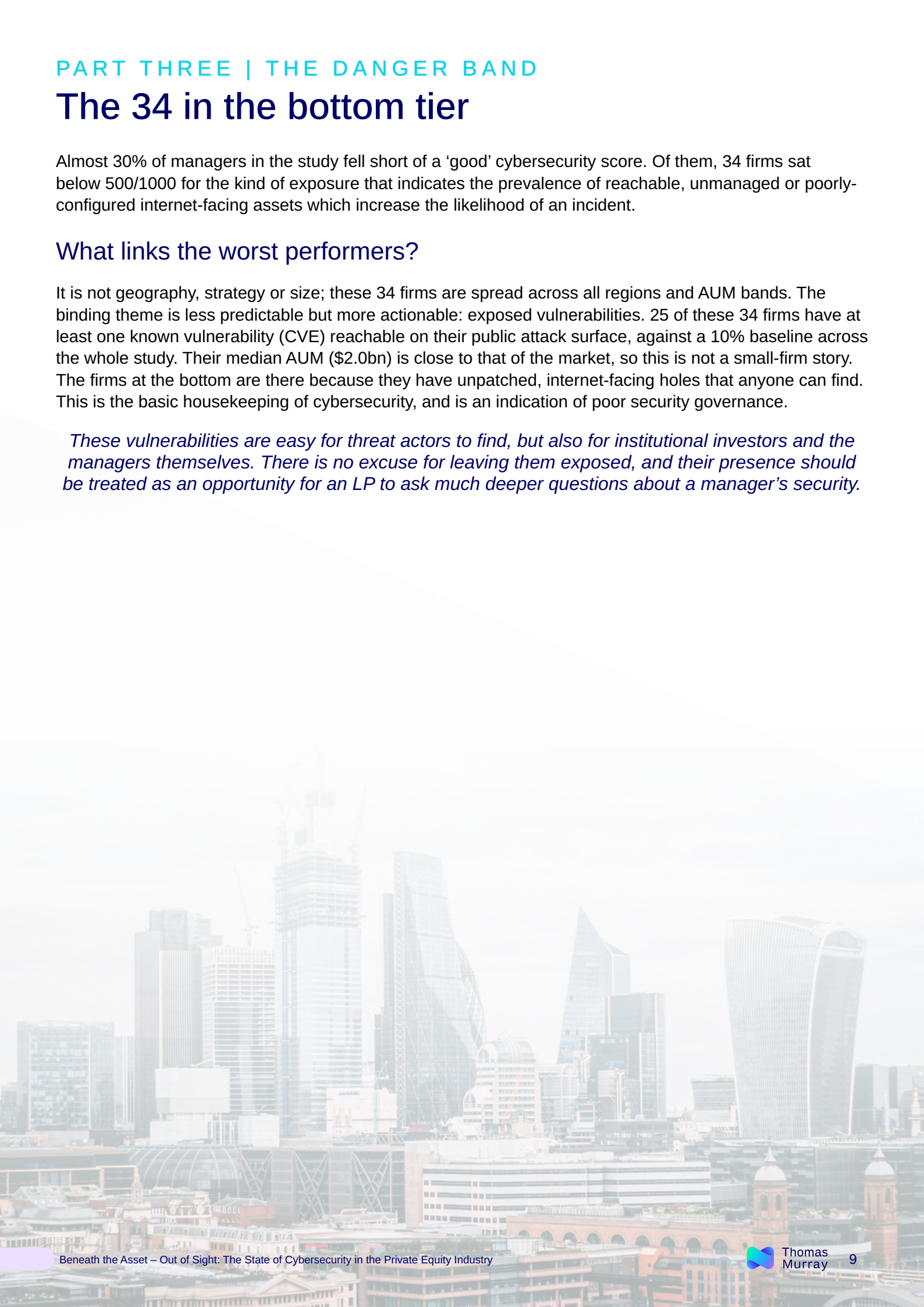
The 34 in the bottom tier

Almost 30% of managers in the study fell short of a ‘good’ cybersecurity score. Of them, 34 firms sat below 500/1000 for the kind of exposure that indicates the prevalence of reachable, unmanaged or poorly-configured internet-facing assets which increase the likelihood of an incident.

What links the worst performers?

It is not geography, strategy or size; these 34 firms are spread across all regions and AUM bands. The binding theme is less predictable but more actionable: exposed vulnerabilities. 25 of these 34 firms have at least one known vulnerability (CVE) reachable on their public attack surface, against a 10% baseline across the whole study. Their median AUM ($2.0bn) is close to that of the market, so this is not a small-firm story. The firms at the bottom are there because they have unpatched, internet-facing holes that anyone can find. This is the basic housekeeping of cybersecurity, and is an indication of poor security governance.

These vulnerabilities are easy for threat actors to find, but also for institutional investors and the managers themselves. There is no excuse for leaving them exposed, and their presence should be treated as an opportunity for an LP to ask much deeper questions about a manager’s security.



The soft underbelly: small firms, the UK and early-stage IP

It is undeniable that the smallest managers have the weakest security, including much of the early-stage venture market. Our analysis revealed approximately a third of sub-$1bn firms fall below the *good* line, scoring only *adequate* or worse.

The most sensitive early-stage IP is being held behind the thinnest walls.

The UK is the epicentre of the small-firm cohort

Of the 126 sub-$1bn firms in the study, the United Kingdom is home to the largest single national group: 34 firms, more than a quarter of the entire small-firm cohort and comfortably ahead of any other country (the Nordics and Ireland follow). A quarter of these UK small firms fall below the good line, and nine of them sit well short of it. The UK's prominence here reflects the depth of Britain's venture and growth-capital ecosystem: the most active in Europe, and the one most closely tied to university spin-outs from Oxford, Cambridge, London and the so-called 'golden triangle'.

Why this is a national-IP issue, not just a firm-level one. These smaller managers invest in the earliest-stage intellectual property in the British economy: the deep-tech, life-sciences and software companies whose entire value is their research. These companies are usually founder-led with a razor focus on proof-of-concept; security is not a consideration. However, we have met too many early-stage firms whose valuation – or continuation – is threatened by IP theft enabled by weak security. The threat actors most interested in Western IP are frequently nation-state backed or aligned groups, who are among the most sophisticated, as well as criminal groups interested in stealing IP for extortion. However, the funds backing early-stage, high-growth UK companies and sitting on their boards do not appear to take even their own security seriously.

For a country like the UK, whose industrial strategy is built on IP-rich industries, weak cybersecurity in the early-stage capital base is a strategic exposure. The same logic applies to other spin-out-rich ecosystems, from the Nordics to Israel and the US universities.

The capital closest to the nation's most valuable early-stage IP is, on average, the least equipped to protect it. For a country trying to create the conditions for growth, with an outsized reliance on innovation, it is a strategic and economic one.

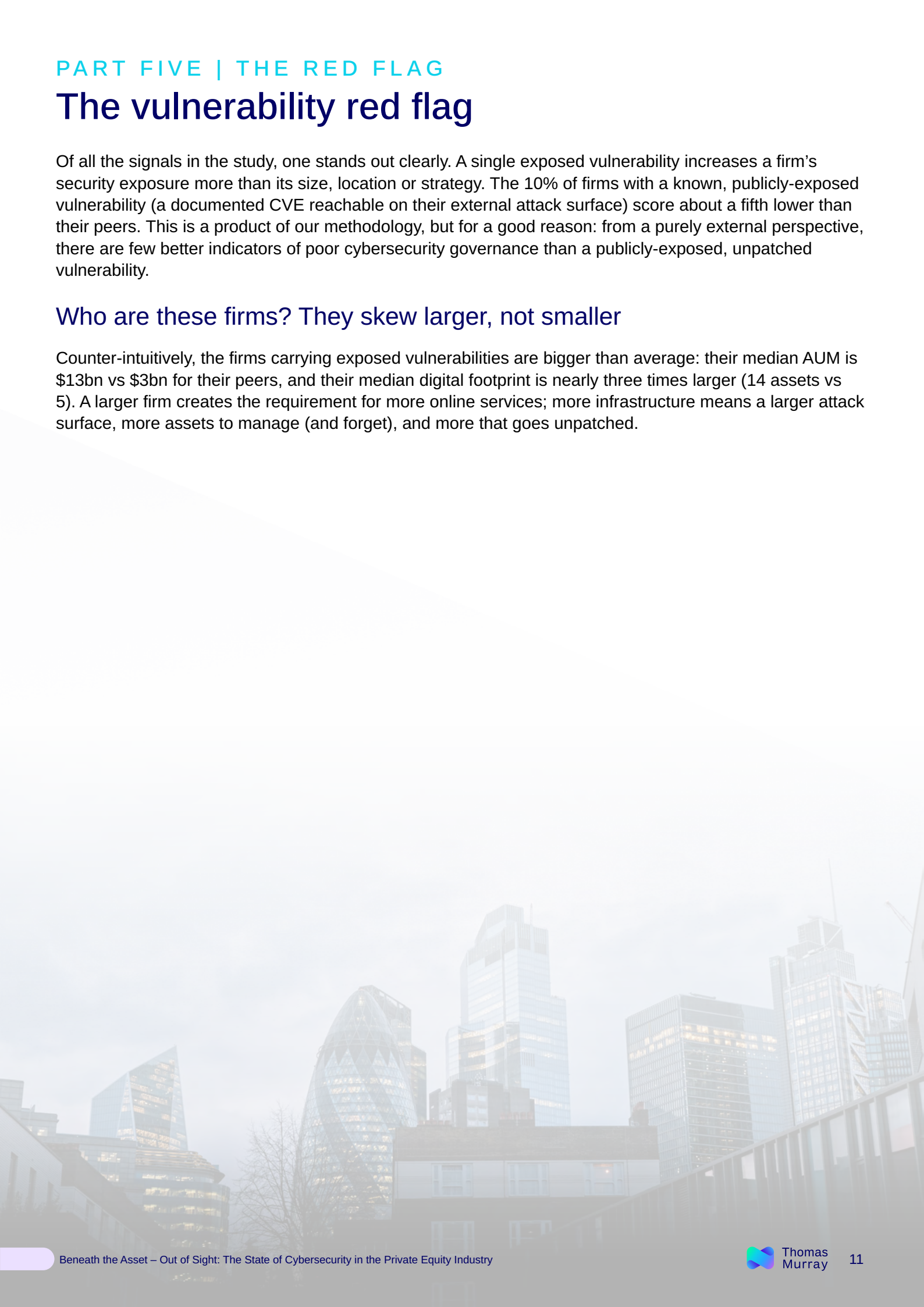
PART FIVE | THE RED FLAG

The vulnerability red flag

Of all the signals in the study, one stands out clearly. A single exposed vulnerability increases a firm's security exposure more than its size, location or strategy. The 10% of firms with a known, publicly-exposed vulnerability (a documented CVE reachable on their external attack surface) score about a fifth lower than their peers. This is a product of our methodology, but for a good reason: from a purely external perspective, there are few better indicators of poor cybersecurity governance than a publicly-exposed, unpatched vulnerability.

Who are these firms? They skew larger, not smaller

Counter-intuitively, the firms carrying exposed vulnerabilities are bigger than average: their median AUM is $13bn vs $3bn for their peers, and their median digital footprint is nearly three times larger (14 assets vs 5). A larger firm creates the requirement for more online services; more infrastructure means a larger attack surface, more assets to manage (and forget), and more that goes unpatched.



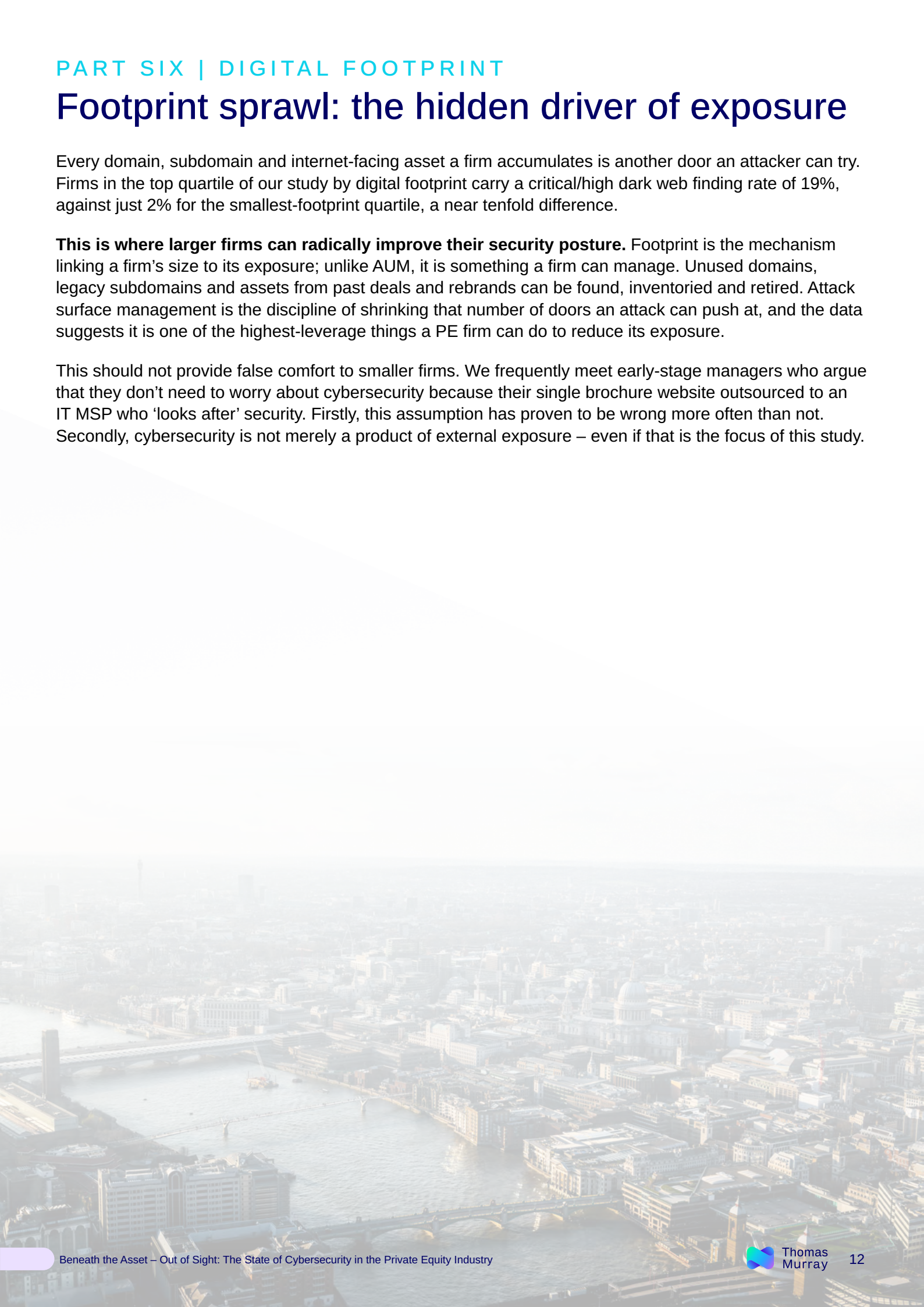
PART SIX | DIGITAL FOOTPRINT

Footprint sprawl: the hidden driver of exposure

Every domain, subdomain and internet-facing asset a firm accumulates is another door an attacker can try. Firms in the top quartile of our study by digital footprint carry a critical/high dark web finding rate of 19%, against just 2% for the smallest-footprint quartile, a near tenfold difference.

This is where larger firms can radically improve their security posture. Footprint is the mechanism linking a firm's size to its exposure; unlike AUM, it is something a firm can manage. Unused domains, legacy subdomains and assets from past deals and rebrands can be found, inventoried and retired. Attack surface management is the discipline of shrinking that number of doors an attack can push at, and the data suggests it is one of the highest-leverage things a PE firm can do to reduce its exposure.

This should not provide false comfort to smaller firms. We frequently meet early-stage managers who argue that they don't need to worry about cybersecurity because their single brochure website outsourced to an IT MSP who 'looks after' security. Firstly, this assumption has proven to be wrong more often than not. Secondly, cybersecurity is not merely a product of external exposure – even if that is the focus of this study.



Where you host matters

A firm's choice of hosting and infrastructure provider tracks measurably with its security. Funds whose primary infrastructure sits behind Akamai or Amazon Web Services average solidly in the *good* band (around 673 and 651 respectively), while those hosting primarily on Google Cloud or Microsoft Azure average roughly 8–9% lower, only just clearing adequate (about 619 and 614). The provider itself does not make a firm secure; rather, the choice and configuration of infrastructure reflects the maturity of the team behind it.

Where does the private equity industry's data actually live?

Looking past the providers to the physical geography of the infrastructure reveals a sprawling, globally-distributed estate. The 558 firms' digital infrastructure spans 52 countries – far more than the 25 they are headquartered in, reaching into Ireland, the Netherlands, Singapore, Hong Kong and South Africa.

Concentration risk. When a large share of firms depend on the same one or two cloud platforms and the same few hosting hubs, a single major outage, misconfiguration or supply-chain compromise at one provider can cascade across dozens of managers at once. Concentration is efficient in normal times and fragile in a crisis: the same lesson the financial system learned about critical third parties now applies to private capital's digital backbone.

Data sovereignty. Because infrastructure is distributed across far more jurisdictions than firms realise, sensitive deal data, LP information and portfolio records frequently reside, legally and physically, outside the firm's home country. Global regulators' direction of travel is firmly towards data localisation: the EU's GDPR and the emerging Data Act and DORA regime, the UK's data-protection framework, and a widening set of national localisation laws (from India's DPDP Act to residency rules across the Gulf, China and Southeast Asia). A firm that cannot say with confidence which country its data sits in faces both a compliance exposure and a due-diligence red flag. For LPs, "where does our data live?" is becoming as important a question as "how well is it defended?"

A distributed infrastructure footprint is not inherently bad, but an unmapped one is. Firms should know, and be able to evidence, exactly where their data resides and under whose laws.

PART EIGHT

Our ESG assumption

It would be logical to assume that a firm which takes ESG seriously also runs a tight security operation: both signal institutional conscientiousness and a focus on good governance. Today, the data does not bear this out.

Signatories of the Principles for Responsible Investment (PRI) do score higher than their peers, but they are 7x larger than their peers (by median AUM); once we controlled for firm size, the effect of this ESG signal and others largely disappeared. As with other large firms, the PRI signatories actually show materially worse dark web exposure compared to their peers.

This finding surprised us. We are frequently contacted by ESG teams who are looking to start or improve their firms' cybersecurity programme; as such we had begun to see ESG as a proxy for modern, proactive governance – including security governance. We were wrong. ESG and cybersecurity programmes can both be features of middle-market firms and upwards, but they apparently bear little relation to one another.

The lesson for LPs is blunt: a GP's ESG record is not a proxy for its cyber hygiene, and should never be read as one.

BEFORE YOU RAISE

What to do before your next fund close

Firms tend to contact us immediately after a fund close, which they see as an opportunity to start ‘doing cyber properly’. This is a good instinct as it means we can help them embed cybersecurity throughout the life of the fund, from diligence to exit. However, it overlooks the growing trend of LPs increasingly asking managers to evidence cybersecurity during a raise; a GP that cannot answer a cyber question is at risk of losing an allocation during operational due diligence, even if it plans to engage a cyber advisor weeks later when it begins making acquisitions. The findings in this report translate into a short, practical list a firm can work through before it next goes to market.

Six things to check before you raise

1. **Scan your own perimeter for a known, exposed vulnerability.** It is the most common hands-off cyber analysis that an LP will perform on you, and the cheapest to replicate.
2. **Reduce your attack surface.** Unused domains, forgotten subdomains and legacy assets from past deals are open doors. Shrinking the door count is the easiest win available to you.
3. **Map where your data physically lives.** Be able to evidence which jurisdictions hold LP, deal and portfolio data, as DORA and GDPR – not to mention geopolitics – are forcing LPs to take this seriously.
4. **Initiate a cyber due diligence stream.** Engage a cyber advisor now to be on standby to carry out rapid diligence; this is even more important if you plan to leave cyber diligence until the final 1-2 weeks.
5. **For AI, quantum, biotech or defence funds, remember nation state threat actors.** Diligence co-investors and insider-threat controls, not just a firm’s perimeter.
6. **Decide what the cyber baseline in your portfolio looks like.** You don’t need to make it up – standards like NIST exist to give you a benchmark which can be easily rolled out across a portfolio.

THE INDEX

Where does your firm rank?

Every firm in this report has a position on the Thomas Murray PE Cyber Index: a continuously-maintained benchmark of the external cyber posture of the private equity market, scoring each firm on a single comparable scale that combines perimeter security and dark web exposure, with a size-adjusted view that isolates genuine performance from the effect of scale. The report is anonymised, but our LP clients increasingly want to access the index to understand where their managers sit relative to the industry.

Request your firm's confidential position on the Index

For GPs: find out where you rank against your peers before an LP tells you; we can give you a report on your current external security posture, and what changes would move you up the index.

For LPs: see how your external managers benchmark against each other and the wider industry; access our ODD support to dig deeper into all aspects of a manager's operations.

Contact the Thomas Murray Cyber Risk team to request a confidential briefing.

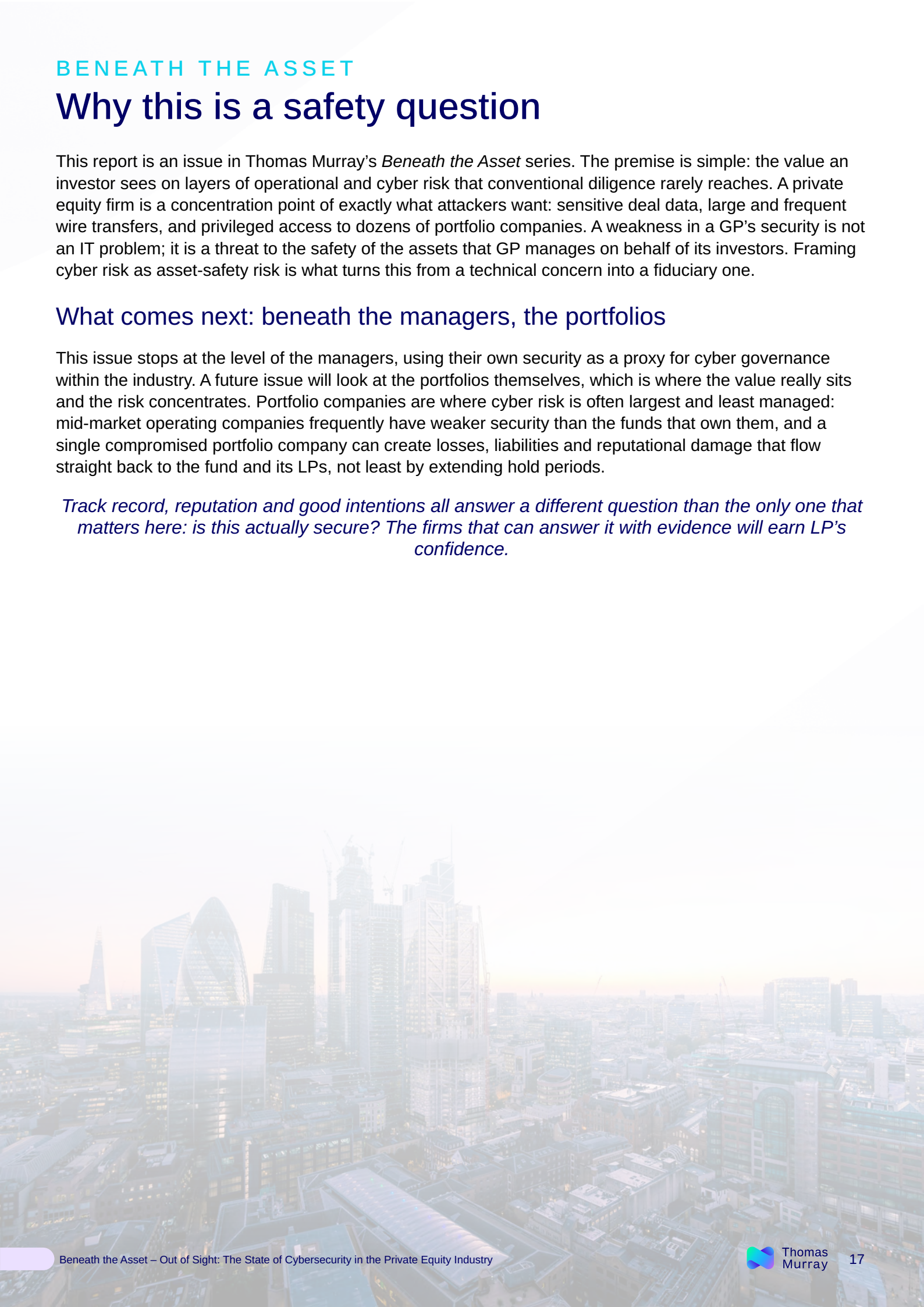
Why this is a safety question

This report is an issue in Thomas Murray's *Beneath the Asset* series. The premise is simple: the value an investor sees on layers of operational and cyber risk that conventional diligence rarely reaches. A private equity firm is a concentration point of exactly what attackers want: sensitive deal data, large and frequent wire transfers, and privileged access to dozens of portfolio companies. A weakness in a GP's security is not an IT problem; it is a threat to the safety of the assets that GP manages on behalf of its investors. Framing cyber risk as asset-safety risk is what turns this from a technical concern into a fiduciary one.

What comes next: beneath the managers, the portfolios

This issue stops at the level of the managers, using their own security as a proxy for cyber governance within the industry. A future issue will look at the portfolios themselves, which is where the value really sits and the risk concentrates. Portfolio companies are where cyber risk is often largest and least managed: mid-market operating companies frequently have weaker security than the funds that own them, and a single compromised portfolio company can create losses, liabilities and reputational damage that flow straight back to the fund and its LPs, not least by extending hold periods.

Track record, reputation and good intentions all answer a different question than the only one that matters here: is this actually secure? The firms that can answer it with evidence will earn LP's confidence.



Methodology

External security posture is measured by the Orbit Security Score, an outside-in rating of a firm's attack surface on a 0–1000 scale (higher is better), in five bands: very poor (0–200), poor (201–400), adequate (401–600), good (601–800) and very good (801–1000). We treat entry to the good band (601) as the level a serious institutional manager should be clearing. Dark web exposure is a separate 0–5 severity score of the most serious finding, recency-adjusted so older findings weigh less. Analysis covers 558 firms with an Orbit score; size-based cuts use the 504 with reliable AUM; HQ resolved for 552 of 558. "Below-expected" security (Part 2) means scoring below the level predicted for a firm's AUM band. ESG matches (Part 8) use documented firm-level awards plus PRI signatory status. Findings are cross-sectional associations, not causal claims; dark web scores reflect surfaced findings, not confirmed breaches. Firms are named only as positive examples; the one breached firm named (Insight Partners) is identified solely from its own public disclosures, not our ratings. All statistics reflect a snapshot as of 15 July 2026.

Contact us

Please get in touch to find out how we can help you to mitigate changing risk.

Find out more: thomasmurray.com
Contact: enquiries@thomasmurray.com

About us

Thomas Murray is a risk intelligence and cybersecurity firm serving the investment industry since 1994. Its cybersecurity services help limited partners to assess and benchmark their managers, and general partners to assess, benchmark and improve the security posture of their portfolios.