Bridging the Cybersecurity Execution Gap in Middle-Market Private Equity

> Cybersecurity has become a critical risk factor for middle-market companies, especially those backed by private equity (PE) and involved in mergers and acquisitions (M&A). Yet a persistent "execution gap"– the disconnect between strategic cyber goals and actual security implementation – leaves many mid-sized firms exposed.

This report explores how the execution gap manifests in cybersecurity programs, the unique challenges facing PE-owned mid-market companies (particularly during M&A), and the financial/regulatory consequences of cyber lapses.

It also examines how leading consulting research frames these issues for PE audiences, and what PE firms prioritize when managing cyber risk in portfolio companies. Finally, we outline how these challenges can be addressed, culminating in a solution that **bridges strategy and execution** to elevate cyber maturity in the mid-market.

The Cybersecurity "Execution Gap" in Middle-Market Companies

In many mid-market businesses, there is a stark gap between cybersecurity **plans on paper and what gets executed in practice**.

Leaders may establish policies or adopt control frameworks, but **implementation lags** due to resource constraints, rapid growth, or siloed teams. As one security expert observes, *"Security is often failing through a gap between what's written down and what actually gets implemented"*.

Most organizations have documented security policies and even compliance tools, **but few can confidently say their IT environments are configured as those policies require**, resulting in avoidable vulnerabilities.

This execution gap is exacerbated by common mid-market realities:

- **Under-resourced IT and Security Teams:** Mid-sized firms often lack dedicated cybersecurity staff (many have no full-time CISO), stretching general IT teams thin. Limited budgets mean they operate with **outdated software, weak firewalls, and minimal employee training**.

Security initiatives are launched but not fully seen through, as day-to-day operational fires take priority over hardening systems.

- **Ad hoc Processes & Tool Sprawl:** Without a strong execution framework, controls tend to be applied inconsistently. Different teams may address security in silos, leading to **misconfigurations and "reinventing the wheel" for each project**. It is telling that a large number of breaches stem from preventable misconfigurations – for example, cloud resources left exposed or users with excessive privileges – rather than sophisticated zero-day attacks. This occurs because dev and IT teams move quickly and are not security experts, while security guardrails are **not embedded by default** into their workflows.
- **Compliance vs. Reality:** Mid-market companies might achieve basic compliance on paper (e.g. policies for data protection) yet **lack enforcement in daily operations**. One study notes that security controls often "exist on paper or in a GRC tool only – with no enforcement in the actual infrastructure". The result is a false sense of security: executives believe risk is managed, while in reality critical patches aren't applied promptly, incident response plans aren't drilled, and access controls aren't consistently maintained. This gap between knowing what to do and doing it grows as companies expand.

> Importantly, middle-market firms in growth mode are especially prone to execution gaps.

These businesses are busy scaling operations (often through M&A), which can distract from cybersecurity. Integrating an acquisition's IT, rolling out new systems, or entering new markets can strain a lean IT staff, delaying security projects. **Cyber hygiene "to-do's" stay on the checklist but get deferred**, creating openings for attackers.

In fact, 1 in 5 middle-market companies suffered a data breach in the past year, and 72% of executives expect unauthorized access attempts – yet **21% still lack a formal business continuity plan** for when attacks occur.

Such statistics underscore the execution gap: even when awareness is high, **preparedness and execution lag**. Bridging this gap is imperative because threat actors are keenly aware of mid-market vulnerabilities.

of middle-market companies still lack a formal business continuity plan

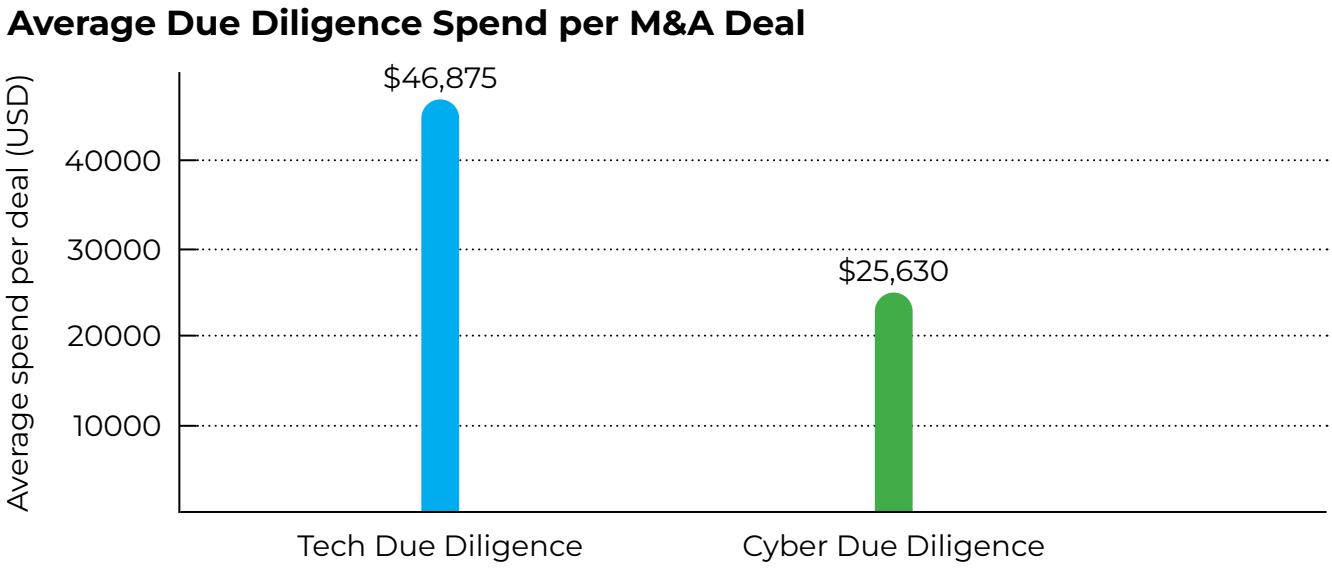
Cyber Risk Challenges for PE-Owned Mid-Market Companies (Especially in M&A)

Private equity-owned mid-market companies face all the above challenges **plus additional risk factors** stemming from ownership structure and transaction activity. PE firms seek to grow value quickly – but if cybersecurity is not executed well, it can undermine an investment overnight.

Key challenges include:

- **Inconsistent Cyber Diligence in Deals:** During acquisitions, cybersecurity often takes a back seat to financial and legal due diligence. Many PE investors acknowledge cyber risk is important, but in practice technical assessments are abbreviated or skipped under tight deal timelines.
    - A 2025 survey of PE professionals found **70% conduct tech due diligence on every target, yet only allocate on average about $25.6K to cybersecurity due diligence per deal** – roughly half of what they spend on broader technology diligence.
    - In other words, buyers may be **under-investing in uncovering security weaknesses** of targets. This gap can leave critical liabilities hidden until after closing. (For example, undiscovered breaches or poor cyber practices at a target can later explode in cost – a risk some firms still "group into general IT costs," an approach now seen as shortsighted.)

Figure 1: Average per-deal due diligence spending on IT vs. dedicated cybersecurity assessments, according to a recent PE survey. Many acquirers still treat cyber reviews as a minor subset of IT diligence, potentially missing serious vulnerabilities.

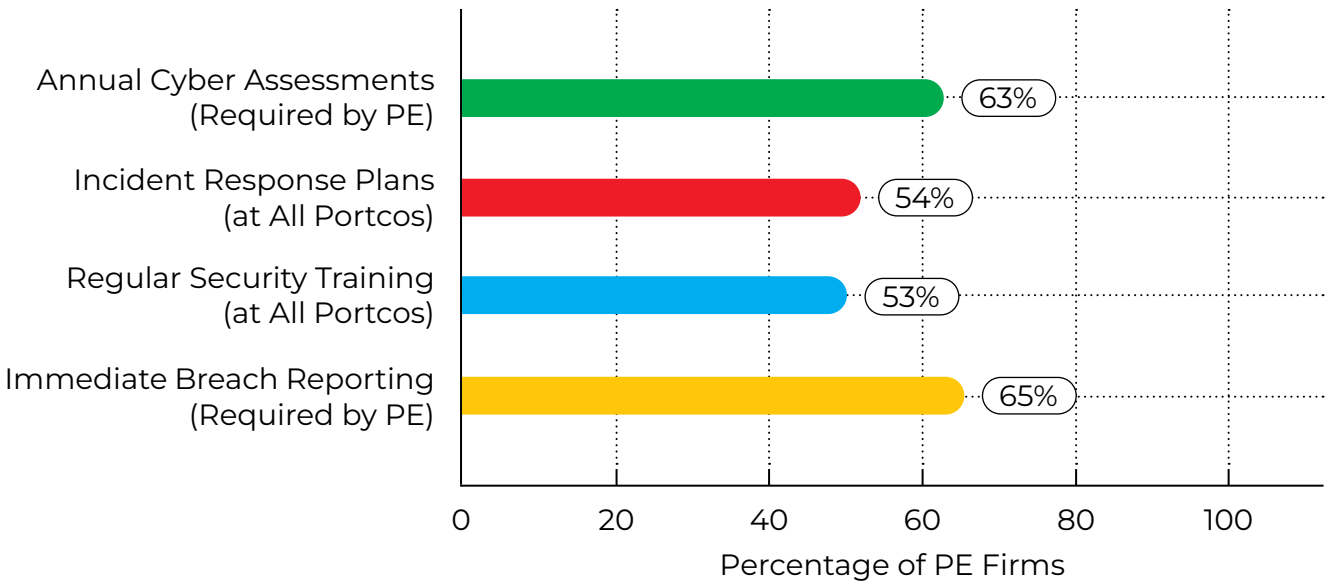


Source: S-RM Cybersecurity in M&A Survey (CYBR.SEC.Media, 2025)

- **Integration & Legacy Vulnerabilities:** When middle-market companies merge or are carved-out, the integration of systems can introduce security gaps.
    - Legacy IT from the acquired entity might be outdated or misconfigured, but **fixes get deferred during integration**.
    - Attackers exploit this chaos: notably, Marriott's acquisition of Starwood uncovered an enormous prior data breach that Marriott hadn't detected during diligence, leading to 383 million records exposed and a £18.4 million fine (≈$23.8M) under GDPR.
    - In another famous case, Yahoo's lack of cyber hygiene reduced its sale price to Verizon by $350M after massive breaches came to light. These examples show how **cyber lapses can directly destroy deal value**.
- **Higher Threat Profile After Investment:** A PE-backed company can become a more attractive target to cybercriminals simply by virtue of new ownership. Public announcements of PE deals can draw attacker attention.
    - Threat actors may assume the company has access to fresh capital or valuable data through the PE network. Indeed, one risk consultancy found that portfolio companies with less mature security are seen as "lucrative targets" once acquired, and there have been cases of **targeted attacks during the transaction process** itself.
    - Such incidents can delay or even derail an acquisition. (One report notes that if a deal's announcement **spurs an attack mid-transaction, it can cause deal closing to be delayed or collapsed entirely**.)
    - PE firms therefore must be vigilant from LOI through post-close, but many are still catching up to this reality.
- **Portfolio-Wide Vulnerabilities:** After acquisition, the challenge shifts to uplifting the portfolio company's security to an acceptable standard – often under time pressure from investors or regulators.
    - Here the execution gap often reappears: **policies may be imposed by the PE parent, but actual implementation at the portfolio company can lag**. In practice, many PE firms lack a consistent approach to monitoring and supporting cybersecurity across all their portfolio companies.

- A 2025 study highlighted that while **63% of PE firms require annual cybersecurity assessments** of each portfolio company, basic security measures were still not universal. Only about **54% ensure every portfolio company has an incident response plan**, and just ~53% ensure regular cybersecurity training for employees at all portcos. Alarmingly, 72% of PE respondents reported a serious cyber incident in one of their portfolio companies within the last three years. Yet only **65% of PE firms require immediate notification to the parent firm when a breach occurs**, meaning many incidents might go unreported to investors. These numbers reveal a disconnect between PE's awareness of cyber risk and concrete actions post-deal.

Figure 2: Survey data on cybersecurity oversight practices among private equity firms for their portfolio companies. Key baseline protections – like incident response plans, employee training, and breach reporting – are not consistently mandated across all portcos, reflecting an execution gap in enforcing cyber standards.



Source: S-RM Cybersecurity in M&A Survey (CYBR.SEC.Media, 2025)

- **Regulatory Pressures:** Middle-market companies are increasingly subject to cybersecurity regulations and investor scrutiny. If a PE-backed firm handles consumer or personal data, laws like the EU's GDPR or U.S. state privacy laws (CCPA, etc.) come into play – with hefty fines for non-compliance. There is also new regulation on critical infrastructure (e.g. the EU NIS2 directive) extending security requirements to mid-sized operators.

- Private equity owners **face liability if a portfolio company fails to meet legal cyber obligations**. For example, regulators can impose penalties or require breach disclosures that damage a company's valuation. PE firms must ensure their investments not only grow, but do so under the umbrella of compliance and secure practices.
- This is reshaping due diligence checklists and post-acquisition plans, as PE operating partners press management teams to shore up any gaps quickly.

In summary, PE-owned middle-market companies confront a perfect storm: they are prime targets for attack (valuable assets but often weaker defenses), they undergo frequent change via M&A that can introduce new weaknesses, and they now operate under stakeholders who expect rapid value creation and risk management.

The next section explores what happens when these challenges materialize – in costs, losses, and lost opportunities.

The High Cost of Cybersecurity Lapses and Execution Gaps

Failing to close the execution gap in cybersecurity can have severe financial and operational consequences for mid-market firms. Some key impacts and trends include:

- **Data Breach Costs Are Escalating:** The average cost of a data breach hit **$4.88 million in 2024** – a figure that has risen steadily year-over-year. These costs include investigation, customer notification, regulatory fines, legal fees, and remediation, which can be devastating for a mid-market business. Notably, breaches that linger undetected are even more expensive: incidents that go **200+ days before detection cost ~23% more** to contain on average. This highlights the importance of robust monitoring and response – an area where execution gaps (e.g. unmonitored logs, undocumented response plans) directly translate into higher damage.
- **Business Survival is at Stake:** A major cyber incident can threaten the viability of smaller enterprises. It's estimated that **60% of small or mid-sized businesses suffering a major breach go out of business within six months**. Whether due to crippling financial losses or irreparable reputational damage, the fallout can be fatal. Middle-market companies often lack the balance sheet to absorb multi-million dollar hits or prolonged downtime. This stark statistic is a wake-up call: **cyber risk is not just an IT issue, but a business continuity issue**. Execution gaps – like not having reliable data backups, incident playbooks, or business

continuity plans – directly increase the odds of such a worst-case scenario.

- **Hits to Valuation and Deal-making:** Cybersecurity has become a material factor in company valuations. We've already seen high-profile examples in M&A: Yahoo's sale price was slashed by $350 million after its historical breaches were revealed, and Marriott incurred tens of millions in fines and remediation costs post-acquisition of Starwood due to an endemic breach. Beyond these, PE insiders report that deals have been delayed or canceled when due diligence uncovers serious cyber vulnerabilities.

- In a recent survey, **89% of PE investors said a target's cybersecurity maturity influenced their acquisition decisions**, and industry groups like the World Economic Forum are now spotlighting cyber resilience as a core due diligence dimension. The lesson is clear: insufficient cybersecurity execution can **torpedo a transaction or reduce the payoff**. Conversely, companies with demonstrably strong cyber programs are viewed as more resilient and command higher confidence from buyers.

of PE investors said a target's cybersecurity maturity influenced their acquisition decisions

- **Ransomware and Fraud Losses:** Middle-market firms have been heavily impacted by ransomware and cyber fraud. Attackers perceive that these companies might pay a ransom to avoid downtime or data leaks, yet may not have the most advanced defenses. According to global insurance analysis, the **average ransomware demand on mid-sized companies is now around $5 million**. Even if a ransom isn't paid, the business interruption and recovery costs average far more. Additionally, funds transfer fraud and email compromise scams continue to prey on companies with weaker controls.

average ransomware demand on mid-sized companies

- For PE owners, a successful $5M–$10M cyber heist at a portfolio company is a direct hit to investment returns. This is driving greater interest in cyber insurance (as discussed later), but insurers, in turn, now require evidence of good security practices to pay claims. **In short, the execution gap can literally become a multi-million-dollar gap in the balance sheet overnight.**

- **Regulatory Fines and Legal Liability:** Governments are increasingly enforcing cybersecurity obligations. Data privacy laws (GDPR, CCPA, etc.) can levy fines up to 4% of annual revenue for breaches or negligence. Regulators have not hesitated to fine mid-market companies for lax security.

  - In critical sectors (finance, healthcare, infrastructure), regulators may impose audits or even revoke licenses if security is inadequate. Furthermore, directors and officers could face claims from investors or customers after a serious breach, arguing oversight failure.

  - In the US, the SEC has introduced cybersecurity disclosure rules for public companies, and while most mid-market PE portcos are private, **many aim to go public or be acquired by public firms – making regulatory compliance a forward-looking concern**. The financial and legal exposure created by cybersecurity lapses adds yet another dimension to the risk; it's not just the attack itself, but the fines, lawsuits, and compliance costs that follow.

Case in Point: A PE portfolio company in the education sector (PowerSchool, acquired by a PE firm) experienced a major breach in 2024 where attackers stole sensitive student data and extorted the company. This incident not only incurred technical recovery costs and ransom payment, but also **invited regulatory scrutiny** due to exposure of children's personal information, compounding the damage. Such cases illustrate how a cyber incident can trigger a cascade of costs – from IT forensics to public relations to regulatory penalties – and harm the company's reputation and relationship with clients. For PE sponsors, this means eroded equity value and a potential public relations crisis affecting the fund's image.

Ultimately, the **operational disruption** from a significant cyber event can be just as harmful as the direct costs. Ransomware that halts production or a data breach that forces customer notification will consume management attention, slow down growth projects, and could lead to loss of clients. For a lean mid-market operation, even a few days of downtime or a tarnished brand can set back performance for an entire quarter or year. This is antithetical to PE firms' goals of rapid value creation.

All the above points to a simple conclusion: **cybersecurity execution is now inseparable from business execution** in the middle market. Companies that do not close the gap between knowing

and doing in cybersecurity are gambling with their financial futures. Private equity stakeholders, in particular, are taking notice – and increasingly demand that their portfolio companies treat cyber risk with the same rigor as other core business risks.

How Private Equity Firms are Addressing Cyber Risk

Recognizing these stakes, many private equity firms are **elevating cybersecurity from an IT issue to a board-level priority** in their investment process. Over the past few years, top-tier PE firms and consultants have advocated a more structured, proactive approach to cyber risk management tailored to PE's unique context. Key trends and best practices include:

- Embedding Cyber into Due Diligence and Investment Thesis: Leading PE firms now treat cybersecurity akin to financial and legal due diligence. Rather than a cursory checklist, they are bringing in specialists to perform cyber risk assessments on targets early in the deal cycle . If a target has low security maturity, investors factor in the cost of remediation or even reconsider the deal.
    - According to an AlixPartners analysis, cybersecurity uncertainty is adding complexity to M&A deals, and savvy investors adjust their valuation and terms accordingly.
    - In some cases, discoveries of major vulnerabilities lead to escrow arrangements or cyber-specific representations and warranties in purchase agreements to protect the buyer.
    - This is a shift toward systematically accounting for cyber risk, rather than treating breaches as one-off surprises. Crucially, PE firms are asking in advance: *"What will it cost and require to bring this company up to our security standards?"* and baking that into the value creation plan.
- **Building Baseline Security Across the Portfolio:** Post-close, PE firms are increasingly enforcing **baseline cybersecurity standards for all portfolio companies**. The idea is to ensure a floor of protection: e.g. every portco must have an incident response plan, must conduct regular employee security training, and must implement critical patches within a defined timeframe.
    - The recent S-RM survey report contends that firms who "establish precise, measurable baseline security requirements for all portfolio companies" are better positioned to prevent incidents. Our research shows many PE firms now provide centralized resources to help portcos achieve these basics – whether via funding earmarked for security improvements (53% of firms provide dedicated cyber budgets to portcos) or by **negotiating portfolio-wide solutions** (for instance, master service agreements with

cybersecurity vendors, bulk licensing of tools, or group cyber insurance programs to leverage scale). This portfolio-level strategy helps overcome the execution gap by not leaving each small management team to figure things out alone. Instead, the PE owner acts as a partner in lifting security maturity across all investments.

- **Active Monitoring and Support:** Rather than assuming each portfolio CEO and CIO will handle cyber risk, PE firms are **creating oversight mechanisms**. Many have started to appoint a **technology or cybersecurity operating partner** – an expert who can assist portfolio companies and monitor their progress. Firms require periodic cyber reports from portcos, and some use centralized dashboards to track compliance with the aforementioned baseline controls. The S-RM study found 63% of PE firms mandate annual cyber assessments of portcos, but forward-thinking firms go further, moving from *"passive to active risk management"* through continuous monitoring.
    - For example, if a new critical vulnerability (like Log4j) emerges, the PE owner may coordinate a cross-portfolio response to ensure every company patches it promptly. This active stance reduces the window of exposure stemming from execution delays. It also serves as an **early warning system** – if a portfolio company isn't remediating issues or reporting incidents, the PE firm can intervene with additional support or pressure.
    - In short, PE firms are learning to act as security shepherds for their flock of portcos, rather than hands-off investors.
- **Economies of Scale and Knowledge Sharing:** Top consulting firms (e.g. West Monroe, PwC) advise PE clients to leverage the **scale of their portfolio** for cyber improvements. This includes bulk purchasing cyber tools or services (reducing cost barriers for smaller companies) and creating peer forums for CISOs/IT heads across the portfolio to share best practices.
    - For instance, a PE firm might host quarterly cybersecurity roundtables with all portfolio CISOs. This breaks the isolation of each mid-market IT team and accelerates adoption of good practices. It also standardizes approaches where sensible – without rigidly imposing one-size-fits-all solutions (as experts caution, each company's security needs and risks differ).
    - Nevertheless, **centralizing certain cyber defenses** (like managed detection & response services, insurance coverage, or third-party risk management processes) can dramatically improve efficiency and consistency. PE firms are essentially treating cybersecurity as a **portfolio-wide program** rather than an afterthought at each company.

- **Cybersecurity as a Value-Creation Lever:** Perhaps most importantly, private equity is reframing cybersecurity from being purely defensive ("value protection") to being part of the **value creation thesis**. This change in tone is evident in recent thought leadership.
    - By investing in robust cybersecurity early in the hold period, PE firms not only reduce the risk of a damaging incident but also make the eventual exit more attractive. A company with demonstrably strong cyber controls and no history of breaches will appear more "resilient and capable of long-term growth" to buyers, potentially commanding a premium. EY's research found that some PE firms see up to **$36 million of value uplift** for large deals by proactively addressing cybersecurity and technology in their portfolio (through cost avoidance, smoother integrations, and higher exit multiples).

value uplift for large deals by proactively addressing cybersecurity and technology in their portfolio

    - As one report put it, treat cybersecurity not just as a cost center, but as a strategic opportunity to **create trust, enable digital innovation, and protect the investment's upside**. This mindset shift encourages portfolio company management to prioritize critical security projects (e.g. securing a new cloud deployment or achieving a security certification that opens up new sales opportunities) as part of the growth plan, not in conflict with it.

- **Insurance and Risk Transfer Strategies:** Alongside direct security improvements, PE firms are also looking at cyber risk transfer mechanisms like insurance and warranties. Representations & warranties (R&W) insurance for M&A deals now increasingly can include cyber coverage, if proper due diligence is done. Similarly, many portcos carry standalone cyber insurance policies. PE firms coordinate with insurers to ensure policies are in place and structured optimally (often using their buying power to get better terms for portfolio companies as a group). However, insurance will not cover every loss, especially if there were **pre-existing security deficiencies** or non- compliance with policy conditions. Thus, PE firms use insurance as a **safety net, not a substitute** for good security practices. The priority remains to prevent incidents, with insurance there for catastrophic scenarios. In fact, insurance underwriters now scrutinize the insured's security controls, essentially enforcing execution of best practices as a prerequisite to coverage.

This has an interesting side effect: it gives PE owners another incentive to ensure each portco hits certain security benchmarks in order to qualify for affordable insurance.

Through these measures, private equity firms are gradually **closing the execution gap from the top-down** – by aligning incentives, providing resources, and requiring accountability for cybersecurity at their portfolio companies.

The tone in private equity boardrooms has shifted to one of **shared responsibility** for cyber risk. As an operating partner quipped, "We're not just financial engineers anymore; we have to be resiliency engineers as well." The next step is enabling mid-market companies to execute on cybersecurity effectively, given their limited internal capacity. This is where structured programs and external partnerships come into play.

Closing the Gap: Cyber Maturity Programs as a Solution

To truly bridge the cybersecurity execution gap, mid-market firms (and their PE sponsors) are turning to dedicated **Cyber Maturity Programs** that provide a roadmap and hands-on support to improve security posture.

One example is **Resourcive's Cybersecurity Maturity Program**, designed specifically for mid-market PE-owned companies. As Resourcive aptly states, "You don't need another assessment. You need an action plan and an execution partner." This philosophy directly targets the execution gap by not just identifying problems, but ensuring they get solved.

Core Components of the Cyber Maturity Program: At its heart, the program delivers a combination of **expert guidance, structured planning, and ongoing execution support** tailored to the client's needs. Key elements include:

- **Live Cyber Dashboard & Risk Metrics:** Upon engagement, the company is onboarded to a platform that provides **real-time visibility into cybersecurity posture and progress**. Instead of one-time reports that go stale, executives get a continuously updated dashboard showing their risk scores, compliance status, and remediation tasks. This creates transparency and accountability – a living scorecard to drive execution. (Point-in-time assessments often lose momentum; a live dashboard keeps the focus on continuous improvement.)

- **Actionable Roadmap (Prioritized by Risk):** Rather than a long list of recommendations, the program delivers a **clear, prioritized action plan** aligned to the company's actual risks. For example, if ransomware risk is high, the roadmap might prioritize offline backups and network segmentation before addressing lower-priority items. This risk-driven sequencing ensures that

limited resources tackle the most critical gaps first – a crucial approach for mid-market firms. The roadmap is effectively a step-by-step maturity plan, so management knows **what to do now, next, and later**.

- **Tool & Vendor Evaluation Support:** Mid-market IT teams can be overwhelmed by vendor marketing and unsure which security solutions fit them best. The program provides **evidence-based evaluation of tools and services**.
    - In practice, Resourcive's cyber advisors help the company review its current tools, identify needs (e.g. do we need a better endpoint detection system?), and then recommend or even run proof-of-concepts to validate solutions – cutting through sales fluff. This ensures that any investments (in say, a SIEM or MDR service) are **aligned with the program's strategy and the company's environment**. It prevents the common execution pitfall of buying products that later sit shelfware due to poor fit or lack of expertise to implement.
- **Policy and Controls Framework ("Evidence-Based Risk Validation"):** A foundational component is building or refining the company's security **governance, policies, and control framework** from the ground up. The program doesn't assume these basics are in place – often mid-market firms need updated acceptable use policies, incident response procedures, access control policies, etc.
    - Resourcive's team helps put these governance pieces in place and maps them to industry standards as needed. They then validate the controls by testing them against real-world scenarios (for instance, verifying that backups can be restored, or that unauthorized devices are indeed blocked). This approach creates tangible proof that security measures aren't just "on paper" but working in practice – directly closing the **policy-versus-reality gap**.
- **"Execution Horsepower" – Ongoing Expert Support:** Perhaps most distinguishing, the Cyber Maturity Program provides **on-demand cybersecurity experts to drive and track execution**. This is essentially an extension of the company's team, ensuring things actually get done. As Resourcive describes, clients leverage their C**yber team to keep on track and ensure the highest- value actions are taken to reduce risk**.
- In practical terms, this could mean Resourcive personnel will help carry out tasks (e.g. configuring MFA, reviewing firewall rules, training staff), or project-manage the effort, or coordinate with outside vendors – whatever it takes to move the needle. This "doer" role is critical for mid-market companies that don't have a large in-house security staff. It turns recommendations into reality. Over time, this also mentors the internal team, building their

capability. The program's goal is not to do a one-time fix, but to **instill operational rigor** so that cybersecurity improvements are sustained.

Benefits and Outcomes: Such a program directly addresses the execution challenges outlined earlier. Management gains **clarity and confidence** that their cyber risk is trending downward over time (something every CEO/CFO wants to be able to report).

Instead of a vague notion of being "more secure," they see specific metrics improving – e.g. number of critical vulnerabilities dropping, or phishing click rates decreasing after training.

The **live dashboard** and periodic reviews ensure accountability at the executive level. Meanwhile, the partnership offloads much of the heavy lifting from the overburdened IT team, **without adding permanent headcount**.

This is an attractive model for PE operating partners and CFOs: they can elevate a portfolio company's security maturity in a cost-effective way, by essentially "subscribing" to expert execution support rather than hiring a dozen new staff across the portfolio.

Crucially, the program is **outcome-focused**.

It frames cybersecurity in terms of business risks, pain points, and tangible goals, rather than technical jargon. In the first kickoff call, the discussion is about what operational or financial risks worry the business most, and what success looks like (e.g. "zero production outages from cyber events" or "meeting customer security requirements to win more contracts").

This ensures that the resulting action plan is aligned with business objectives, which garners buy-in from leadership. By translating cyber into business terms, the program facilitates better decision-making at the board/PE level and creates a sense of urgency and ownership – key ingredients to closing the execution gap.

Finally, the **measurable progress** provided by a cyber maturity program is exactly what private equity stakeholders want to see. Operating partners can log into a dashboard or read monthly reports that show how a portfolio company is improving its maturity scores, addressing open risks, and tracking compliance. This makes cybersecurity an ongoing agenda item in portfolio reviews, with data to discuss rather than anecdotes. It also serves as evidence to bring back to investors (LPs) or regulators, demonstrating a proactive stance on cyber risk management.

In effect, a program like Resourcive's becomes the **bridge between high-level intent and on-the-ground action**, ensuring that cybersecurity doesn't fall victim to the execution gap that has plagued so many mid-market enterprises.

Conclusion

Middle-market companies and their private equity owners can no longer afford to treat cybersecurity as a secondary concern or a theoretical exercise.

The stakes – in dollars, deals, and reputations – are simply too high. As this report has detailed, the "execution gap" in cybersecurity is the Achilles' heel that many attackers are exploiting, and many firms unknowingly expose themselves to risk even while believing they are protected.

The good news is that awareness is rising, and practical solutions are at hand. By learning from top-tier industry research and peer experiences, PE firms are tightening their approach to cyber due diligence and oversight. And by leveraging programs like Resourcive's Cybersecurity Maturity Program, mid-market organizations are gaining the tools, roadmap, and horsepower to **operationalize cybersecurity** effectively – turning plans into outcomes.

In doing so, they are not only mitigating risk but also strengthening the very foundation of business value in the digital age.

Bridging the cybersecurity execution gap is now a strategic imperative for anyone investing in or leading a middle- market company, and those who succeed in this effort will be rewarded with more resilient, higher-value businesses.

Sources

1 ILYAH Simuni, “Cloud Security Execution Gap – Companies are hacked not for lack of policies...,” LinkedIn Pulse, Apr. 24, 2025.

2 LG Networks, “How Cybersecurity Failures Are Quietly Killing Lower Middle Market Deals,” LG Networks Blog, Jul. 10, 2025.

3 RSM US Middle Market Business Index Special Report: Cybersecurity 2025, Apr. 17, 2025.

4 Willis Towers Watson (WTW), “Cyber risks in Private Equity,” Olivia Lovitt, Dec. 17, 2024.

5 AlixPartners, “How cybersecurity risk is disrupting the M&A landscape...,” June 2019.

6 S-RM (via CYBR. SEC. Media), “Private Equity Firms Face Serious Cybersecurity Disconnect,” Jul. 10, 2025.

7 Resourcive, Cybersecurity Maturity Program (Private Equity) – Program Overview and Features, 2025.

8 Additional data from EY, PwC, and industry analyses on PE cybersecurity trends, and case examples from FTC, TechCrunch, etc. for Marriott and Yahoo breaches. (All links accessed July 2025)

9 Cloud Security Execution Gap - Companies are hacked not for lack of policies, regulations, control frameworks or tools

10 How Cybersecurity Failures Are Quietly Killing Lower Middle Market Deals - LG Networks, Inc.

11 Private Equity’s Cyber Due Diligence Gap

12 Alixpartners.com

13 Cyber risks in Private Equity - WTW

14 Cybersecurity Program Management

15 Cybersecurity Special Report | MMBI | RSM US