

Cyber Risk at Scale:

Safeguarding Portfolio Value in Private Equity



Table of Contents

03	Executive Summary
04	Key Findings
05	Cyber Risk Is Disruptive During the “Hold Period” in PE Firms
09	Serious Financial Impact Is at Stake
12	Larger PE Funds Are Leading the Way
17	How to Prepare for the Year Ahead
18	Conclusion
19	How Kroll Can Help
21	Methodology
22	Real World PE Challenges
23	Contributors

Executive Summary

Exits are poised for a rebound in 2026, as improved market conditions and a wave of [M&A activity in late 2025](#) unlocks pent-up demand. Alternative exits rose in 2025, reflecting firms' willingness to wait out a sluggish market, but the coming year may see more traditional deals return.

The middle-market remains a bright spot for private equity capital deployment which will continue to drive demand for quality acquisition targets. With PE firms continuing to deploy capital, more portfolio companies will be acquired and managed, escalating the cyber risk to PE firms.

PE firms are exposed as cybersecurity has evolved into a material transaction risk. Cyber risk is no longer merely an operational concern; it has also become a direct threat to deal flow and valuation.

Kroll surveyed more than 300 global PE executives to understand cybersecurity risk and fund-level management practices. It found that incidents are becoming more frequent and there is an **average financial impact of \$2.1 million (mn)**, often scaling up to \$10 mn. Larger firms tend to have stronger defenses, governing through strict mandates and centralized platforms, causing smaller firms to suffer disproportionately more from costly remediation and disrupted deals.

PE firms should take measures to govern cyber risk more effectively and encourage the adoption of enterprise-grade security protections across their portfolio to avoid disruption, limit financial losses, and protect exit value.

Key Findings:

- Cybersecurity incidents are rising, increasing the need for strong portfolio-level risk management.
- Incident impact is typically \$2.1 mn, and larger financial impacts are not uncommon.
- Larger firms have established effective practices to enable portfolio company leaders to protect their business.
- Smaller firms have less robust risk management practices and are more likely to experience additional remediation costs and deal disruption during exit transactions.



Key Findings



Cybersecurity risk is disruptive in PE, particularly during the “hold period”:

- Eighty percent of PE firms have experienced disruption during the hold period over the past year.
- Forty-four percent of respondents experienced unexpected remediation costs associated with a cybersecurity issue in the hold period.
- Twenty-seven percent of respondents experienced business disruption due to a cybersecurity incident in the hold period.
- Nearly 70% of respondents indicated that the frequency of hold period incidents has increased year over year, with 20% reporting a significant increase.



Serious financial implications are at stake:

- Nine out of 10 respondents have experienced some financial impact due to cybersecurity risk.
- Financial impact is reported as being composed of increased ongoing compliance costs and remediation costs.
- On average, PE firms suffered \$2.1 mn in financial impact to deals disrupted due to cybersecurity risk.
- Thirteen percent of PE firms reported loss events to be over \$5 mn.



Larger firms are leading the way to building cyber resilience:

- Fifty-five percent of respondents representing firms over \$25 billion (bn) in assets under management (AUM) reported governing cybersecurity risk through a formal mandate to portfolio company managers, compared with 12% for firms under \$25 bn in AUM.
- Fifty-eight percent of respondents representing firms over \$25 bn in AUM reported use of a dedicated platform for tracking and managing cybersecurity risk across the portfolio, compared with 9% of those with under \$25 bn in AUM.



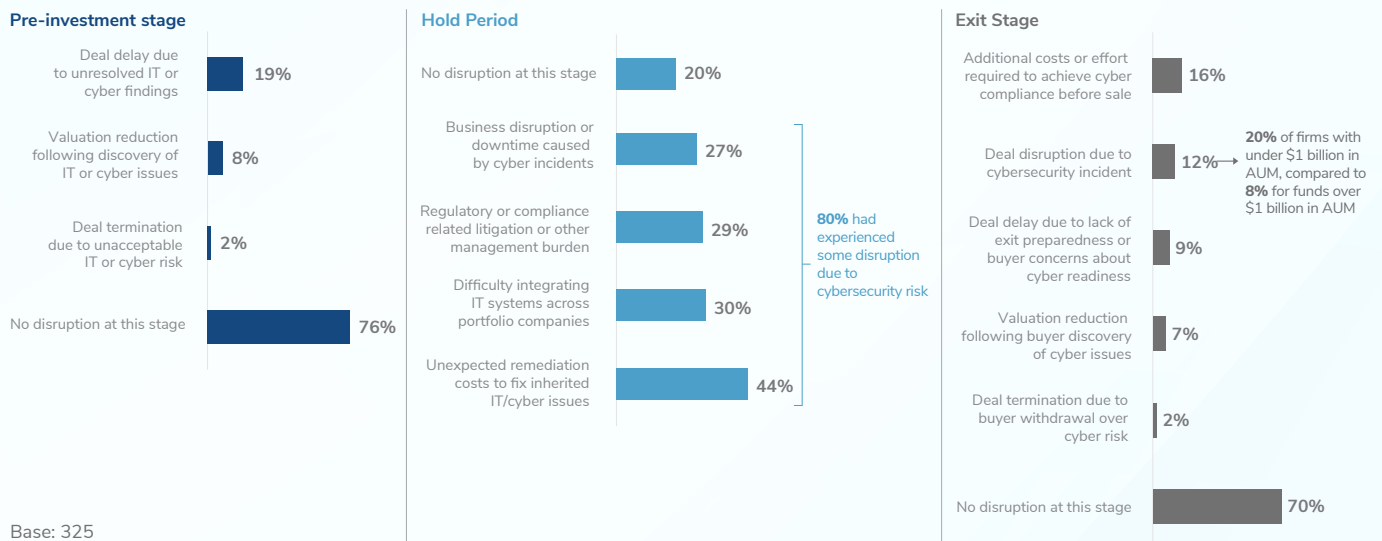
Be prepared for the year ahead:

- Ninety-six percent of PE firms agree that portfolio cybersecurity will grow in importance in the coming year.
- Fifty-three percent of PE firms believe that the financial impact of cyberattacks will increase in the next year.

Cyber Risk Is Disruptive During the “Hold Period” in PE Firms

Cybersecurity risk impacts PE firms hardest during the hold period, the window where value is built and exits are planned. Disruption is not limited to just one stage, however, and this study examines disruption across three key stages of portfolio management.

- **Pre-investment** – evaluating potential acquisitions before purchase
- **Hold period** – after an acquisition, when a fund is driving operational and performance improvements
- **Exit** – preparing for and executing the sale of a portfolio company



Q. Within the past 12 months, has cybersecurity risk caused any of the following issues during the pre-investment, hold period and exit stages? Select all that apply

Pre-Investment Stage

Even before a deal closes, cybersecurity risk is a threat to PE firms. Nearly a quarter (24%) reported disruption at this stage.

The stakes are high as 19% suffered deal delays due to unresolved IT or cyber findings; 8% saw a reduction in valuation following the discovery of IT and cyber issues; and 2% had deals terminated.

Even a single misjudged risk could jeopardize millions of dollars before the ink is dry.

Hold Period

The hold period saw the largest amount of disruption from cybersecurity risk issues. This is where the pain peaks, with 80% of respondents having faced disruption during a hold period during the past year. This is an intuitive finding due to hold period duration compared with pre-investment and exit periods.

Among the most common disruptions firms experienced during the hold period:

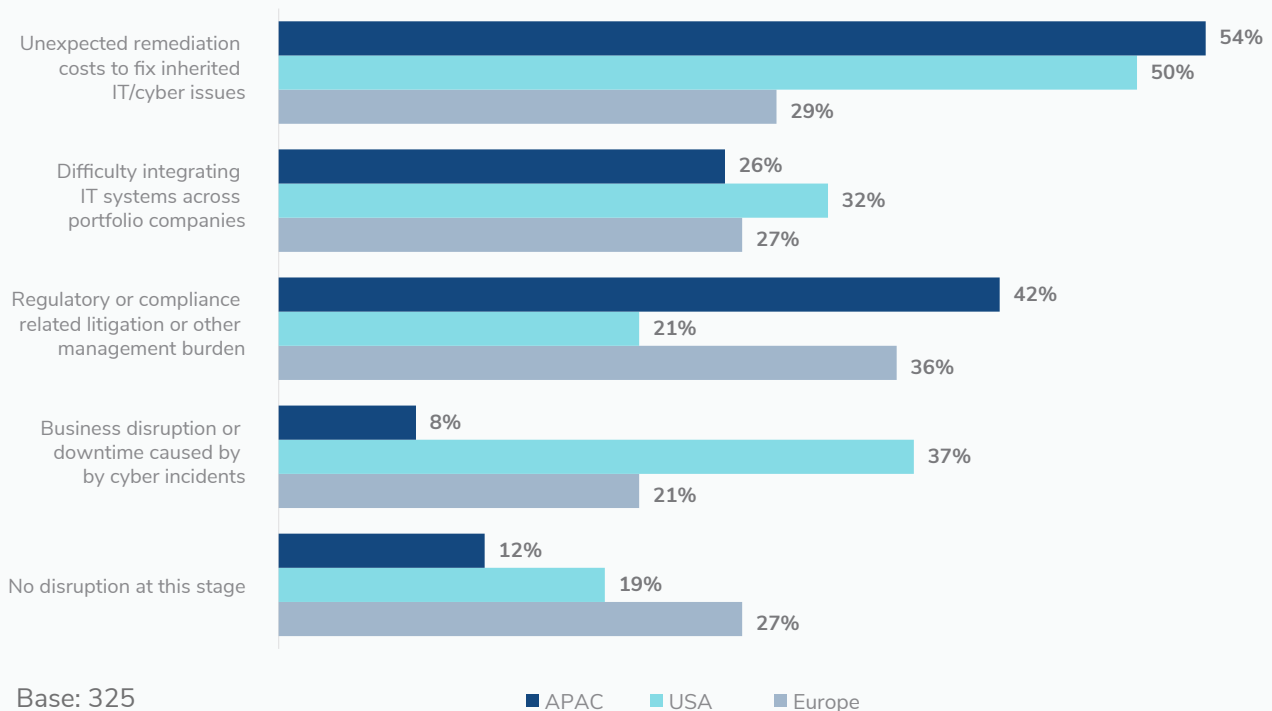
- Forty-four percent were hit with unexpected remediation costs.
- Thirty percent struggled to integrate IT systems across portfolio companies.
- Twenty-nine percent dealt with compliance or regulatory related litigation.
- Twenty-seven percent suffered outright business disruption or downtime due to cyber incidents.

The frequency of these incidents is rising fast. Almost 70% of firms say hold period cyber events are happening more often, and 1 in 5 (22%) call the increase “significant.”

80% of PE firms have experienced disruption during the hold period over the past year.

Regional Perspective

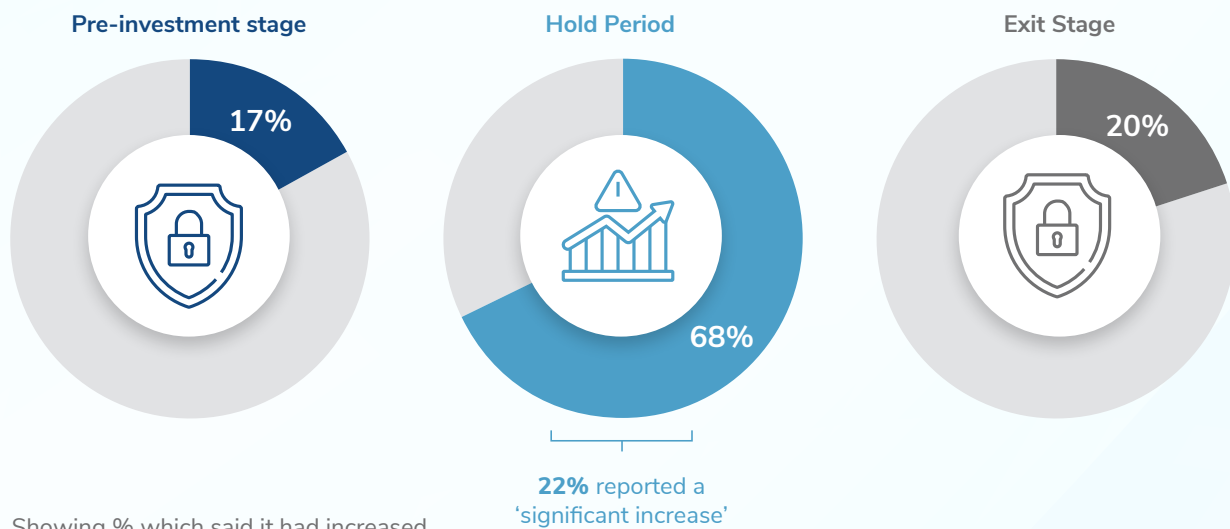
A regional view shows distinct patterns of disruption. Business disruption or downtime due to cybersecurity risk issues was most common in the U.S. (37%), compared with Europe (21%) and APAC (8%). In contrast, regulatory or compliance related litigation was a bigger disruptor in APAC (42%) and Europe (36%), compared with the U.S. (21%). These differences highlight the need for firms to stay alert to evolving regulatory requirements.



Q. Within the past 12 months, has cybersecurity risk caused any of the following disruptions during the hold period?
Select all that apply

Cybersecurity incidents are rising fastest during the hold period, more than at any other point in the deal life cycle. Nearly 70% of respondents reported an increase in cybersecurity incidents during this stage, including 22% who said the increase was significant. By comparison, only 17% saw increases in cybersecurity incidents pre-investment and 20% at exit. This trend aligns with the broader escalation in cyber threats and reflects the hold period's longer window of exposure.

Nearly **70%** of respondents indicated that the frequency of hold period incidents has increased year over year, with **22%** reporting a significant increase.

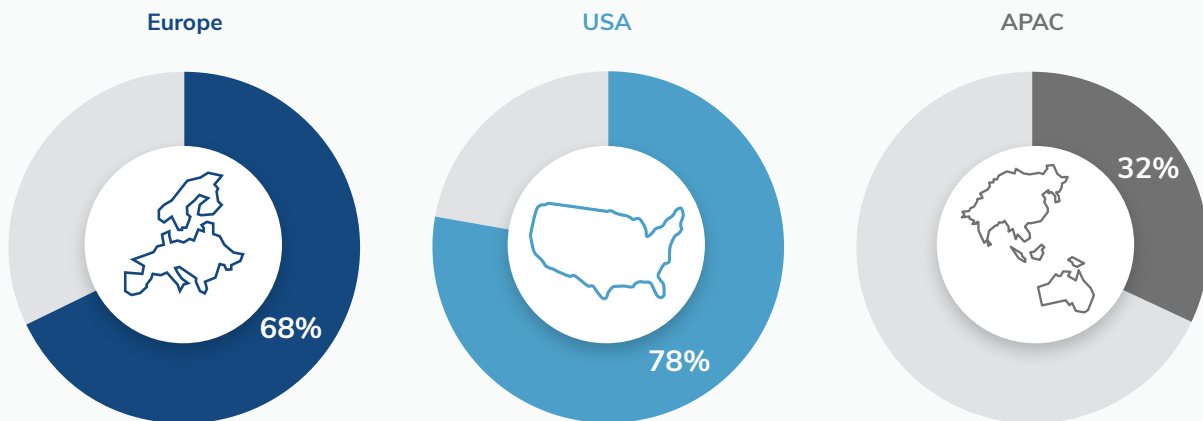


Q. Please indicate whether you have seen a change from last year to this year in the frequency of cybersecurity incidents in your portfolio companies during the following phases? Select one per row



Regional Perspective

Across the world, both Europe (68%) and the U.S. (78%) reported an increase in cybersecurity incidents during the hold period, with those in APAC slightly less likely to have reported an increase (32%).



Base: 325

Q. Please indicate whether you have seen a change from this year to last year in the frequency of cybersecurity incidents in your portfolio companies during the hold period?

Exit Stage

Cybersecurity risk does not disappear at the finish line and should be a key consideration for exit readiness. The survey indicates that issues uncovered late in the hold period can erode returns precisely when they are most critical, threatening deal value or even derailing an exit.

12% chance of a deal being disrupted in exit period due to cybersecurity incident.

Fund Size Perspective

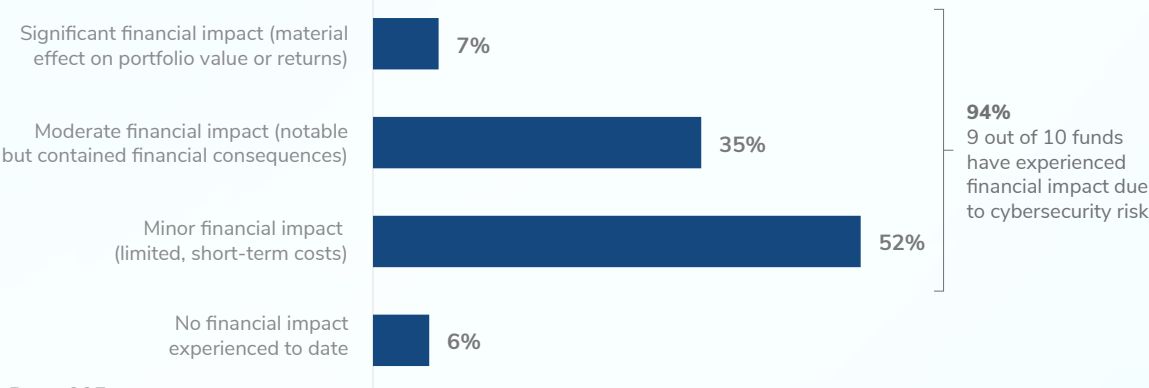
Deal disruption during the exit stage disproportionately affects smaller firms, with 20% of respondents representing firms under \$1 bn in AUM seeing deal disruption due to a cybersecurity incident. This compares to those with over \$1 bn in AUM, 8% of whom noted disruption due to cybersecurity issues.

Serious Financial Impact Is at Stake

Financial Impact of Cybersecurity Risk

The financial impact is undeniable. Almost all (94%) of PE firms have absorbed losses from cyber-related disruption, with the average approximate financial impact to deals reaching \$2.1 mn, and 13% reporting losses more than \$5 mn. The bulk of these costs stem from heavy compliance demands and costly remediation efforts.

Nine out of 10 respondents have experienced some financial impact due to cybersecurity risk.

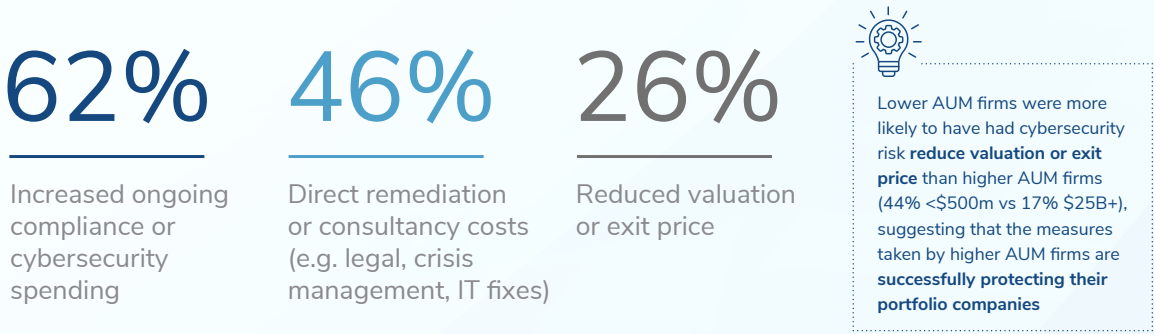


Q. Has cybersecurity risk had any financial impact on your portfolio companies?

Forms of Financial Impact

When respondents were asked more specifically about the type of financial impact suffered, increased ongoing compliance costs were most common for nearly two-thirds (62%), followed by remediation costs (46%), and finally a reduced valuation or exit price for over a quarter (26%) of PE firms.

More than a quarter of PE firms suffered reduced valuation or exit price due to cybersecurity risk.



Base: 307*
Asked only to those who experienced a financial impact
Q. What form did that financial impact take? Select all that apply

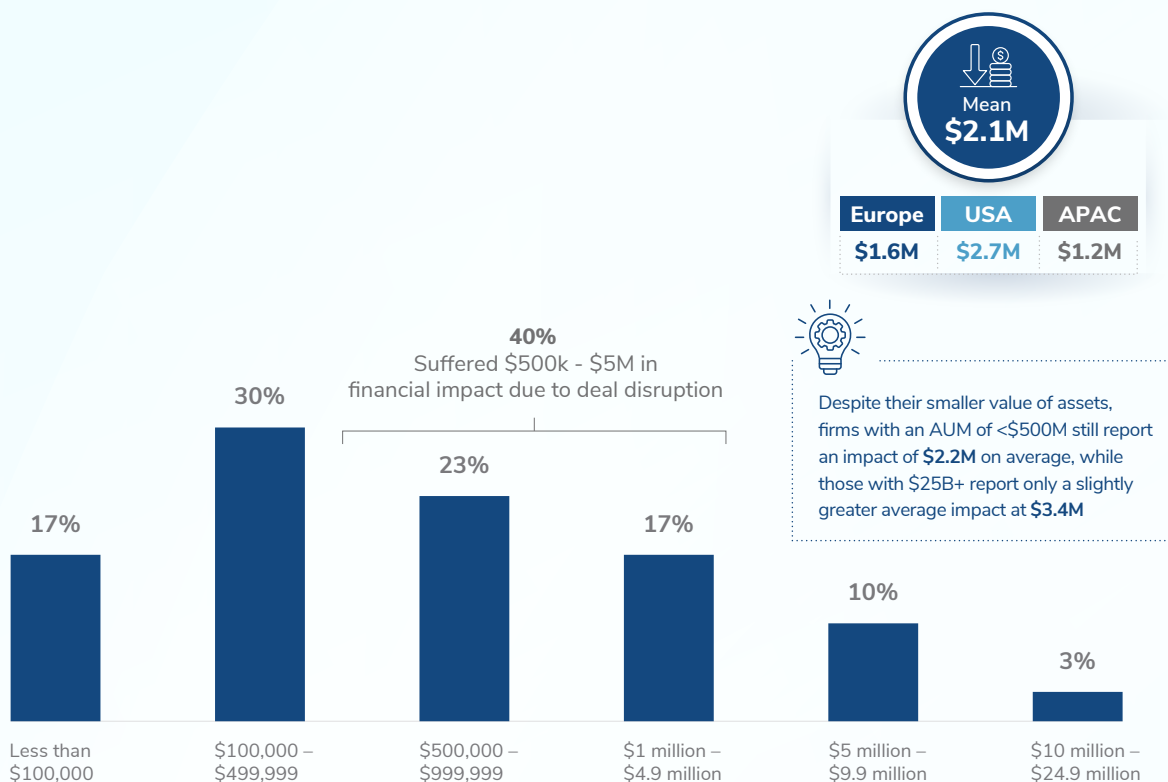
Fund Size Perspective

Lower AUM firms are far more likely to see valuation or exit prices reduced due to cybersecurity risk. Forty-four percent of firms with under \$500 mn in AUM reported a valuation reduction, compared with just 17% of firms with an AUM of above \$25 bn.

Financial Impact on Deal Disruption

The average approximate financial impact to deals that were disrupted due to cybersecurity risk was \$2.1 mn, and larger impacts were not uncommon.

- 53%** chance that a PE firm will lose more than \$500K due to cyber risk.
- 30%** chance that financial impact due to deal disruption will be more than \$1 mn.
- 13%** chance that financial impact of cybersecurity risk was more than \$5 mn.



Base: 307*

Asked only to those who experienced a financial impact

Q. What is the approximate financial impact to deals that were disrupted due to cybersecurity risk (USD)? Select one

Recent Incidents

The average loss of \$2.1 mn reflects many lower-level cyber incidents. In practice, funds must be prepared for far larger financial impacts, as recent high-profile attacks demonstrate.

[Marks & Spencer](#) suffered four months of downtime and saw nearly all profits erased. [Jaguar Land Rover](#) faced a five-week production halt, a 17.1% drop in quarterly retail sales, and £1.9 bn in costs.

A portfolio company hit with an incident of similar scale would face disruption far exceeding \$2.1 mn, which could jeopardize or even terminate a deal.

Fund Size Perspective

Larger PE firms reported larger financial impacts, while smaller firms reported smaller financial impacts.

- Thirty-seven percent of respondents representing PE firms over \$25 bn in AUM reported impacts of between \$1 and \$5 mn, with 20% of respondents reporting impacts of between \$5 and \$10 mn.
- Firms under \$25 bn in AUM reported typical impacts of between \$100K and \$500K, although impacts of between \$500K and \$1 mn were also common.

Comparing firms with an AUM of <\$25B to those with more than \$25B

		AUM in USD	
		Under \$25B	\$25B+
Financial Impact	Less than \$100,000	18%	3%
	\$100,000 – \$499,999	31%	20%
	\$500,000 – \$999,999	23%	17%
	\$1 million – \$4.9 million	15%	37%
	\$5 million – \$9.9 million	9%	20%
	\$10 million – \$24.9 million	3%	3%
	\$25 million or more	0%	0%
Mean		\$2.0M	\$3.4M

Base: 307*
Asked only to those who experienced a financial impact

Q. What is the approximate financial impact to deals that were disrupted due to cybersecurity risk (USD)? Select one



Larger PE Funds Are Leading the Way

Kroll's research shows a noticeable difference in how PE firms manage cybersecurity risk. Large firms have built disciplined, repeatable frameworks that help portfolio companies strengthen their defense. Measures larger PE firms take to govern cybersecurity risk include:

- Definition of expected security practices
- Collective procurement for security technology and services
- Adoption of fund-level risk management platforms and services

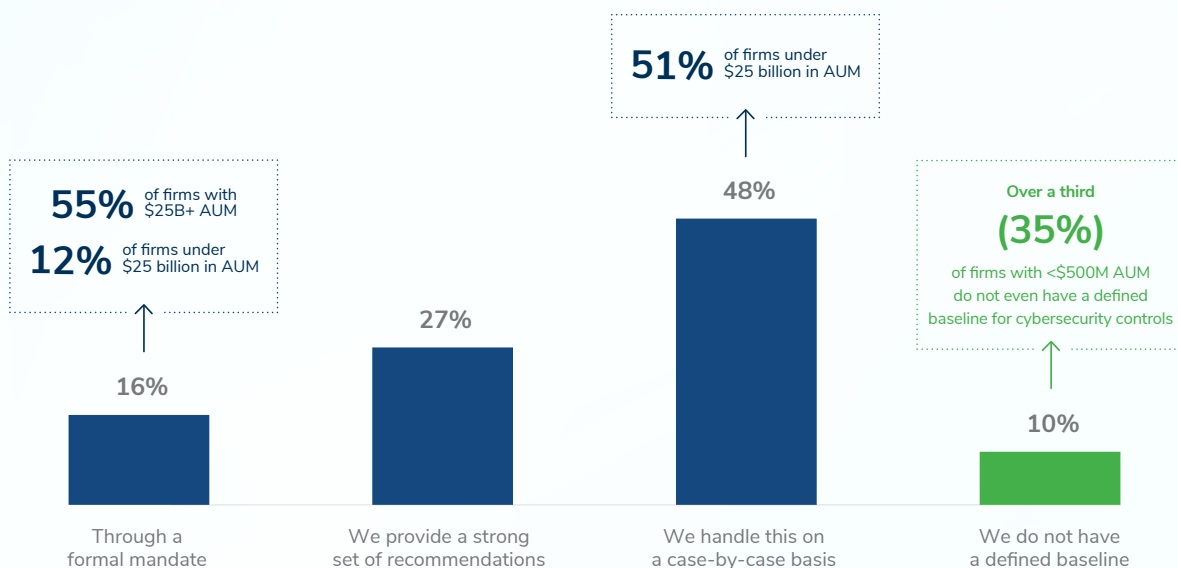
Smaller firms, by contrast, tend to operate with less robust risk management practices. That gap leaves them more exposed to costly remediation and a higher risk of deal disruption during exit transactions.

Baseline of Cybersecurity Controls

Only **12%** of smaller PE firms govern through a formal mandate, compared with **55%** of larger PE firms.

PE firms take very different approaches to baseline cybersecurity controls depending on their size. Among firms with more than \$25 bn in AUM, 55% enforce a formal, mandatory set of controls for portfolio companies. That drops sharply to 12% for firms with under \$25 bn in AUM.

Smaller firms are far more likely to manage cybersecurity on a case-by-case basis (51%), with only 27% offering strong but non-mandatory guidance. Most concerning, 35% of firms with under \$500 mn in AUM have no defined baseline at all, leaving them disproportionately exposed to financial and operational risk



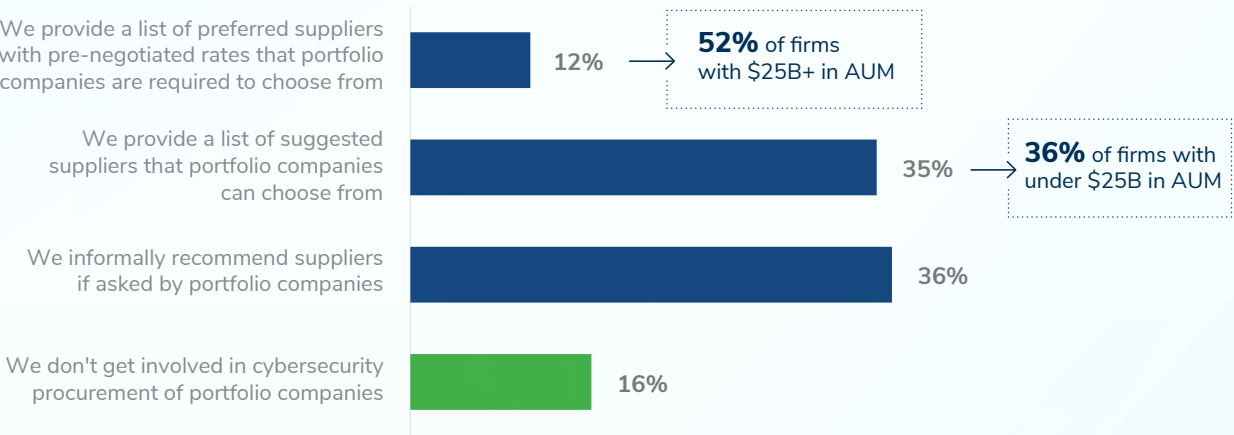
Base: 325

Q. To what extent does your organization implement a mandatory baseline of cybersecurity controls for portfolio companies?
Select one

Collective Procurement for Cybersecurity Technology and Services

Larger firms have built formal vendor relationships with pre-negotiated pricing, giving their portfolio companies access to stronger, more cost-effective cybersecurity solutions. Among firms with more than \$25 bn in AUM, 52% have established preferred technology and services providers.

Smaller firms, by contrast, rely far more on informal guidance, typically offering supplier recommendations on request (38%) or providing a suggested vendor list (36%). This indicates limited use of structured, collective procurement among lower-AUM firms.



Base: 325

Q. Does your firm engage in collective procurement for cybersecurity technology and services on behalf of the portfolio companies?
Select one

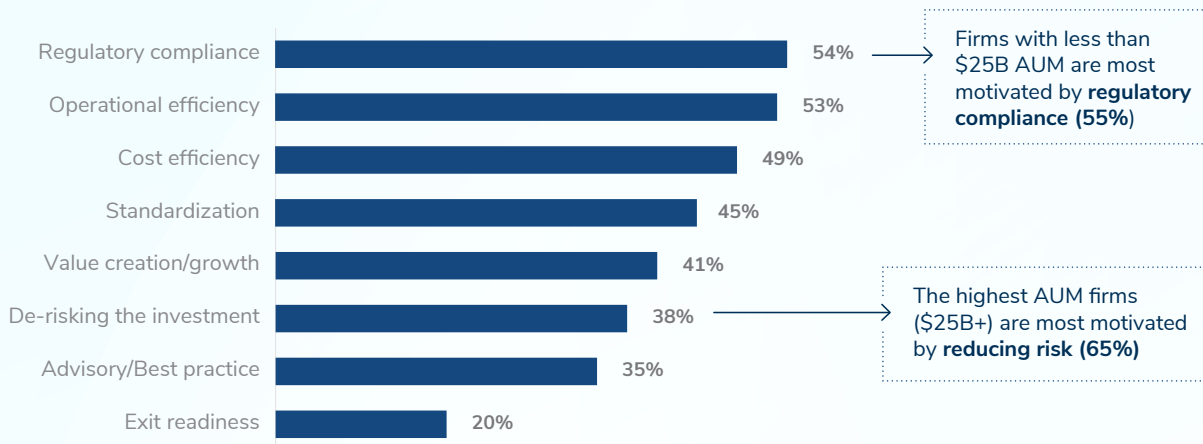


Reasons for PE Funds' Involvement in Procurement

The top drivers of collective procurement are regulatory compliance (54%), operational efficiency (53%) and cost efficiency (49%).

Smaller firms (those with under \$25 bn in AUM) follow this pattern, with 55% citing regulatory compliance as their primary motivator. For larger firms, however, the focus shifts: 65% say their involvement in cybersecurity procurement is driven by de-risking the investment. This split indicates differing levels of risk management maturity. Smaller firms concentrate on meeting regulatory requirements, while larger firms treat compliance as a baseline and prioritize reducing portfolio-level risk.

Collective procurement: **65%** of larger firms use it to de-risk investment, **55%** of smaller firms use it to comply with regulation.



Base: 279*

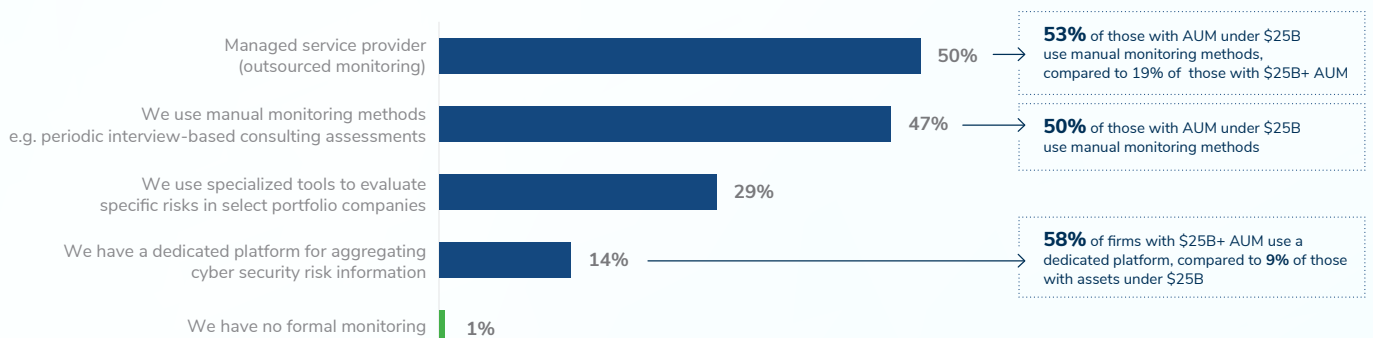
Asked only to those involved in procuring cybersecurity technologies

Q. What are the primary reasons your fund becomes involved in the procurement of cybersecurity technologies? Select all that apply

Cybersecurity Risk Management Tools

Larger PE firms take a more structured approach to managing cybersecurity risk across their portfolios. Fifty-eight percent of firms with more than \$25 bn in AUM use dedicated platforms to track and manage cyber risk, compared with just 9% of smaller firms.

Smaller firms rely heavily on manual monitoring methods (50%) and managed service providers (53%), whereas less than a fifth of large firms do the same (16% and 19% respectively).

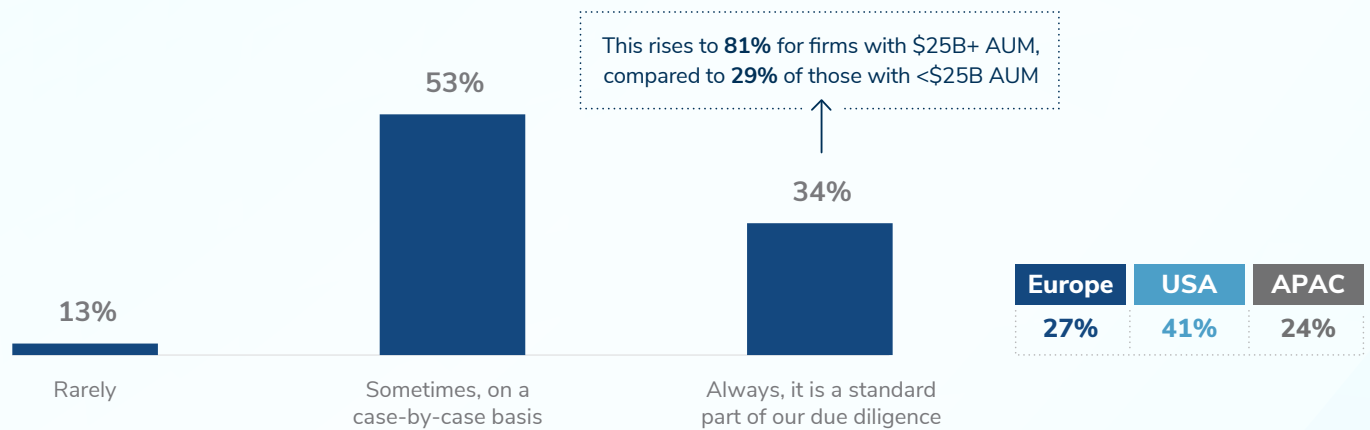


Base: 279*

Asked only to those involved in procuring cybersecurity technologies

Q. What technology and services does your firm use to monitor cybersecurity risk across your portfolio?

This discipline extends into dealmaking. Larger firms also apply far more rigorous cybersecurity due diligence. Eighty-one percent of firms with more than \$25 bn in AUM include cybersecurity as a standard part of transaction diligence, compared with just 29% of firms below that threshold.



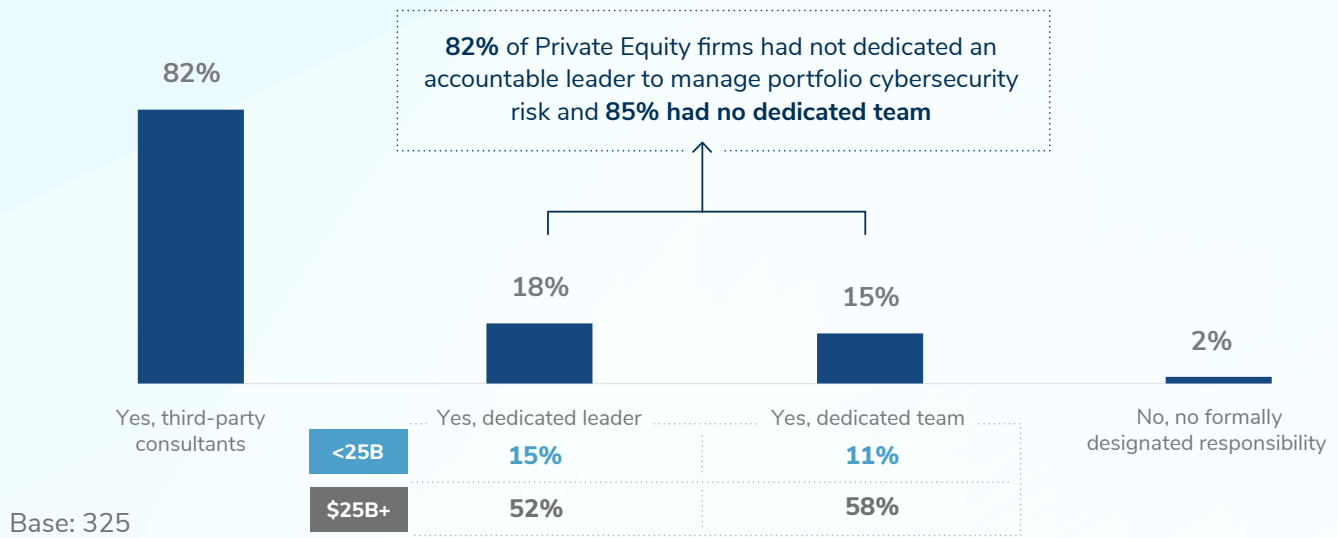
Q. How frequently are cybersecurity risk assessments conducted during your deal due diligence process? Select one

Due diligence as a standard part of transactions: **81%** of larger PE firms, **29%** of smaller PE firms.



Dedicated Cybersecurity Risk Leaders

Finally, larger firms with AUM of more than \$25 bn were much more likely to have a dedicated leader (52%) or team (58%) to manage cybersecurity risk for their fund's portfolio of companies. Comparatively, of those firms with under \$25 bn in AUM, only 15% had a dedicated leader and 11% had a dedicated team.



Q. Is there someone dedicated to managing cybersecurity risk for your fund's portfolio of companies?
Select all that apply

Dedication of an accountable leader or team to manage portfolio cybersecurity risk:

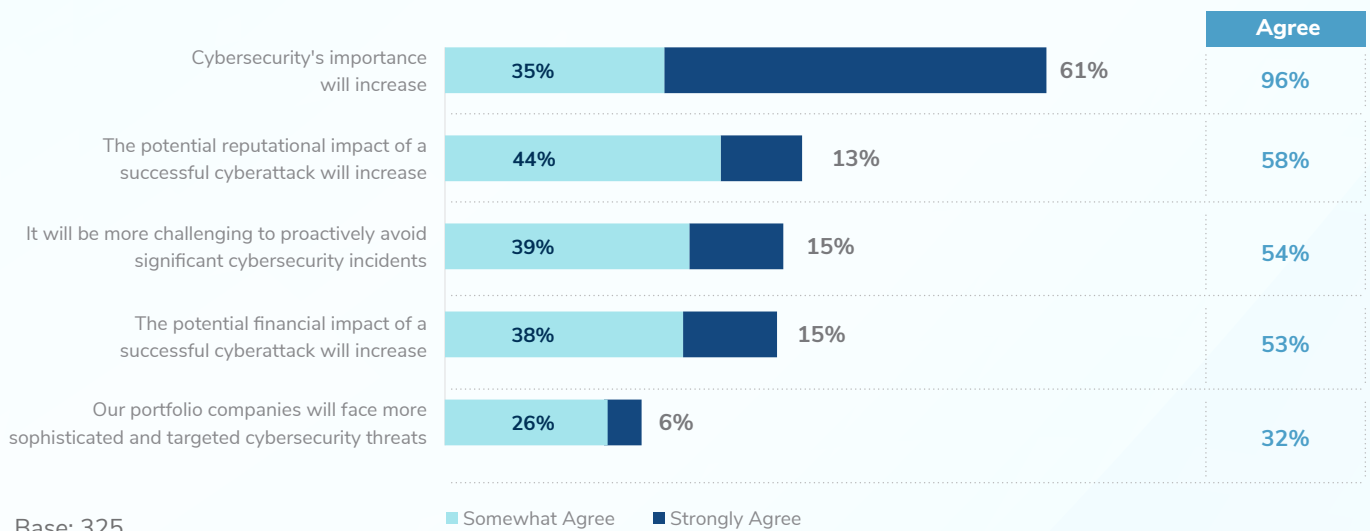
- **82%** of PE firms had no dedicated leader.
- **85%** of PE firms had no team in place.

How to Prepare for the Year Ahead

Nearly all respondents (96%) expect portfolio-company cybersecurity to grow in importance over the next year. Confidence is strongest in the U.S., where 79% “strongly agree” compared with 50% in APAC and just 33% in Europe.

Most respondents also anticipate tougher conditions ahead:

- Fifty-three percent expect the financial impact of cybersecurity incidents to rise.
- Fifty-eight percent foresee greater reputational fallout.
- Fifty-four percent believe avoiding major incidents will become more challenging.



Q. Thinking ahead over the next 12 months, please indicate your level of agreement with the following statements regarding your portfolio companies' cybersecurity? Select one per row

96% of PE firms agree that portfolio cybersecurity will grow in importance in the coming year. 61% strongly agree. This breaks out regionally to:

 **33%**
Europe

 **79%**
USA

 **50%**
APAC



Conclusion

In an increasingly volatile economic and geopolitical climate, effective risk management has become a defining capability for PE. Kroll's research shows how cybersecurity weaknesses inside portfolio companies now pose a material threat to deal value, often running into the millions when disruptions or unexpected remediation costs surface.

The pressure will only intensify. Rapid IT change driven by M&A, the rise of agentic systems and AI-enabled adversaries are reshaping the threat landscape. Firms that actively govern cybersecurity risk across their portfolios will feel less impact on valuations and deal timelines.

Mid-market and smaller PE firms are bearing the brunt today, facing outsized financial losses from cyber incidents. Larger firms—those above \$25 bn in AUM—are investing in more mature, fund-level risk-management frameworks and, in turn, experiencing fewer costly disruptions.

Looking ahead to 2026, PE funds should elevate cybersecurity to a formal portfolio-wide risk category. That means building visibility, adopting proven controls, and fostering a community of portfolio leaders who can share insights and raise standards collectively. Smaller firms that follow this path can replicate the protections already benefiting their larger peers.

For firms with more advanced capabilities, deeper involvement—such as technical validation of cybersecurity posture in higher-risk investments and at critical deal stages—will further strengthen resilience.

The message is clear: By taking measures to govern cyber risk across portfolio companies, PE firms will avoid disruption, limit financial impact, and secure exit value.



How Kroll Can Help

Kroll provides tailored [cybersecurity advisory services](#) that help PE firms manage cyber risk, protect portfolio value, and meet regulatory obligations such as [Regulation S-P](#), all while reducing exposure to reputational damage.



Example Client Journey

Kroll partners with you to enable business objectives while effectively managing cybersecurity risk. Our team of practitioners will tailor annual services to fit your business context, strengthen your defensive posture, and be resilient to cybersecurity threats.

	Year 1	Year 2	Year 3
Client Objectives 	Understand cybersecurity capabilities, risk exposure, compliance posture and raise awareness with staff	Transition a key system to a cloud service to support business growth	Prepare for a fundraiser or diligence visit – therefore addressing closed and open ended funds
How Kroll Supports 	• Cybersecurity Assessment and Roadmap • Governance Artifacts • Staff training	• IT Hygiene & Cloud Security Assessment • Penetration Testing • Managed Service Selection Support	• Investor & insurer due diligence support • Regulatory exam support
Outcomes 	Establish a three-year plan to improve cybersecurity resilience	Confidence that key systems are secure	Ability to successfully and efficiently respond to external inquiries

Why Choose Kroll

- o **Frontline Intelligence from 1000s of Acute Events Each Year** – we leverage frontline risk intelligence from handling thousands of incident response, regulatory response, financial crime and M&A due diligence engagements per year to anticipate the most likely risks to your business and reduce your unique risk profile.
- o **On the Panel of 85+ Insurance Carriers** – Kroll has a dedicated insurance team for insurance and legal channels, with extensive relationships with 85+ cyber insurance carriers and exclusive benefits to insureds.
- o **Experienced, Accredited Cybersecurity Professionals** – 650+ skilled and certified cybersecurity experts across the globe.

Methodology

Kroll commissioned independent firm, [Sapio Research](#), to conduct a study into the cyber risk presented by portfolio companies to PE firms globally.

The research surveyed 325 portfolio leaders involved in the oversight of technology and cybersecurity risk within a PE fund. Their area of responsibility was predominantly in investment and portfolio management (55%) but also included legal/compliance (23%), risk management (12%) and IT/Security (10%).

Thirty-seven percent of funds studied had between \$1 bn and \$4.9 bn AUM. Thirty-two percent had more than \$5 bn AUM, 13% between \$500 mn and \$999 mn, 19% less than \$500 mn.

The study includes PE firms operating worldwide, with respondents based in USA (175), UK and Ireland (50), Australia (25), Germany (25), Switzerland (25), Singapore (13) and Japan (12).

All research was gathered using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate.

The field research was done in December 2025 and publicly announced in 2026.



Real World PE Challenges

PE firms face persistent challenges gaining visibility into the cyber maturity of portfolio companies, limiting fund-level risk management practices and increasing the likelihood of deal disruption or value erosion.

Kroll works with private equity firms across the full PE landscape, including the PEI 300.



Common Cybersecurity Challenges:

- Limited visibility into portfolio wide cyber risk
- Difficulty implementing consistent security capabilities across the portfolio
- Regulatory and compliance exposure driven by insufficient controls



Core Solutions:

- Cyber due diligence embedded as a standard deal process
- Ongoing, portfolio level cyber risk monitoring
- Standardized baseline of cybersecurity controls
- Advisory support for portfolio company leadership teams



Business Impact of Cyber Portfolio Monitoring:

- Increased risk visibility across the portfolio during the hold period
- Ability to drive remediation within high-risk portfolio companies
- Reduced deal disruption and execution risk
- Improved ability to realize value within investment timelines
- Ability to provide assurance to LPs regarding cybersecurity risk management



Contributors



Dave Burg

Global Group Head of Cyber
and Data Resilience
+1 202449 1844
dave.burg@kroll.com



Rachel Posner

Chief Client Officer
+1 21 283 33471
rachel.posner@kroll.com



Brent Tomlinson

President, Risk Advisory
+1 84 772 72361
brent.tomlinson@kroll.com



Jon Pratt

Managing Director,
Growth Team
+1 85 732 76000
jon.pratt@kroll.com



Adam Malone

Global Head, Acute Events
Cyber and Data Resilience
+1 67 840 33245
adam.malone@kroll.com



Ross Hostetter

Managing Director
Global Alternative Asset Advisory Leader
+1 21 287 15977
ross.hostetter@kroll.com



Eric Hasty

Associate Managing Director
Cyber and Data Resilience
+1 31 269 74712
eric.hasty@kroll.com



Ryan McNelley

Managing Director
EMEA Portfolio Valuation Leader
+44 20 708 94822
ryan.mcnelley@kroll.com



Owen Wagoner

Senior Vice President
Cyber and Data Resilience
+1 21 2833 3293
owen.wagoner@kroll.com



Anna Cuisia

Director
Marketing
+1 21 283 33362
anna.cuisia@kroll.com



Simon Onyons

Managing Director
Cyber and Data Resilience
+44 207 029 5388
simon.onyons@kroll.com



Lindsey Challis

Senior Manager
Marketing
+1 41 636 12590
lindsey.challis@kroll.com



Nicole Koopman

Global Head of Commercial Office
and Managing Director, Enterprise
+1 212 833 3258
nicole.koopman@kroll.com



About Kroll

As the leading independent provider of financial and risk advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at [Kroll.com](https://kroll.com).

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.