KPMG

When cyber breaks the deal

How a single breach could erase M&A value in the energy sector

AI generated image

Introduction

Larger, portfolio-defining merger and acquisition (M&A) transactions are reshaping the energy sector. Deal value surged 38 percent in the second half of 2025,[1] building momentum for further consolidation. With these bigger deals comes greater execution risk, and cybersecurity is emerging as a critical fault line as complex transactions move faster than diligence processes can support. In energy, the vulnerability that matters most often appears after the handshake when integration exposes weaknesses missed during deal diligence.

Energy acquirers prioritize predictable cash flows and reliable systems to mitigate strategic and valuation risk and limit execution uncertainty. Bridging wide valuation gaps in the sector with deal-structuring workarounds such as minority rollups, buyers are counting on smooth integrations to preserve upside and quickly move to executing their long-term strategies. That reliance on fast, frictionless integration leaves little margin for error, making latent cyber risk far more likely to surface as a value-eroding event during execution.

Adverse cybersecurity events can quickly unravel that integration logic. Companies struggle to integrate technology in a sector dependent on legacy, bespoke infrastructure, often inherited through years of prior consolidation. As operational, information, and artificial intelligence (AI) platforms converge, integrations expand attack surfaces precisely when access controls, visibility, and accountability are in flux. In that environment, a single cyber incident can delay integration, erode deal value, and expose risks that diligence never had time to surface.

That risk is compounded by limited visibility into the target's cybersecurity practices during the deal process. Without line of sight, acquirers risk inheriting embedded vulnerabilities across legacy infrastructure and operational systems. Short timelines, restricted access, and incomplete documentation frequently limit meaningful assessment ahead of close. The result is exposure to latent "gotchas" that can undermine confidence in the target asset, erode potential value, and consume critical integration capacity.

[1] KPMG, "M&A trends in energy, natural resources, and chemicals: H2 2025," February 20, 2026.

Meanwhile, cyber risk across the energy sector is accelerating. Recent KPMG industry analysis shows that ransomware activity against energy and utilities organizations increased sharply from 2024 to 2025, with third-party software and service providers accounting for a significant share of reported breaches. As digital interconnections increase, acquirers face a higher likelihood that material cyber exposures already exist inside a target's operating environment before diligence begins.[2]

Deals can turn latent cyber exposure from theory to reality. The act of integrating systems, extending trust relationships, and altering network boundaries can activate previously dormant vulnerabilities, converting inherited cyber risk into immediate operational and financial exposure at precisely the moment organizations are least able to absorb disruption. This is often where cyber risk shifts from a diligence concern to an integration challenge that unfolds in real time as systems, teams, and controls are brought together.

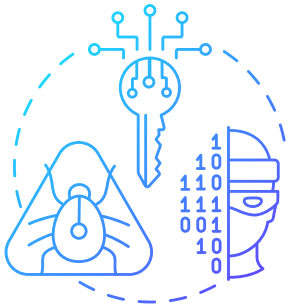
In the energy sector, AI is already embedded in operational technology (OT), supporting predictive maintenance, real-time grid optimization, distributed energy-resource coordination, and cyber-physical anomaly detection. When transactions combine or reconfigure these systems, they expand the digital footprint of energy infrastructure and heighten the operational and safety consequences of integration missteps—particularly while cyber controls are still being rationalized postclose.[3]

Here we outline how energy dealmakers can assess a target's cybersecurity posture before, during, and after a transaction to facilitate the safety and success of their acquisition.

[2] "A Quantitative Analysis of Cyber Risks in the U.S. Energy Supply Chain," SecurityScorecard and KPMG LLP, October 23, 2024

[3] "Grid Security: New Vulnerabilities in Solar Power Systems Exposed," Forescout Research – Vedere Labs, March 27, 2025

How energy deals raise the stakes



Heavily regulated and vital to everyday life, energy companies operate in an environment where operational failure carries immediate public and economic consequences. Energy infrastructure underpins power delivery, industrial production, and public safety, placing cyber risk squarely within the realm of national security and economic resilience. As these systems become more digital and interconnected, cyber incidents can disrupt essential services, destabilize markets, and strain public trust, especially amid heightened geopolitical tension and increased targeting of critical infrastructure.

During M&A integration, acquirers can unintentionally trigger dormant threats embedded in target-company systems, open security gaps to attackers, or weaken defenses through integration shortcuts. Integration is the inflection point where inherited exposure, expanded access, and execution pressure converge, allowing missteps to escalate quickly into operational, regulatory, and resilience risks with consequences that extend well beyond the deal itself.

Where M&A integration exposes latent cyber risk

M&A creates a transition state that threat actors actively seek to exploit. In that window, cybersecurity attention must focus on critical infrastructure and vendor dependencies, along with two core considerations:

1 Legacy systems power modern risk

OT supports critical energy infrastructure and was designed for long-term reliability, often relying on isolation rather than continuous connectivity for protection. M&A integration disrupts those assumptions. As energy companies digitize operations and connect information technology (IT) and OT environments, systems never built for frequent change or shared controls gain new access paths, introducing risk at the moment they are being reconfigured.

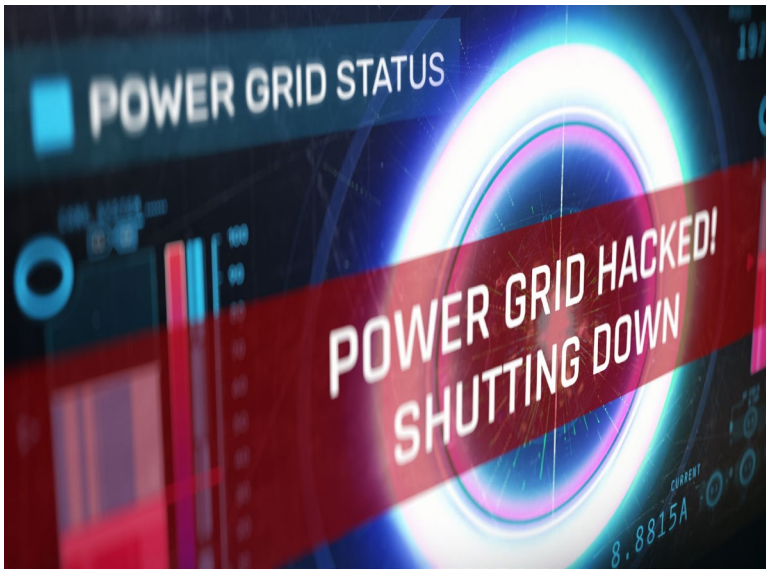
These integration activities create new cyber risk seams—points where disparate systems, processes, and controls intersect—making it easier for vulnerabilities to emerge and harder for organizations to maintain consistent security.

Identifying and addressing these seams early is critical to reducing exposure during integration. That exposure is structural. The energy sector consistently accounts for a high share of disclosed industrial control system and OT vulnerabilities, many embedded in legacy platforms that are difficult to patch or replace. As distributed energy assets and internet-exposed control interfaces proliferate, acquirers may inherit latent cyber risk that diligence has limited ability to surface.[4] During integration, failures in inherited OT environments can escalate quickly—into operational disruption, regulatory scrutiny, and erosion of deal value—precisely when execution.

2 Third parties expand the attack surface

As the sector's dependence on original equipment manufacturing partners and other third-party software and services vendors grows, so does the number of system connections—each a potential attack point. Third-party security practices are frequently opaque, and inconsistent standards can result in misalignments that introduce new vulnerabilities.

Integration amplifies that risk. Third-party connections extend trust beyond the enterprise boundary, introducing exposure through vendor access, remote connectivity, and outsourced system administration. In many energy transactions, vendors govern these dependencies through contractual assurances rather than direct technical control, limiting an acquirer's ability to detect issues or enforce remediation during integration.



[4] "Industrial Control Systems Advisories," U.S. Cybersecurity and Infrastructure Agency (CISA), 2024–2025; "Grid Security: New Vulnerabilities in Solar Power Systems Exposed," Forescout Research – Vedere Labs, March 27, 2025

Why contracts alone aren't enough

Sellers can support the acquisition process by sharing details about their cybersecurity practices, but responsibility ultimately lies with acquirers to examine the systems, practices, and compliance of the assets they are buying. Contractual safeguards, while helpful, can't replace the rigor of a comprehensive technical evaluation. In the event a seller discloses an actual breach, acquirers should promptly engage cyber response professionals to support digital forensics, incident investigation, and remediation planning. Securing evidence; understanding the breach; and evaluating its legal, regulatory, and reputational fallout during the deal process are essential.

Sometimes the challenge of assessing a target's cyber posture falls to the acquirer, which may lack the experience needed to evaluate cyber risk under deal pressure. Too often, legal and strategic priorities crowd out technical diligence, leaving material cyber risks insufficiently examined during the transaction.

How acquirers regain control

With a disciplined approach to cybersecurity evaluation, acquirers in the energy sector can reduce the likelihood that cyber risk becomes a deal breaker, protect critical assets, and preserve value during integration. Early compromise assessments, which are designed to determine whether a threat actor is already present in a target's environment, provide real-time insight into vulnerabilities and inform integration decisions. While deploying these capabilities before an acquisition can be challenging, rapid deployment during clawback evaluation periods helps confirm whether the target's actual cyber risk posture aligns with acquisition representations.

Centralize cyber authority early

With the support and oversight of company leadership, form a specialized cybersecurity task force to identify industry-specific cyber and control risks and align deal objectives with operational technology capabilities. This "tiger team" guides information collection, ensuring that seller documentation explicitly correlates remediation costs with potential operational and financial impacts.

Assessment strategies should account for industry-specific risk factors, acquisition objectives, and applicable regulatory and compliance requirements—particularly in cross-border transactions. Acquirers should also weigh the cost of assessment and prevention against the potential cost and complexity of breach response.

Make cyber diligence nonnegotiable

During the critical 30–60-day presigning period, gather preliminary information on the target's cybersecurity posture, policies, and procedures. This high-level diligence should combine document reviews, interviews, and structured questionnaires to identify critical risks and assess compromise exposure, breach risk, and relevant threat intelligence. Acquirers should request detailed security posture representations from the seller and follow up as needed to obtain greater specificity.

During the negotiation phase, rigorous definition of OT technical controls within the transition services agreement is critical to their integration into the cybersecurity framework.

Acquirers should clearly understand what services are being provided, how they will be delivered, and who is responsible for them to maintain continuity of operations and an appropriate cybersecurity posture.

Verify reality before integration begins

After closing the transaction, promptly identify and assess cyber risks within the new enterprise and verify them against the statements and assurances made during due diligence. Before full integration and the conclusion of the clawback period, identify any discrepancies that could lead to additional costs or trigger previously agreed-upon clawback provisions. If the seller has disclosed a prior breach, then evaluate its scope, remediation status, and any residual risk.

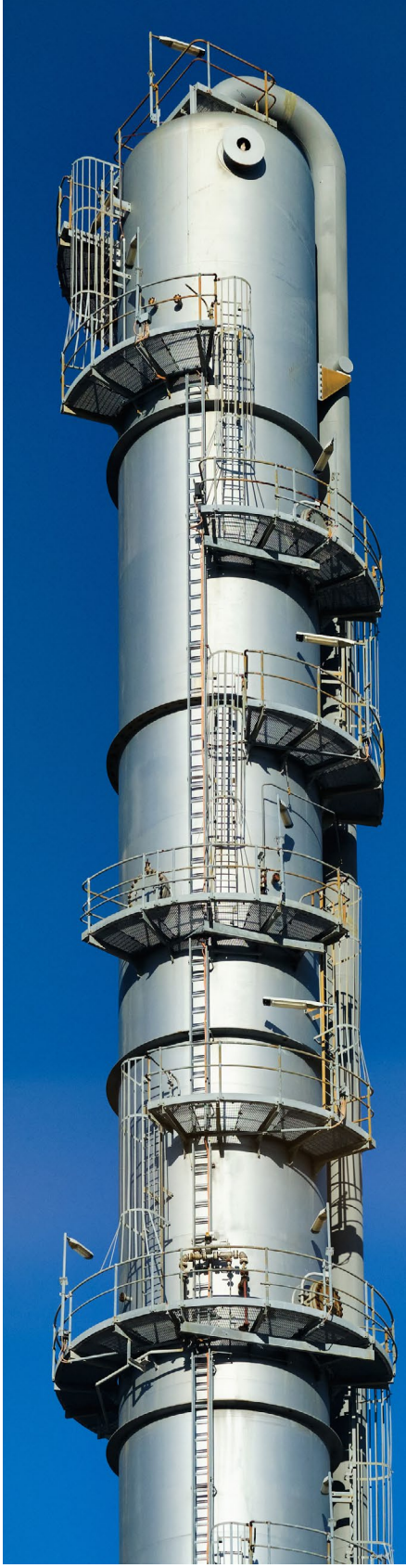
Assume risk doesn't end at close

Ongoing assessments are critical to identifying and defending against new vulnerabilities long after the deal closes. This phase should focus on continuously evaluating and strengthening security measures to help ensure the integration process does not introduce new weaknesses.

The most effective mitigation strategy is to plan a holistic IT integration—one that encompasses all systems, processes, and controls—and drive it through to completion. By approaching integration comprehensively and following through on execution, companies can minimize cyber risk and preserve deal value Implement enhanced security controls—including OT detection capabilities, segmentation, and endpoint detection and response and extended detection and response—for near-real-time alerts, and integrate the new entity into existing incident response plans. Connect key stakeholders with the acquirer's Security, IT, and SecOps teams to provide coordinated oversight and seamless integration.

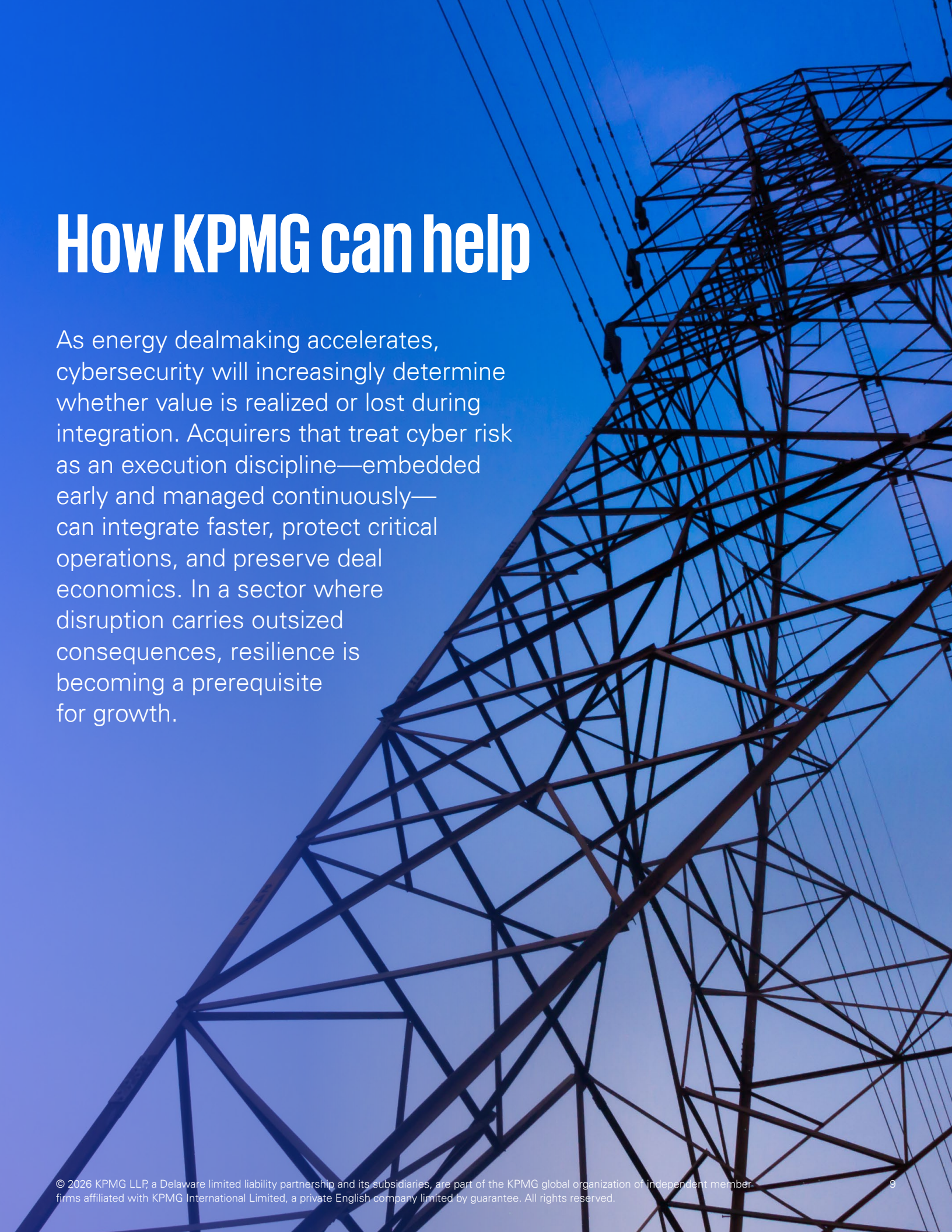
Integration succeeds or fails with people

Following an acquisition, integration pressures can strain established controls and introduce new behaviors, systems, and ways of working. Embedding cybersecurity as a shared responsibility across daily operations helps reduce reliance on technical controls alone and limits risk introduced during integration. This requires building awareness, shaping behaviors, and reinforcing proactive security practices across the combined workforce. Clear policies and procedures—supported by education, accountability, and recognition—are essential to embed cybersecurity expectations and sustain resilience over time. Where a prior breach is disclosed, integration leaders should clarify ownership for remediation, confirm that root-cause findings have been validated and addressed, and incorporate lessons learned into integration planning to prevent recurrence.



How KPMG can help

As energy dealmaking accelerates, cybersecurity will increasingly determine whether value is realized or lost during integration. Acquirers that treat cyber risk as an execution discipline—embedded early and managed continuously—can integrate faster, protect critical operations, and preserve deal economics. In a sector where disruption carries outsized consequences, resilience is becoming a prerequisite for growth.



Authors

Jason Haward-Grau

Principal, Advisory – Energy & Chemicals, Cyber & Tech Risk, KPMG LLP

Jason is the Global Cyber Recovery Services leader and a principal at KPMG in the US. He brings more than 20 years of experience leading cybersecurity, IT, and risk transformations for complex organizations, with deep experience in industrial and operational technology environments. In recent years, Jason has focused on helping energy and industrial companies strengthen cyber resilience across OT systems, integration programs, and large-scale transformations. He is also an experienced former chief information security officer, having led enterprise-wide cyber, risk, and compliance programs.

Jay Teinert

Principal, Advisory – Energy & Chemicals, Transaction Strategy, KPMG, LLP

Jay is the energy industry lead principal for the KPMG Deal Advisory & Strategy practice. He advises clients on large, complex transactions, with a focus on buy-side integration, sell-side separation, and value realization across the deal lifecycle. With more than 25 years of experience in M&A and corporate finance, Jay has led some of the firm's largest energy transactions. Prior to joining KPMG, he held senior commercial and M&A roles at a global energy company, where he managed multibillion-dollar investment programs and integration initiatives.

Brad Stansberry

Partner, Advisory – Energy & Chemicals Consulting Leader, KPMG LLP

Brad brings more than 25 years of experience delivering results on complex projects for finance function leaders in the energy and utility industry. As the leader of the Energy & Chemicals Advisory practice at KPMG, his focus is on helping chief financial officers and finance executives in the energy and chemical industries to run the "business of finance" better. This includes a focus on defining finance organization strategy and objectives, improving finance processes, deploying enabling technologies, enhancing finance talent and skills, and being a more valued service provider to their business constituents.

We would like to thank our contributors:

Karen Henrie, Leah Lockwood, and Kathy Wheeler

For more information, contact us:

Jason Haward-Grau
Principal, Advisory – Energy & Chemicals, Cyber & Tech Risk
713-319-2079
jhawardgrau@kpmg.com

Brad Stansberry
Partner, Advisory – Energy & Chemicals Consulting Leader
214-840-6026
bstansberry@kpmg.com

Jay Tienert
Principal, Advisory – Energy & Chemicals, Transaction Strategy
214-840-8082
jtienert@kpmg.com

Related thought leadership:

CISO Boardroom Strategy

M&A trends in energy, natural resources and chemicals H2-25

Buy smarter, not riskier: Cyber resilience in life sciences M&A

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: **kpmg.com** **Subscribe**

DASD-2026-20044