



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

Protecting IP  
and privacy in the  
life sciences M&A  
deal cycle

---

[kpmg.com](https://kpmg.com)



Sweeping shifts in corporate technology and accelerating digitalization are testing cybersecurity resilience. Although companies are using advanced techniques to defend their internal systems and monitor third-party dependencies, even the most sophisticated are challenged to identify threats across a new, larger attack surface.

For life sciences organizations, mergers and acquisitions (M&A) raise the stakes. In this highly regulated, data-sensitive industry, safeguarding customer privacy and intellectual property is critical—and uncovering cyber vulnerabilities early can make or break a deal.

M&A often introduces unfamiliar systems, inconsistent controls, and inherited vulnerabilities that can go undetected without early, rigorous scrutiny. Securing a dynamic technology estate already presents a formidable challenge; evaluating the cybersecurity posture of an unfamiliar acquisition target, often under intense time pressure; adds to the challenge. Yet dealmakers often consider cyber risk as an afterthought, rather than as foundational to deal evaluation.

In this article, we examine critical cybersecurity considerations in life sciences transactions and outline emerging standards for due diligence and assessment. We also offer practical steps that acquisitive life sciences companies can take to mitigate risk, safeguard deal value, and protect their most precious asset: information.





# The hidden costs of cyber in M&A

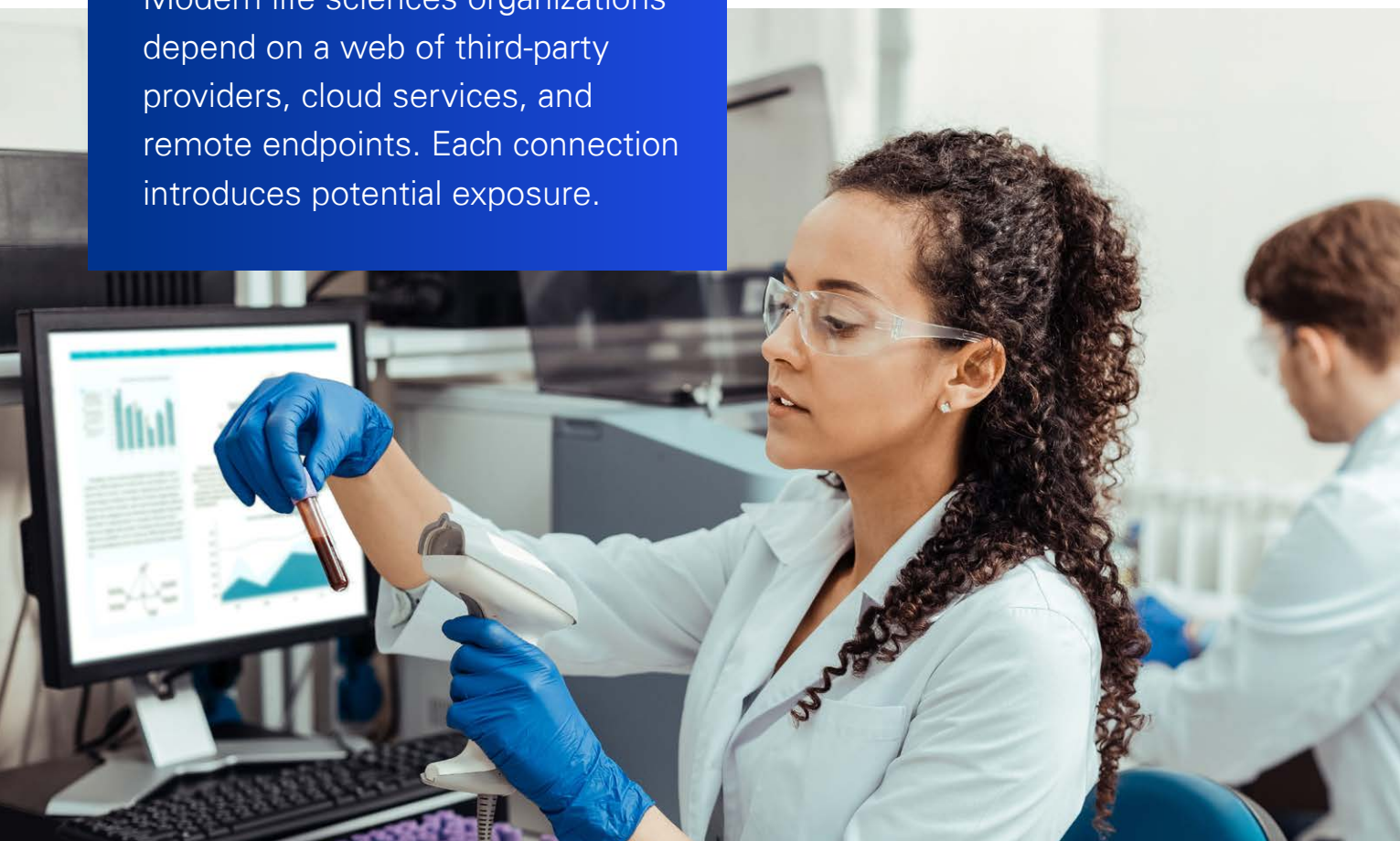
Acquirers may inherit substantial cyber risk along with a target's valued assets. Whether the target is a sprawling enterprise with legacy systems or a nimble startup built on cutting-edge IP, the cyber risks are real, and often underestimated. Modern life sciences organizations depend on a web of third-party providers, cloud services, and remote endpoints. Each connection introduces potential exposure.

The vulnerabilities are varied and often hidden. For example, they may include open-source code with undisclosed flaws, opaque service providers, or unsecured data transfers between legacy and modern systems.

Emerging technologies add complexity. Generative AI (GenAI) and automation promise efficiency but introduce additional risks—black-box algorithms, ethical concerns, and regulatory uncertainty.

Although the responsibility for identifying and remediating cybersecurity target risk rests with acquirors, they may bring critical weaknesses in their process. These include insufficient skills to evaluate the target's cyber risk posture, cybersecurity teams' subordination to business and legal considerations within the due diligence process, compressed deal timelines, and inexperience in M&A generally.

Modern life sciences organizations depend on a web of third-party providers, cloud services, and remote endpoints. Each connection introduces potential exposure.



# Distinct cyber considerations in life sciences M&A

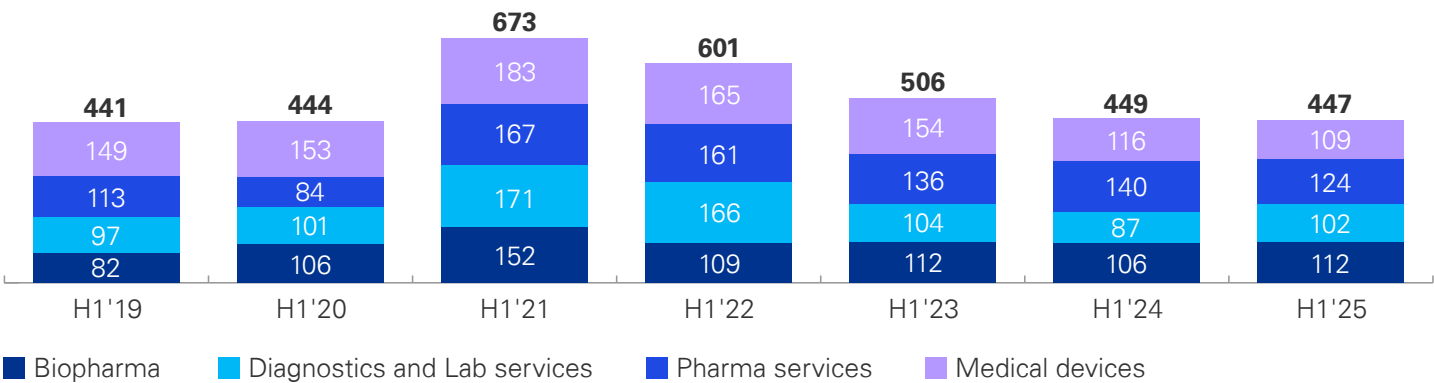
M&A valuations across life sciences are mixed in 2025. Companies are paying a premium for desirable assets, including late-stage oncology and GLP-1 (obesity) adjacent treatments, while multiples remain subdued in areas such as biotechnology and medical technology.

Cyber threats not only pose operational risks but also may have regulatory and reputational consequences, making early intervention essential. Avoiding cybersecurity

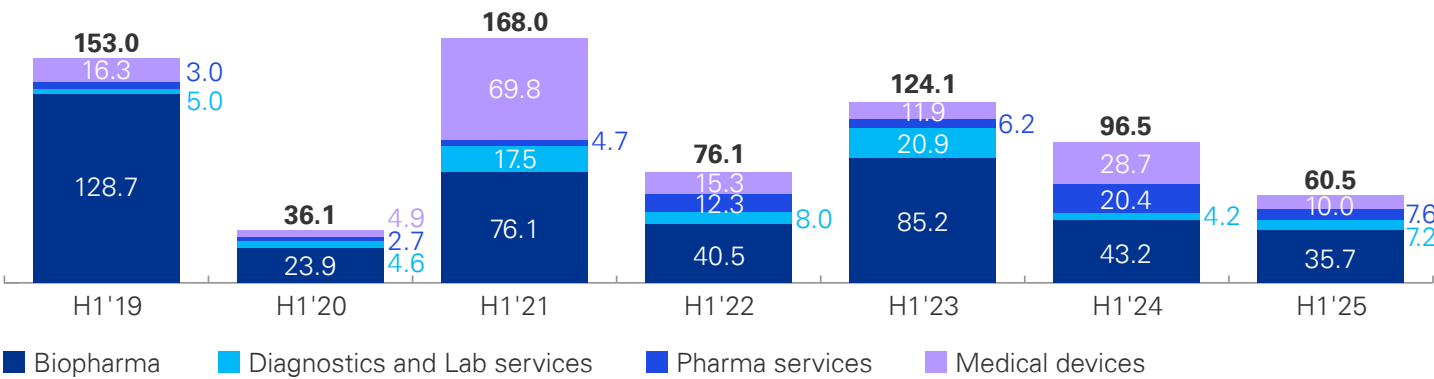
“gotchas,” especially in the high-demand subsectors, can preserve return on investment and the strategic value of a deal, while safeguarding the customer privacy and intellectual property that are the lifeblood of the industry.

With the deal pipeline more selective, fewer megadeals, and lower aggregate value in H1, acquirors are emphasizing targeted diligence, including cyber, earlier in the process.

## Life sciences deal volume by subsector



## Life sciences deal value (US\$B) by subsector



Source: Deal data has been sourced from Capital IQ, Refinitiv and Pitchbook, and then further refined and analyzed by KPMG LLP. The cited values and volumes cover US deals announced or closed during the timeframe, including both majority and minority stakes. Deal values are based on publicly available data and are not exhaustive. Only transactions with US-based targets are included. Previously published statistics may be revised to incorporate new data or changes.

Larger companies are focusing on innovation, especially in areas like precision medicine, biotechnology, and personalized therapies. They are taking chances on start-ups with potentially breakthrough intellectual property (IP) but limited operating experience and potentially less cybersecurity awareness.

These targets often operate within complex ecosystems of vendors, partners, and interconnected systems that multiply potential vulnerabilities. The life sciences industry's unique risk profile extends from broad external dependencies through regulatory requirements down to the protection of core assets and specific technical vulnerabilities.

**Acquirers must evaluate these interconnected layers of risk, starting with the full ecosystem view and drilling down to specific vulnerabilities:**



### Third-party and "nth-party" risk exposure

Acquirors should assess not only direct third-party risks but also the extended chain of dependencies, including opaque AI-driven platforms and automation tools that may introduce hidden vulnerabilities.



### Compliance with regulations

Life sciences companies must comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and regulations in Europe. These regulations mandate strict data protection standards and impose heavy penalties for noncompliance. M&A activities should include thorough compliance checks to ensure the acquiree adheres to these regulations and has policies and practices in place to maintain compliance.



### Intellectual property protection

This often represents a company's most valuable asset, including patents, proprietary research, and unique technologies. During M&A, this involves ensuring robust cybersecurity measures prevent unauthorized access and safeguard sensitive information throughout the transaction process. Due diligence should include assessing the strength of the target's IP protection mechanisms and understanding any potential IP-related disputes or vulnerabilities.



### Patient data protection

The protection of patient data, especially information such as genetic profiles, biomarker data, and individualized treatment plans, requires rigorous safeguards given the privacy and ethical stakes. This involves implementing stringent data encryption protocols and access controls and complying with relevant healthcare laws and regulations. During M&A, understanding how the target company manages and secures patient data is crucial to avoid breaches that could lead to significant legal and reputational risks.



### Fragmented technology systems

The acquisition process often exposes varied levels of cybersecurity maturity across different networks and systems. Fragmented technology systems can pose integration challenges and increase vulnerabilities. Conducting a cybersecurity assessment of the target's networks is essential to identify weak points and develop a strategy for harmonizing the cybersecurity posture across all systems, particularly in diverse environments such as patient and provider offices.



### Connected medical devices

The rise of Internet of Things (IoT) devices in healthcare, such as connected medical equipment, introduces new security considerations related to resilience and protection against cyberattacks. Ensuring these devices are secure is crucial to preventing data breaches and unauthorized access. M&A due diligence should evaluate the security measures in place for IoT devices and consider necessary upgrades to meet cybersecurity standards.






# Preparing for the deal

When equipped with the right process and tools, organizations can close critical cybersecurity gaps in acquisition targets, implement remediation plans, and concentrate on realizing the deal's strategic and integration objectives. Addressing these areas requires a comprehensive strategy that engages cybersecurity experts, legal teams, and business leaders early in the M&A lifecycle, well before deal closing, to mitigate risks

and support the seamless integration of technologies and data protection practices

But the work on identifying, planning for, and remediating cybersecurity vulnerabilities really begins even before there is a deal. Given these high-stakes challenges, life sciences companies must be particularly attentive to compliance, protecting against data breaches, and mitigating target vulnerabilities.

## Exhibit Mitigating cyber risk across the deal life cycle:

Deal phase		Actions
Strategy & evaluation		<ul style="list-style-type: none"><li>• Form cyber "tiger team" (cyber, legal, compliance, risk)</li><li>• Develop cyber due diligence playbook</li><li>• Identify sector-specific risks (e.g., HIPAA, GDPR, connected medical devices)</li><li>• Conduct early threat intelligence scans</li></ul>
Pre-signing due diligence		<ul style="list-style-type: none"><li>• Deploy automated vulnerability scanners &amp; EDR/XDR tools</li><li>• Use AI-powered risk analytics to quantify exposures</li><li>• Review incident history &amp; compliance posture</li><li>• Conduct preliminary compromise assessments</li></ul>
Integrate cyber risk into deal economics		<ul style="list-style-type: none"><li>• Translate risk findings into financial impact models</li><li>• Adjust valuation and indemnities (e.g., escrow, indemnities)</li><li>• Incorporate remediation requirements into integration planning</li></ul>
Pre-closing maturity assessment		<ul style="list-style-type: none"><li>• Conduct technical penetration testing &amp; architecture review</li><li>• Assess regulatory compliance gaps (HIPAA, GDPR, FDA)</li><li>• Map data flows and access-controls</li><li>• Align high-priority remediation items</li><li>• Establish post-close integration roadmap</li></ul>
Post-close integration & continuous monitoring		<ul style="list-style-type: none"><li>• Implement continuous monitoring (SIEM, SDAR, threat intel feeds)</li><li>• Strengthen incident response plans on tabletop exercises</li><li>• Harmonize policies and controls across merged entity</li><li>• Conduct periodic post-integration maturity assessments</li></ul>



# Acquirors can take steps to prepare before dealmaking:



## Create a cybersecurity “tiger” team

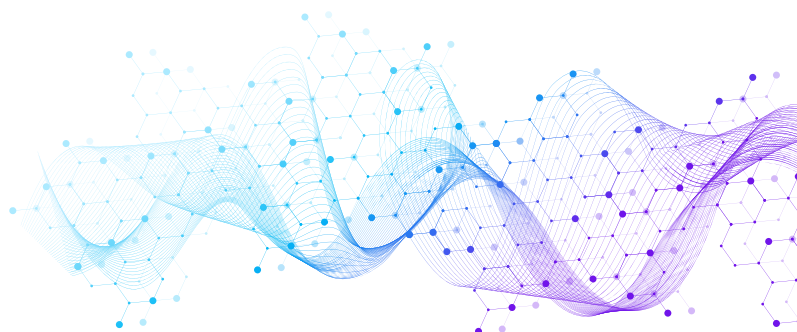
This team is responsible for assessing, managing, and mitigating cybersecurity risks associated with the transaction process. The team includes a cyber lead, security and privacy specialists, a risk management expert, and other specialists in technology, risk, and compliance.

## Make an M&A playbook

This provides a structured approach to identifying, evaluating, and remediating cybersecurity risks throughout the acquisition process, including steps to secure executive buy-in for cyber review and activate the tiger team.

## Address talent and skill gaps in cybersecurity teams

Cybersecurity talent is in short supply, and many targets, especially start-ups, may lack the internal expertise to manage risks effectively. Acquirors should be prepared to supplement or restructure cyber capabilities postclose.



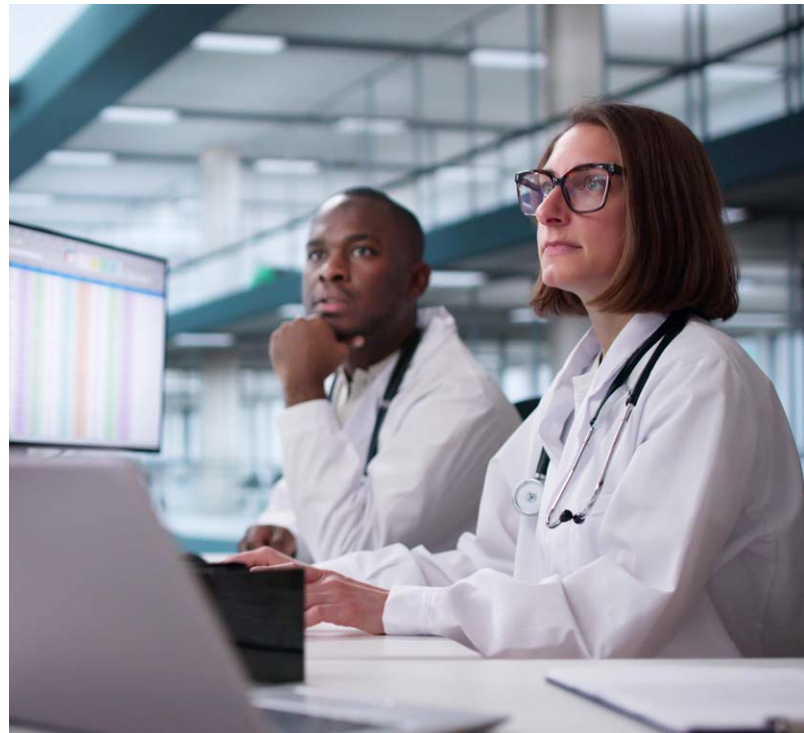
## Deploy real-time threat intelligence and automation tools throughout the deal lifecycle

Advanced security technologies should be embedded into the M&A playbook to provide continuous visibility and accelerate risk identification across all phases. These technologies transform cyber assessment from point-in-time snapshots to dynamic, continuous intelligence that informs decision-making and accelerates remediation throughout the transaction. Key tool categories include:

- Threat intelligence platforms to monitor for deal leaks, target-specific threats, and dark web activity.
- Automated security assessment tools, including vulnerability scanners, penetration testing platforms, and security rating services to accelerate due diligence.
- Continuous monitoring solutions such as EDR/XDR, SIEM, and security orchestration platforms (SOAR) for real-time threat detection from presigning through integration, helping acquirors avoid costly breaches that can erode deal value and reputation.
- AI-powered risk analytics for identifying patterns, prioritizing vulnerabilities, and quantifying cyber exposure impact on deal value.
- Secure collaboration platforms and virtual data room monitoring tools to protect sensitive deal information while enabling efficient due diligence.

## Tailor your focus for the deal

Different kinds of acquisitions demand distinct areas of focus in cybersecurity assessments. Platform acquisitions are complex integrations requiring broad cybersecurity review. Bolt-ons involve smaller companies, often with less-mature cybersecurity capabilities. Carve-outs can have fragmented controls and incomplete cyber governance. And international and cross-border deals come with regulatory complexity and geopolitical cyber risk.



Engaging with key personnel from the target company at the earliest stages of deal talks can help uncover critical vulnerabilities. This collaboration empowers the target to remediate risks while protecting the acquiring entity from inherited exposures. Much like a home inspection, it gives acquirors the opportunity to plan postclose fixes and factor remediation costs into the proposed sale price.

Early compromise assessments are especially vital in life sciences, as smaller, less-protected entities are frequent targets for threat actors and nation states seeking to exploit transitional periods. “Sleepers” sometimes lurk unnoticed in these systems, waiting until postintegration to spring traps in the acquiror’s systems and gain access to a much bigger cyber prize.

Leveraging real-time insights from advanced security technologies provides a comprehensive view of potential exposures, enabling a more informed and resilient integration process. This intelligence supports strategic decision-making and strengthens postacquisition security posture.



# Cybersecurity assessments by M&A lifecycle phase typically include:



## Strategy and evaluation

This involves preparation and initial planning to identify key cybersecurity concerns and objectives for the merger or acquisition. It entails assembling a dedicated cybersecurity team and setting goals for the assessment.

These may include:

- Considering industry-specific risk factors and tailoring cybersecurity assessment strategies based on industry and acquisition goals.
- Understanding regulatory and compliance requirements, especially those that are often inherited in cross-border deals.
- Weighing the cost of assessment and cost-effective prevention against the cost of responding to breaches.

## Presigning due diligence

In the 30- to 60-day window before a deal is signed, the acquiror gathers preliminary information about the target company's cybersecurity posture, policies, and procedures. This high-level assessment involves reviewing documents, conducting interviews, identifying critical risks, and performing an initial assessment of compromise exposure, breach risk, and threat intelligence. Tactics acquirors can take during this phase include conducting breach resilience and compromise assessments.

## Integrate cyber risk into deal economics

Establish processes to translate cyber findings into financial terms. This includes developing models to quantify remediation costs, potential breach impacts, and effects on projected synergies. Having this framework ready ensures that cyber discoveries during due diligence can quickly inform valuation adjustments and deal structure decisions.



## Preclosing maturity assessment

During this phase, the acquiror conducts a thorough evaluation of the target company's cybersecurity infrastructure. This involves a detailed review of its security measures, including policies, practices, systems, and historical security incidents. The assessment also examines compliance with relevant regulations, evaluates the strength of data protection protocols, and identifies vulnerabilities and potential risks. It includes conducting detailed assessments, planning remediation strategies, performing a deep-dive breach risk assessment, analyzing threat intelligence, and identifying vulnerabilities. A thorough investigation at this phase enables an acquiror to:

- Catalogue vulnerabilities before deal closing.
- Prioritize remediation of high-risk issues and develop integration and remediation plans.
- Include cybersecurity considerations in negotiations and costs into deal pricing.

## Postclose maturity assessment:

After the transaction closes, teams must actively monitor and strengthen cybersecurity to prevent new vulnerabilities from emerging during integration and beyond, while also implementing the hardening and resilience measures identified during the breach resilience assessment. This phase also includes continuously assessing and enhancing security controls, conducting regular audits, maintaining incident response readiness, and adapting to the evolving threat landscape.

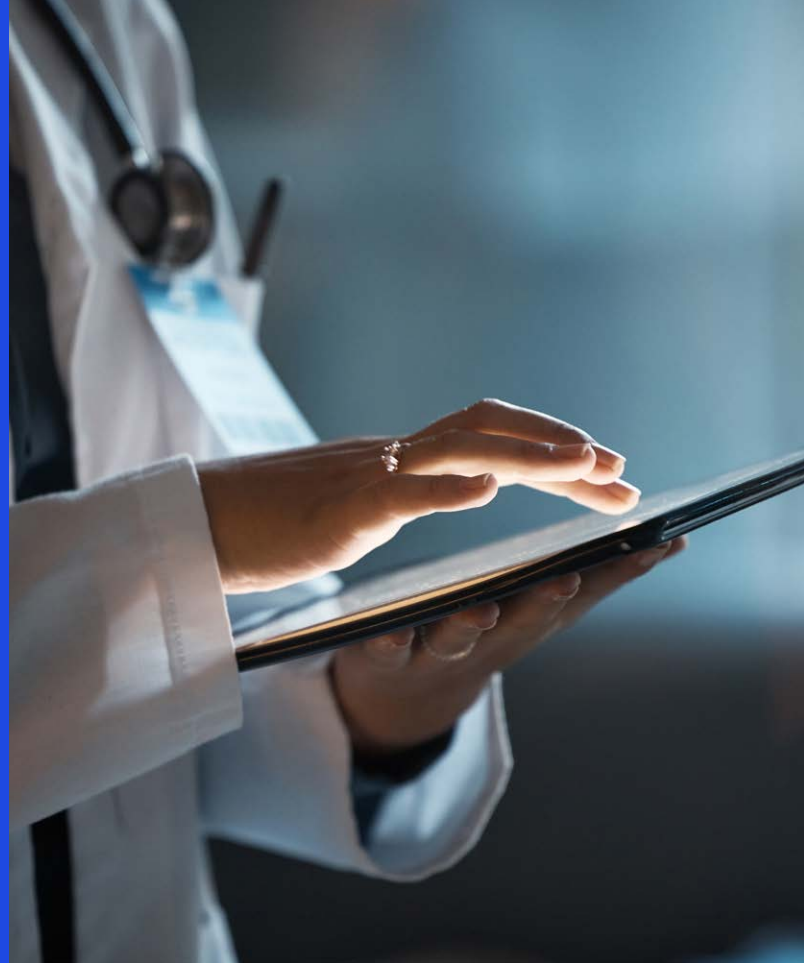


Each of these phases is crucial for successfully managing cybersecurity risks throughout the M&A process and ensuring the protection of sensitive data and information technology (IT) assets. They are key to identifying potential vulnerabilities that might compromise the target and ultimately the deal itself. With a clear understanding of the target's cybersecurity posture, the acquiring company can more accurately budget for remediation, negotiate deal protections such as clawbacks, and assess whether the assets justify the level of cybersecurity risk involved.

## An essential dimension of the M&A playbook

Ultimately, a proactive cybersecurity strategy safeguards both the acquired assets and the acquiring organization's existing infrastructure. It preserves established standards and controls, reduces the overall threat surface, and ensures continuity in a highly regulated and innovation-driven sector. With technology, data, and IP at the core of value in life sciences, companies can ill-afford to ignore potential cyber exposures and the risks acquisition targets introduce to their expanding technology footprint.

In short: In life sciences M&A, cyber resilience is now among the crucial determinants of deal success. The acquirors who integrate cybersecurity from the start will not only protect IP and patient data but also accelerate value creation postclose.



## How KPMG can help

KPMG LLP (KPMG) assists organizations with cybersecurity acquisition and divestiture services by providing specialized guidance on due diligence, risk assessment, and regulatory compliance, helping to ensure both the acquiring and divesting parties adhere to necessary data protection standards like GDPR and HIPAA.

KPMG helps identify and mitigate cybersecurity risks (e.g., assess risk, integrate security, safeguard IP, and build resilience), develop integration plans for aligning security measures across entities, and establish robust data governance frameworks to protect sensitive information. We support incident response planning, evaluate IT and security architectures for resilience, and secure IoT and medical devices, particularly in life sciences transactions. We offer a differentiated, rapid approach to assessing breach resilience, and can quickly identify immediate breach risks.

Additionally, KPMG offers continuous monitoring and improvement services and conducts training and awareness workshops to help ensure stakeholders understand cybersecurity risks and leading practices, thereby safeguarding assets and helping to ensure successful, secure outcomes in M&A transactions.



# For more information

## Authors



**Steve Sapletal**

Principal, Advisory,  
Transaction Strategy  
[ssapletal@kpmg.com](mailto:ssapletal@kpmg.com)



**Katie Boswell**

Managing Director,  
Advisory, Risk Services  
[katieboswell@kpmg.com](mailto:katieboswell@kpmg.com)



**Simon Hodson**

Director, Advisory,  
Transaction Strategy  
[shodson@kpmg.com](mailto:shodson@kpmg.com)



**Jordan Barth**

Principal, Advisory,  
Cyber Security Services  
[jbarth@kpmg.com](mailto:jbarth@kpmg.com)



**Paul Van De Haar**

Principal, Advisory,  
Cyber Security & Tech Risk  
[paulvandehaar1@kpmg.com](mailto:paulvandehaar1@kpmg.com)

## Life Sciences leadership team



**Kristin Ciriello Pothier**

Life Sciences Sector Leader,  
Global and Americas Life Sciences  
Deal Advisory and Strategy Leader  
[kpotheir@kpmg.com](mailto:kpotheir@kpmg.com)



**Dipan Karumsi**

Life Sciences Consulting Leader  
[dkarumsi@kpmg.com](mailto:dkarumsi@kpmg.com)



**Christine Kachinsky**

Life Sciences Tax Leader,  
US Tax Sectors Leader  
[ckachins@kpmg.com](mailto:ckachins@kpmg.com)



**Sean Marikakis**

Life Sciences Audit Leader  
[smarikakis@kpmg.com](mailto:smarikakis@kpmg.com)

---

### We would like to thank our contributors:

Michael Bender, Karen Henrie, Leah Lockwood, and Lara Volpe

## Related resources



**Trusted AI: Powering life sciences breakthroughs**



**The M&A Dance: Orchestrating synergies and value creation in public company acquisitions**

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](https://kpmg.com)



**Subscribe**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

DASD-2025-18928