KPMG

Deal value up, cyber stakes higher:

M&A in industrial manufacturing

Actionable strategies for embedding cybersecurity from predeal diligence to postclose integration

kpmg.com

Across industrial manufacturing (IM), the race for innovation is accelerating, and for many, acquisition remains the fastest lane to efficiency and growth. Deal values are climbing sharply, signaling a decisive shift toward larger, more strategic transactions, with transportation, logistics, and aerospace and defense leading the charge to secure advanced technologies and tech-enabled logistics capabilities.[1] Consider Union Pacific's $85 billion merger with Norfolk Southern: A bold move that underscores the sector's appetite for transformative deals.[2]

Yet amid this optimism lies a critical blind spot: cybersecurity. In today's hyperconnected manufacturing environment, where cloud-based supply chains intersect with automated production lines, the complexity of digital ecosystems makes cyber-risk assessment a formidable challenge. Tight deal timelines only amplify the difficulty. Too often, cybersecurity is relegated to an afterthought, leaving acquirers exposed to hidden vulnerabilities that can derail integration and erode deal value. The stakes are high: Ransomware downtime costs manufacturers an average of $1.9 million per day, and global cyber incidents continue to set new records for financial and reputational damage.[3]

The question isn't whether cyber risk exists. Instead, it's about whether you can afford to ignore it. The good news: building cybersecurity assessments into due diligence helps protect deal value and can be the difference between closing with confidence and taking an unnecessary gamble. With the right strategy and partners to support evaluations and cyber risk management, acquirers can defuse potential deal-breakers, safeguard critical assets, and strengthen operational resilience.

In this paper, we show IM dealmakers how to thoroughly evaluate a target's cybersecurity posture before and during a transaction to better protect postclose value.

[1] M&A trends in industrial manufacturing, Q3 2025, KPMG LLP.

[2] M&A trends in industrial manufacturing, Q3 2025, KPMG LLP.

[3] Rebecca Moody, "On average, manufacturing companies lose $1.9 million per day to downtime from ransomware attacks," Comparitech, December 4, 2024.

Understanding the challenge

The array of information technologies (ITs) powering today's IM companies depends on an ecosystem that unites producers, suppliers, and third-party vendors. As IT integrates and converges with operational technology (OT) controlling and monitoring industrial equipment, the fragmented network of connections, endpoints, and system interactions expands the risks to already-stressed cyber defenses. While companies are using advanced techniques to protect evolving technology and monitor third-party dependencies, even the most sophisticated strain to surveil this new, larger attack surface.

Acquiring a company with an existing vulnerability can compromise the acquiror after the transaction closes. For example, a poorly remediated incident can leave a backdoor into target-company systems, poised to be exploited postintegration and designed for a broader and more nefarious cyber objective.

The list of potential threats and vulnerabilities extends across the tech stack, from fragile open-source code used in software development to insecure sensors exposing data or opening backdoors to major systems. Many sensors and Industrial Internet of Things devices, for example, have limited processing power and memory, making it hard to integrate robust encryption or authentication protocols. In addition, for most IM companies, data protection is essential to safeguarding intellectual property such as design specifications and supplier technical drawings.

Technical debt is another widespread issue in IM. Companies often struggle to integrate new technology into older production and supply chains, including on the shop floor, where purpose-built physical systems and machines didn't need to be connected to an external network. But as IT and OT converge, IT is opening pathways to OT, creating vulnerabilities. Quick solutions, while well intentioned, can inadvertently compound the problem and force cybersecurity teams to shoulder a bigger burden.

Divestitures and cyber risk

In a divestiture scenario, cybersecurity must be front and center throughout the separation process, especially if transition services are being offered. Access and security controls must remain firmly in place so the environments of the seller and the new business stay separated until migration is complete.

There is also urgency for a newly separated business to establish its own cyber operational capabilities. Without a robust cyber strategy, the new entity faces heightened risks, including data breaches, regulatory noncompliance, and operational disruptions. Careful design and planning are essential to ensure security controls aligns with business objectives and regulatory requirements.

Disclosures help but aren't a guarantee

Sellers can assist in the acquisition process by disclosing their cybersecurity status before finalizing a deal, but contractual safeguards, while helpful, aren't enough to replace the rigor of a comprehensive technical evaluation. Relying exclusively on this approach can leave companies vulnerable to unexpected technical weaknesses, additional expenses, and reputational damage.

Ultimately, the responsibility ultimately lies with acquirers to meticulously examine the systems, practices, and compliance of the assets they are buying. In the event the seller discloses a breach, the acquirer needs to alert and engage cyber response professionals for digital forensics, incident investigation, and suggested remediations. Securing evidence; understanding the breach; and evaluating its legal, regulatory, and reputational fallout during the deal process are essential.

Sometimes the challenge of assessing cyber posture is a lack of experience evaluating cyber risks under tight timelines, or at all. And too often legal and strategic considerations subordinate technical due diligence in a deal.

Key recommendations

In IM, early compromise assessments and breach resilience are crucial. Utilizing real-time insights from advanced security technologies offers a comprehensive view of vulnerabilities, facilitating a more informed and robust integration process. Such intelligence not only supports strategic decision-making but also fortifies postacquisition security. While deploying these tools before an acquisition can be challenging, rapid deployment during clawback evaluation periods ensures that the target's actual cyber risk posture aligns with acquisition representations.

01 Appoint a cybersecurity tiger team

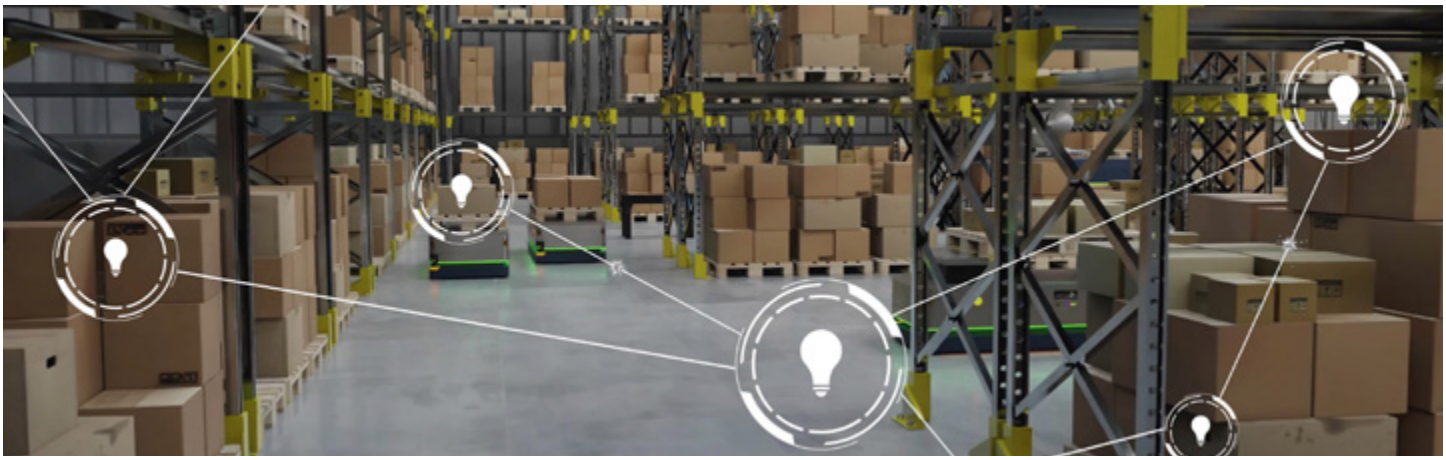
With the support and oversight of company leadership, form a specialized cybersecurity task force dedicated to identifying industry-specific cybersecurity and control risks and setting deal objectives tailored to industrial manufacturing. This team should guide information collection, ensuring that seller documentation explicitly correlates costs with potential impacts. Prioritize assessment strategies that account for industry-specific risk factors and align with acquisition goals. Additionally, evaluate regulatory and compliance requirements, particularly in cross-border transactions, and weigh assessment and prevention costs against potential breach response costs and complexities.

A time-tested approach for addressing these shortcomings is leveraging cyber managed-service partners, who can quickly deploy scalable, efficient, and effective operations to manage cyber risk. This not only accelerates the transition but also provides access to specialized expertise, reducing vulnerabilities during a period of significant change.

02 Include cybersecurity in due diligence

During the critical 30- to 60-day presigning period, gather preliminary information on the target company's cybersecurity posture, policies, and procedures. This high-level assessment should involve reviewing documents, conducting interviews, distributing questionnaires, identifying critical risks, and performing initial technical assessments of compromise exposure, breach risk, and threat intelligence. Request detailed security posture representations from the seller, utilizing questionnaires for key cybersecurity information, and follow up for greater specificity as necessary.

This presigning diligence can be structured to directly inform any related representations and warranties (R&W) in the transaction purchase agreement. Work with targets to conduct technical scanning, compromise assessments, and architectural reviews and use the findings for detailing specific contractual clauses. In the case of weak encryption standards, for example, the acquirer should demand that the seller warrant the security of data in transit and at rest, backed by an indemnity.



03 Conduct postclose maturity assessment and contract review

After closing the transaction, promptly identify and assess the cyber risks within the new enterprise, verifying them against the statements and assurances made during due diligence. Ensure that R&W insurance explicitly covers cyber-related breaches of representations and be prepared for insurers to conduct their own specialized cyber underwriting.

Before full integration and the clawback period's conclusion, identify any discrepancies that could lead to additional costs and trigger previously agreed-upon clawback provisions if required. Touch on what happens if a company has disclosed a prior breach.

04 Monitor and strengthen cybersecurity

Ongoing assessments are vital to uncover and defend against new vulnerabilities long after the deal closes. This phase should focus on the continuous evaluation and enhancement of security measures to prevent the integration process from introducing new weaknesses. Implement enhanced security controls, including EDR and XDR, for near-real-time alerts, and integrate the new entity into existing incident response plans. Connect key stakeholders with the acquiror's Security, IT, and SecOps teams for seamless integration.

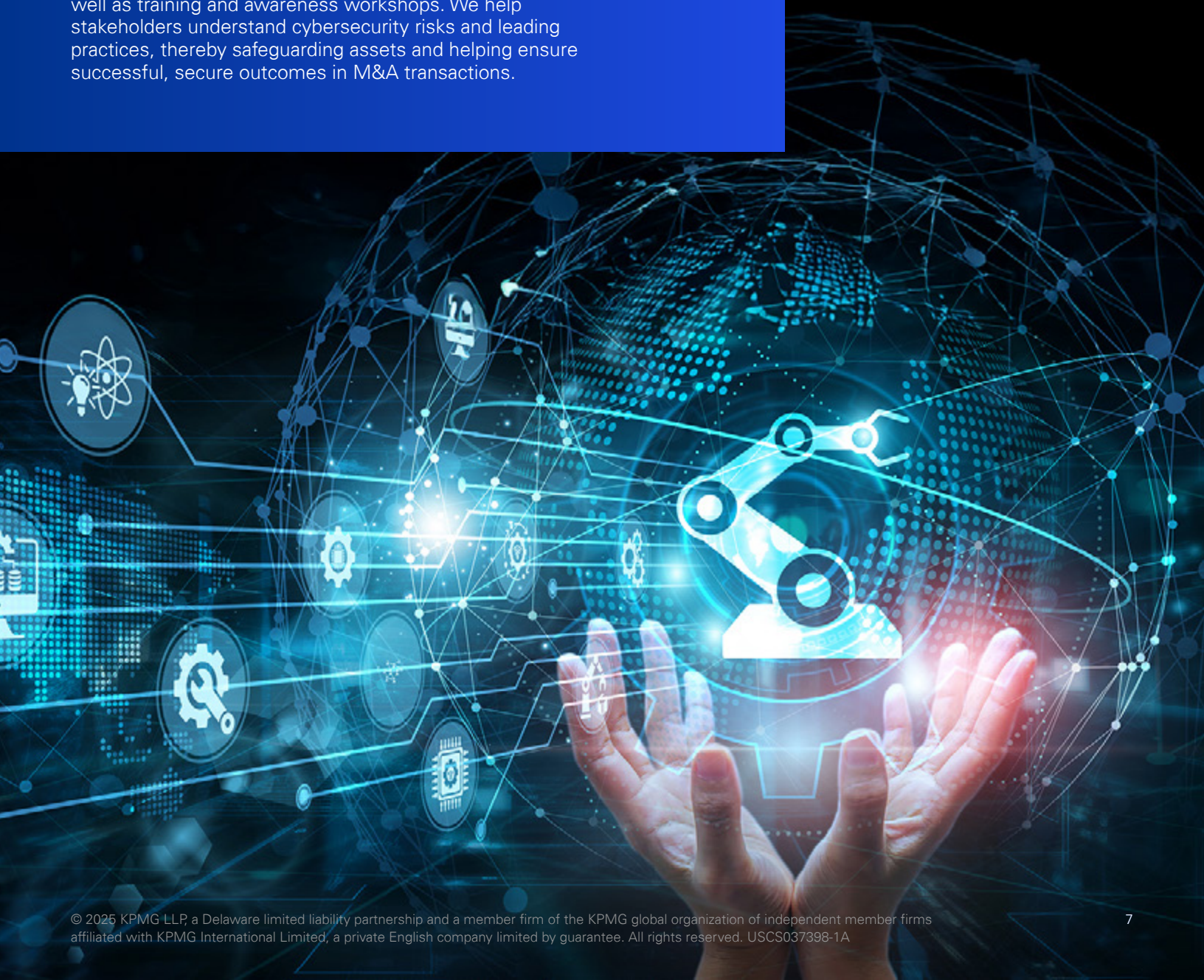
05 Reinforcing a cybersecurity culture

Developing a cybersecurity culture is an ongoing process in industrial manufacturing, requiring an environment where cybersecurity is a shared responsibility and integrated into daily operations. This cultural transformation focuses on building awareness, changing behaviors, and promoting proactive security practices among all employees. Establish a clear set of policies and procedures, emphasizing education, accountability, and recognition, to embed cybersecurity within the organizational culture effectively.

How KPMG can help

KPMG assists organizations with cybersecurity acquisition and divestiture services by providing knowledgeable guidance on due diligence, risk assessment, and regulatory compliance. We help acquirers and divestors adhere to necessary data protection standards like the General Data Protection Regulation and the Health Insurance Portability and Accountability Act.

KPMG helps identify and mitigate cybersecurity risks, develop integration plans for aligning security measures across entities, and establish robust data governance frameworks to protect sensitive information. We support incident response planning and evaluate IT and security architectures for resilience. Additionally, KPMG offers continuous monitoring and improvement services as well as training and awareness workshops. We help stakeholders understand cybersecurity risks and leading practices, thereby safeguarding assets and helping ensure successful, secure outcomes in M&A transactions.



Authors

Brian Higgins

US & Consulting Sector Leader for Industrial Manufacturing, KPMG US

BHiggins@KPMG.com

Brian is a partner in KPMG Advisory Services practice with a dual role that includes serving as the National US & Consulting Leader for Industrial Manufacturing. With an operational focus on industrial manufacturing, Brian's experience extends deep into competitive strategy and operational design, enriched by over 20 years of industry and consulting experience.

Beth McKenney

Principal, Technology Risk Management, KPMG US

BMcKenney@KPMG.com

Beth is a Principal in the KPMG Technology Risk Management practice in the Detroit, MI office. Beth is an effective leader with over 17 years of experience helping clients manage risk, deliver value through IT internal audit, and strengthen their governance capabilities. Beth's primary industry focus is industrial manufacturing. Beth is engaged nationally with the firm's industrial manufacturing leaders to advise clients on managing the emerging technology risk.

Hugh Nguyen

Partner, M&A Technology Center of Excellence Leader, KPMG US

HughNguyen@KPMG.com

Hugh is a senior leadership executive who helps companies create deal value by leveraging technology. His experience spans close to twenty years driving strategic transaction and technology initiatives for companies across a wide range of industries, including both corporate and private equity clients.

Jason Dayaw

Managing Director in the Technology Strategy Center of Excellence, KPMG US

JDayaw@KPMG.com

Jason is a Managing Director in the Technology Strategy Center of Excellence. He brings more than 19 years of professional experience delivering advisory engagements to leading entities in the industrial manufacturing sector, including aerospace and defense, automotive, and chemical industries. His background includes competencies in buy-side/sell-side IT due diligence assessments, IT separations and integrations, IT and business process and control reviews, business process analysis and re-design, and finance transformation.

Contributors:

The authors thank Lisa Bigelow, Michael Bender, Melissa Falcon, Leah Lockwood, and Karen Martini for their contributions to this paper.

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**