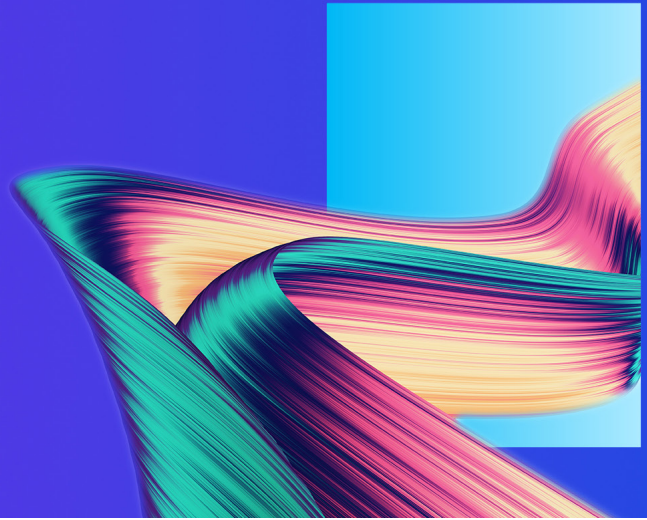




Cybersecurity

A rapid diagnostic opportunity for portfolio companies



KPMG offers a diagnostic process to help quickly assess an organization's cybersecurity maturity level, leading to recommendations for improvement

Addressing critical cybersecurity challenges

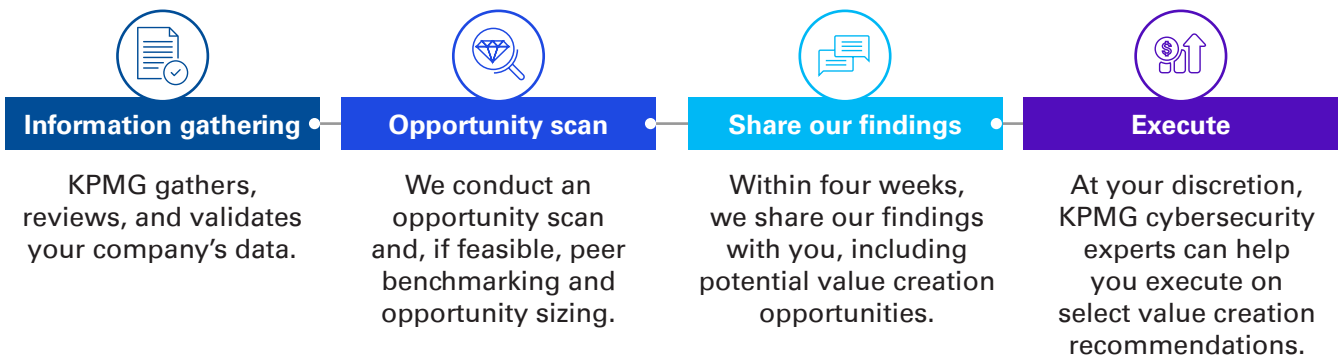
KPMG's cyber maturity advisory solutions help organizations remain vigilant to new cyber threats while prioritizing key cyber investments in a cost-effective manner aligned to their investment strategy. We also offer a managed detection and response solution, providing a range of managed services to help organizations address specific business challenges.

The range of KPMG's cybersecurity services includes:

- Our cybersecurity diagnostic offers a step in understanding your organization's cyber strategy needs.
- The diagnostic combines advanced technology with customized support from leading industry-aligned professionals who have significant expertise helping clients manage their cybersecurity investments and cyber risks.

Our approach

Through our initial diagnostic exercise, which is a light-touch process on your part, we quickly identify potential opportunities to advance your cyber strategy. Then, at your discretion, senior KPMG cyber experts can further guide you through the execution of select value creation opportunities that have been identified.



Deliverables from the cybersecurity diagnostic include:

- Key observations and challenges identified during the rapid assessment
- Perspective on current state maturity versus leading practices
- High-level quantification of costs and potential value creation opportunities
- Prioritized list of initiatives and preliminary roadmap
- Considerations and next steps

KPMG cyber solutions for portfolio companies



Cybersecurity maturity analysis

Leveraging a commonly used framework (NIST CSF) to identify gaps in security and outline a high-level roadmap to reach the desired maturity.



Business and technology resilience

Preventing and reducing the impact of potential cyber and other disruptive events through careful analysis, strategy and planning; performing crisis response exercises.



Cyber defense

Developing customized strategies that leverage advanced security technologies to safeguard valuable data against cyber threats—without limiting productivity.



Cloud security and AI

Providing a strategic approach to governing and architecting solutions for cloud platforms; enhancing cyber posture through advanced AI technology.

Case study: Strengthening cyber position during high-acquisition growth period



The challenge

Shore up enterprise cybersecurity in preparation for bolt-on acquisitions and an increased reliance on proprietary systems for exponential growth



What KPMG did

- KPMG met with 12 stakeholders across various executive leadership teams and technical functions to understand key business processes, technical infrastructure and application stack, and anticipated changes to the environment
- Reviewed latest security reports, system architecture diagrams, and other supporting documentation provided by the client
- Developed an executive-level overview of the company's sensitive data landscape and associated risk of storage



Results

- Defined six key initiatives the organization should prioritize over a 12-month period to reduce the risk of cybersecurity incidents impacting business operations and decrease the volume of security debt that has accumulated in the platform
- Provided high-level project details (e.g., key milestones, definition of success, budgets) to help the organization quickly translate the roadmap into actionable work plans
- Identified an opportunity to decrease the storage of sensitive data by 59% by de-duplicating records and implementing data-retention standards within the backup architecture

Contact us

Keith Swiat

Director Advisory | Strategy – COE

T: +1-212-997-0500

E: kswiat@kpmg.com

Badr Khudeira

Manager Advisory | Strategy – COE

T: +1-312-665-1000

E: khudeira@kpmg.com

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

kpmg.com/socialmedia



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.

© 2023 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. USCS003417-1D