Seizing opportunities to build business value

KPMG Cyber Security services and capabilities

kpmg.com
It is time to view Cyber Security as a business strategy

It is no surprise that cyber security continues to be a key area of focus for today’s organizations. What is changing is how top business leaders view cyber. For many, it is no longer just an IT issue, but a critical part of their overall business strategies.

How critical?
According to KPMG’s 2017 U.S. CEO Outlook Survey, CEOs expect to make significant cyber investments over the next three years. In fact, 75 percent of them believe such investment is an opportunity to find new revenue streams and innovate.

Today’s leaders increasingly understand that by adopting this new perspective, they can expand the value of their cyber security efforts—from protecting critical assets to embracing new business opportunities and improving their competitive advantage.

But this transformation will not happen overnight. It takes help from an adviser who can show you how to understand, prioritize, and manage your cyber security risks so you can take control of uncertainty…increase your agility…and turn risk into advantage.

That adviser is KPMG.
Seeing Cyber Security through the lens of your business

It is impossible to compete effectively in today’s global marketplace without embracing digital information and emerging technologies. Yet, this can also make your organization more vulnerable to cyber risk. The question becomes how do you take advantage of these powerful business tools, while protecting your critical data assets?

At KPMG, we believe the best approach to cyber security is one that delivers value by:

— Protecting your critical assets
— Enabling your business strategies
— Providing resilience for sustainable business growth.

This starts by recognizing that different organizations have different challenges—and different appetites for risk. That is why we work closely with you to help determine which risks you can accept, and which you need to manage.

We base our approach on your company’s strategy and on the insights we gather from asking questions, such as:

— What kinds of threats would cause the greatest harm to your business today?
— What data do you rely on for mission-critical processes?
— How can embedding cyber security strategies into your products and services give you a competitive advantage?

This results in a new perspective on cyber security. One that provides you with strategy, processes, and technology to manage your cyber security issues, and allows you to replace uncertainty with confidence and agility as you pursue new opportunities.

“As new technologies accelerate disruption, new innovations in cyber security will enable businesses to keep pace. This will bring increased focus to cyber issues and the cyber agenda—and establish cyber leaders as valued partners to the C-suite.”

Tony Buffomante
Global Co-leader of Cyber security services, KPMG
Defend, enable, and maintain your business

Organizations universally agree, cyber resource and investment allocations must be balanced among traditional reactive safety measures, more proactive business enablement, and advanced sustainability objectives. That is, they must defend, enable, and maintain their business.

Cyber defense

Includes actions and infrastructure intended to defend the perimeter, protect sensitive data, and thwart malicious attackers, which involves pre-breach and post-breach activities.

Business enablement

Involves cyber teams working collaboratively with business owners to achieve growth and strategic objectives (e.g., digital transformation), allowing the business to grow at its own pace while aligning to security policies.

Resilience

Represents an organizational commitment to cyber maturity, enablement, and integration, which involves business, financial, and cultural alignment to security, process automation, and technical automation.
"Understanding and communicating cyber risks to all levels of the organization and the board helps companies turn cyber into a competitive advantage. Our strategy and governance capabilities assist clients in aligning the cyber agenda with their dynamic business strategies and compliance priorities, bringing a business context to cyber security and helping to maximize return on investment."

Michael D. Gomez  
Principal, Cyber security Services

"In cyber defense, we think like the bad guys. We help clients identify their threats, design security operations programs, deploy monitoring technologies, detect insider attacks, simulate fraud and cyber scenarios to evaluate defenses, design threat-resistant applications, and measure the cost effectiveness of cyber monitoring investments."

Deron Grzetich  
Managing Director, Cyber security Services

KPMG looks at the world from your perspective, bringing a business context to cyber security for all levels of your organization—from the boardroom to the back office.

This begins with helping you understand, prioritize, and manage your cyber security risks through four distinct capabilities that take you from strategy through implementation.

**Strategy and governance**  
This set of services is designed to help clients understand how best to align their cyber agendas with their dynamic business and compliance priorities—including risk management. Among the approaches we follow are: assessing cyber maturity and compliance, providing reports and metrics to chief information security officers (CISOs), and more.

**Transformation**  
We help clients fulfill their cyber agendas by building and improving their programs and processes. This is accomplished through support by the right organization and technology, and includes identity and access management (IAM), security governance, risk management and compliance (GRC), and other services.

**Cyber defense**  
KPMG’s cyber defense professionals help clients maintain their cyber agendas as their business and technology programs evolve. We do this by providing greater visibility and understanding of changing risks through such processes as technical assessments and security operations and monitoring.

**Cyber response**  
These services are designed to help organizations respond to cyber incidents effectively and efficiently, as well as conduct forensic analysis and detailed investigations. Among the specific areas these cover are incident response readiness and planning and digital investigations and remediation.
We recognize that we’re living through a time of accelerating change—in the world in general, but also especially related to cyber. Our cyber transformation services are aimed at helping clients keep up with that change. We specialize in implementing real-world solutions that protect our clients and their business interests.

Kyle Kappel
Principal, Cyber Security Services, KPMG
Transformation

“In cyber response, it’s important to be one step ahead of our adversaries. We focus on knowing our client’s environment and being embedded with them through on-call agreements. Rapid pinpoint response with the right resources during a breach is the critical aspect of containment and minimizing overall impact to our clients.”

Edward L. Goings
Principal, Cyber Security Services, KPMG
Cyber Response
Why KPMG?

KPMG brings a business context to cyber security for all levels of your organization—from the boardroom to the back office.

We know Cyber Security is a business issue, not just an IT issue.
Cyber security is a strategic enterprise risk that goes far beyond IT. Uncontrolled, it can impact product integrity, the customer experience, investor confidence, operations, regulatory compliance, brand reputation, and more. That is why cyber security demands attention not only from the chief information officer—but also from the rest of the C-suite, the board and, indeed, employees and business partners throughout the organization.

We translate Cyber Security into a language your business can understand.
Cyber security affects different parts of your business, and we translate cyber risks into an appropriate language for each. Whether we are working in your boardroom, back office, or data center, we seek to provide a jargon-free explanation of your cyber threats, the potential impact to your critical assets, and the recommended response.

We provide a business-led approach, supported by deep technical skills.
We bring a combination of technical domain experience and extensive cross-functional business skills—including people and change, financial management, risk management, global compliance, organizational design, and more. KPMG professionals understand cyber security risks in the various layers of your business—not just the technology layer—so we can advise you in a context that is relevant to you.

We work collaboratively with you to meet your Cyber Security needs.
Instead of coming to you with a preconfigured approach, KPMG professionals take the time to understand your business priorities, strategic direction, and operations—so we can bring an appropriate context to your cyber security risks and help protect your critical business processes.

We know your industry.
As you are navigating cyber security, it is important to have an adviser at your side who understands the challenges, threats, and strategies in your industry. At KPMG, we bring both the business context and the industry context to cyber security. Leveraging the industry experience of KPMG professionals around the world, we understand where your industry is coming from in cyber security—and where it is going.

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 696889

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 696889
Putting cyber security on the board’s agenda is critical in adopting a holistic strategy. Because we understand the business issues, challenges, and concerns facing today’s senior management and boards, KPMG can help start this discussion. Among the credentials we bring to the table are:

**Board-level credibility developed over 125 years**
KPMG is a respected global network of member firms, providing audit, accounting, and professional services, and we are the trusted adviser to the majority of the FORTUNE 100, along with smaller companies throughout the world.

**Knowledge of emerging issues**
In our Global I-4 Forum, also known as the International Information Integrity Institute, we convene leading cyber security professionals from around the world to discuss emerging threats, regulatory challenges, and solutions for various industries.

**Proven track record as an objective, knowledgeable adviser**
Our global network of regulated member firms has an unwavering commitment to precision, quality, and objectivity in everything we do.

What is more, we can help you deliver on the promise of cyber security to all levels of your enterprise by providing:

**Technical security that aligns with your culture**
We combine technical proficiency with deep, cross-functional business experience to create a security culture throughout your respective functions and activities.

**An ecosystem approach**
In addition to our own cyber security experience, we are able to leverage experience from across our cyber security ecosystem. This allows us to tap into knowledge and insight from key alliance partners in areas such as emerging threats, new technologies, competitive intelligence, and more.

**Enterprise-wide security transformation**
Technology is only one part of a transformation. We also help you design processes for employees, customers, suppliers, and other stakeholders; prepare your organization to adopt the new technology; and help change behaviors throughout the enterprise.

**Security transformation across different geographies and cultures**
KPMG understands cyber security risks, regulatory impacts, change management, forensic investigations, and other factors that may change from one country to the next. We have a global network of more than 3,000 cyber security professionals, plus multidisciplinary collaboration with 189,000 other professionals in KPMG member firms across more than 152 countries.
Case Study: Securing customer identity management

The challenge
A global leader in network technology solutions was looking to transform itself into a subscription-based software company. A chief concern for the organization was the need for a modern, standard, and scalable identity management platform that would enable a stronger digital customer experience across the company’s range of products and solutions.

The KPMG solution
An integrated team represented by KPMG Cyber, KPMG Digital, and Privacy professionals brought the firm’s technology experience and cyber security knowledge to work for the company. Working side by side with the client, the KPMG team developed a next-generation customer identity and access management strategy, road map, and business case. These were aligned to the client’s broader ongoing digital business transformation and focused on consolidating single customer identities across the client’s various product portfolios. On the front end, the solution is helping to create an improved, secure, and consistent user experience and choice, while providing the back-end business systems with a 360° view of a customer’s interactions. It also provides insights that can help grow the business, such as discovering cross-selling opportunities by looking at what similar clients are purchasing. Finally, the solution supports the client’s commitment to securing customer data and meeting the ever-changing global privacy requirements.
Seize the Cyber Security opportunity

New markets. Mergers. Sales channels. These and other new revenue opportunities appear almost daily. The question is whether your organization has the confidence and agility to seize them. That is why you should speak with KPMG. We can show you how to protect your critical business assets so you can embrace new opportunities and build your competitive advantage. Now and for the future.

KPMG* named a leader in The Forrester Wave™: Global Cybersecurity Consulting Providers, Q2 2019

Independent evaluation recognizes KPMG in evaluation on Global Cybersecurity Consulting Providers

KPMG is cited as a leader among Global Cybersecurity Consulting Providers, and was noted for standing out with “clear concise executive level engagement abilities.”

The report recognizes that “executive engagement is a key part of [KPMG’s] strategy with cybercrisis simulations, a deep metrics offering for CISOs and an initiative that helps security leaders understand the next crisis, not just the current one.”

The report acknowledged that “KPMG consistently advances three messages: 1) Cybersecurity helps businesses grow; 2) cybersecurity problems now require multidisciplinary expertise; and 3) cybersecurity protects core business functions. And KPMG doesn’t just say those things in its marketing; it infuses those themes into its cybersecurity services portfolio.”

* The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester’s call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgement at the time and are subject to change.

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 696889
Contact us

Tony Buffomante  
Principal, Co-leader, Global Cyber Security Services  
E: abuffomante@kpmg.com

Steve Barlock  
Principal, Cyber Security Services  
E: sbarlock@kpmg.com

Edward L. Goings  
Principal, Cyber Security Services  
E: egoisngs@kpmg.com

Michael D. Gomez  
Principal, Cyber Security Services  
E: michaelgomez@kpmg.com

Kyle Kappel  
Principal, Cyber Security Services  
E: kylekappel@kpmg.com

Deron L. Grzetich  
Managing Director, Cyber Security Services  
E: dgrzetich@kpmg.com

KPMG Cyber Security Emergency Hotline 855-444-0087

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 on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 696889