KPMG

Conquer security threats and ignite innovation

Cyber security puts a protective arm around the day-to-day operations of your business.

KPMG Powered Enterprise | Cyber

visit.kpmg.us/poweredCyber

Cyber serenity

Cyber security risks are mounting, and the cyber security function has the potential to offer more than just a defensive strategy.

By transforming the cyber security function, organizations can reap benefits beyond the protective layer of the business by also safeguarding its digital assets and reputation.

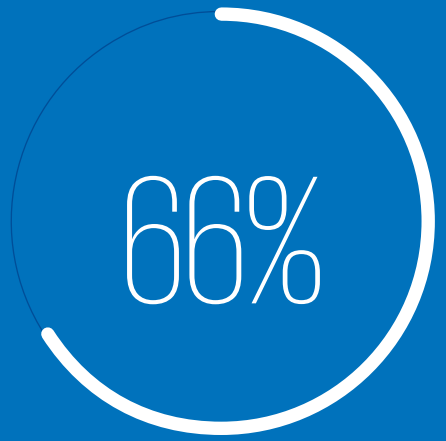
"It's important that businesses have the 'cyber serenity' to adapt to changing conditions with confidence," says Prasanna Govindankutty, Principal, Advisory, Cyber Security Services, KPMG in the U.S. "When organizations weave cyber security into the fabric of their business, they can protect critical assets, win trust, and confidently seize opportunities."

Effective identity and access management (IAM) and security operations (SecOps) serve as a foundation for cyber security programs, and the importance of a leading cyber security function increases day by day.

Technology is an integral component of almost every business, and cyber security is there to protect the future.

The cyber security challenge

For most companies, a security monitoring function of some description is a given. However, it is often a costly and reactive approach.



of digital transformation leaders plan to **increase investments in data security** measures in the next 12 months.

Base: 820 professionals involved with digital transformation strategy decisions

Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG, April 2021

It's a familiar story in many organizations of all shapes and sizes across the globe: technology solutions have been implemented across siloed departments to solve an existing and discrete problem.

"In a lot of cases, businesses are detecting threats too late, or postmortem following a breach response," says Deron Grzetich, managing director, Cyber Security, at KPMG in the U.S.

"They identify opportunities to improve monitoring in the future, but they don't have a solid strategy around how they are going to deploy and implement those improvements. They haven't wrapped the right people around the technology. They've just turned it on, and it's often not effective at detecting threats. So they are spending a lot of money for limited risk reduction."

The consequence is a patchwork of technology with variable levels of security and little integration—often at great expense.

"Businesses are using so many different tools and ineffective methods of tracking such as spreadsheets and emails, that many don't even know what their weaknesses and vulnerabilities are," says Grzetich.

While the importance of SecOps is increasingly well understood, IAM is a niche component. Its gravity isn't always appreciated.

Managing identity access across a multitude of software and systems—both from the internal enterprise and external consumer perspective—is a significant challenge.

Get it right and it's the first line of cyber defense. Get it wrong and it's an open door to a would-be attacker.

"The transformation of identity access is sometimes viewed as too complex," says Martijn Verbree, partner, Cyber Security, KPMG in Australia.

"However, there are practical answers. The structured KPMG Powered Enterprise | Cyber transformation, for example, is a tested methodology to change the way enterprises handle and transform identity management, and it guarantees efficiencies while improving overall security."

One of the critical areas of IAM focus from an enterprise perspective is around joiners, movers, and leavers. Typically, this has been managed inconsistently in onboarding people, issuing and recording permissions, and removing the credentials of people who've departed the business. Too often as employees change roles, they keep their existing permissions and that can lead to an accumulation of out-of-proportion access to highly sensitive data and applications.

From a consumer perspective, IAM is focused on ensuring that a customer's identity is as protected as possible and guarded against malicious activity, without compromising the ability to access services. The customer experience is as crucial as the security aspect of identity management.

In a recent example, the onboarding process for a university to move potential students from the offer of a place to acceptance required creating an account that included 28 people, each of whom had a different role in the process. It could take more than seven days to create an account, and during that period, 25 percent of prospective students typically dropped out.

This process was transformed by KPMG Powered Enterprise | Cyber; a four-stage process was introduced, enabling accounts to be opened within 40 minutes. The dropout rate of 25 percent was immediately reduced to 5 percent.

To achieve that level of efficiency, a new leading practice operating model is required.

Turning risk into competitive advantage

A transformed cyber function can be a springboard for innovation and can deliver an enviable level of trust, both with customers and clients at an enterprise level as well.

"Everybody looks at risk—of which cyber is a component—as a cost center," says Govindankutty. "But good cyber security can bring a strong competitive advantage."

A new operating model with a proactive and forward-thinking approach to cyber can transform an organization's cyber security function, building trust throughout the enterprise and its customers.

By identifying skills gaps and modeling the organization's maturity around its operations, organizations can embed new ways of working, delivering change across the enterprise to support and sustain high performance.

From a SecOps perspective, a threat assessment or threat profile is performed to identify the threats and the preventative controls an organization has in place.

The results are then balanced against the threat actors that are likely to target them, why they are likely to be targeted, and how these threat actors would operate. When you bring these components together, it shows the most significant potential risks for the business.

By implementing holistic technology across the business, the cyber security unknowns are significantly reduced, if not eliminated, engendering greater confidence levels from internal and external stakeholders alike.

When it comes to IAM, it's critical to understand who is accessing different systems and why.

"A strong identity system needs multiple data points to build trust about the person who's accessing the system," says Verbree.

Some of those authentication factors are obvious—for example, device type, location, browser version. Increasingly, however, more complex elements are being added: biometrics, impossible travel, behavioral patterns (such as how an individual swipes), usual time of log-on. Incorporating a variety of authentication factors makes it more difficult for threat actors to take over credentials.

Implementing this level of cyber security is a crucial step toward changing the perception of cyber from a protector to a proactive, strategic contributor to the business.

Cyber security can be proactive and reduce the amount of time spent on "protection" by minimizing weaknesses and using validated technology solutions with tested real-world usability to automate many mundane day-to-day tasks.

> Everybody looks at risk—of which cyber is a component—as a cost center...but good cyber security can bring a strong competitive advantage.

Prasanna Govindankutty
Principal, Advisory
Cyber Security Services

Don't just manage risk. Master it

Thanks to preconfigured cloud technologies, processes, and organizational designs tailored to unique businesses, Powered Cyber is designed to significantly accelerate the delivery of IAM and SecOps programs.

Transformation of the cyber function focuses on delivering business outcomes that combine the six layers of the **KPMG Target Operating Model**: functional process, people, service delivery model, technology, performance insights and data, and governance.

"The TOM helps businesses to change, to implement leading practices, to fast-track transformation and keep it on course," says Verbree.

Once a new operating model is established, businesses can expect a range of business outcomes, including:

SecOps

1. **Broad views of security; IT; and governance, risk, and compliance:** Drives risk management processes across the organization through automated security control testing and enhanced reporting of risk and compliance posture.
2. **Faster, integrated, and standardized response:** Who does what, why, and how. Identifying the skills, roles, and responsibilities your business requires.
3. **An accurate view of current security posture:** Where the work gets done, shared service center, centers of excellence, and outsourcing operating models to optimize service delivery.

IAM

1. **Control of user access to applications, systems, file shares, and sensitive data:** Manages user access across the business, gaining efficiencies through policy-driven access control rules both on premises and in the cloud. Significantly reduce the risk of "insider threat" by applying the principle of least privilege.
2. **Improved quality and effectiveness of reporting and analytics to support decision-making:** Feeds real-time user access data to risk and security information and event management (SIEM) systems, reducing the risk of systemic malicious activity
3. **Automated processes to reduce reliance on IT:** Achieves efficiency—for example, access requests, lifecycle management events, certification campaigns, password management.

"Businesses can immediately benefit from deep IAM and SecOps knowledge and quickly achieve security operations transformation in the cloud," says Govindankutty. "Powered Enterprise is an outcome-driven transformation solution that drives sustainable change, rising performance, and lasting value."

Cyber at the heart of the business

By jump-starting the digital transformation of the cyber function, businesses can take advantage of leading best practices with reduced implementation risk and a quick time to value.

In addition, a trusted cyber function can be the springboard for new business activity. From product launches to acquisitions and mergers, having a robust cyber function provides the confidence and reliability needed to seize opportunities and respond to market challenges quickly, efficiently, and effectively.

With optimal confidence in cyber capabilities both internally and externally, cyber can genuinely be a strategic business partner and value contributor rather than a reactive security effort.

And for a business that's going to flourish over the coming years, that's exactly what it needs to be.

Key takeaways

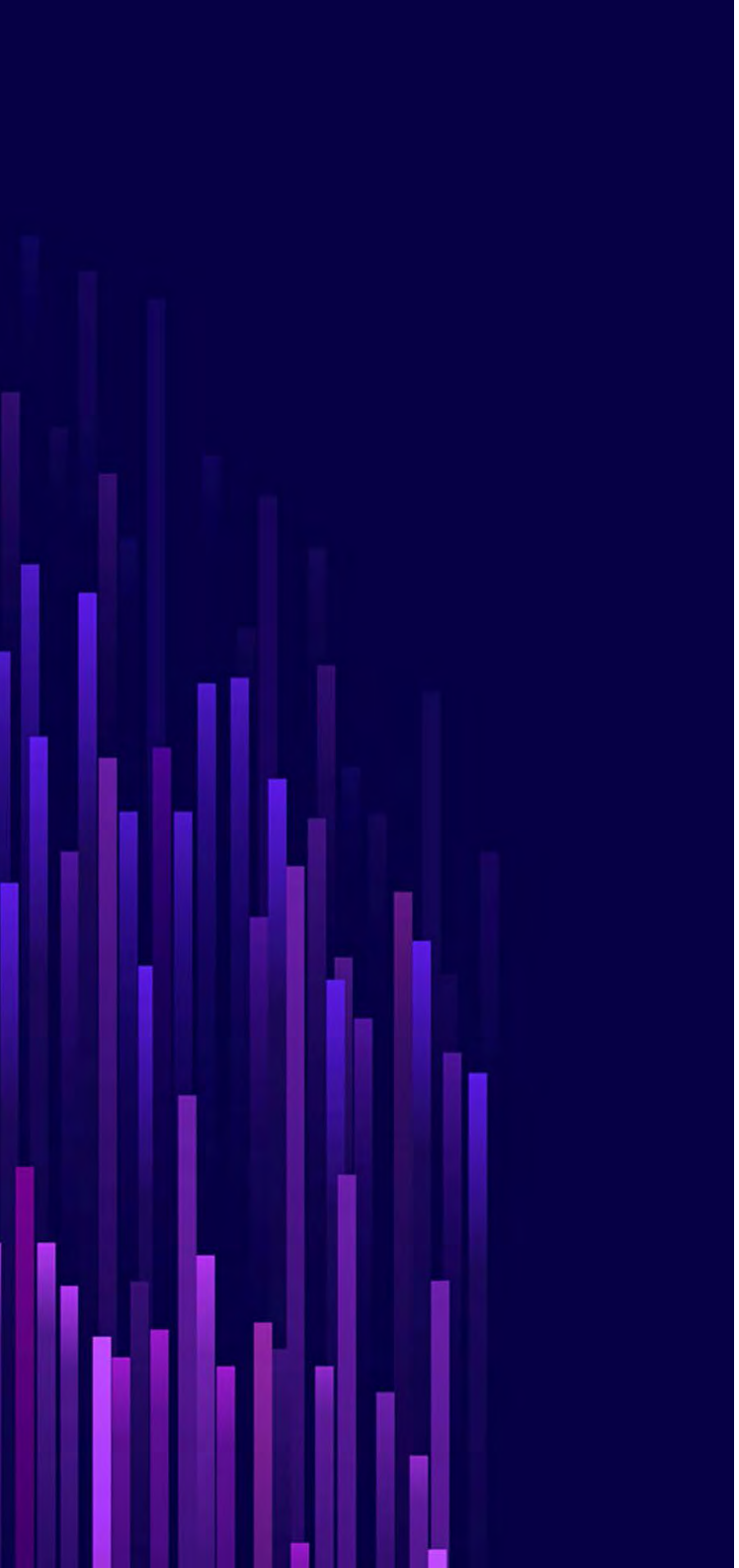
1. **Cyber is a fundamental part of a business**, not just a tick box.

2. When organizations weave cyber into the fabric of their business, **they can protect critical assets, win trust, and confidently seize opportunities.**

3. Effective IAM and SecOps **serve as a foundation for cyber security programs.**

4. A proactive and reliable cyber function gives **stakeholders and other departments the confidence to execute their roles effectively.**

5. **Powered Cyber drives transformation in your business**, allowing you to more effectively use identity technology to protect your assets and enforcing industry-leading security.



Discover more

How KPMG Powered Enterprise can help:

- **KPMG Powered Enterprise**
- **KPMG Target Operating Model**

Contact us:

Prasanna Govindankutty
Principal, Advisory
Cyber Security Services
T: + 973-255-2409
E: pkgovindankutty@kpmg.com

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

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.