KPMG

All hands on deck: Key cyber security considerations for 2020

Cyber threats are mounting.
Are you prepared to protect your environment?

kpmg.com/cybersecurity

Business is changing and the fourth industrial revolution is underway. Data has become the lifeblood of the organization as Boards seek to harness the potential of our digital economy, create new customer experiences, transform their services, and drive efficiencies and cost savings. The future is being created from a fusion of new business models, new technologies, and new partnerships.

In this changing world, there are ruthless entrepreneurs who are making money in this new economy. Unfortunately they are cyber criminals and they are on the wrong side of the law. They pose new challenges to legitimate businesses, and companies need to think differently about how to protect their competitive advantage and develop new models with a goal of becoming and remaining cyber secure.

Cyber security professionals need to demonstrate they can protect the heart of the transformed business with an agility of thought and action that recognizes the pace and speed at which cybercriminals operate.

They need to assemble the kind of collaborative talent — across the enterprise — that is able to take a proactive stance and meet these issues head on. The CISO can't do it all. New partnerships are needed, technology is an opportunity, not a threat, and cyber security is becoming a key business enabler.

We* picked six key cyber considerations that will shape the way we approach security in 2020 and beyond, and asked our professionals to share their insights and experiences to help you meet the challenges ahead.

Aligning business goals with security needs

Digital trust and consumer authentication

The evolving security team

The next wave of regulation

Cloud transformation and resilience

Automating the security function

> **Successful ongoing cyber resilience will require the strategic alignment of cyber strategies with incident response, business continuity and disaster recovery planning. We've got to involve the entire enterprise — from front office to back.**
>
> **Akhilesh Tuteja**
> Global Cyber Security
> Co-Leader
> KPMG International

> **As SecOps teams work to integrate security priorities with software and process development, essential tasks should be automated wherever possible across analytics-based solutions — from access and fraud alerts to data privacy and risk mitigation, to name just a few — for both effectiveness and cost reduction.**
>
> **Tony Buffomante**
> Global Cyber Security
> Co-Leader
> KPMG International

*Unless otherwise indicated, throughout this document, "we", "KPMG", "us" and "our" refer to the network of independent member firms operating under the KPMG name and affiliated with KPMG International or to one or more of these firms or to KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

Aligning business goals with security imperatives

Many organizations have spent massively on cyber security, both on tooling and personnel. Today, some feel the need to cut back. In that sense, the cost of security has became a major focus — perhaps as much as security itself. In an effort to manage costs and ensure that business and security priorities are aligned, companies are automating significant portions of their cyber functionality by putting digitized cyber risk management processes in place to ensure they ladder up to the organization's top-line operational and business strategies.

The landscape as we see it

In reviewing many risk models, we find the concept of business-driven risk scenarios to be lacking. The viewpoint of the business needs to go hand-in-hand with the viewpoint of the cyber security team and that is not the case at enough organizations. The identification of these risk scenarios should be led by the business.

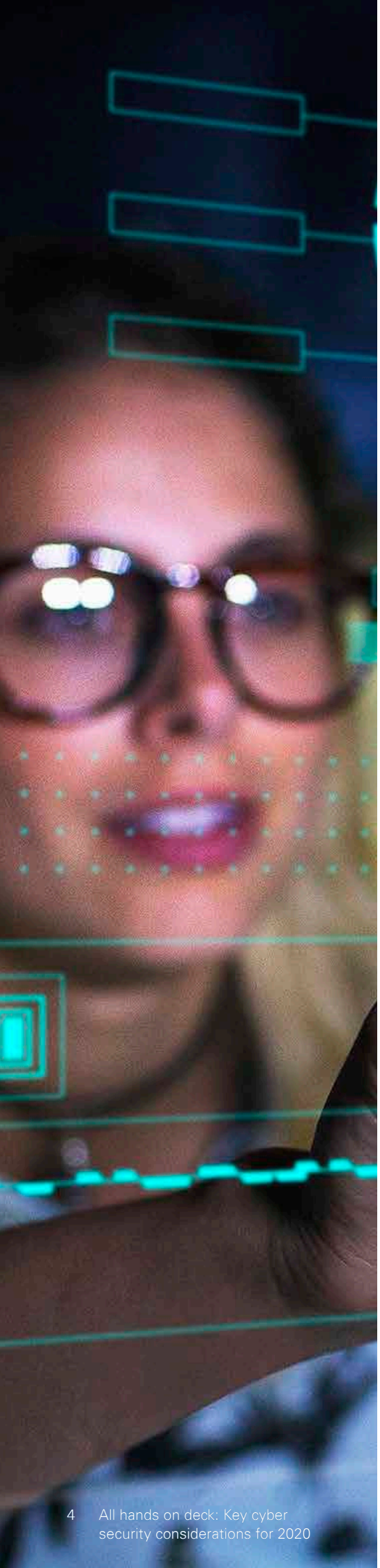
And the process would be much more effective if it were informed by a model that enables business leads to better understand the impact security controls may have on those risk scenarios. Many companies don't get that insight consistently, making it challenging to formulate a fluid ongoing relationship between the controls and the business.

In the cyber community, we try to plan for worst-case scenarios, but many incidents happen in relative obscurity and are not earth-shattering, let alone business-shattering. From that perspective, we see many companies working to embed security, not only within the second line of defense, but within the more operationally focused first line as well as the audit-driven third line.

Larger organizations have spent, over the last 10 to 15 years, big money on IT security. Now they are acknowledging that they need to develop a new model focused on lowering costs through an automated approach to security and putting the right people in the right roles.

> **In multiple countries, companies — big banks in particular — are setting up shared service centers to bundle a variety of cyber capabilities. They clearly see that doing it all themselves is not cost effective, and standard outsourcing isn't practical because those third parties don't have a clue about what they should protect from a business perspective.**
>
> **John Hermans**
> Partner
> KPMG in the Netherlands

> **We need to analyze the entire enterprise in terms of risk. Look at your IT risks and then express them in terms of your business risks — that will give you a line of sight from top to bottom. The security function needs deeper insight into the priorities of business to determine where the potential vulnerabilities reside and what the impact might be if those weaknesses were exploited.**
>
> **Ben Krutzen**
> Partner
> KPMG in the Netherlands



What we believe you should do about it

Think holistically about where you need to invest. Consider what risk scenarios need to be in place, and what controls are most relevant. Most companies are now engaged in a digital transformation, which suggests they should also explore automating their cyber and risk management processes.

Many incidents would be quite easy to detect if security policies and controls were embedded in the business. Bottom line, companies are encouraged to integrate cyber security across all three lines of defense, rather than operating in silos.

Make security an end-to-end priority. The foundational action is to establish an ongoing dialogue between the security organization and the rest of the enterprise to ensure security is in sync with the business in terms of strategic and operational planning.

To that end, implement engineering approaches — such as secure by design and privacy by design — that are intended to introduce security into the daily mindset of the DevOps team as they craft new applications and services.

Ultimately, we're hoping to see cyber security professionals move away from being perceived as an IT-driven function. As such, the cyber team needs to be business-led and business-aware. Otherwise, that symbiotic handshake between business and cyber is never going to solidify.

Digital trust and consumer authentication

Clearly, younger generations of consumers are bringing their expectations to their online lives, particularly in terms of banking and financial services. And many large global brands are feeling threatened. Brick and mortar is slowly disappearing, and whoever reigns supreme in terms of the digital customer experience is likely to enjoy the greatest market share.

The landscape as we see it

Ultimately, customers will likely go wherever the interactions are easiest and they feel safe and secure.

In the current environment, the way to offer a better customer experience is to reduce friction. And for customers who forget a password, having a PIN sent to a mobile device via text message that has to be reentered and confirmed is friction.

In response, many companies are leaning into a machine learning-based approach that enables them to understand their clients' typical, yet unique characteristics and behavioral patterns, such as finger or voiceprints and a variety of physical biometric traits. Financial firms, in particular, are working to understand how clients interact with them: how and when they usually log in, the types of transactions they perform, the dollar amount range they tend to withdraw or transfer, etc. These elements can be aggregated to produce a unique client snapshot.

For any company that maintains an interface, it's all about optimizing the customer journey, establishing trust, and keeping the journey short and efficient enough to maintain engagement. If customers feel as though they're jumping through too many perceived "hoops," they will likely simply take their business elsewhere. While the customer needs to be happy and enjoy a friction-free journey to their desired outcome, it is the responsibility of the product or service provider to make the entire endeavor is secure.

> **Companies have to start rethinking the way they harvest data and make it available to be correlated with specific threat scenarios. The idea of data lakes certainly isn't new, but the data that is pulled in, how it's kept secure, and ensuring that only the most relevant people can access and leverage that data are all critical factors.**
>
> **Charlie Jacco**
> Principal
> KPMG in the US

> **There's been a core focus in recent years, particularly in the U.S., on security fusion centers. It's all about becoming data driven in the way you work to detect security incidents, and enabling a rapid-response process that is leaner, continuously adapts to the threat landscape, and seeks to remain a step ahead of the bad actors.**
>
> **Alex Anisie**
> Director
> KPMG in the US

What we believe you should do about it

First and foremost, companies — regardless of industry — should work to connect the data, authentication, and fraud teams systematically and programmatically. Understand the governance requirements, what data you're pulling, who owns it, where it's coming from, and how it's going to be leveraged. Build a holistic culture of security.

From there, think about how to drive a better experience for your customers where they're being asked questions to authenticate, making it easier for them to identify themselves, but perhaps more demanding to do atypical transactions. Make your clients' day-to-day interactions as easy and painless as possible, but add a little friction where it makes sense algorithmically based on common behaviors.

Make it a priority to understand the privacy and data concerns around how, and by whom, your data is going to be used. Going forward, much of it will likely be in the cloud. Think about how to encrypt and protect it. It's an enterprise-wide matter that can be solved by technology, but is ultimately based on the business's desire for customers to have a better end-to-end user experience across every way they interact with the company digitally.

And companies would do well to rethink the way they evaluate data. The traditional approach of applying a massive set of rules to various data sets is no longer tenable. It's creating too many false positives and causing too many use cases to fall through the cracks for fraudsters to pick up on. The idea of leveraging machine learning algorithms to parse that data in a more efficient manner to identify behavior-based trends is key.

Finally, be alert to the correlation between people and technologies across your overall prevent/detect/respond process. Recognize that the process spans the entire organization internally, but also impacts the world outside your literal and figurative walls, considering issues can be triggered by a third party. In the end, it's about lessons learned. When it comes to authenticating users, take the time to review past incidents and reintroduce them to your security protocol for stress testing in an effort to avoid reoccurrences.

The evolving security team

Over the last few years there's been a broad attempt to elevate the importance of cyber security at the board level. In 2020 many board members are well aware of the cyber agenda. While they understand the importance of cyber, one of the biggest challenges for security professionals is translating that knowledge into an actionable appreciation for what it actually means to the business.

The landscape as we see it

At many companies, the cyber security team remains a collection of technical, operational compliance professionals, but a transformation is underway into a more strategic, forward-looking resource that employs its worldview to impact business dynamics.

Many Chief Information Security Officers (CISOs) and their teams, in many industries, are working to adjust to the changing dynamics of the business and become a trusted and relevant voice at the strategy table. They are also working to visualize the organization's specific operational priorities and partner with internal business heads to incorporate those insights into the company's cyber security plan as expeditiously as possible. Another critical security team focus, especially in financial services and health care, is satisfying regulatory requirements in a manner that is efficient from both time and cost perspectives.

The skill sets of security professionals continue to evolve. Overall, the core team needs to increase its general business acumen and product knowledge so they can better articulate cyber risk in relation to enterprise risk.

What we believe you should do about it

Security teams need to get off their own island, listen to different perspectives and communicate more with business heads about what the organization really needs to worry about in this evolving ecosystem.

For companies that are undergoing a digital transformation — which is most of them — the cyber security team should look to insert itself into the middle of those conversations from a strategic perspective and present themselves as the connective tissue between the business, digital, and security. Have common goals.

Identify the type of data the business is planning to place on the cloud. Understand the type of interactions that will be required between the development and production environments — then map those expectations within the security plan.

Work very closely with corporate communications and the teams that are intimately involved with customer experience. Be part of the messaging strategy. Even if a worst-case scenario materializes, ensure the organization continues to instill trust in consumers.

Ascertain what artificial intelligence (AI) is able to handle and what truly requires the nuance of human thought. Challenge yourself to automate the basic controls in your security environment. Shoot for at least 50 percent.

Finally, advocate for cyber security to be a prominent feature in the organization's environmental, social and governance (ESG) agenda to demonstrate your comprehensive view of cyber security governance and ability to handle a broad array of incidents.

> **Accept the fact that the new world is different. Don't sit there and say, 'I've been doing security for 20 years and the way we do it is A, B, C, D — there's no other way.' Be humble enough to ask, 'What are we really trying to do as an enterprise?' Then assess the available technology and devise the best plan for your environment.**
>
> **Dani Michaux**
> Partner
> KPMG in Ireland

> **The CISO has become a trusted internal adviser and important operational leader. Between digital transformations, a drive to extract extended value from data assets, and global priorities, every company can benefit from a business-aligned and strategically aware cyber executive with a strong, focused team to help protect and enable the organization as it pursues new phases of growth.**
>
> **Rik Parker**
> Principal
> KPMG in the US

The next wave of regulation

When you examine technology risk, you're talking about IT. But when you talk about cyber risk, the ownership and accountability live outside the technology department. The trend we see in the direction and magnitude of cyber-based regulations is moving toward a more holistic approach, focusing on business priorities and responsibilities, such as customer-oriented business activities like building trust; middle- and back-office operational tasks; and Board-driven corporate governance functions. In short, the focus is on management within the first line of defense, as it should be.

The landscape as we see it

In 2020 and beyond, we expect to continue to see increased regulation on a variety of topics from a variety of regulators. In Asia, specifically, we've seen new regulations around cyber security where they've actually used the word "cyber." Previously, the regulations in that region used the word "technology," which had an IT connotation. The increased precision is a welcome development.

With so many countries having issued rules to comply with certain elements of the General Data Protection Regulation (GDPR), or their own privacy laws, we're seeing — especially with larger multinational companies — the creation of new, proactive data management departments. Essentially, businesses are looking to master data analytics as a discipline and understand not only where the data is located across the organization, but also who owns it, what's being done with it, and, perhaps most critically, what rights and permissions users have in relation to that data.

Companies are recognizing the need for additional investment, not just in tooling and process development, but in terms of a lack of cyber talent, from cyber governance and risk strategy to configuration and maintenance. There's still a large gap in this space, and, unfortunately, many companies hire IT professionals who lack cyber security perspective in relation to the regulatory environment. The result is advice that is often ineffective or well intentioned, but misunderstood or inadequately implemented by management and the board.

> **I've become a huge fan of multilayered attack simulations — so-called red teaming and ethical hacking. It's critical to test your security operations to see whether they are able to detect different kinds of attacks, and if they are being detected, stress test the response plan and procedures. More and more regulatory teams are factoring this into their core processes.**
>
> **Ton Diemont**
> Director
> KPMG in Saudi Arabia

> **There are three areas — I call it the trilogy — on which cyber regulations are focused: the underlying operational technology; outsourcing for data that is processed through third parties; and resiliency, meaning the overall ability of the company to detect, respond to, and recover from cyberattacks.**
>
> **Daryl Pereira**
> Partner
> KPMG in Singapore

What we believe you should do about it

Regarding the three lines of defense model, we suggest embedding the responsibilities of cyber security, as well as the role of the CISO, in the first line — preferably formally — and linking these tasks to annual performance targets. The CISO role, at its core, should reside in the first line to cover security strategy and vision, and he or she should have a clear hierarchical or at least functional alignment with security operations regarding daily monitoring and tool configuration.

The second line (i.e., IT risk) should support design quality and resiliency policies and standards, and report back to management and the board. The third line would review and assess the work of the first two lines. This optimal state seeks to extend the company's cyber security needs, including regulatory compliance, across the entire organization.

We also believe it's critical to institute ongoing testing of your regulatory compliance program in terms of design, implementation and effectiveness to identify where improvements are needed. Also, ensure operational cyber resilience is embedded into your overall architecture and processes to solidify security for both IT and OT.

Appoint an individual who is not strictly an IT person to oversee regulatory compliance. In fact, new CISOs should become more comfortable speaking the language of business in order to ensure his or her messages are understood and executed. This individual should have a broad mindset regarding the company's operating model — a Chief Risk Officer, Chief Financial Officer, or Deputy CEO would be ideal because they also have perspective on the company's overall risk agenda. This individual would be the sponsor or champion for cyber security across the entire organization, working in close partnership with the Chief Operating Officer and CISO.

Take the time to unify all of your regulatory requirements, from internal controls and policies to the various regional and country-specific regulations, into a single Unified Control Framework to help enhance the effectiveness of your internal governance, risk, compliance, and testing efforts. Look for synergies between the controls demanded by privacy, resilience, and security regulations — you may be surprised by what you find.

Companies are encouraged to shift their focus from systems and technology to information. Pinpoint what it is that makes you competitive in the market. It could be intellectual property, or your supply chain, or your pricing power. Whatever it is, that's what you need to protect from a cyber security perspective.

Cloud transformation and resilience

One of the things many companies need to work on is aligning the CISO's organization with the rest of the enterprise regarding the maturation and efficacy of the cloud. The business may say "We're going to do x, y, and z in the cloud over the next 18 months." Meanwhile, down the hall, the CISO and his or her team are developing processes and tooling that are vital to, but may not necessarily be aligned with, the business drivers and the technology needed to support the desired business outcomes. That's got to change.

The landscape as we see it

Historically, IT has been responsible for infrastructure provisioning, and, before the cloud, was primarily focused on the challenges on the ground (pun intended). The security team is charged with scanning that infrastructure for vulnerabilities, but they often don't know what to scan because there often is a disconnect with IT on an updated threat list. Managing infrastructure and the related assets has always been demanding, but in the cloud, where everything is faster and more ephemeral, getting security involved early and hardcoded into the provisioning plan is a challenge many companies are struggling with.

In terms of the cloud, across multiple industries, the CISO's organization is largely not prepared to enable the business, neither in terms of skills nor talent. In the cloud, the priority is information protection. What we're finding more and more is that the way data is being deployed in the cloud is often not necessarily resilient. We're not simply talking about multiple availability zones, but the ability to recover critical assets if there's a major breach.

At many companies, we're seeing two camps that seemingly operate at opposite ends of the security spectrum. On one side are the old-school practitioners who have been working in security architecture for 20 years or more, but haven't fully adapted to life in the cloud. On the other you've got cutting-edge security professionals who are all in on today's technology and are trying to promote and enable the cloud mindset so security can be embedded by design and at scale. Getting these factions on the same page is a priority.

> **Security teams have to realize that it's okay to break things as long as you learn something from it quickly and apply that knowledge productively. A lot of organizations don't have the confidence to think this way. A culture of experimentation and learning is what will attract the type of cyber talent companies need in today's rapidly evolving marketplace. The cloud enables you to build and break things fast, rebuild, and realize incremental successes.**
>
> **Caleb Queern**
> Director
> KPMG in the US

> **More and more, we're finding security architects that come from a computer science background and have dabbled in the code-writing process. They realize they've got to take the lead and enable their colleagues to use this new set of cloud tools and support security in the design. So we're starting to see that bridging of the cloud and security — the role of the cloud security professional is starting to emerge, but they're still few and far between.**
>
> **Katherine Robins**
> Partner
> KPMG in Australia

Security team action

Become a learning organization. The thing that attracts cloud talent, beyond money, is culture. Prospective employees need to know they're not walking into a classic, hyper-risk-averse, slow-moving organization. You can attract strong cloud talent by creating a culture that's open to innovation and experimentation.

Similarly, think small, but act fast. Send the message that you build things fast, break things faster, and then rebuild based on what you've learned. Security can enable success through incremental steps. For example, go live with a new container protection strategy in small bites, and enable the business to move fast.

Shift left and push controls as early into your software testing cycle as possible in an effort to deliver maximum value to both customers and users. Apply security — again, in small bites — as far left in the process as possible, which typically involves infrastructure as code. Make it happen by empowering developers to hard code the required security measures without the security team's involvement, which the cloud can facilitate.

Have an appreciation of the underlying code — the ability to read and write code can earn the respect of DevOps engineers. And seize the opportunity to really understand where you should embed yourself. Increasingly, that's what we're going to see from security professionals — the ability to code, because more and more, we're moving away from that traditional security architecture role of measuring diagrams and handing it over to a solution designer or solution architect to then build a solution, which then goes to an engineer to stand up physical infrastructure.

Work to understand — and communicate to the entire enterprise — the connection between business enablement, business resilience, and information protection. It's not much of a departure from how you would do it on premises, but it's a little bit different when you've got critical data across regions in the cloud. Making this part of your DNA enables you to weed out the "noise" from an operations perspective so you can focus on the bigger security priorities.

> **As CISOs look to reduce spend and improve the effectiveness of their teams, automated deaccessioning of outdated digital assets should become a pillar of their overarching strategy. They should similarly explore automating their security operations center playbooks, fraud decisioning, and cyber response through partnerships with leading cloud and security information and event management providers.**
>
> **Anthony Gawron**
> Director
> KPMG in the US

> **Companies are investing in technologies to help determine what they know about their customers' digital behavior. Not only to verify their identity from an authentication standpoint, but to know, behaviorally, how they interact with the environment. They're really following the lead of the intelligence community, where this kind of work has been done quite effectively for the last decade.**
>
> **Ronald Plesco**
> Principal
> KPMG in the US

Automating the security function

We're seeing a convergence of data in the interest of automating security from identity authentication through threat detection and response. A broad set of know-your-customer (KYC) data is being gathered and analyzed by many sectors, including financial services, eCommerce/retail, technology, media and telecommunications, and automotive, among others. This information typically has been heavily siloed. But companies are beginning to realize they are sitting on a treasure trove of data that — if better organized and made more efficiently accessible — can be extracted and analyzed for a variety of value-added purposes.

The landscape as we see it

Companies are working hard to automate functions that until very recently have been purely manual, by pulling together historically disparate data sets.

Not only are businesses better able to confirm that digital customers are who they say they are, they are also acquiring deeper information, such as who has a virus on their computer, who recently received a phishing email, and who tried to enter a network to which they don't have access.

Security professionals are combining third-party tools and in-house solutions to automate as much of the overall cyber playbook as possible, and align it with the organization's business development and customer experience objectives. Companies are looking to automate the first and second lines of defense via the cloud to better respond to threats across the enterprise without a human having to do that work, while simultaneously confirming that the security controls they expect to have in place are indeed operating as expected.

What we believe you should do about it

Always remember: Whoever controls the data has the power. With that firmly in mind, the first step is to transfer your critical enterprise data from the different third-party vendors that so many companies maintain across their systems into a centralized, accessible location.

We also suggest advocating for a data normalization initiative within the organization to scrub and properly label the data so you understand what data you have, how it's being posted, and what features are available within the datasets.

Organizations in the early stages of maturity in terms of data normalization may not be equipped to jump right into insight extraction through AI and machine learning. For these companies, it's important to prioritize the use cases they want to address — fraud detection, customer experience enhancements, operational efficiency improvements, for example — and determine how to plug in the right tools, technologies, and advanced analytics to leverage the data once it's available.

How KPMG can help

At KPMG, our global network of business-savvy cyber security member firm professionals understands that businesses cannot be held back by cyber risk. KPMG member firm professionals recognize that cyber security is about risk management — not risk elimination.

No matter where you are on your cyber security journey, KPMG member firms can help you reach your destination: a place of confidence in which you can operate without crippling disruption from a cyber security event. Working should-to-shoulder with you, KPMG member firm professionals can help you work through strategy and governance, organizational transformation, cyber defense, and cyber response. And our cyber security professionals don't just recommend solutions — they also help implement them. From penetration testing and privacy strategy to access management and cultural change, KPMG member firms can help you every step of the way.

kpmg.com/cybersecurity

Contact us

Tony Buffomante
KPMG Cyber Security Services Global Co-Leader, KPMG International and Principal
KPMG in the US
E: abuffomante@kpmg.com

Akhilesh Tuteja
KPMG Cyber Security Services Global Co-Leader, KPMG International and Principal
KPMG in the US
E: atuteja@kpmg.com

John Hermans
Partner
KPMG Cyber Security Services
KPMG in the Netherlands
E: hermans.john@kpmg.nl

Ben Krutzen
Partner
KPMG Cyber Security Services
KPMG in the Netherlands
E: Krutzen.Ben@kpmg.nl

Charlie Jacco
Principal
KPMG Cyber Security Services
KPMG in the US
E: cjacco@kpmg.com

Alex Anisie
Director
KPMG Cyber Security Services
KPMG in the US
E: Alexandra.Anisie@kpmg.co.uk

Dani Michaux
Partner
KPMG Cyber Security Services
KPMG in Ireland
E: dani.michaux@kpmg.ie

Rik Parker
Principal
KPMG Cyber Security Services
KPMG in the US
E: rikparker@kpmg.com

Ton Diemont
Director
KPMG Cyber Security Services
KPMG in Saudi Arabia
E: antondiemont@kpmg.com

Daryl Pereira
Partner
KPMG Cyber Security Services
KPMG in Singapore
E: darylpereira@kpmg.com.sg

Caleb Queern
Director
KPMG Cyber Security Services
KPMG in the US
E: cqueern@kpmg.com

Katherine Robins
Partner
KPMG Cyber Security Services
KPMG in Australia
E: krobins@kpmg.com.au

Anthony Gawron
Director
KPMG Cyber Security Services
KPMG in the US
E: agawron@kpmg.com

Ronald Plesco
Principal
KPMG Cyber Security Services
KPMG in the US
E: rplesco@kpmg.com

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

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: All hands on deck: Key cyber security considerations for 2020
Publication number: 136862-G
Publication date: March 2020