What's next: Key cyber security considerations for 2019

Protect corporate and customer data by maintaining a clear view of the evolving threat landscape

kpmg.com/us/cyber

Over the past several years, a broad array of factors have propelled many organizations' increased focus on cyber security and information protection: rapid shifts in technology, the growing volume and sophistication of threats, the ongoing migration to automated and cloud-based services, the explosion of and focus on data, and more rigorous regulatory requirements, to name a few. Lapses in security can be devastating, both to an organization's bottom line and reputation. It is critical for companies to remain vigilant and informed regarding emerging threats and the available solutions for mitigating those threats. This report is by no means an exhaustive review of all the of the cyber challenges companies are likely to encounter in 2019. Rather, it is intended to highlight some of the issues we've observed in the marketplace, along with our perspectives for consideration. The topics we discuss include:

1. **The industry wide deficiency of cyber skills**
2. **The ongoing weaponization of AI**
3. **Data privacy and protection**
4. **Fraud and cyber risk**
5. **The importance of identity and access management (IAM)**
6. **Phishing**

"We view today's evolving cyber threats with caution, but also as an opportunity to help clients across industries augment their security capabilities in a way that's not only timely, but reveals cyber security's value as a business enabler. Companies have to be a little creative, there has to be a shared vision from the top down around adopting advanced solutions. And then, at the enterprise level, they must develop a framework for protecting the entire operational ecosystem—especially the automated aspects."

—Tony Buffomante
Principal,
KPMG Cyber Security Services—US Leader

Most companies are looking to automation not to reduce headcount, but to refocus people on the creative and clever versus the rote and repeatable.

— Gavin Mead
Principal,
KPMG Cyber Security Services

Skills shortage

Across the cyber landscape, the skills shortage manifests itself across the spectrum, in public and private companies, as well as consulting and government.

What we're seeing

There continues to be a dearth of adequately trained, appropriately skilled personnel to protect vital processes, intellectual property and sensitive data at numerous organizations across virtually every industry.

What you should do about it

The lack of seasoned cyber professionals, coupled with tightening budgets, amplifies the importance of automation—this is the most efficient course of action for organizations focused on addressing cyber risk expeditiously.

Look for tasks that are manual and time consuming and move aggressively to automate them. The goal is to pull people up a level strategically and remove some of the repetitive aspects of collecting and analyzing data about intruder activity. Instead, hand that over to an integrated SOAR platform (Security, Orchestration, Automation, Response).

It's not just a numbers game. Some companies have adequate IT headcount, but in many cases have people who aren't focused on the right things, often through no fault of their own—threats have evolved so quickly, companies haven't been able to keep up. In these cases, it's an exercise in re-prioritizing what people are doing.

And to keep your bench deep, pay attention to your company's new talent plan. Aggressively hire digital natives right out of college—they come to the table with an innate sense of cyber issues and opportunities—and develop a bespoke training program to build the next generation of cyber professionals.

KPMG

AI: A powerful weapon in the attacker's—and cyber team's—arsenal

In today's arms race the advantage goes to the attacker. The defender has to be good everywhere; the attacker only has to be good at the spot where they are attacking.

What we're seeing

Cyber attackers are increasingly likely to employ AI, using deep learning and machine learning algorithms to make malware and targeted attacks more effective and more targeted and harder to detect.

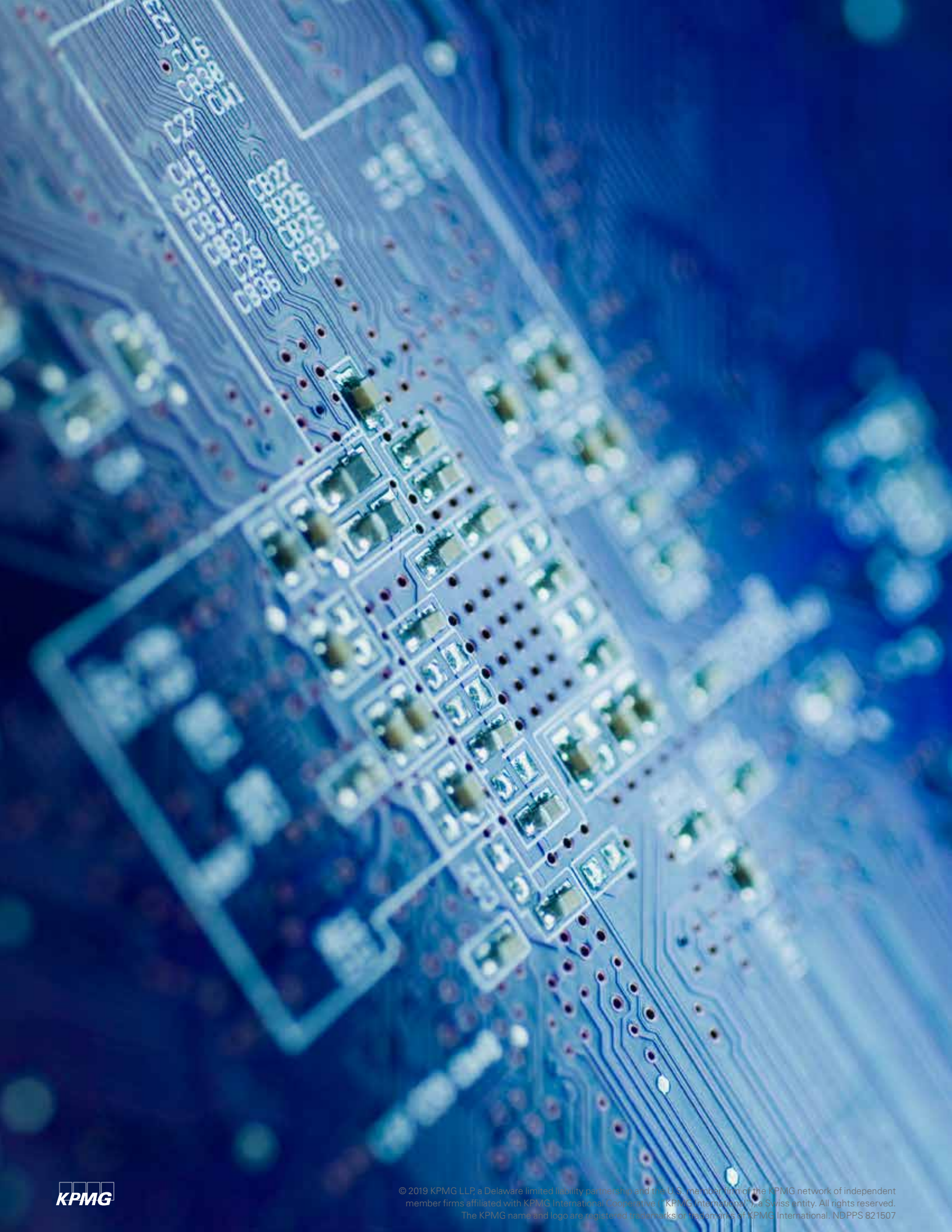
What you should do about it

The goal in 2019 is to turn the noise down as much as possible and weed out the false positives. Whether through API-based services, open source software or a packaged product, we suggest cyber teams acquire and employ AI solutions to help identify security incidents and assess system-wide vulnerabilities.

AI has the ability to correlate numerous data sources to identify patterns or anomalies that might point to malicious activities. As a self-learning technology, AI offers the prospect of adaptive improvement as organizations strive to produce positive cyber security outcomes.

In 2019, we encourage companies to avoid reflexively addressing automation or security telemetry issues with off-the-shelf, bolt-on AI tools. Cyber professionals should think about AI—and security in general—in the context of the organization's longer-term platform strategy. In that way, cyber professionals can ensure they are one of the stakeholders at the table when companies engage in strategic business planning.

> **"AI represents opportunities not only in improving fidelity of detection and response, but also in re-establishing protection and prevention in balance as viable approaches for key parts of the enterprise."**
>
> — Gavin Mead
> Principal,
> KPMG Cyber Security Services



KPMG

Sustainable data privacy compliance

In an age when proprietary and customer data are a company's most valuable assets, getting the privacy strategy right can give an organization a competitive edge.

What we're seeing

The board's view of data privacy sets the tone at the top for the way privacy is addressed throughout the entire company. With cyber security now firmly an enterprise-wide priority, full engagement across the organization is growing as security professionals look to embed privacy into the DNA of business operations and customer engagement.

What you should do about it

Organizations must chart a plan that encompasses not only the immediate regulatory challenges, but also for a shifting regulatory climate and consumer expectations of greater individual control of data.

Businesses must move beyond compliance, which is table stakes, and work to ensure data privacy processes are an integral component of the business model. In creating a sustainable and effective data-protection strategy, we believe companies should develop a solid framework of best practices and infuse those practices—both procedurally and culturally—within the organization, opening up the flexibility to quickly adapt to new (GDPR) and evolving (HIPAA) regulations.

As regulations similar to GDPR are enacted in the United States like CCPA (California Consumer Privacy Act) and globally, companies should take a more strategic approach to privacy and information governance to reduce their overall cost of compliance and enhance customer trust.

"Companies that can demonstrate a commitment to customer privacy and data protection have the opportunity to stand out among their peers. To stay ahead of the curve, plan and adopt a data protection strategy based on privacy principles that can be easily modified as new regulations go into effect."

— Orson Lucas
Managing Director,
KPMG Cyber Security Services

— Steven Stein
Principal,
KPMG Cyber Security Services

Companies will need to determine how to tailor their digital interactions based on customer preferences. Customers—especially millennials—want options, and if they don't get it from their current provider, they'll get it somewhere else.

— Charles Jacco
Principal,
KPMG Cyber Security Services

The intersection of fraud risk and cyber risk

To provide consumers with the experience they desire and protect against fraudulent activity, financial institutions need more personal information about their customers' tendencies and preferences. This will have the beneficial effect not only of better serving customers, but also of facilitating better response to digital threats and fraud.

What we're seeing

Companies in all sectors are getting away from a one-size-fits-all security model—it's just not sustainable in today's environment. From an enterprise perspective, and in terms of collecting and leveraging client data, fraud prevention and cyber security are converging.

What you should do about it

Organizations, financial institutions in particular, should focus on fraud reduction. Large and mid-sized companies are looking to reduce fraud and make the customer experience both more secure and more personalized.

Companies need to determine how to tailor their digital interactions for a better customer experience, whether on a phone or tablet, the company's website or the next generation of ATMs. Customers—especially Millennials—want options and if they don't get it from their current provider, they'll get it somewhere else. Not everyone should be forced to continually create one-time logins, but similarly it's not realistic to expect everyone to use a biometric authentication method, such as a thumb print or retinal recognition either.

In 2019 and beyond, fraud and cyber should garner equal attention from a security perspective. New and improved strategies for collecting and leveraging client data, particularly authentication data, should be in the pipeline.

The goal is to understand the customer's typical behavior, recognize anomalies and educate customers about the value of using personally identifiable information conscientiously to prevent fraudulent activity.

A step-up in authentication can be a win-win

The perception of identity and access management (IAM) is evolving from a security-driven initiative to a driver of business enablement.

What we're seeing

Over the coming year, the industry will focus heavily on advanced authentication, identity proofing, fraud and analytics—the complete digital security story, connecting consumer, business, marketing and the ultimate benefits from a security and privacy perspective.

In the IAM space we've broadened the term to digital identity. That's the emerging area. It includes the needs and priorities of both consumers and businesses, but it also drills down into the other important areas that encompass the customer experience.

What you should do about it

For businesses to do digital right, IAM has to be an integral part of the design. The ability to have and maintain a 360° view of the customer—critical in today's environment—is informed and underpinned by an integrated identity platform.

Another focus in 2019 is expected to be a move away from passwords. Not only are people simply tired of them, but weak passwords are often the source of a lot of identity theft. Companies are getting to a point where they are going to have to be much more aggressive about employing advanced authentication methods, such as touch or face ID or voice recognition, to replace passwords. Companies should give serious consideration to trading passwords for biometric-enabled apps.

> **"Since businesses today use data to better understand their customers' behavior, preferences, and buying habits in virtual settings, it's critical they use that data to know who exactly they are dealing with at all times."**
>
> — Kyle Kappel
> Principal,
> KPMG Cyber Security Services

APTs—advanced persistent threats—are changing daily, so security professionals need to be agile. Software by itself is not agile. People write software to solve specific problems. Coupling software with human experience doesn't add the possibility of human failure, it increases the platform's ability to fill in the gaps.

— Edward Goings
Principal,
KPMG Cyber Security Services

What's old is new: The phishing threat persists

No organization has the ability to defend all vectors consistently. When it comes to phishing, there is no perfect tool, no perfect monitoring platform that is going to defend your network at all times. Companies have to be both analytical and agile as they work to identify attack patterns.

What we're seeing

Attackers are continuing to target the weakest link and that is often the user sitting behind the computer. It may sound somewhat old school from a cyber perspective, but despite the growing sophistication of today's attack methods, phishing remains one of the toughest threats to defend.

What you should do about it

We see the market moving toward a broad, managed cyber response posture. A key differentiator of this stance is that the internal analysts are constantly engaged, tuning the network as the business, and the threats, evolve. In this way, the cyber team is out front in a protective state versus a purely defensive state. The efficiency of this proactive structure, combined with the right human factor to fill in the gaps, is powerful.

And yet more and more companies are cutting back on funding for cyber personnel as they subscribe to new software solutions. There truly is no "easy fix" button out there. No single software package is going to end the woes of all the issues that you have to defend against. Sooner than later, both companies and government entities will see the value of committing a greater portion of their budgets to the human component of cyber security.

Phishing is not just a seasonal threat. These campaigns unleash spyware, ransomware, wiper attacks and APTs. Security professionals have to be flexible year round, depending upon the trending threat.

KPMG

How KPMG can help

Cyber security is a strategic enterprise capability that goes far beyond IT. Whether we are working with your board, back office or data center, we will provide a clear, jargon-free explanation of your most pressing cyber threats, the potential impact to your critical assets and the recommended response. Ultimately, we view cyber security through a cross-functional business lens, encompassing people, change, financial and risk management.

Contact us

Tony Buffomante
Principal
Cyber Security Services – US Leader
E: abuffomante@kpmg.com

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

Edward Goings
Principal
Cyber Security Services
E: egoings@kpmg.com

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

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

Charles Jacco
Principal
Cyber Security
US Financial Services Industry Lead
E: cjacco@kpmg.com

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

Orson Lucas
Managing Director
Cyber Security
E: olucas@kpmg.com

Gavin Mead
Principal
Cyber Security Services
E: gmead@kpmg.com

Steven Stein
Principal
Cyber Security Services
E: ssstein@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