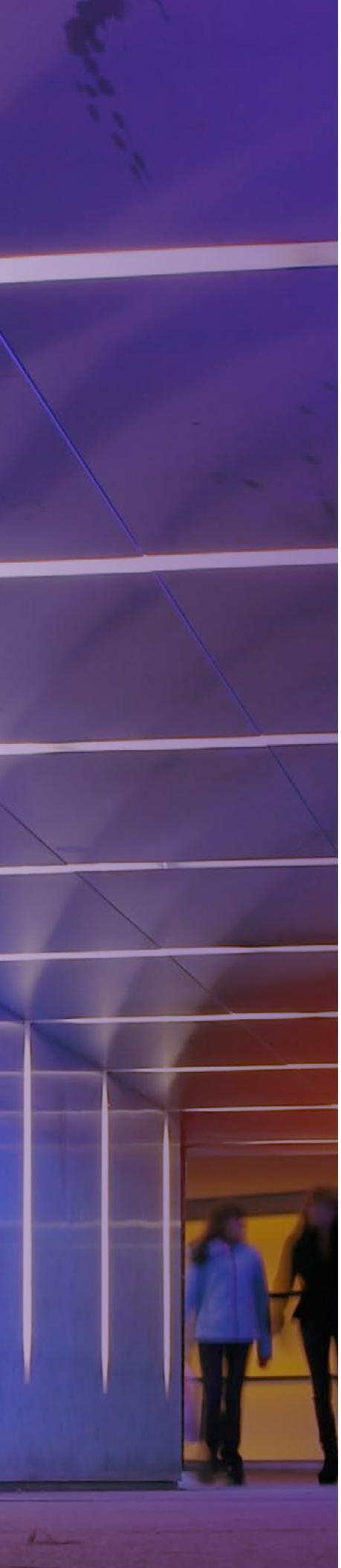
KPMG

Speed, Scale and Trust

On-Call Services from KPMG

kpmg.com



Introduction

Today's global companies are managing overwhelming volumes of physical and electronic information that may be subject to discovery in a regulatory proceeding or be at risk of a cyber breach. The ever-growing volume of data, presence of new data sources, numerous forms of communication, rapidly evolving technologies and a changing regulatory landscape all present unique evidence discovery ("eDiscovery") and cyber security challenges.

Cyber risk has tripled since 2013 and is intensifying. Companies face increased global regulatory scrutiny on data privacy, data management, and integrity in financial reporting. There is also continued growth in litigation worldwide. This makes it essential that companies are adequately prepared to respond to requests for the disclosure of their electronic data. As every sector and industry around the world is becoming more and more digital, so is the speed with which cyber-crime is affecting everything and everyone globally. Effective data security and evidence discovery management processes and procedures are key to helping minimize data risks.

The news is ripe with articles about companies involved in incidents of fraud and misconduct that suddenly face regulatory inquiries requiring large-scale evidence discovery efforts. You are all also hearing more and more about companies that are victims of recent, large-scale cyber-attacks, costing them millions in ransom payments, crippling their infrastructure, and destroying trust. COVID-19 and the increase in employees working remotely without strong security or using unapproved data storage devices has propelled both cyber-attacks and less than effective data identification and management protocols.

The hard truth of today's environment is that everyone needs to be mindful of their safety.

From global multinationals to smaller non-profit companies, fraud, regulatory enforcement, and cyber-crime can affect all organizations, no matter the size.

Did you know?

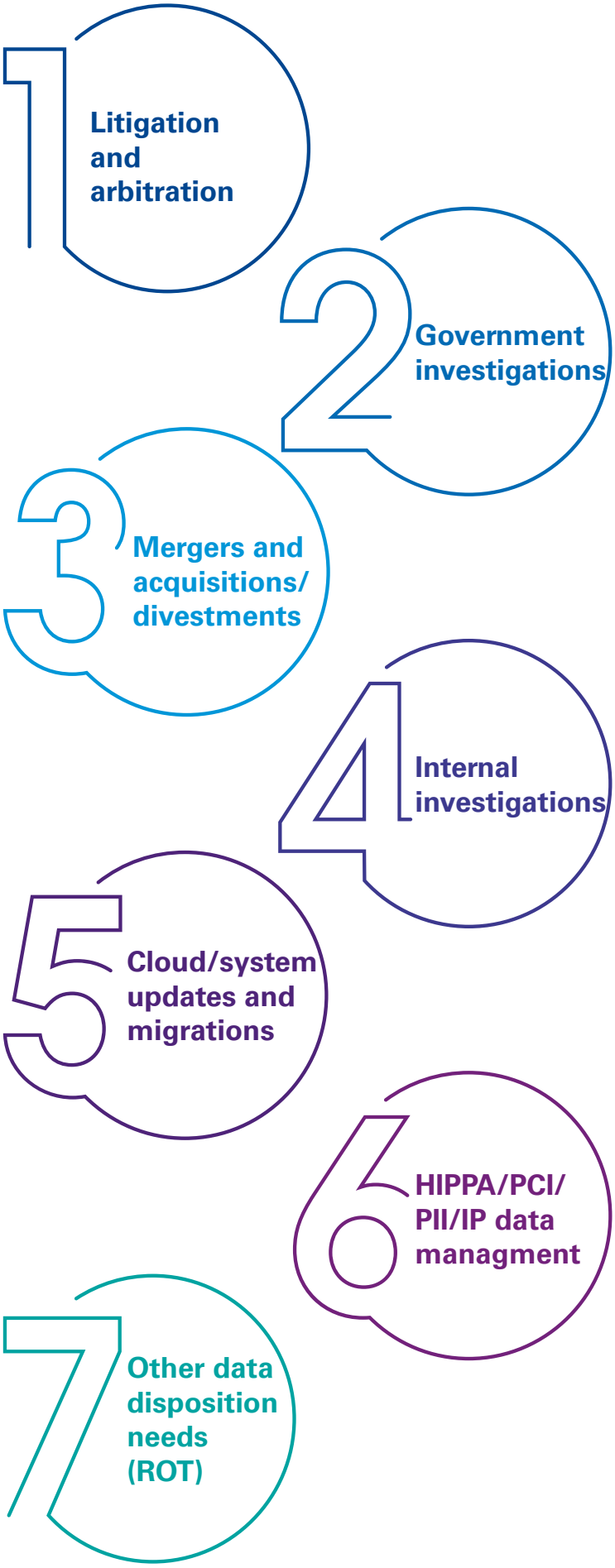
74% of CEOs surveyed in KPMG's 2021 CEO Outlook Pulse Survey say the speed of digitization has accelerated by a matter of months.

The majority point to the amazing progress made in digitizing their operations, business models and revenue streams during the pandemic. Forty-nine percent of CEOs are also investing heavily in new technologies and plan to spend more on digital technologies compared to a year ago.

Increasingly, these scenarios are happening around the world:

- A company has been notified by a regulator of an inquiry into allegations of violations of laws or regulations in foreign markets.
- A CEO receives a call from their Chief Information Security Officer saying unauthorized access was detected on their company's financial systems–a crown jewel storing millions of customers' data and putting the integrity of their company's financials at risk.
- A corporation receives a whistle blower complaint through its hotline that alleges widescale fraud, financial reporting / earnings management or other serious allegations. It now needs to urgently comb through mountains of data to investigate the complaint.
- A global national company is involved in litigation, requiring the identification, collection and production of large amounts of data that needs to be reviewed and redacted prior to discovery.

Everything may now be put into question – audit, regulatory compliance, and financial reporting.



On-Call Services

When you need to move quickly

A rapid response to allegations of fraud, regulatory data requests and cyber breaches is critical and often complex, especially if the incidents are reported in a company's foreign operations. Having resources with the right skills set, fluency in the local language, knowledge of local customs, and ability to be deployed within hours is a tall order for any organization.

To help improve response time, efficiency and costs, many organizations are proactively establishing collaborative relationships with KPMG. Allowing us to be under contract and respond as soon as possible on an as-needed basis. KPMG firms around the globe have 6,000 forensic and cyber professionals in over 100 countries who stand at the ready to assist. KPMG can help you and your outside counsel respond with speed and at-scale to these needs with forensic analyses and detailed investigations.

What can we do to help?

KPMG's on-demand response services model is a custom-tailored service to collectively address many of KPMG's cyber and forensics services in one package. Our on-call service helps reduce risks and can proactively inform clients of threats. It also focuses on the long-term development of a cyber response capability, while providing quick access to KPMG's know-how and professionals.

KPMG wants to be your organization's preferred provider of digital forensic and incident response services and/or act as an extension of your internal team – augmenting with forensic investigations, malware analysis, or other highly specialized jobs.

Through an on-call arrangement, you can benefit from our existing knowledge of your culture, operations, managed vendor relationships, and more. This approach can also help minimize the challenges inherent in using multiple service providers to conduct small or multijurisdictional investigations.

> "Clients who have onboarded with KPMG's on-call services in advance of an incident have found they were able to respond to incidents within minutes instead of days."

David Nides
Principal, US Cyber Response, KPMG in the US

There are two ways of working with us

1. On a retainer basis. (For example, by pre-purchasing a number of hours.)
2. On a time-and-materials basis. There is no cost to put this arrangement in place in advance of an incident, so we can respond immediately when you need assistance.

Onboarding in advance – the key to a speedy incident response

When a cyber security incident, fraud, regulatory inquiry, or litigation occurs, you have to act fast to identify and secure the data.

To prepare and help ensure our team can respond quickly, we will start with a tailored on-boarding process (e.g., a two- to three-hour meeting) at no cost to you.

KPMG will:

— meet with key stakeholders who are part of the eDiscovery process and/or cyber incident response team

— review your documentation (including litigation readiness assessments, incident response plans, fraud risk management program, and crisis management procedures)

— learn about your network, system and application infrastructure and security tools to understand where and how your data is managed, stored and preserved.

Should an incident occur in your environment, our pre-existing knowledge of your business and infrastructure can help our analysts begin the incident response process without extensive background and exploratory discussions.

Simple and effective execution

How KPMG can help

1. Incident Response

If an incident occurs (such as a cyber-attack, a regulatory inquiry, an allegation of fraud, or a litigation filing), organizations have to act fast.

At the time of crisis, we can leverage KPMG professionals globally who have deep experience across sectors and jurisdictions. They have all been consistently trained on our global methodologies and can quickly identify key risks and develop appropriate remedial actions.

To help mitigate initial risks, we will start by providing an actionable plan to identify which tasks need to be performed and when. We can then help with either a portion of the investigation as a supplement to your own internal investigations team. Or, we can conduct the entire investigation independently at the direction of management or counsel.

2. Investigation

We will conduct forensic analysis and detailed investigations to assist in determining what happened, how it happened, and, if applicable, who was involved. Our IP and proprietary tools can help accelerate these efforts. For example, in instances of a cyber attack, we automate common forensic triage tasks in a timely and consistent manner through the use of KPMG's digital responder. In instances of fraud investigations and regulatory enforcement, we use proprietary and licensed eDiscovery tools to conduct forensically sound, targeted collections and data preservation, helping our clients reduce the amount of non-relevant data. Throughout the eDiscovery process, we use KPMG's evidence tracker to document and maintain a chain of custody of all data we acquire and receive.

3. eDiscovery

To support the investigation, litigation or anticipation of litigation, we use our vast array of both internally developed and licensed technologies to help ensure we bring the right capabilities to each case. In cases of forensic investigations and regulatory enforcement, we help oversee the data and apply artificial intelligence and active learning to identify documents of interest in a fraction of the time as compared to a linear review. Through a combination of principles, we can focus on helping to reduce the costs and drive a well-positioned process – from collection to review and production – consistenly enhancing quality, efficiency, and productivity and providing transparency throughout the investigation.

All of the above steps are key to implementing an effective eDiscovery lifecycle strategy to help ensure data is moved through the identification, preservation, collection, processing, and analysis stages accurately and efficiently.

4. Rebuilding Trust

When our clients inspire trust, they create a platform for responsible growth, bold innovation and sustainable advances in performance and efficiency.

- KPMG professionals have deep skills in risk and regulation, advanced digital solutions and well-established change expertise in one powerful and global approach. We can help you build trust with everyone who has a stake in your business, from customers, employees and suppliers, to regulators, shareholders and the communities in which you operate.
- We are bringing risk out of the back room, with a positive shift from passive compliance to active value generation. Trust is a multiplier of benefits.
- We can help you build trust with everyone who has a stake in your business, from customers, employees and suppliers, to regulators, shareholders and the communities in which you operate.
- Additionally, KPMG can help you provide a neutral and court-appointed expert — The need for a neutral voice is common when technical issues are at hand. KPMG's professionals are experienced at explaining even the most complex technical challenges and developing objective procedures to help reduce confusion. Our team understands the legal process and the need for a truly unbiased and impartial voice.

Did you know?

Businesses often consider the enormous tangible costs of a cyber attack – loss of revenue while systems are down, the cost of remediation and customer compensation or litigation. But the intangible costs, although harder to measure, can have even bigger long-term consequences – for example, the damage done to your reputation and the erosion of stakeholder trust.

Knowledgeable Professionals at Scale

- KPMG provides access to deep forensic and cyber capabilities around the world. Our highly collaborative global team consists of multi-language subject matter professionals who reside in more than 100 countries, and we are committed to delivering with consistent processes that may be accepted by local regulatory bodies.
- Our data-driven approach includes access to extensive global databases, intelligence analytics, and trained resources. We provide market-leading insights and artificial intelligence (AI)-enabled solutions to help you challenge the norm and drive better outcomes.
- KPMG has shared global methodologies and streamlined project management models that focus on risks and simplify complexities for our clients. We have invested heavily in automaton processes, allowing us to help drive consistency, increase quality, and lower client costs.
- Leveraging technology, we have developed specialized knowledge to identify and analyze corporate systems to assess how employees communicate, correspond, and maintain business records. We also provide defensible data and remediation services, helping companies to isolate data that needs to be preserved, carved out, or disposed of.
- We have deep experience with an array of IT landscapes and systems, enabling us to provide a holistic approach to forensic collections.
- Combined with our global capability, KPMG also has local knowledge and presence in nearly every market where you do business. So, we understand the risks and ramifications that may change from one country to the next.
- We can help you build trust with everyone who has a stake in your business, from customers, employees and suppliers, to regulators, shareholders and the communities in which you operate.

Speed

Our approach enables for increased speed and accuracy.

KPMG helps accelerate the investigation and remediation efforts through the significant use of IP and proprietary tools.

- KPMG's digital responder (patent pending) automates common forensic triage tasks in a timely and consistent manner. This allows organizations to respond to cyber incidents by helping to increase responsive effectiveness and efficiency.
- Proprietary tooling for containing and investigating large-scale incidents in leading cloud platforms.
- Proprietary workflows to deal with structured/unstructured sensitive data identification and document review. This helps in the mandatory notification process (regulatory, legal).
- Shift to cloud, particularly in light of increasing regulatory requirements about the cross-border transportation of data.

US$1m

The average cost globally to remediate a ransomware attack[1]

21%

of attacks are via email or phishing[2]

29%

of attacks are via remote access[3]

[1] H1 2020 Cyber insurance Claims Report, Coalition inc. 2020.

[2-3] Sophos Whitepaper, May 2020.

Why KPMG?

Decades of experience dealing with cyber breaches, regulatory response and investigations of fraud/financial crimes

We have worked on some of the most high-profile financial reporting investigations; regulatory inquiries into misconduct allegations; ransomware, APT, and insider attacks; and litigations.

We have significant experience working with all the stakeholders involved – outside counsel, general counsel, internal audit, compliance, law enforcement, regulators, fidelity insurance, cyber insurance, and the broader business on all aspects of incident response.

Global and local
Combined with global capabilities of KPMG firms, KPMG professionals have local knowledge, capabilities and presence in nearly every market where you do business. This deep local expertise allow KPMG to understand the risks and ramifications that vary from one country to the next. We leverage a consistent engagement governance structure globally and assign you a single point of contact to help ensure consistent delivery across the world.

Independent and vendor neutral
We're entirely driven by our experience. You can have the confidence in our bias-free judgement and advice.

We are on cyber insurance carrier lists
We are pre-approved as a preferred vendor on many major cyber insurance carrier lists. This can help streamline your cyber insurance claims.

Key Differentiators

- No-cost, no-subscription model allows KPMG to respond quickly to your needs.
- Low onboarding means KPMG invests in the relationship too.
- KPMG is part of a reputable, global network of member firms.
- KPMG's ability to leverage resources across the globe means wide-ranging investigations for multinational companies.
- KPMG can provide on-demand malicious code analysis, host- and enterprise-based forensics, network forensics, threat intelligence, and expert testimony.
- We are entirely driven by our knowledge and experience to help provide the right approach for you.
- KPMG can temporarily deploy our enterprise forensic tool licenses in your network if existing capabilities do not already exist.

“KPMG takes a comprehensive approach to cyberincidents through its integrated cyberpractice. Incident readiness services include cyberstrategy and planning, security configuration and monitoring, security controls testing, and business and technical simulations. KPMG Incident Response includes digital forensics, case and incident tracking, data analytics and source log analysis, disaster recovery, remediation, and business improvement.”

IDC MarketScape: Worldwide Incident Readiness Services 2021 Vendor Assessment, Doc # US46741420, November 2021

Did you know?

KPMG is positioned in the **Leaders category in the 2021 IDC MarketScape** for worldwide incident readiness services.

Case Studies

Global insurance provider

The challenge

A cyber security investigation prompted by an FBI notification to the insurance provider regarding data leakage.

What we did

KPMG assembled 24/7 operation that began by scanning the client's network for externally facing servers, performing vulnerability assessments of key systems, and reviewing available network logs for signs of suspicious activities. Further details from external sources enabled KPMG to focus their investigation and identify compromised systems. In addition to identifying the compromised hosts stemming from a VNC exploit, KPMG was able to identify other security weaknesses within the client's environment and other potentially compromised machines that were not related to the incident under investigation.

The outcome

The organization had a dramatically improved overall security posture.

Evidence preserved by KPMG was provided to the government through proper legal channels.

The suspect responsible for the data leakage was arrested shortly after and later sentenced to several years in prison and ordered to pay nearly US$3 million in restitution to the client.

Global Life Sciences Company

The challenge

A Fortune 50 global pharmaceutical, medical device, and consumer markets company retained KPMG to provide forensic accounting and on-call investigation services outside the US.

What we did

KPMG conducted a multitude of investigations around the globe ranging from allegations of financial reporting matters (such as earnings management, complex accounting fraud and channel stuffing), bribery and corruption, and conflict of interest concerns. KPMG also assisted the company with corporate intelligence and anti-bribery and corruption-focused due diligence services to the company's compliance and legal groups. In some instances, KPMG was requested to work under the direction of outside counsel and internal audit, while in other cases, we helped to provide in-country resources to augment the client's internal resources leading the investigations.

The outcome

Our on-call investigations assistance has helped the company enhance its incident response protocols, improve its response time to investigate fraud and misconduct allegations, and reduce the time it takes to complete investigations. As part of our work, we also provided insights into fraud risk factors, root cause analyses, remediation, recommendations, and other enhancement opportunities to the company's processes and controls to help prevent, detect and respond to fraud and misconduct.

Case Studies

Mexico retail

The challenge

A Mexican retail company identified a payroll payment to an unregistered account in their employee master. It was found that the account belonged to an IT employee.

What we did

KPMG carried out the forensic collection and analysis of electronic communications of the IT employee and key system logs. At the same time, we collected and processed one year of payroll data from more than 20k employees to identify deviations.

As deviations were confirmed, our analysis led to the identification of an unauthorized program in the ERP system that allowed the automatic discount of a certain amounts from all employee's payroll. The amount deviated was automatically applied to a bank account. Furthermore, this program was design to overwrite payroll disbursement files, overcoming security controls.

It was also identified that several third parties were granted remote access to the ERP system by the IT employee.

The outcome

As a result of our work, the company implemented more robust controls over the payroll payment process, conducted an in-depth review for unknown programs running on the ERP system, improved their remote access monitoring process and began legal action against the involved employee.

Pharmaceutical company

The challenge

Due to an internal complaint, the company asked us to investigate the possible loss of intellectual property as a result of the departure of an employee from the commercial area.

What we did

Our analysis included forensic collection and analysis of information on the devices assigned to the departed employee, as well as to their corporate email. The analysis also focused on identifying the activities carried out on the computer during the week prior to the employee's departure.

The outcome

As a result of our analysis, the company identified activities indicative of a possible leakage of company information – connection of external hard drives, presence of anti-forensic tools for the secure deletion of information and sending information to personal accounts, among others.

From these results, the company implemented additional control measures on their technology assets to prevent information leakage and contacted their legal advisors for a possible complaint before the authorities.

Contact us

Amanda Rigby
Forensic Americas Leader*
Principal, Advisory
KPMG in the US
amandarigby@kpmg.com

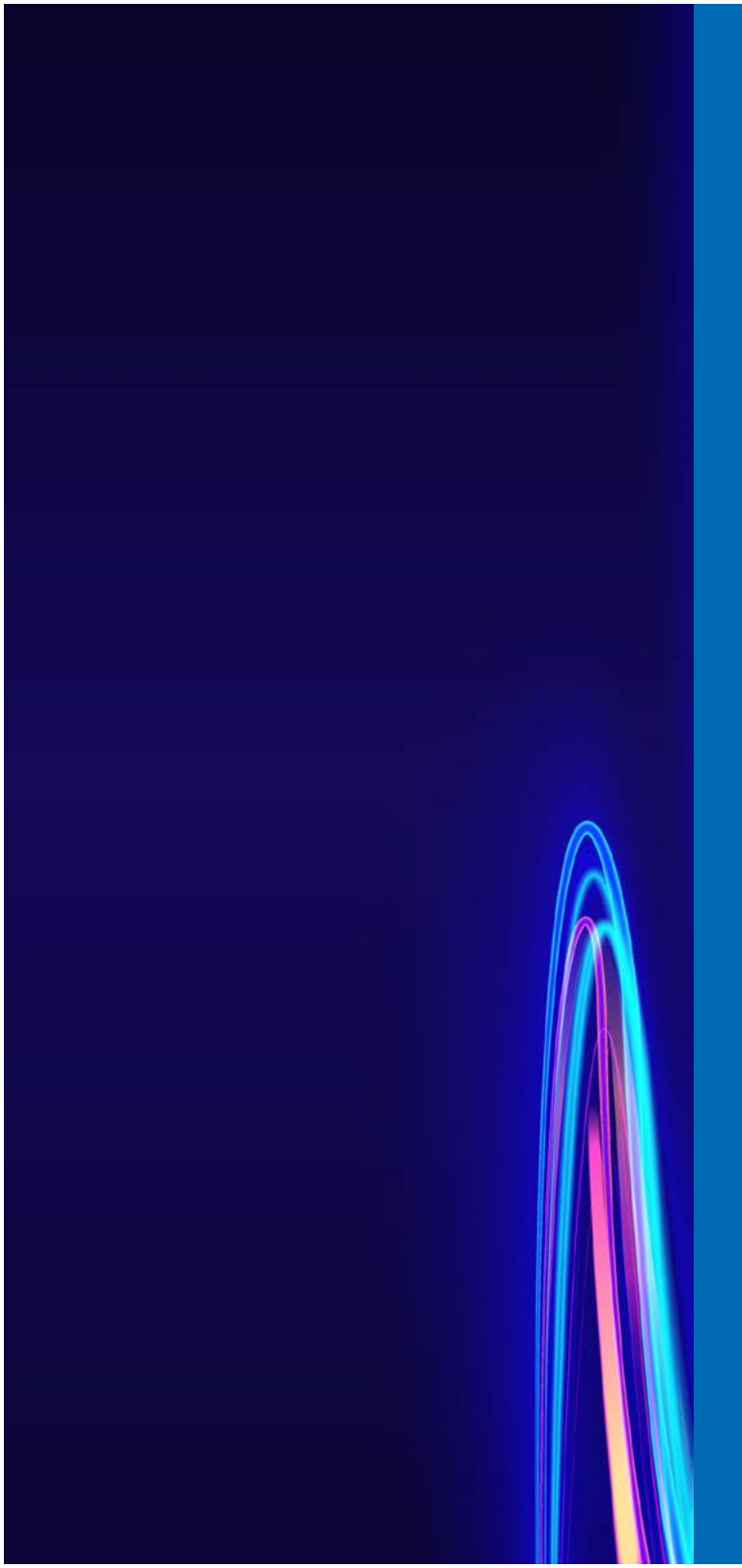
Luis Preciado
Lead Partner, Risk Advisory
KPMG in Mexico
luispreciado@kpmg.com.mx

David Nides
Principal, US Cyber Response
KPMG in the US
dnides@kpmg.com

Ivan Velez-Leon
Managing Director, Forensic
KPMG in the US
ievelez@kpmg.com

Ana Lopez Espinar
Partner, Forensics
KPMG in Argentina
ablopez@kpmg.com.ar

Emerson Melo
Partner, Forensics
KPMG in Brazil
emersonmelo@kpmg.com.br



* All professional services are provided by the registered and licensed KPMG member firms of KPMG International

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

MADE in KPMG | MDE137902A January 2022