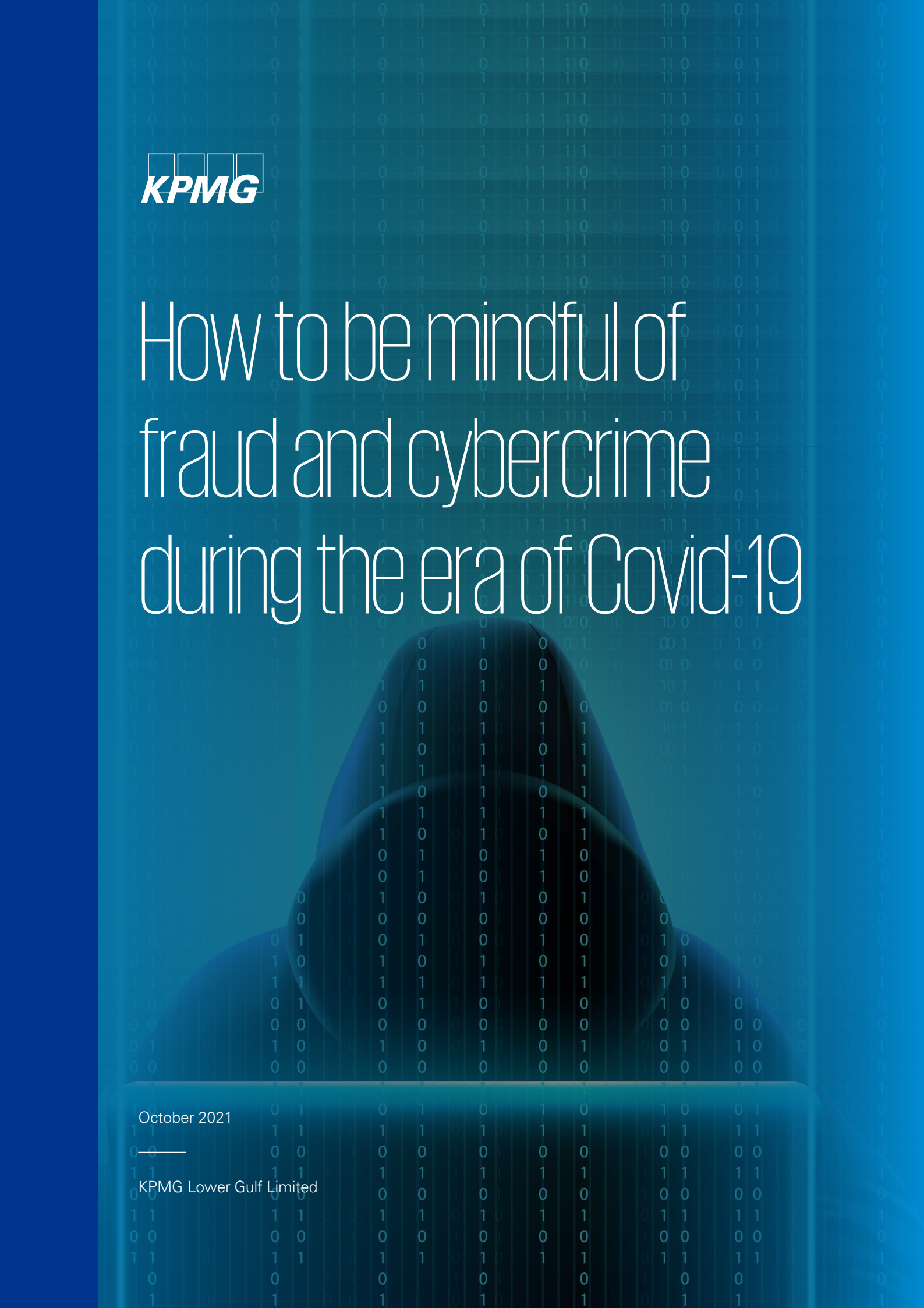
KPMG

How to be mindful of fraud and cybercrime during the era of Covid-19



October 2021

KPMG Lower Gulf Limited

Troubled and uncertain times

The impact of Covid-19 on organizations and supply chains is being felt around the globe. Aside from the financial effect, there has been an upsurge in cybercrime and business fraud, as criminals strive to take advantage of vulnerabilities during these uncertain times.

In the current crises, it is particularly important that organizations are aware of the latest approaches being used by the criminal fraternity, how to fortify their security and controls, and also how to minimize vulnerabilities and exposure to risk.

To survive and thrive, organizations will need a well-planned approach to curtailing disruption, its impact on income and fluctuating share prices. Otherwise, fraud and cybercrime may create another wave of commercial transgressions, which could in turn have a greater effect on shareholder value and revenue.

A successful crime is likely to require both an opening and poor security and/or controls within an organization; the current global situation has exacerbated the frequency of both.

Growing fraud challenges

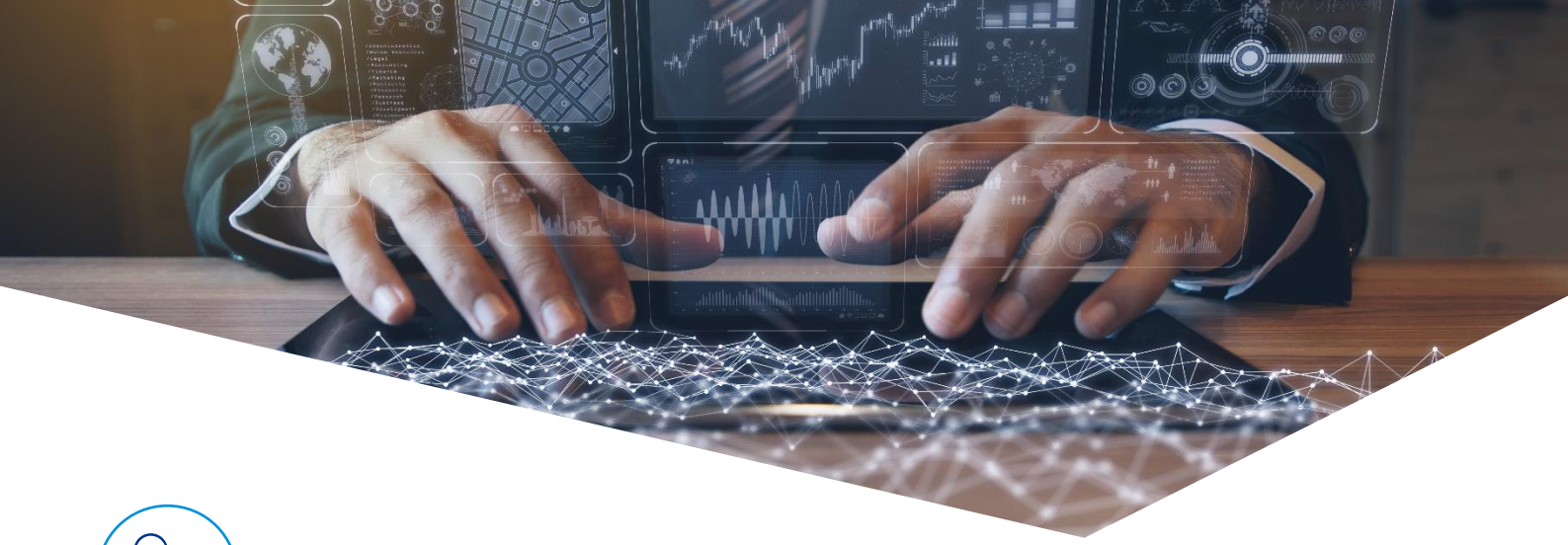
KPMG' Fraud Barometer annual report for 2019[1] identified trends in the types of fraud that have dominated court cases, as well as the latest fraud patterns affecting the economy. These insights help businesses remain vigilant to new threats and respond to fraud risks in an appropriate and proactive manner. The 2019 report found that the average value of each fraud case over the past three years has reached USD 1.8 million.

More recently, KPMG's Covid-19 Fraud Survey[2] revealed that 42% of respondents believed their capability to investigate fraud and corruption was inhibited by the current pandemic. Operating in a Covid-19 environment has highlighted multiple challenges for businesses to overcome when conducting investigations.

In this shifting global financial landscape, where organizations are shrinking, volumes of digital payments are increasing and outflows are being processed in seconds, fraudsters are likely to find creative new ways to steal from businesses and their clients.

Consequently, it is more important than ever for businesses to be able to combat internal and external threats and build their response and resources allocation to reduce these risks. One way to counter threats is to be fully aware of the risks. KPMG Lower Gulf routinely monitors active frauds, and, in the following pages, we review the current situation.

[1] https://home.kpmg/uk/en/home/insights/2015/12/fraud-barometer.html
[2] https://home.kpmg/au/en/home/insights/2020/04/coronavirus-Covid-19-fraud-survey.html



Cybercrime to double

Multiple intelligence sources have confirmed that cybercriminals are taking advantage of the Covid-19 pandemic by defrauding businesses and individuals of capital or thieving personal identifiable information. One way is by distributing real-time, detailed statistics about infection rates tied to the Covid-19 pandemic. When successful, this enables the criminal to steal credentials such as usernames, passwords, credit card numbers and other sensitive information that is stored in the user's browser. Users believe that the statistics, usually in the form of a map, are genuine and click on it. In doing so, it allows malware to compromise the computer.

The threat of cybercrime is not focused on the one scam – ransomware, business email compromise and phishing attacks are on the rise across all sectors of the economy. According to Cybersecurity Ventures' Official Cybercrime Report, cybercrime is poised to double during the Covid-19 pandemic. The global cost of cybercrime is forecast to be USD 6 trillion annually by 2021, up from USD 3 trillion in 2015. The rise denotes one of the largest transfers of economic capital in history.

The criminal fraternity prospers in a disaster. Uncertainty and anxiety offer a perfect storm for cybercriminals. During the Covid-19 crisis, businesses and individuals are concerned about the invisible threat perpetrated by anonymous people. They are also circumnavigating constant change and the unpredictability of the situation. These anonymous criminals will also use the shift to remote work in order to target businesses, which may not have full-fledged work-from-home procedures in place.

Cybercriminals are targeting people looking to purchase medical supplies online, sending emails offering fake medical support and scamming people who may be vulnerable or increasingly homebased. These frauds and cybercrimes try to bait individuals with offers that look too good to be true, such as high-return investments and healthcare opportunities, or make appeals seeking support for bogus charities or causes.

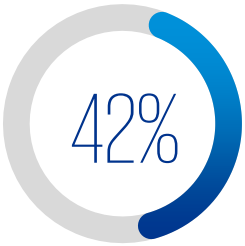
To date, these include online shopping scams where people have ordered protective face masks, hand sanitizer, and other goods, which have never arrived, and a number of cases where fake testing kits have been offered for sale.

When an instance of cybercrime, fraud, corruption or serious misconduct is identified, it is essential that businesses undertake an investigation to determine whether the facts can be substantiated. Investigations are shown to deter or disrupt other potential inappropriate actions and assist in setting standards during indeterminate times.

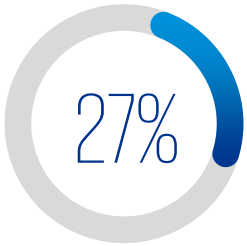
[3] https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/

Statistics during Covid-19[4]

Fraud and corruption risk is increasing dramatically but controls are decreasing:

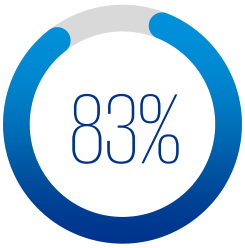


of executives said that their ability to conduct investigations into fraud and corruption was inhibited by COVID-19

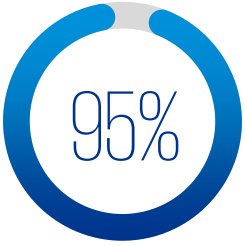


of executives said that their organisations have had to delay their fraud and corruption prevention programs due to the impacts of COVID-19

COVID-19 is delivering as increases fraud and corruption risk:

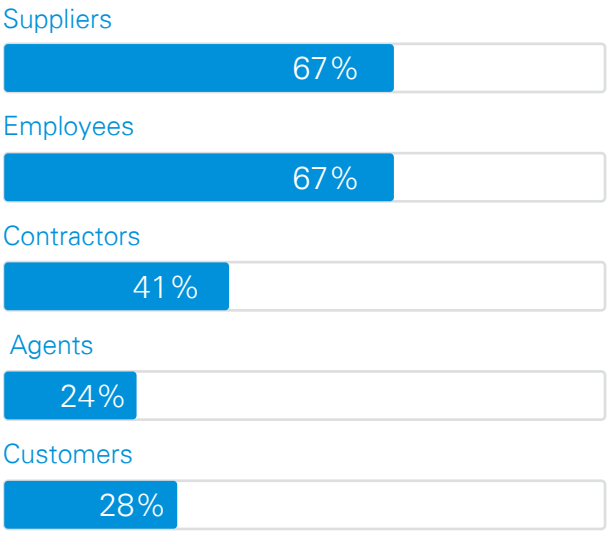


of executives believed their organisation was vulnerable to fraud taking place in this new working environment.



of executives believe that cyber-enabled fraud and corruption will rise during COVID-19

Biggest threat for organisations:



[4] https://assets.kpmg/content/dam/kpmg/au/pdf/2020/Covid-19-fraud-survey-2020-infographic.pdf

Be proactive

Businesses are not immune to the devastating consequences of fraud and corruption, and during this current pandemic they are under threat from a host of risks, including fraud and cybercrime. The latter include risks which are rapidly growing. These may affect organizations across a broad range of industries, in both the public and private sectors.

In order to evaluate the importance, quantity or quality of controls required, management must first identify these risks through a detailed evaluation process to define both numerical metrics and quality.

Investigative procedures and processes need to be put in place or reviewed if already in existence. These will establish a basic structure of how, why and by whom computer-based crime and dishonest actions should be handled. This process should be supported by clear internal and external reporting lines. Computer insurance policies may also need revisiting to make sure coverage for computer-based crimes is adequate.

The pandemic is likely to change the way corporations handle their commercials. To that end, businesses should not lose sight of the possible follow-on dangers that this pandemic presents – especially increased reliance on managing money and the supporting electronic environment needed to operate. Managing cash flows has become a vital part of a business' overall pandemic risk assessment and action planning in the short term. Even for businesses that have not thus far been badly affected, but have fears about the effect of the pandemic, need to actively assess their cash money management requirements, develop appropriate actions under various situations, and assess potential risks in and to their client base and provider network.

Both aspects are essential to appropriate risk evaluations and implementing the correct security protocols and controls.

Once all risks have been identified, adequate controls to detect and prevent fraud or cybercrime should be implemented.

The future

A massive increase in the number of people working remotely means that more people will be vulnerable to cybercrimes, including fraud, where criminals will try and convince individuals to provide access to their computer or divulge login details and passwords. Many are also anticipating a glut of phishing scams or calls claiming to be from government departments offering grants, tax rebates, or compensation.

We have also seen, and will continue to see, more fake websites that seek to take advantage of supply shortages for essential goods. Rather than providing fake products, these websites simply pocket the money before disappearing. To date, such scams have included but are not limited to, online shops which may use the names of legitimate retailers and bulk consignment of protective face masks that are never delivered.

Non-profit organizations will continue to be exposed to financial and reputational risks. In March of this year, criminals using a phishing attack impersonated the World Health Organization (WHO) to steal Bitcoin Covid-19 donations originally collected for the WHO's Covid-19 Solidarity Response Fund.

There is often also an increased risk of bribery when people are placed in difficult situations. This is likely to be of concern for businesses with overseas operations, but domestic issues should not be discounted. Similarly, staff working in an overseas subsidiary can face pressure to make enabling payments or bribes to release imported items from customs or to continue to function during a lockdown. For example, the Anti-Corruption Resource Centre found that during the 2014 Ebola crisis, residents in Liberia were commonly bribing soldiers and police officers to escape quarantine[5] .

Notably, some business that normally consider themselves to have a low corruption risk may come into increasing contact with foreign government officials. Bribing government officials is specifically targeted by the United States Foreign and Corrupt Practice Act.

Investigation planning and strategy

Organizations need an investigation plan and strategy that is flexible throughout the lifecycle of the investigation. In addition, investigation plans now need to be reassessed with Covid-19 in mind. They need to consider whether they can make use of electronic sources of information and evidence which may be able to be accessed remotely. Electronic sources of information could include but would not be limited to laptops, workstations, file servers, document management systems, financial systems and server mailboxes. Due to Covid-19, it may not be possible to access these to obtain intelligence and evidence.

When initiating investigations, determine whether physical attendance is vital and evaluate Covid-19 risks at the workplace, travel and other locations, prior to being present to lessen risk for all parties. During this crisis, businesses should be more vigilant and act with extreme caution, as many fraudsters and cybercriminals are attempting take advantage of the sense of urgency generated by Covid-19.

[5] https://www.cmi.no/publications/file/5522-ebola-and-corruption.pdf

KPMG Lower Gulf's services

How KPMG LG can assist

KPMG LG's fraud investigation services team works closely with clients to understand an investigation's objectives and coordinate our approach to utilize the appropriate resources. Through detailed enquiries and examinations, including the use of leading data analytic techniques, our professionals establish truths, evaluate implications, identify appropriate remedial actions, and submit restatements if necessary and communicate with regulators or outside auditors if needed.

Our fraud investigation team includes:

— Forensic accountants, investigative and technology professionals

— A team which has interacted closely with the law enforcement authorities across the GCC

— Banking, finance, construction, real estate and family-owned conglomerates experience

— Accounting, investigation, project management and forensic technology experience

— Multilingual support, including native Arabic speakers

For leading businesses, cybercrimes may pose a direct threat to the safety of their people, data and brand. We can assist organizations to effectively and efficiently respond to such events, after which it may be necessary to collect incident related data, secure evidence and support legal and law enforcement inquiries. We conduct cybercrime investigations to determine the cause of incidents and support preventative measures to detect future threats.

Our cybercrime investigation team provides:

— Detection and assessment of the nature and impact of the cybercrime

— Cybercrime response coordination and communication protocols

— Entrance of data and documents into the chain of custody and analysis

— Assistance with communicating the cybercrime to law enforcement agencies

— Guidance and ad-hoc advice on implementation of additional computer security controls to contain the incident

Our approach to wrongdoings

— Responding to potential wrongdoing requires leveraging many fact-finding disciplines, which are the

— foundation of our services, in order to support investigations. The primary objective

— is to identify the problem(s) and take the appropriate measures to address it, while taking steps to

— retain the reliability and integrity of the evidence.

Client gain

— KPMG LG's incident response services provide access to professionals who already know their

— environment in times of crisis, shortening the learning curve and allowing our clients to reduce

— the time needed to address an incident. This enables our clients to 'get back to normal' faster.

Our aim

A client's experience during a fraud or cybercrime, regardless of its severity, is not a comfortable situation. As a part of our engagement process, our teams actively solicit feedback throughout the process. This is reviewed at all levels, in an effort to manage expectations, improve satisfaction and build long-standing relationships.

Our goal is to make it as easy as possible for our clients to call on us in the event of an investigation.

Contact us

Nicholas Cameron
Partner, Head of Forensics
Forensic Technology
KPMG Lower Gulf Limited
e: nicholascameron@kpmg.com
t: +971 4 424 8992

Simon Crowther
Partner
Forensic Technology
KPMG Lower Gulf Limited
e: scrowther1@kpmg.com
t: +971 4 330 1515

Alan Zhang
Associate Director
Forensic Technology
KPMG Lower Gulf Limited
e: azhang68@kpmg.com
t: +971 4 405 0935

www.kpmg.com/ae
www.kpmg.com/om

Follow us on:

@kpmg_lowergulf

Publication name: KPMG LIBOR transition framework Publication number: 2932

Publication date: October 2021