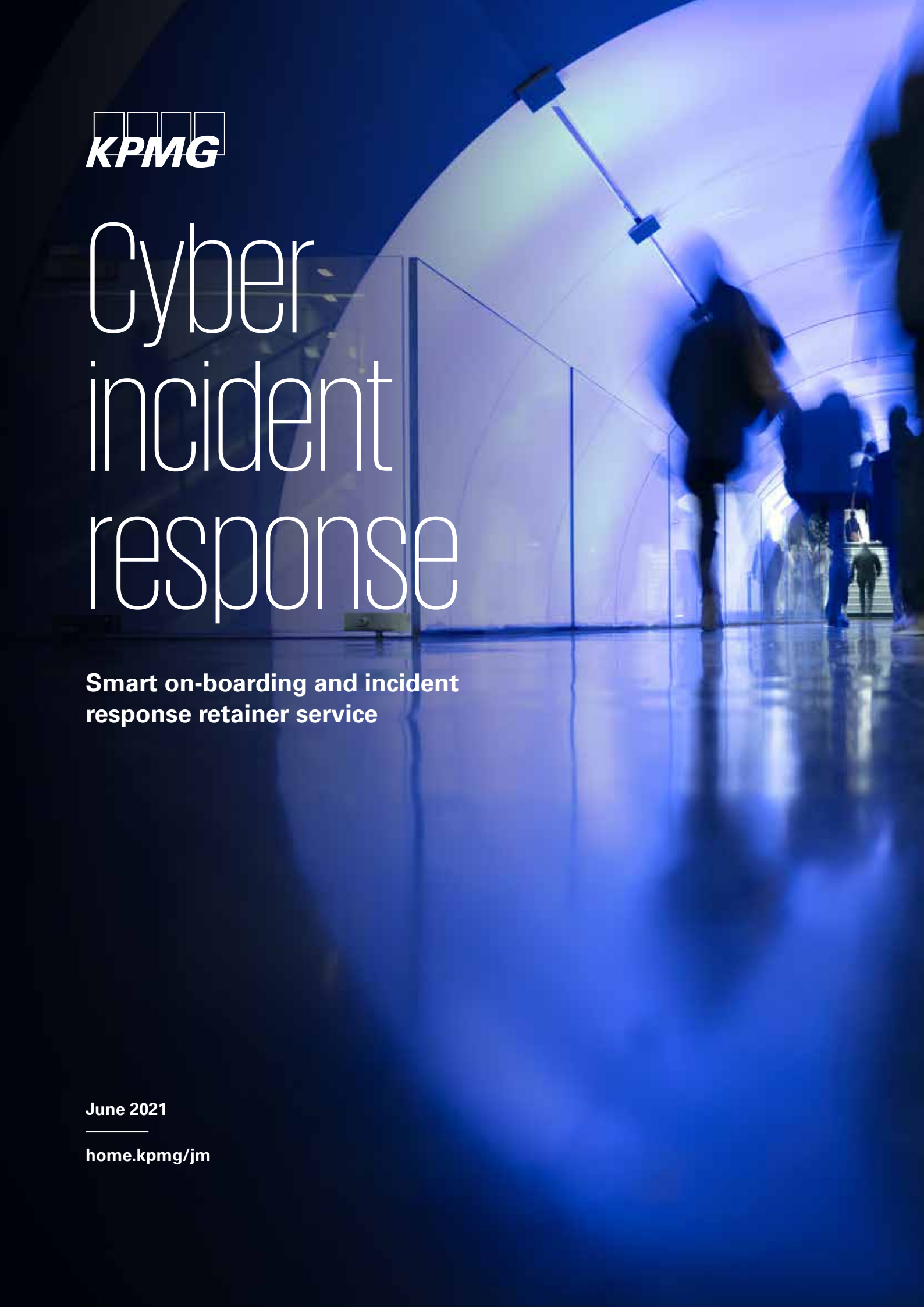


KPMG

Cyber incident response

Smart on-boarding and incident response retainer service

June 2021

home.kpmg/jm

Why you need incident response?

Cyber security breaches are on the rise as we are now living in a world that is heavily reliant upon technology and internet based communication. Whether it is a low-level security attack or a highly sophisticated and targeted one, no organisation is immune. With the intelligence and skills of cyber attackers moving at a pace as fast as technology is advancing, a breach is inevitable regardless of industry, location or organisation size. A highly skilled and persistent attacker is capable of penetrating the security defences of any organisation and compromising the assets, which can bring business operations to a standstill. Not only can this result in severe financial and reputational damage, it can also cause the loss of customer trust and confidence, especially if the breach involves sensitive data. Below are few questions that CEOs and senior executives should be asking:

Is my organisation prepared well enough to deal with a cyber attack?

How do I know if I am being attacked by digital, organised crime groups?

Is it possible to recover from internet worms or malware that take over workstations and systems?

How can I take more control so my organisation can operate with confidence?

Effective cyber response

In the event of a cyber attack, KPMG understands that containing the attack is the first priority, as well as helping to answer questions such as what needs to be done to minimize the impact, what has been lost, and is there any financial or data loss?

At KPMG, we provide a multi-disciplinary approach and effective global coordination, focusing not only on the technical aspects, but also assisting you to get back to normal operations as soon as possible. Our team will be on hand to address all your requirements when a breach occurs. You can avail of an incident response service that provides:

- Professional management of cyber attacks, with practical assistance and advice on containment, mitigation and restoration of normal business operations
- An independent view of the risks your business faces based on your cyber attack detection capabilities and procedures
- Confidence in the state of your cyber response procedures and controls, and the technologies which underpin them
- A network of member firms spanning 146 countries and territories. We have a truly global cyber response capability, so we can quickly investigate geographically spread networks and systems.

You are in safe hands

Business-focused approach/sector specific understanding

To keep your business running after an incident, you will require the return of essential services quickly. That's why at KPMG we focus on your business-critical processes first. Our response will cover the full breadth- from datacenter to boardroom and client customer, so you can return to business as usual as soon as possible.

A stock brokerage customer suffered a devastating targeted ransomware attack. After initial investigation, KPMG's team advised that the best course of action was to rebuild the central Active Directory systems because the losses due to business disruption was much higher if not brought up. The investigation effort was re-prioritized to the recovery of business via manual operations then to determine the root cause analysis.

- Reduce commercial impact
- Knowledge of relevant business risks
- Get back to business as usual quickly

Global coverage

KPMG's cybersecurity consulting practice is one of the largest worldwide, with the KPMG network of member firms operating in every corner of the globe. This combined with our 24/7 cyber incident response support services means that no matter when or where an incident occurs, you will have industry experts on hand, as soon as possible with local expertise.

A major financial services client suffered a data loss incident with assets spread across its subsidiary in India, Belgium, UK etc. KPMG were able to provide on-site presence within 24h and around the clock support from India and global offices providing consistency in delivery.

- Global access to skills
- Experts on the ground at short notice
- Local expertise, globally

Technical prowess

As a multi-disciplinary advisory firm, we provide the highest quality of service thanks to our team's breadth across all areas of cyber security and forensic procedures. We have custom developed tools, scripts and carefully selected, licensed security products and labs to securely investigate, retain artefacts and analyse.

During one of the business email compromise incidents, KPMG reviewed more than 100 GB of O365 logs using advanced analytics tools to provide rapid results and threat intelligence via KPMG proprietary platforms. It facilitated faster business recovery and definite knowledge of data leakage resulting in reduced claims.

- Technically skilled and certified team members
- Specialised forensic and incident response labs

Practice makes perfect

In 2020 itself our India team alone responded to more than 35 cyber incident cases, spanning the full spectrum of attack types – be it dealing with phishing e-mail fraud, ransomware attack to advanced persistent threats.

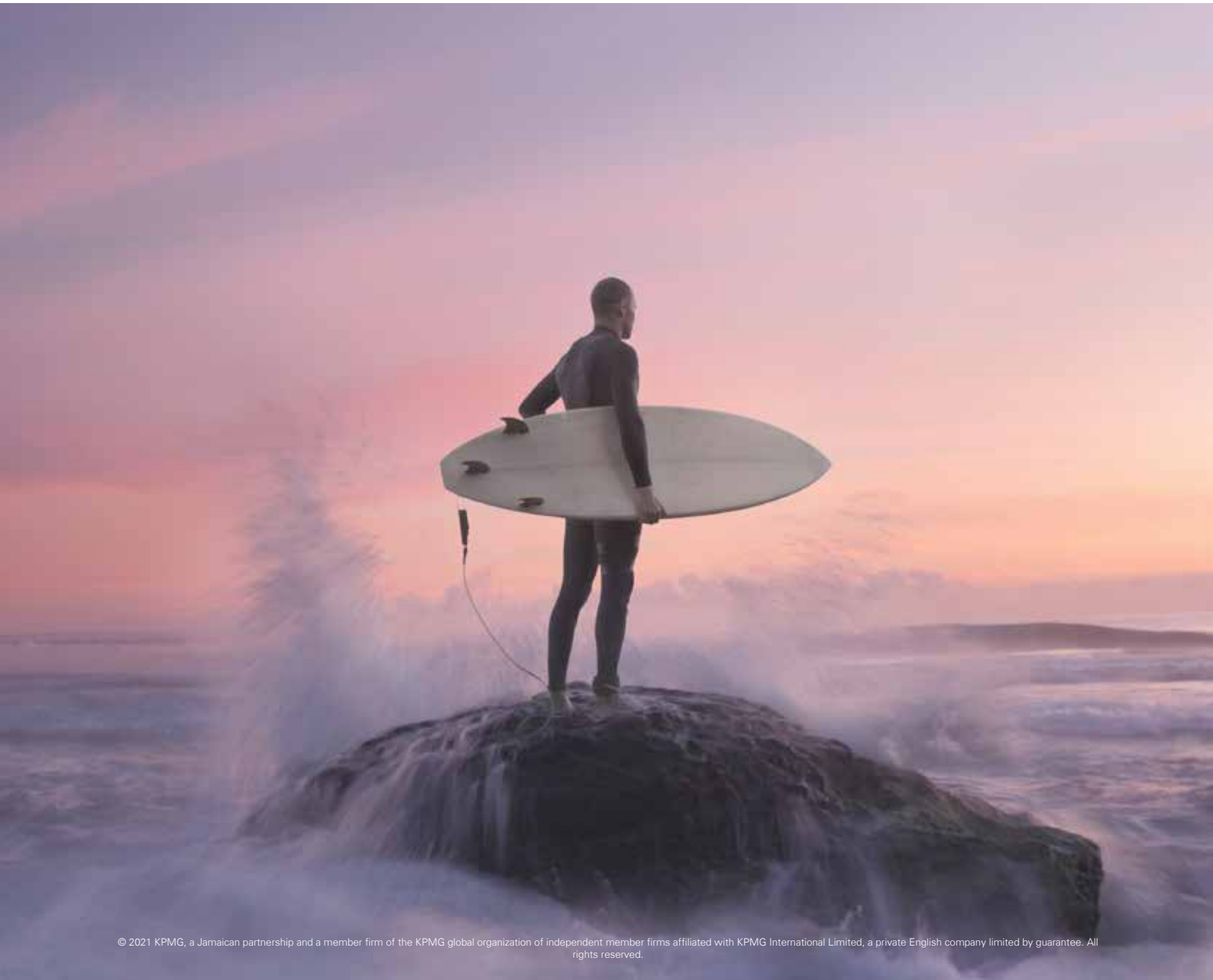
Our clients have provided us with positive feedback and have invited us to do follow-on work to investigate other incidents and also build IT systems resilient to advanced known and unknown cyber attacks.

- Experienced professionals
- Positive client feedback

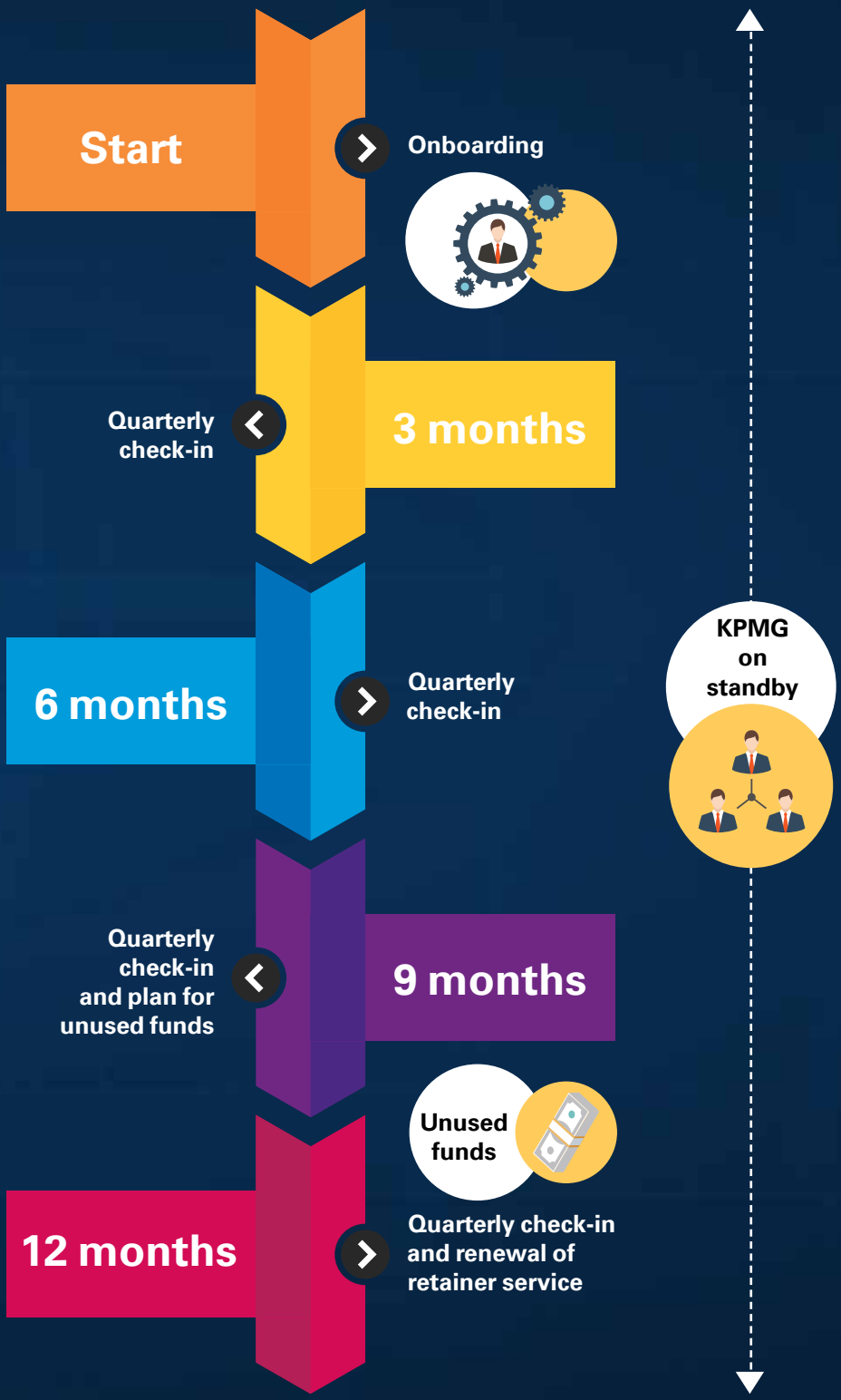
Not only incident response

While we take pride in our people's extensive technical ability, we go beyond this: you will benefit from expertise from other incident areas such as crisis management, communications, forensics and technology advisory. With KPMG you will effectively get a wide-ranging service, ready-made solution for various cyber incident and advanced threat intelligence to immediately contain the situation.

- Breadth of cyber knowledge
- Combination of technical and non-technical skills



The IR retainer process



Onboarding

- We meet with you to discuss Incident Response requirements
- We agree the best option, based on your requirements
- You sign the incident response (IR) retainer contract
- A workshop is held with Silver, Gold and Platinum clients to gain an understanding of their infrastructure systems and current risks

Cyber IR team on standby

- Incident occurs – you contact KPMG over agreed channels such as hotline number, mobile, email etc
- Incident triage and first response call. We attend site if needed
- Quarterly check-ins to review the general threat landscape and your overall cyber needs

Unused funds

- Silver, Gold & Platinum clients can put unused retainer fees towards other cyber security services
- Discussion of how to use any unused retainer fees at the nine- month quarterly check-in

Support levels

We offer different support levels to ensure we meet your incident response requirements.

	Bronze	Silver	Gold	Platinum
Onboarding and security workshop(a):	Basic onboarding	Standard security workshop	In-depth security workshop	Bespoke
24/7 incident notification hotline	✓	✓	✓	✓
First response(b):	4 business hours	8 hours	4 hours	4 hours
Coverage and on-site response within SLA	Next business day, single India agreed location (Delhi/ Mumbai/Pune/ Chennai & Bangalore)	Next business day at any3 pre-agreed India locations from Delhi/Mumbai/Pune/ Chennai/Bangalore	24 hours at any 3 pre-agreed India locations from Delhi/ Mumbai/Pune/ Chennai/Bangalore & anywhere globally	Bespoke (anywhere in India & globally)
Service:	Time & Materials	Prepaid (80 hours) + Time & Materials	Prepaid (210 hours) + Time & Materials	Bespoke
Discount on KPMG incident response rate card	None	None	Standard discount(d)	Bespoke
Use the remaining retainer on other cyber security services	✗	✓	✓	✓

Note:

a. Please see the "What's in the onboarding and workshop?" page 7

b. Time from the initial notification by client (you) until a KPMG incident triage call with a specialist incident manager. Business hours defined as 9am to 6pm Mondays to Fridays excluding public holidays.

c. SLA time from completion of the triage call. KPMG will perform commercially reasonable endeavors to provide remote assistance sooner, but within the on-site service level agreement window. Location will be agreed at the contracting time.

d. To be determined at time of contract agreement.

What's in the onboarding and workshop?

Why onboarding and workshop are important?

It is a good idea to be familiar with each other before an incident happens. This is why the on-boarding and workshops are very important – the better we know each other, the more efficient we will be. During basic we will discuss at a high level your security architecture and processes and agree on general ways of working.

During workshops, together we will explore common incident response situations to identify how to best respond to those and if there are any issues that can hinder.

The type of onboarding and workshop depends on service level you have selected:

1 Basic onboarding

- One hour meeting at KPMG in India's offices or a conference call involving you and the appropriate business stakeholders
- Exchange of key contact information
- Network, system and application environment overview
- High level security recommendations gathered from the onboarding meeting.

2 Standard security workshop (single day)

- Three hour workshop at your chosen location including yourselves and members of ncident response team
- Exchange of key contact information
- One standard incident scenario walkthrough (table-top exercise) testing your current crisis management processes.
- Review of current security documentation including current incident response plan, communications plan and past cyber incident reports
- Security control recommendations based upon the knowledge we've gathered from the workshop on your current incident response vulnerabilities.

3 In-depth security workshop (single day)

- One day detailed security workshop at your chosen location involving your company stakeholders and our incident response team
- Exchange of key contact information
- Detailed walkthrough of three cyber incident table-top exercises in technical detail, where we observe your current process and suggest recommendations to improve the process
- Review of current security documentation including current incident response plan, communications plan and past cyber incident reports
- Security control recommendations based upon the knowledge we have gathered from the workshop on your current incident response vulnerabilities.

Related services for unused funds

Table top exercise

A discussion based simulation exercise for emergency situations helping to refine:

- Crisis management processes
- Incident response readiness
- Crisis communications
- Gaps in current proceedings

Vulnerability assessment and penetration testing

Assessment of security weaknesses and vulnerability on environment varying from:

- Application testing
- Network testing
- Infrastructure examinations
- Configuration assessment

Red teaming

A collaborative cyber exercise engaging red and blue teams for a live simulated attack that:

- Covers technical and non-technical spheres
- Splits attack and defence between two technical teams
- Aids preparation for an attack
- Helps to determine security posture

Threat hunting

A proactive defence activity focused on:

- Network discovery
- Malware detection
- Attacker analysis
- Persistent risk investigation

Cyber emergency?

Please contact our 24*7 Cyber Response hotline +91 9176-471-471

KPMG in Jamaica contacts:

Raymond Campbell
Partner
Head of Advisory
T: +1 876 922 6640
E: raymondcampbell@kpmg.com.jm

Ravi Sankar
Principal
Cyber Security Services
T: +1 876 922 6640
E: rsankar@kpmg.com.jm

Anish Mitra
Associate Director
Cyber Security
E: anishmitra@kpmg.com

Asmit Raj
Assistant Manager
IT Advisory
E: asmitraj1@kpmg.com

home.kpmg/jm

KPMG in Jamaica Cyber Team works with organisations to help prevent, detect and respond to cyber threats. We can help your organisation be cyber resilient in the face of challenging conditions. Have a cyber emergency? Contact us : firmmail@kpmg.com.jm

Follow us on: