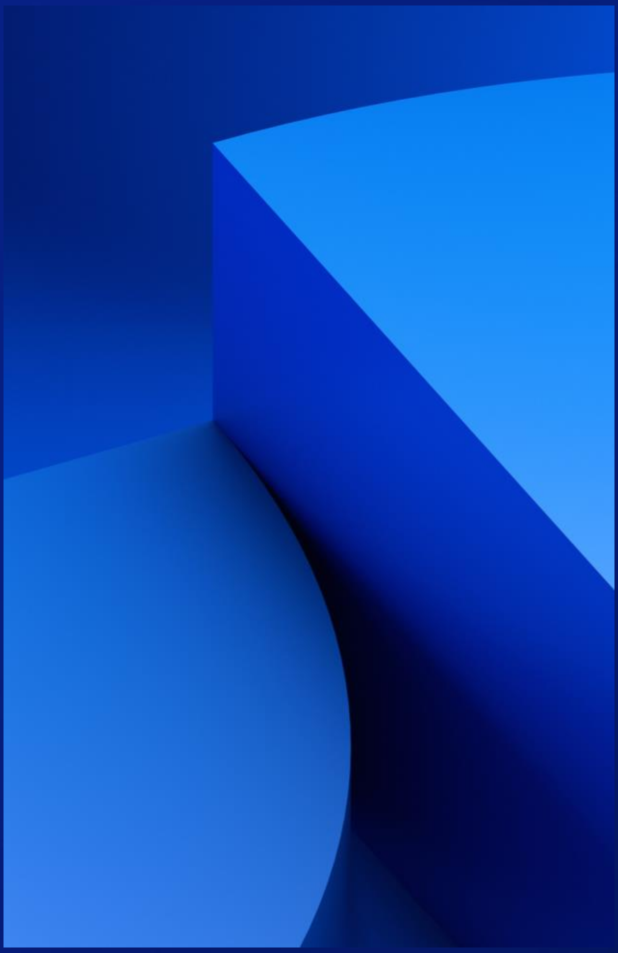
KPMG

Cyber Security Forensic Investigations



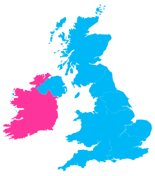
A KPMG Service for G-Cloud 14

May 2024
kpmg.co.uk

KPMG – About us

Our UK Cyber team

We've worked with countless organisations across multiple sectors, including financial services, life sciences, healthcare, government, telecommunications, energy and natural resources, and legal services. Our clients range in sizes, span across geographies and industries and are subjects to various regulatory requirements and obligations.



330+ professionals

15 office locations

Part of a global team of 6200+ individuals

Our services

UK Cyber operates across 8 different service lines, catering to a wide range of governance and technical needs.

- Cyber strategy
- Cyber risk
- Cyber and enterprise resilience
- Privacy compliance
- Cyber tech trans-formation
- Identity and access management
- Cyber defence services
- Cyber incident response

Our Cyber team is complemented by our Connected Technology team.

We have access to a 2000-strong team of client-facing technologists combined with alliance partners, with a diverse range of skills and experience. This enables us to bring to our clients the most suitable resources, expertise and insights when needed.

We apply a data and technology driven approach to drive change through our digital transformation services.

Cyber Investigations Service

Service Description:

When an inevitable security incident or data breach occurs, rapid and effective incident response is critical. KPMG's Cyber Forensic Investigations team is on standby to 1) provide incident triage during the critical first hours; and 2) to investigate the attack, determine impact and remediate to minimise future cyber risks.

Key Services

- End to end Cyber Forensic Investigation Services:
- Business Email Compromise Ransomware
- Network intrusion Intellectual property (IP) theft Botnets and malicious code
- Spear phishing and account take overs Court-appointed neutral expert
- Expert testimony
- On-demand cyber response
- Remote, Stealth and Cloud Collections
- Secure processing, hosting and review environment
- Secure Forensic Laboratory & Evidence Store
- Experienced Evidence Reviewers
- Deep bench of Cyber, eDiscovery, compliance, investigation and legal and expert witness specialists (oral & written testimony) available

What are the benefits of KPMG Cyber Security Forensic Investigations service?

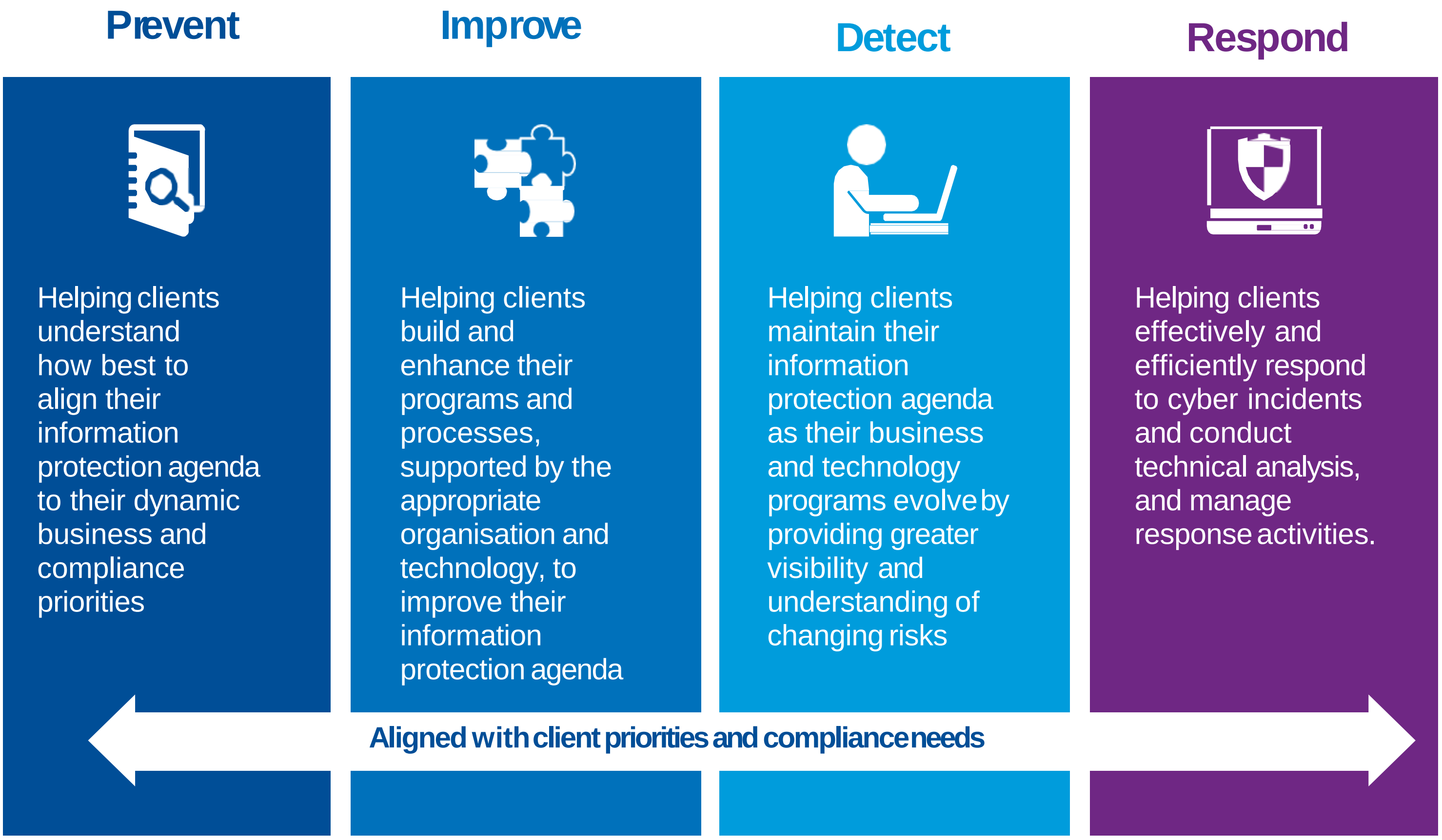
- Identify, mitigate & respond to IP theft and data loss
- Experienced incident managers
- Technical incident containment, business co- ordination and operations management
- Identify and remediate against people, process or security vulnerabilities
- Rigorous risk management during incident handling
- Security Cleared teams
- Delivers projects on time and within budget
- Provides market leading speed to insight giving your investigation team(s) an edge
- Our clients receive consistently high quality support from our global team of specialists
- Typically realises between 5
- – 15% productivity and cost avoidance savings
- Allows you greater focus on high-value activities of strategic importance

Our service features

- Over 15 years experience in cyber investigation and incident response
- Respond to critical cyber incidents across five continents
- Maintain a focus on minimising adverse business impact
- Methodology developed in line with NIST and SANS best practice
- Utilise forensic techniques to capture and analyse data
- Malware / payload identification & analysis
- Root cause and gap-analysis processes
- Accreditations include: CISSP, CISA, GCFR, GCFA, CREST, ACFS, EnCE and ACFE
- High precision forensic approach covering the entire investigation life cycle
- Real-time reporting and accurate MI provide a complete view on every matter
- Extensive suite of custom tools and scripts for automation

Our Approach

A holistic approach to cybersecurity is more effective and more realistic than simply building digital walls. Beginning with the individual goals and operations of our client, we build a customised cyber investigation strategy informed by the latest threat intelligence and leading practices that stays on top of key drivers impacting cyber: External threats, change in the way business is conducted, rapid technology change, regulatory compliance, threat awareness.



Prevent

Helping clients understand how best to align their information protection agenda to their dynamic business and compliance priorities

Improve

Helping clients build and enhance their programs and processes, supported by the appropriate organisation and technology, to improve their information protection agenda

Detect

Helping clients maintain their information protection agenda as their business and technology programs evolve by providing greater visibility and understanding of changing risks

Respond

Helping clients effectively and efficiently respond to cyber incidents and conduct technical analysis, and manage response activities.

Aligned with client priorities and compliance needs

Why KPMG: Efficient Execution

KPMG Evidence ManagementSystem

KPMG utilises industry-leading collection, preservation, and analysis methods for every situation. Evidence acquisitions are handled in accordance with KPMG's digital evidence handling protocols, which include chain-of-custody procedures, authenticityofevidence, encryption, andtracking of physical/logicalevidence.

KPMG understands the importance of simplifying evidence management for large and diverse data sets, staying in control of budgets, and maintaining project timelines, all while providinga defensible audit trail to avoid adverse rulings levied incourt.

KPMGbelieves that evidencetracking should be integrated into the incidentresponse processin order to help ensure accuracy, efficiency, and awarenessof the data throughout the variousphasesofa project.

Tool agnostic

KPMG is tool agnostic and vendor neutral. KPMG is entirely driven by our experience and our confidence in our ability to provide value-added assistance using tools including but not limited to the below.

Our Approach

Network forensics

- — Fidelis Cybersecurity™
- — RSA NetWitness™
- — Suricata™
- — Wireshark™

Log data

- — ArcSight™
- — Elasticsearch, Logstash,Kibana™
- — LogRhythm™
- — Plaso™
- — QRadar™
- — Splunk™

Endpoint detection& response

- — Carbon Black™
- — Crowdstrike Falcon™
- — Cylance Optics™
- — FireEye HX™
- — Google Rapid Response™
- — Microsoft DefenderATP™
- — Tanium™
- — Sysmon™

Evidence
Management

KPMG's Evidence Management System

Host forensics

- — Encase™
- — AccessData Forensic™
- — F-ResponseEnterprise™
- — NUIX™
- — Axiom Forensicssuite™
- — TZworks™

Memory forensics

- — Volatility Framework™
- — Rekall™

Malware analysis

- — CuckooSandbox™
- — FalconSandbox™
- — Ghidra™
- — IDA Pro™
- — REMnux™
- — ThreatAnalyzer™

Case Studies

Large hospital—ransomware

For a large affiliated hospital network, KPMG led the recovery following a ransomware attack that resulted in complete loss of access to its electronic health records database—to the point which impacted multiple hospitals from servicing patients. After another IR vendor was unsuccessful, KPMG reverse-engineered the ransomware to determine how it encrypted the data and developed an innovative approach to fully recover their data and help restore operations—an effort most would have considered impossible. KPMG was then further engaged to assist with the structured data sensitive data review to assist with notification obligations.

Health Organisation—Digital evidence collection

As part of ongoing litigation and anticipation of a government investigation, KPMG was retained by one of the largest health organisations to coordinate the collection of digital media and hard copy documents from an active research facility. To meet the client's request to minimize disruption to the research facility and quickly complete the collections, KPMG assembled a team of 25 forensic professionals to collect over 130 TB of electronically stored information from 3,900 Cyber media devices and 500 boxes of hard copy documents in 108 hours.

The media collected was part of the hospital's infrastructure and bring your own device (BYOD) program with varying specifications and configurations, including Macintosh (MAC), Windows, and Linux systems. KPMG had to work with outside counsel, in-house counsel, IT professionals and the medical staff to develop the most effective way to collect the data with minimal operational disruption to the ongoing research. KPMG followed its standard operating procedures to help ensure forensic imaging and document the transfer of chain of custody per leading industry practices. KPMG also developed a customized methodology to meet the client's expectations and successfully collected data from the individual custodians, lab workstations, medical equipment, external media, network shares, personal shares, e-mail servers, and hard copy documents leveraging the industry leading and proprietary forensic tools.

Why KPMG

Implementation Plan

Timescales are driven by a number of variables including the scale and complexity of each Customer's scope together with quality of data and availability of resources.
We would agree the implementation plan, resource requirements and project milestones as part of the process of procuring our services.

Onboarding and offboarding support:

The range of on boarding activity required for clients adopting a KPMG Powered service would be agreed as part of the procurement of the service. As part of the service we build and agree a plan covering all relevant activities, planned times, durations, responsibilities, accountabilities and outputs.
Typical elements comprise:

Onboarding:

- Development of the project charter, if needed, and associated project guiding principles
- Assistance to develop / articulate the case for change
- Change management and communications strategy to aid who needs to be communicated with, how and when in relation to the changes the project is planning to implement

Onboarding and offboarding support:

Onboarding…continued

- Provision of orientation sessions in our methodologies and assets, for the program, including workshop execution
- Engagement with client teams to understand the 'as is', to take into account in change impact assessment during workshops
- Definition of collective roles and responsibilities including that for outputs
- Execution of a Project kick off event and associated materials to formally launch the project and to aid new joiners in orientation

Offboarding:

Each implementation has a post go live ("Evolve phase") in which KPMG will provide post go live support working with each Clients Business as Usual (BAU) team to fully transition on going service delivery to the Clients' BAU support team according to the agreed plan.

Pricing overview, including volume discounts or data extraction costs

Consulting Prices are as per the G Cloud 14 rate structure.

Projects can be charged using either Fixed Price and Time and Materials approaches, according to the situation, and can be delivered on site and/or remotely.

Volume discounts would be considered on a case by case basis.

Service constraints like maintenance windows or the level of customisation allowed

Maintenance:

This is not applicable for this service.

Customisation:

This is not applicable for this service.

Service Details

Service levels like performance, availability and support hours

This is not relevant as this service does not involve a standard software solution.

How you'll repay or compensate buyers if you do not meet service levels

Any service credit regime for Cloud software vendors are per the relevant authority's direct agreement with that vendor.

KPMG can discuss specific service credit requirements on a case by case basis.

The ordering and invoicing process

The ordering process for G Cloud services is laid out in the 'G Cloud buyers' guide on the www.gov.uk website.

Invoicing arrangements will be as per the agreed G Cloud order form and will vary from engagement to engagement.

How buyers or suppliers can terminate a contract:

Our terms provide for a range of scenarios where both Buyer and Supplier are able to terminate contracts, to defined notice periods, for:

- convenience,
- failure to remedy a material breach and
- insolvency.

In addition, Supplier has the right to terminate if: (a) circumstances arise or have arisen which KPMG reasonably considers does or may impair its impartiality, objectivity or independence in respect of the provision of the Services; or (b) for legal, regulatory or other justified ethical reasons.

After sales support

KPMG can provide a range of services to assist users of this service post implementation ranging from managed services, staff secondment, impact assessments on the implementation due to cloud software vendor upgrade / major patches and associated regression testing.

Any technical requirements

Each Cloud software vendor provides details directly of their supported web browsers and personal computer and related requirements. These are not onerous and typically do not present an issue for the majority of organisations.

KPMG also uses a range of collaboration tools, as appropriate, to assist in the delivery of the Services. Microsoft Office 365 & Teams are used by all colleagues within the firm, with other tools such as Jira and Confluence being used if required for the project. KPMG is also able to use other collaboration tools if used on client provided laptops.

Project team members will need to be provided with a software VPN and virtual machine or client laptop.

kpmg.com/uk

This proposal is made by KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent firms affiliated with KPMG International Limited (“KPMG International”), a private English company limited by guarantee. The proposals set out in this document do not constitute an offer capable of acceptance. They are in all respects subject to satisfactory completion of KPMG's procedures to evaluate prospective clients and engagements, including independence and conflict checking procedures and, the negotiation, agreement, and signing of a specific engagement letter or contract. KPMG International and its related entities provide no services to clients. No member firm has any authority to obligate or bind KPMG International, any of its related entities or any other member firm vis-à-vis third parties, nor does KPMG International or any of its related entities have any such authority to obligate or bind any member firm.

Document classification: KPMG Public