Cyber Attacks
A board level risk

Cyber Response Services

KPMG Forensic

Everyone is affected by cyberattacks in our fast-changing, hyperconnected digital world. With more funds at hand, attackers are employing modern techniques such as Machine Learning and Artificial Intelligence to find novel ways to attack organisations. Keeping attackers at bay is becoming increasingly difficult.

Business resilience

It is evident that attackers will maintain an edge over your defenses with the recent increase in zero-day vulnerabilities, so it is essential that you have a resilient approach to coping with cyber attacks, especially events that disrupt business services and force a company wide response.

Global economic and political situation

While the global pandemic pushed your capabilities for how you could use technology, cybercriminals and state sponsored attackers have also increased their activities, raising the associated risks in the cyber space. Due to the value you place on technology, cyber criminals and state-sponsored attackers are increasingly targeting systems.

Ransomware attacks

Computer malware can disrupt or shut down a company's operations when it encrypts critical business systems. Ransom demands can range from hundreds of thousands to millions of Rands.

Internal Threat

The breach of trust by employees and contractors can compromise an organisation's competitive advantage. Every year,
courts evaluate evidence of employee misconduct and theft of intellectual property. Companies require support from forensic investigators to address these cases.

In the KPMG Global CEO outlook survey 2022, cyber breaches were identified as the top concern of CEOs. As part of their digital transformation programs, CEOs are looking for stronger partnerships to maintain cyber resilience. With our incident response retainer program, we help organisations establish the partnerships they need to succeed in their transformation efforts.

You're in safe hands

With cyber security threats increasing in size, complexity and maturity, effective incident response is a critical business asset to an organisation. The experience during any one incident, regardless of how big or small, is not a comfortable situation. As part of KPMG's engagement process, our teams actively solicit feedback during every engagement. Client feedback is reviewed at all levels, including the lead client account team, in an effort to manage client expectations, satisfaction and build long standing relationships.

Global Coverage

Our cybersecurity consulting practice is among the largest in the world, with cyber response members located around the globe. Our 24/7 support service means that you'll have industry experts on hand no matter when or where an incident occurs.

Technical Prowess

It's critical to have expertise when it counts. The breadth of our team's expertise in all aspects of cyber security allows us to provide the highest quality of service. When needed, we can provide our own security tools or make the most of yours. Custom-developed tools, scripts, and licensed security products are part of our toolkit.

Regulatory coverage

Our firm's comprehensive understanding of regulatory requirements in multiple jurisdictions allows us to assist our clients in clarifying their concerns regarding subject notification, liability, and business resilience.

Sector Insights

Our clients come from diverse industries and sectors, and we have gained a deep understanding of what's critical for them within their sectors - especially which data assets and processes create value for them, and which may hold value for threat actors.

Our Alliances

Together with our digital partners, we provide services that give us a competitive advantage. KPMG leverages technology from a number of industry leaders.

Our Cyber Response and Investigation Services

Despite efforts to maintain tight security across the networks and systems, cyber-attacks remain inevitable. This means there's a strong business case for embedding a proactive cyber security strategy and effective response capabilities.

PREPARE

Ensuring your organisation is fully prepared in the event of a cyber-attack.

Cyber Incident Playbook development

We can assist with the creation and development of technical playbooks on a per application, technology, or scenario basis by:

- Advising on leading practices and industry standards.
- Providing standardised templates.
- Maintaining an open dialogue to support with playbook development.
- Ensuring all company decisions regarding response plans and playbooks are documented.

Incident Readiness Review

We can engage with the business and stakeholders to perform simulated attacks which help to assess how well the business handles and responds to an incident, as well as identify any skill or performance gaps that need addressing.

Training and Awareness support

We can assist with the training and awareness of your response and recovery plans by:

- Performing interactive simultaneous multi-team testing and war games to harden defences.
- Supporting with the creation of standard and role based training materials for response and recovery to ensure incident response is understood by all.

RESPOND

Providing an expert incident response service to help safeguard your IT and OT assets during and after an attack.

Attack Disruption

Our team of experts will work swiftly to identify the root cause of the cyber-attack, contain the attack itself, and remediate it. They will ensure that any access an attacker may still hold on your systems, networks or services is identified and disrupted quickly to avoid any further damage.

Threat hunting

Our team of threat hunters will monitor your network to ensure that recovery teams safely recover your systems and bring your services back to usual business operations.

Digital Forensic Investigation

KPMG has a dedicated Forensic Technology lab which enables the recovery and analysis of critical digital evidence to support investigations and litigation.

Threat Intelligence

Threat Intelligence Service complements your organisation's cyber response by providing actionable, relevant and timely information about the attack. In addition to researching threat actor campaigns, monitoring brands, credential leakage, and supply chain threats, it includes insights into operational and strategic decisions.

RECOVER AND BEYOND

Supporting the fast recovery and restoration of your systems and services, and helping to identify key improvement areas to your cyber capability through lessons learned.

Crisis Management

For significant breaches affecting multiple regions, we will setup a crisis management office that will coordinate with relevant committees for driving the recovery of systems and services across each region..

Restoring Business and Technology Services

We understand that in case of an incident you may lose access to your servers and data thereby affecting your services to your wider business. We will assemble a team of infrastructure, cloud and data architects who will help you recover your business services.

Legal and eDiscovery

Our team of eDiscovery specialists will build a clear picture of data and subjects affected by the breach which will help you notify regulators and customers in the most informed way.

Contact us

Déan Friedman
Director, KPMG South Africa
T: +27 (82) 719 0336
E: dean.friedman@kpmg.co.za

Rupesh Vashist
Associate Director,
KPMG South Africa
T: +27 (66) 101 6590
E: rupesh.vashist@kpmg.co.za

Sameer Vyadally
Senior Manager,
KPMG South Africa
T: +27 (66) 010 7878
E: sam.vyadally@kpmg.co.za

kpmg.com/socialmedia