Responding to cyber attacks

Cyber incident response at KPMG

2023

With an ever increasing number of cyber breaches and their subsequent impact becoming increasingly detrimental to both the organisation and customers, there's a strong business case for embedding a proactive cyber security strategy and effective response capabilities. It is important to consider who will be there to walk you through the incident and minimize the impact on your business. With KPMG you have a trusted partner to assist when a cyber incident occurs that not only understands your business and technology, but is able to translate these problems to your business stakeholders.

Key cyber incident response challenges

- Is your organisation as well prepared as it can be to deal with a cyber attack?
- Can your organisation recover from Internet worms or malware that take over your workstations and servers?
- Does your organisation comply with relevant laws and regulations when dealing with cyber incidents?
- How do you know if your organisation is being attacked by criminal gangs, competitors or nation states?
- Does your organisation have adequate resources including personnel, tools and technology to effectively respond?
- Can your organisation detect an cyber incident in a timely manner?

How can we help?

KPMG can work with you to help you detect, contain and recover from cyber incidents. Our experienced team of incident responders can quickly mobilize to help you secure your infrastructure, and partner with you to operate your incident response processes in line with industry standards such as NIST SP 800-86, SANS 6-STEP IR, and ISO 18044:2004. We do this through the following approach:

Repair

- An effective response to cyber security incidents requires proactive measures in the form of technical, procedural and legal preparations to minimize its impact rather than simply reacting to a breach when it occurs
- KPMG's incident response (IR) framework is designed to assist clients evaluate their readiness and personnel capabilities in responding to incidents

Respond

- KPMG's IR service portfolio focuses on offering prompt and effective solutions to cyber security incidents. Our experts are dedicated to helping clients regain control, providing them with the necessary insight they need when the urgency is high.
- KPMG's cyber investigative support service is designed to uncover information on the scope, impact and root cause of the incident, enabling clients to make informed decisions

Recover

- The objective of our solution is addressing cyber incidents and technical systems, while facilitating the recovery of our clients' business operations
- Our expertise in various cybersecurity areas such as cloud, network architecture, crisis management, communications, forensics and legal advisory offers a one-stop-shop for all post-incident activities

Our incident response services

Incident preparation*
To mitigate the effects of a cyber incident, proper preparation is essential. KPMG is able to help ensure your organization is prepared in the event of a cyber-attack.

Incident response
In the case of a cyber incident, resources from out team of highly skilled incident responders will be mobilized and triage activities initiated.

Incident recovery
Following an incident, the KPMG team will be on hand to ensure your mind is at ease and will help your organization return to business as usual as quickly as possible.

Monitoring
During and after a cyber-attack, it is essential to monitor the network for any indicators of compromise.

Communication
KPMG's communications team is able to minimize the impact by providing advice on speaking to media and clients.

Legal help
The recent privacy and data protection law contains detailed regulations which must be followed in the event of a breach. Our team of IR and crisis management experts is trained to assist legal firms in such situations.

Forensic investigation
In line with recent regulations, it is often necessary for companies to run forensic investigations if they are the subject of a cyber incident. Our forensic team assists wit initial triage and investigation.

Crisis management
In the event of a cyber crisis having a comprehensive crisis management strategy is invaluable. KPMG's crisis management experts regularly assist with designing and implementing crisis management procedures.

Why KPMG?

KPMG Cyber Incident Response service provides our clients with an immediate response to assess and control the impact of their cyber breach. We combine multi-disciplinary teams across our business with backgrounds ranging from board and executive advisors with national/international defense and military backgrounds, business operations senior leaders (C-level advisors) and tactical senior cyber security and technology experts with decades of experience in their specific fields.

KPMG's Cyber Incident Retainer model allows you to work with KPMG's cyber experts to develop an effective incident response process that will be rigorously tested, in readiness of response to an incident. Should you be affected by a cyber attack, our team will provide immediate support to help you respond to the cyber attack.

Our global incident response foot print

North America
1000+

Latin America
550+

EMEA
2700+

Asia Pacific
2100+

KPMG has over 6,300 professionals dedicated to delivering Cyber Security services around the world, with over 45,000+ additional risk-focused consultants available to support our client needs.

We combine our deep business process, risk and industry experience with our alliances and digital partners.

** This is a proactive service and is conducted separately from the reactive response service.*

Contact us

Dimitrios Petropoulos
Partner – Cyber
T: +971 506284305
E: dpetropoulos1@kpmg.com

Shehnaaz Sonde
Associate Director – Cyber
T: +971547474301
E: ssonde4@kpmg.com

Follow us on:
www.kpmg.com/ae
www.kpmg.com/om

Publication name: Responding to cyber attacks
Publication number: 4562
Publication date: March 2023