KPMG

KPMG Cyber Incident Management

Insights from KPMG Incident Response Team

February 2023

Identify, Prepare, Detect and Respond

As cyber threats grow in volume and complexity, the loss of intellectual property, customer data, and other sensitive information can put your entire organization at risk. Recent cyber breaches at major corporations highlight the increasing sophistication, stealth, and persistence of cyber attacks that organizations are facing today. Successfully defending and recovering from a cyber attack is a holistic process and encompasses extensive preparation at the people, process and technology level

The preparation against cyber attacks starts from the identification of key assets, knowing individuals role during crisis management, understanding regulatory obligations and maintaining key data artifacts for enabling technical experts to unfold a clear picture of the events leading to cyber incidents

KPMG's approach to cyber incident management is to assist organisations with detecting and responding to cyber breaches by helping them to prepare and defend against cyber attacks successfully. KPMG cyber incident handlers can assist organisations effectively by utilizing their experience gathered from responding to several cyber incidents and utilize that experience in preparation, investigations, digital forensics, recovery and help organization's secure evidence, understand what happened, mitigate risks, and support internal, legal and/or law enforcement inquiries.

Keys gaps in organizations preparedness while responding to cyber incidents

1 Inadequate documentation of organizations crown jewels

Lack of documentation, up-to date IT asset inventory and categorization of critical systems leads to delay in addressing vulnerabilities and implementing isolation and containment measures during a cyber incident. These delays have a negative impact on the overall recovery of business operations

2 Unclear of roles and responsibilities of crisis management team

Lack of clarity of roles and responsibilities within crisis management team leads to delays in the decision making process during cyber incidents. This results in implementation of inadequate measures for mitigating incidents and causing significant risks to the organizations business operations, reputation and might lead to exposure for regulatory inquiries

3 Ineffective Incident response plan

Absence of a well defined incident response plan leads to misclassification of severity of a cyber security incidents, delayed response to protecting key IT assets resulting in deployment of incomplete threat isolation, containment measures causing increased damage to organizations business operations, reputation, customer trust and regulatory consequences.

4 Insufficient data retention

Insufficient data retention results in loss of critical information and evidence. This hinders the analysis of events leading to cyber incidents and impact the overall gap mitigation and remediation exercise.

"Cyber threats have emerged as a pervasive threat to the very continuity of business operations, preparing against cyber-attacks is no longer an option but a necessity for organisations looking to defend themselves effectively and to recover from these attacks efficiently"

KPMG's approach to building cyber incident maturity in organizations

Protect

Table top/simulated cyber incidents

- Tailored exercises that mimic real world incidents with injects as challenges faced by organization during incidents to strengthen decision making process, build understanding of individual roles and mitigate process gaps

Maturity assessment

- Review of an organization's ability and readiness to respond to cyber security incidents.
- Recommendations to improve the incident response programme.

Incident response plan and playbook development

- Assistance in creation of an incident response program and process design aligned with organizations risk framework
- Development of cyber playbooks tailored to organizations workflows, tools for typical incidents for holistic mitigation

Detect

On-Demand Threat Hunting

- Proactive monitoring checks and early warnings based on analysis of logs and incidents to help reduce risks and threats of cyber incidents
- This may include hunting for indicators due to recent vulnerabilities, exposed IT assets and services or threat intel driven approach

Blue Team Exercise

- Assist security teams in testing defense against common threat, tactics, procedures (TTP's) and help in identifying gaps, integrate new data sources and increase visibility for strengthening detections and reducing noise

Pre-exit forensics

- Tailored review of certain individuals assigned IT asset to identify instances of IP theft/ sensitive data transfer to personal accounts/USB drives/ cloud storage, etc. using forensic techniques to identify and mitigate insider risk threats

Investigate

Compromise assessment

- Proactive assessment/review of an organization's technical infrastructure including host- based log analysis, and/or network analysis to determine if any unidentified compromise has occurred previously.

On Demand Incident management

- On Demand assistance in resolving cyber incidents end-to-end which includes all phases of incident response process, viz. forensic triage, containment, investigation, remediation and reporting.

Independent verification and validation

- The verification of investigation findings and extent of intrusion, crime, fraud scheme or financial reporting from an independent voice. KPMG's tested track record of independence can help ensure the accuracy and completeness of any investigation.

Contact us

Key contact and Subject Matter experts, as well as relevant links

Chad Olsen
Partner and Head of Forensics – Hong Kong
Hong Kong
KPMG China
T: +852 3927 5576
E: chad.olsen@kpmg.com

Mohit Kumar
Director, Cyber Incident Management
Hong Kong
KPMG China
T: +852 2685 7428
E: mohit.kumar@kpmg.com

kpmg.com/cn/socialmedia