Cyber incident response

Advisory

home.kpmg/in

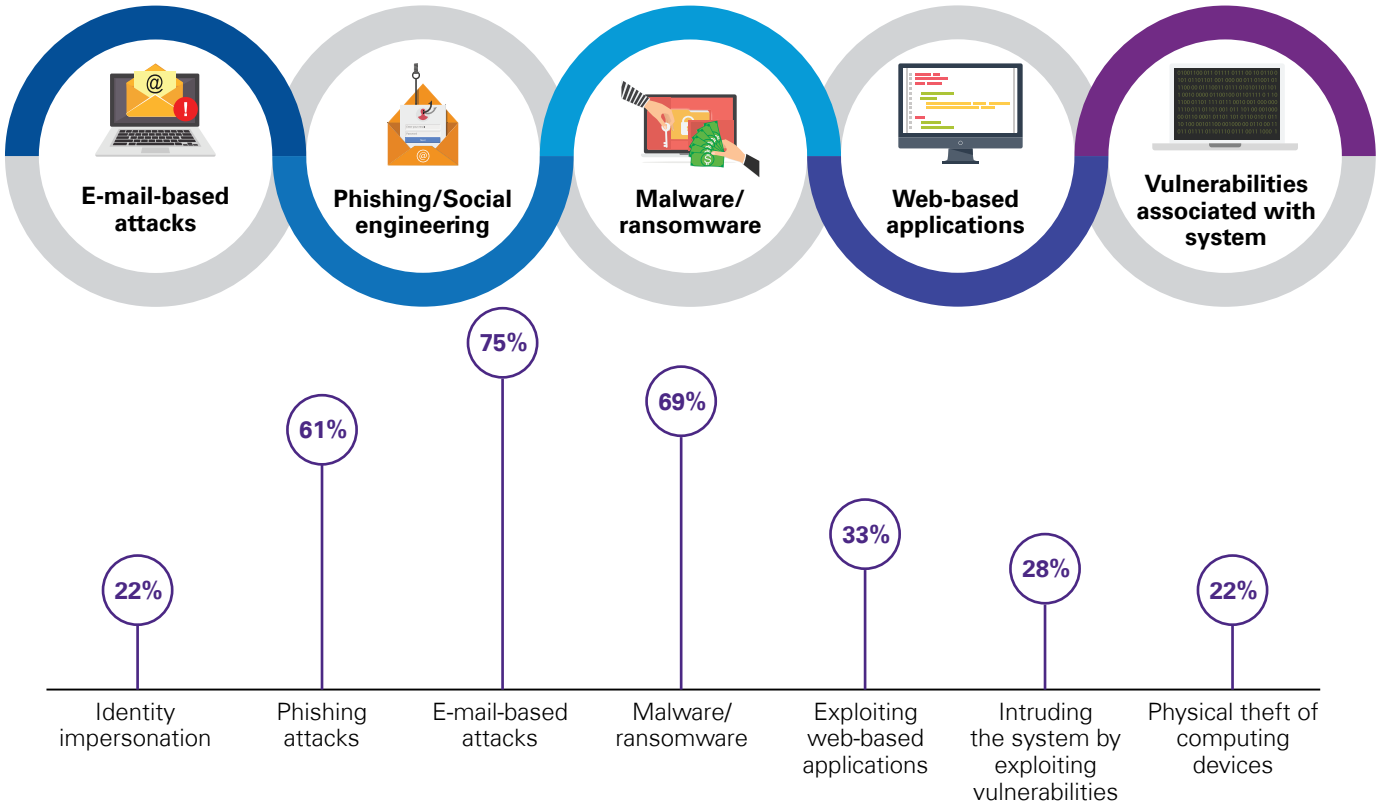
Since the advent of the information age, economies have grown at a breakneck speed with information technology pervading every sphere of human life. However, this phenomenon has given rise to an ever evolving class of cyber threats, affecting individuals and organisations. The recent breaches at major organisations highlight an increasing sophistication, stealth and persistence of cyber attacks resulting in regulatory oversight and negative business impact. It is, therefore, imperative that organisations develop effective incident response frameworks to counter cyber attacks.

Cyberattacks in the current era have become more specialised and concentrated in nature, targeting individuals and organisations. The cyber threats are no longer IT centric, and can be pervasive throughout an organisation with a high chance of reoccurrence.

With the attack patterns becoming more targeted and sophisticated, the impact due to cyber incidents have caused enormous damages spanning financial losses, erosion of shareholder value, intellectual property theft and trust.

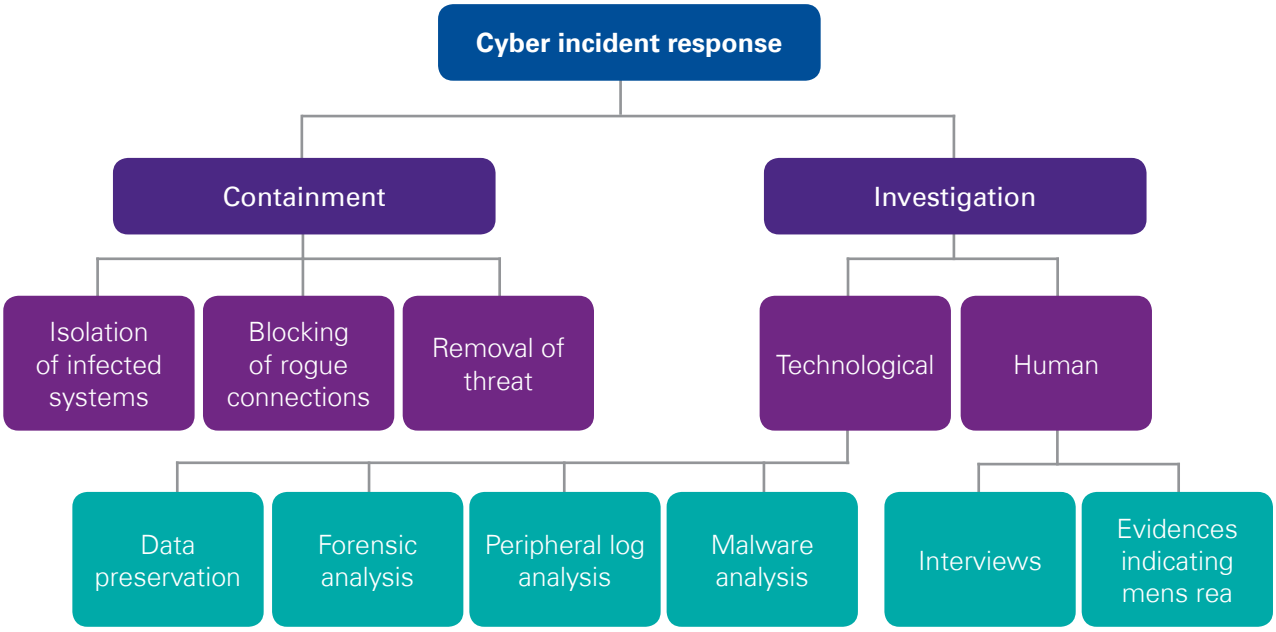
KPMG in India can help your organisation respond to cyber threats effectively and efficiently, with our bouquet of services ranging from rapid cyber incident response, containment of threat, continuous monitoring to training and capacity building. Our team comprising certified forensic experts, malware analysts, network forensic analysts, cyber law experts and former law enforcement officials help your organisation respond to suspected cyber incidents and take measures to mitigate such incidents in future.

Based on KPMG in India's Cyber Crime Survey 2017, the top five cyber-attacks being faced by organisations are:



KPMG in India's cyber incident response methodology

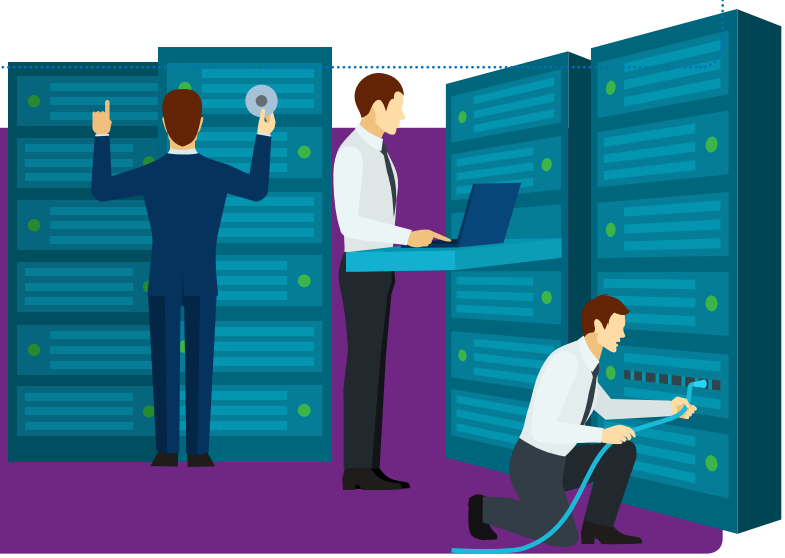
Our incident response process was created according to several internationally accepted frameworks, including National Institute of Standards and Technology - Special Publication 800 86 (NIST SP800-86), the International Organization for Standardization publication 18044:2004 (ISO 18044:2004) and the SANS Institute's published six-step incident response process. While these guides were utilised to verify completeness of framework and methodology, KPMG in India's approach as depicted below was further refined through real world experiences, evidentiary rules and deep technical knowhow during incident response engagements:



We have successfully assisted several organisations to respond to their large, complex and sensitive cyber incident situations, including many high profile cases in the public domain. Our team is well versed with the sensitivity, urgency and complexity associated with business disruption and interruption situations.

KPMG in India's multi-locational cyber labs

- Agentless remote acquisition capabilities
- Integrated threat intelligence based analysis
- Automated malware analysis using multiple sandbox environments
- Automated multiple antivirus reverse lookups
- Dedicated platforms for analysis of network peripheral logs



Cyber incident response services

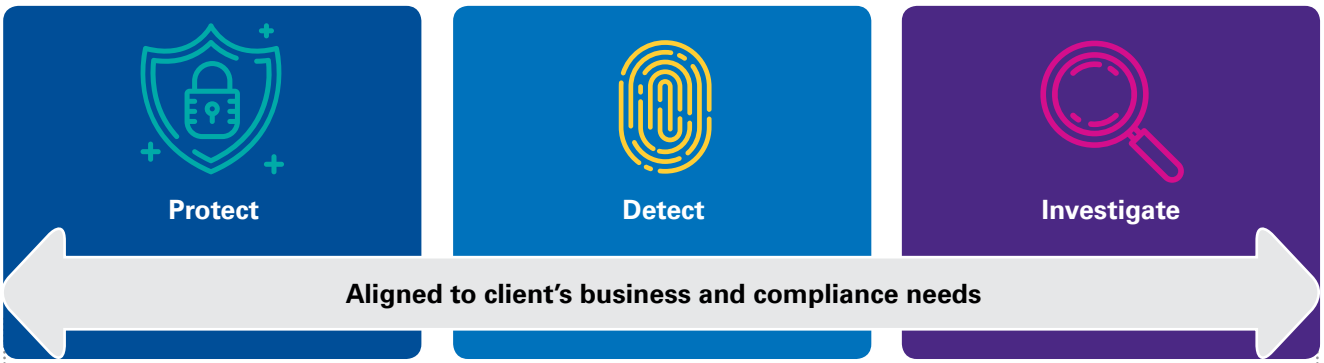


Table top/simulated cyber incidents

- Assistance in protecting and mitigating risks
- Tailored exercises that mimic real world incidents
- Simulation of a real world scenario to respond to incidents.

Monitoring/early warnings

- Proactive monitoring checks and early warnings based on analysis of logs and incidents to help reduce risks and threats of cyber incidents
- Creation of long-term development and sustenance of cyber-response capability.

Compromise assessment

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

Maturity assessment

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

Staff Augmentation

- Continuous monitoring of known issues for a limited period, to detect and contain the cyber frauds.
- This may include review of an organization's technical infrastructure including host-based log analysis and/or network analysis.

Incident management

- Assistance in resolving cyber incidents, which includes all phases of incident response process, viz. forensic triage, containment, investigation, remediation and reporting.

Incident response programme development

- Assistance in creation of an incident response programme, process design and playbook development.

Pre-exit forensics

- Review of certain individuals assigned asset laptop/desktop to identify instances of IP transfer to personal accounts/USB drives, etc. using forensic techniques.

Expert witness

- Post investigation, deposition of KPMG in India personnel in the court of law as expert witness in the matter to present case facts.

Training and capacity building

Select credentials

Incident type	Details	KPMG in India's intervention	Engagement outcome
Bank SWIFT breach investigation	One of the largest private commercial banks in South Asia with a network covering all major financial institutions	• Forensic preservation and root cause analysis (RCA) of the incident • Cyber security review of the client's infrastructure, including: - SWIFT environment - Domain controller - E-mail infrastructure - Internet-facing infrastructure.	• Identified and analysed the timeline of SWIFT cyber heist • Uncovered modus operandi of attackers in penetrating the bank's technical infrastructure • Advised the client to take reasonable containment measures.
Investigation of ransomware attacks	An automobile manufacturing company with a substantial market share in India, and having significant exports across Asia, Europe, etc.	• Forensic analysis of infected systems • RCA using system files, event logs, e-mails, web browser • Reverse engineering of identified malicious files in a controlled sandboxed environment • Assistance in remediation	• Blocked malicious files from causing infection on other machines • Identified the root cause of the malware infection and blocking of the command and control (C&C) server IP address at the network level • Provided recommendations for strengthening the IT environment.
Bank ATM Cyber Heist	One of the large private sector commercial banks in India with a network covering all major financial institutions.	• Forensic acquisition and analysis of ATM Switch Servers and other computer systems • Cyber Security review of internet facing infrastructure,including the Email Server • Analysis and review of ISO 8583 messages generated in ATM machines	• Clearly identifying root cause of incident, along with the timeline and modus operandi • Support for containment of malware • Identification of control weaknesses in Bank's digital payment systems
Web application breach investigation	A multinational tele-communications company, and one of the largest cellular service providers in India	• Determining the modus operandi of provisioning free data bundles to non–eligible users from web based graphical user interface • Assessing the financial exposure of the company • Identifying involvement of an insider in the cyber fraud.	• Identified the users who had re-ceived free data bundles using the fraudulent provisioning method • Revealed nexus of fraudulent beneficiaries with external hackers by means of data analysis.
Man in the e-mail attack	The Client is one of the largest intellectual property management companies in the world, having an exposure in India	• Determining timeline of potential man in the email attack, and its root cause • Identifying control weaknesses and providing suitable recommendations.	• Uncovered the modus operandi of highly targeted Office365 spear phishing attacks • Conducted searches on Threat Intelligence Platforms to identify patterns of rogue IP addresses and malicious domains • Assisted the Client in continuous monitoring and taking real time containment measures.

KPMG in India contacts:

Nilaya Varma
Partner and Head
Markets Enablement
T: +91 124 669 1000
E: nilaya@kpmg.com

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-Leader – Global Cybersecurity
T: +91 124 307 4800
E: atuteja@kpmg.com

Atul Gupta
Partner and Head
IT Advisory Services
Leader: Cybersecurity
T: +91 98100 81050
E: atulgupta@kpmg.com

Jagvinder S Brar
Partner and Co-Head
Forensic Services
T: +91 124 336 9469
E: jsbrar@kpmg.com

Maneesha Garg
Partner and Co-Head
Forensic Services
T: +91 120 386 8501
E: maneesha@kpmg.com

Varun Batra
Technical Director
Forensic Services
T: +91 124 307 4809
E: vbatra@kpmg.com

Manish Tembhurkar
Technical Director
IT Advisory Services
T: +91 98181 99432
E: mtembhurkar@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/social media