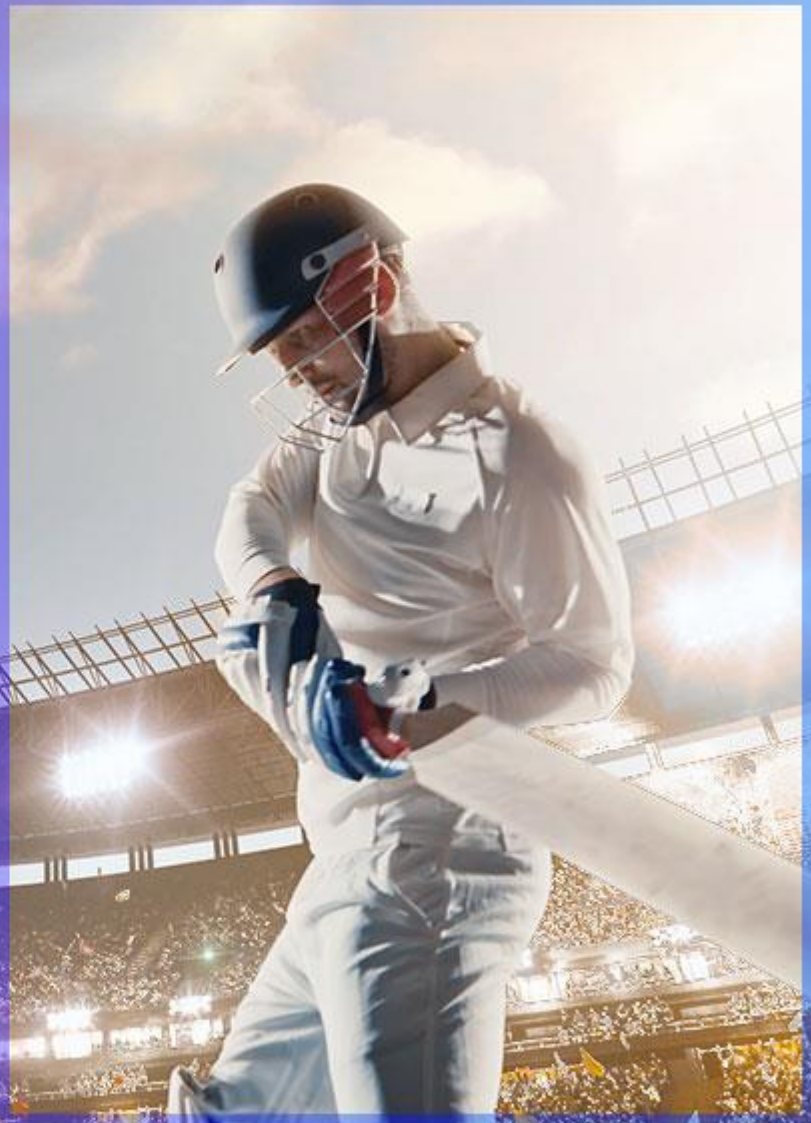
KPMG

The game is on - are you ready?

Cyber incident readiness

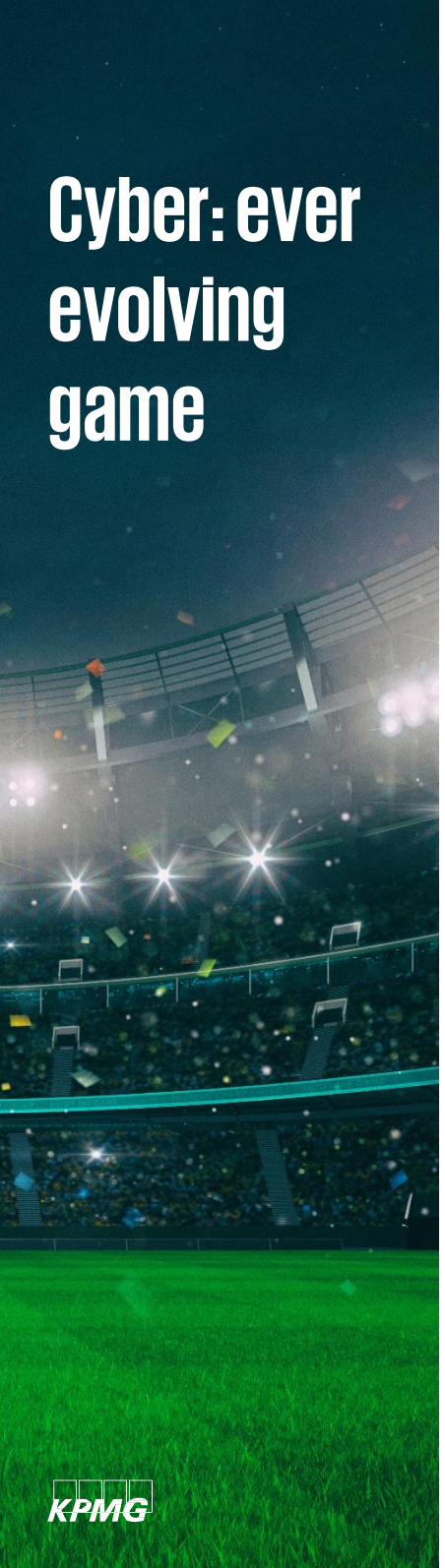


kpmg.com/in

Contents

01	Cyber: ever evolving game	3
02	Learnings from the game… so far	5
03	Rules of the game are transforming	6
04	Game ready: have the right team	7
05	Staying on top of the game	9
06	Being a winner: adopt the right strategy	10
07	How KPMG in India can help	12

Cyber: ever evolving game



The cyber threat landscape is expanding, and security incidents are a reality today. Every day brings news of more cyberattacks and even more sophisticated types of attack. We are operating in an environment where cyber events are inevitable and security teams must be ready to respond, recover and re-establish the trust as quickly as possible. As per KPMG 2021 CEO Outlook, 75% CEOs believe a strong cyber strategy is critical to engender trust with key stakeholders .

Cyber incidents are inevitable due to increased reliance of business on digital ecosystem and the changing threat landscape. In addition, challenges in following effective incident response procedures, have made it imperative to have strategically planned and professionally managed cyber response programme. We have explored key critical elements of cyber response management that would help organisations to play and win in the on-going cyber game.

Cyber incidents – direct business impact

- Hyperconnected technology systems: Any impact on a part of technology propagates across the organization's environment and has a significant impact on business operations

  Cyber attack in oil pipeline system at Texas demonstrated how a cyber incident can have cascading disruption to societies and economies

- Supply chain getting impacted is leading to direct impact on business operations

  A global automobile manufacturer had to suspend operations in production line after a strategic supplier was hit by a cyber attack

- Data breach cases have been in rise leading to sensitive, confidential or otherwise protected data has been exposed or disclosed

  A leading telecom company reported appx 7.8 million customer records including SSN, date of birth, device ID information was compromised

- Business Email Compromises (BEC) impersonates senior executive to obtain confidential information or commit financial frauds

  The government of Puerto Rico fell victim to BEC attacks that attempted to steal more than USD 4 million, in 2019 and 2020

- Ransomware cases: Cyber criminals have industrialized the scale at which ransomware attacks can be launched e.g. Ransomware as a Service (RAAS)

  A major Indian oil company intimated malware infection followed by a demand for ransom in bitcoin.

Cyber: ever evolving game

Changing threat landscape leading to increase in number of security incidents

78%

of Indian organisations fell victim to ransomware in the last year[1]

:

72%

of organizations experienced an increase in volume/complexity/impact of cyber attacks[1]

77%

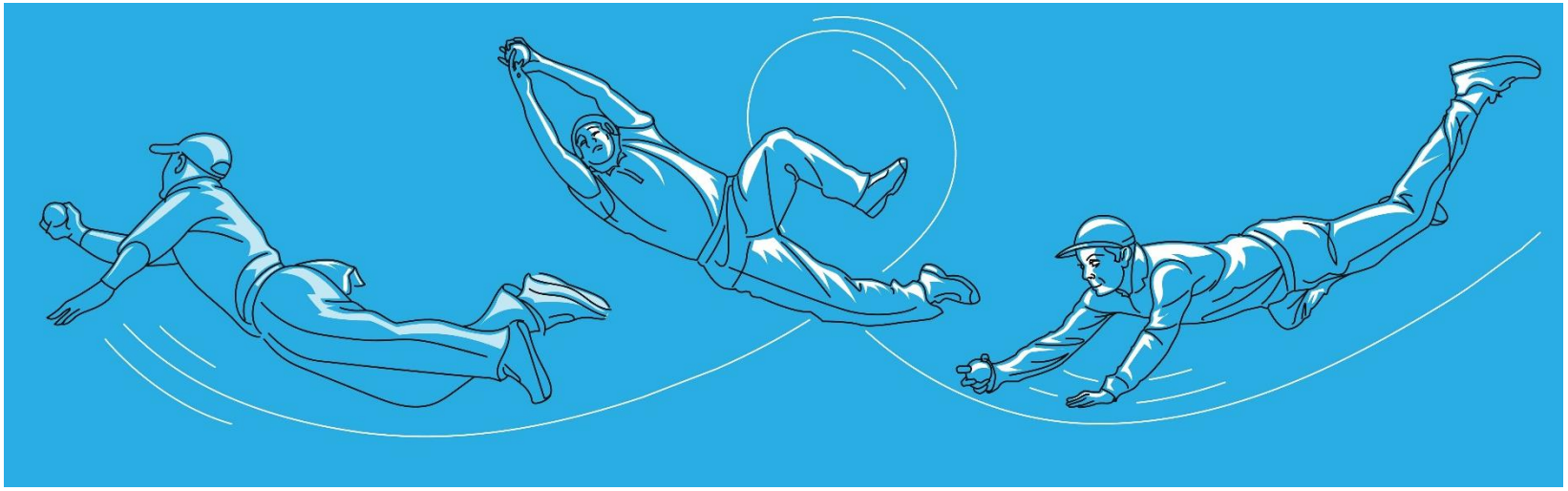
of intrusions are suspected to be caused by three initial access vectors: phishing, exploitation of known software vulnerabilities and brute-force credential attacks[2]

28 days

is the time threat actors spend in a targeted environment before being detected[2]

21%

year-on-year increase in cyber incidents reported to CERT-In (appx 674,021 were observed up to June 2022).

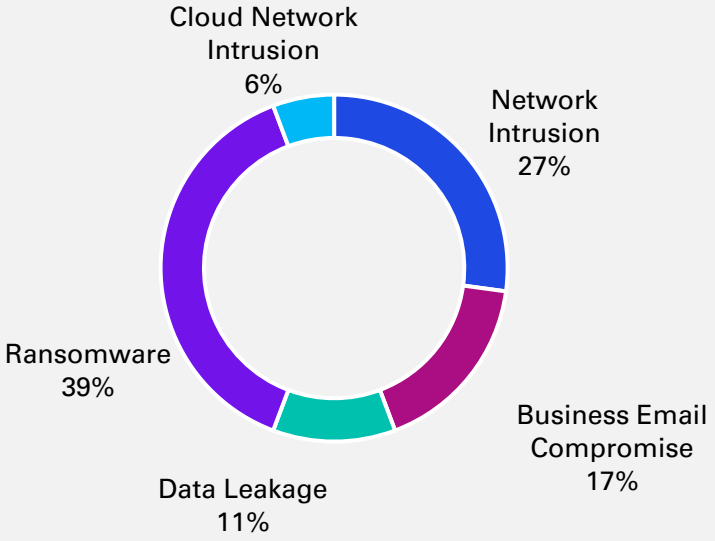


1. Sophos, The state of Ransomware 2022, April 2022
2. PaloAlto Networks Incident Response Report 2022

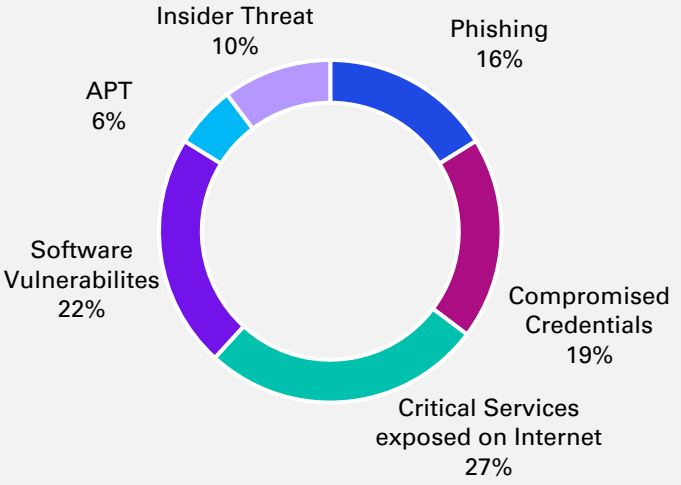
Learnings from the game... so far

KPMG has been recognised as 'Leader' for Worldwide Incident Readiness Services considering cyber response services provided globally. We have closely observed the number of organisations, that have gone through different types of cyber incidents and followed incident analysis, containment, remediation and recovery procedures. Based on our study, over the last three years, the following patterns and trends have been observed.

Type of Cyber Incident Cases



Initial attack vector (entry point for Threat Actor)



Traditional approaches have not been effective and require adoption of a more agile approach to investigate and recovery planning to go hand-in-hand in order to eliminate persistent backdoors.

- Sophistication in initial access techniques together with RAAS business models have significantly increased number of ransomware cases

Management involvement is essential and everyone in the team has to play a role for quick decision making and action on implementation.

- As we can see increased phishing attacks, software vulnerability and credentials are primary initial attack vectors which can be avoided with active participation from everyone in the team

Having a response plan and practicing it ensures to minimise uncertainty during the incident.

- Organisations with tested and simulated cyber crisis response plans, were able to identify and recover faster in most of the cases

Right strategy to respond to cyber incident scenario is essential.

- Handling complex threat scenarios such as data leakage, cloud intrusion require to work with specialists, threat intelligence provider and cyber insurance for rapid recovery

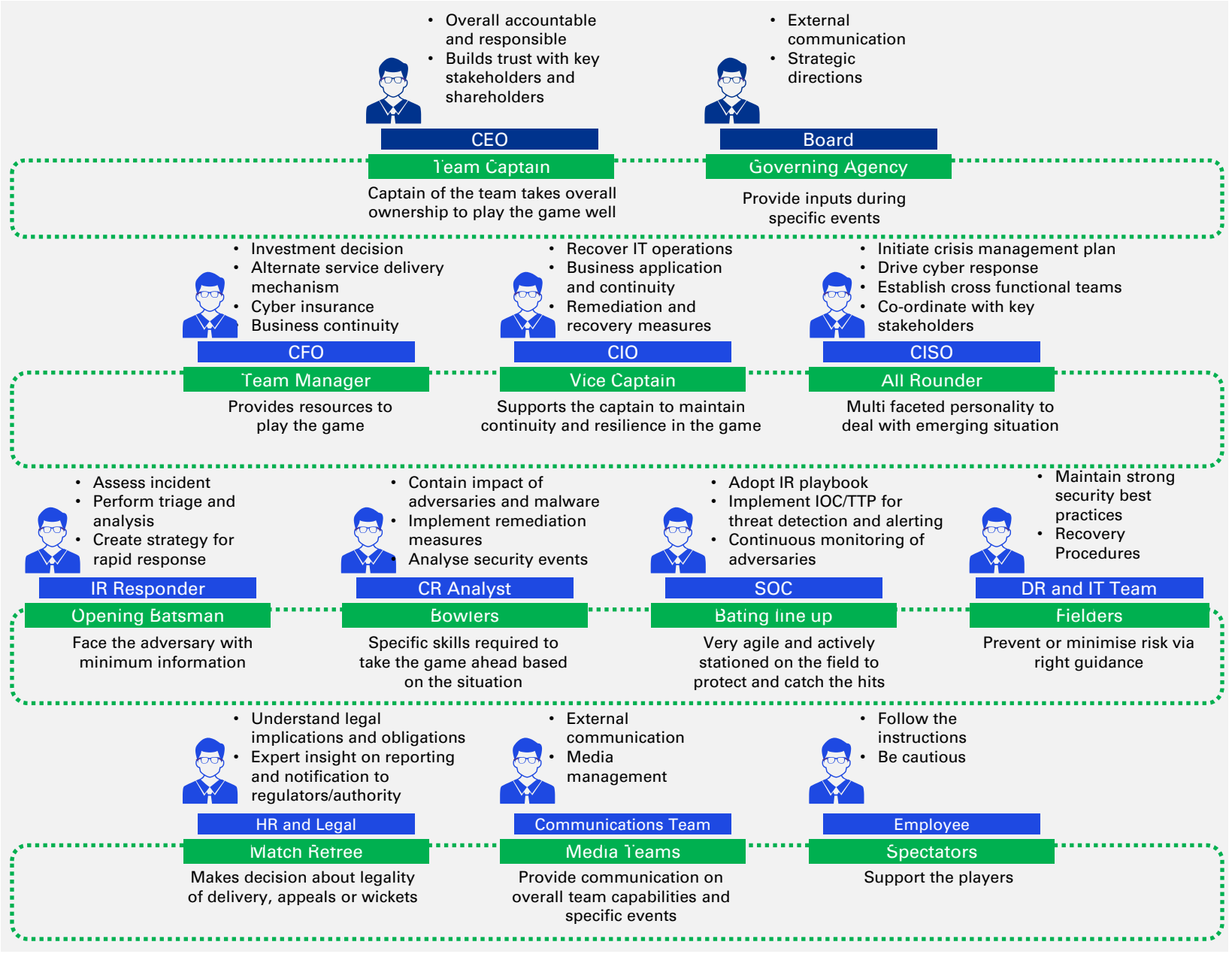
Rules of the game are transforming

Fallout from an unprofessional response to an incident has been more damaging than the incident itself, therefore cyber response measures in today's digital age require agility, comprehensiveness and standardisation to think beyond organisational boundaries and known threat landscape. Incident management and response practices must evolve with more automation and advanced strategies for early detection, automated response and rapid analysis within the legal and compliance boundaries to deal with new-age cyber attacks.

Traditional approach	Current age approach
Linear approach to collect, preserve, analyse and report evidences from digital sources	Agile and iterative approach to perform live triage, contain, acquire, analyse, report are adopted repeatedly for rapid recovery
Manual process that involves trial-and-error methods and requires highly skilled manpower	Automated process, that leverages tools, technology, remote analysis and visualisation techniques to present datasets for quick analysis and decision making
Offline analysis limited to affected machines and manual/semi automated review of available logs	Real time analysis covering enterprise-wide ICT systems and often goes beyond organisation's boundaries to include supply chain ecosystem and consumers
Limited threat intelligence inputs are factored, without leveraging information on adversaries	Enriched digital analysis from multiple sources with customised, curated cyber threat intelligence for insights about threat actors, Tools, Techniques, Procedures (TTP) etc.
Cyber incident was perceived as IT issue leading to full remediation and reporting taking long duration	Remediation and regulatory reporting are performed simultaneously that require organisation-wide involvement

Game ready: have the right team

Organisations need to take response strategy seriously and understand that incident response management requires adopting a multipronged approach to have the right skill set and diverse experience to work together with common objectives. Engaging with all stakeholders to ensure appropriate support and decision-making, is essential in order to provide strategic and tactical insight in end-to-end response to incident.



Game ready: have the right team

Organisations need to take response strategy seriously and understand that incident response management requires adopting a multipronged approach to have the right skill set and diverse experience to work together with common objectives. Engaging with all stakeholders to ensure appropriate support and decision-making, is essential in order to provide strategic and tactical insight in end-to-end response to incident.

Responding successfully starts at the top

The C-suite should be responsible for ensuring operational continuity and should appoint a cyber security team to manage the necessary tools for success.

Key decisions before an event are not technical

Critical decisions cannot be made exclusively by cyber security and technology teams. Some are strategic and may require government coordination, for example when critical national infrastructure is concerned.

Everyone has a role to play in crisis

Responding to large-scale ransomware attacks requires everyone in the organisation to fully understand their role in a crisis. To help prepare and raise awareness of the implications of an effective response, it's highly encouraged for organisations to engage in testing and rehearsal exercises.

First response needs to be in a timely manner

First incident responder needs to be responding in the "Golden Hour" to minimise the impact and establish appropriate strategy to recover.

Need for collaboration

During a cyber security incident, everyone with different specialised skill set like operations, network, malware RE, forensics, legal, operations, markets, finance, etc would be required to work towards a unified goal.

Being Agile

IR planning is also all about being agile and adapting to the changing situational circumstances in such a way that containment, impact and business recovery objectives are in sight and achievable.

Staying on top of the game

In today's environment, it is imperative to have a state-of-the-art cyber response readiness. There are multiple dimensions that need to be established ranging from specialised skill set, technology setup, intelligence and stakeholder involvement and practicing the ways of working, to reduce uncertainties.

Management involvement and communication plan

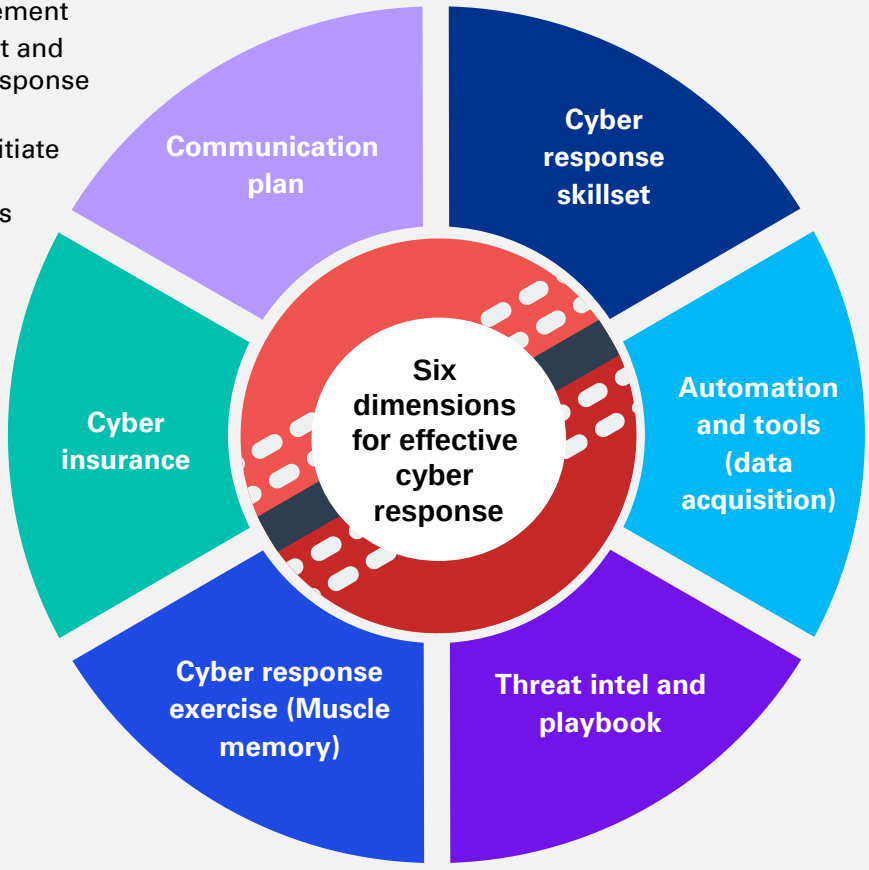
- Stakeholder management
- Pre-prepared content and plans to speed up response
- Defined roles and responsibilities to initiate communication with relevant stakeholders

Cyber insurance

- Provides coverage on business impact
- Enable initial cyber response and assess the impact
- 'Slow burn cost' related to reimbursement, litigation, fines, etc.

Practice and exercise

- Table top simulation of real attacks
- Test the strength through cyber drills, Red Team



Response skillset

- First Incident Response team to immediately assess impact, preserve evidence and contain
- Analyst to investigate details of cyber incident and associated impact
- Engage on-demand incident response specialist

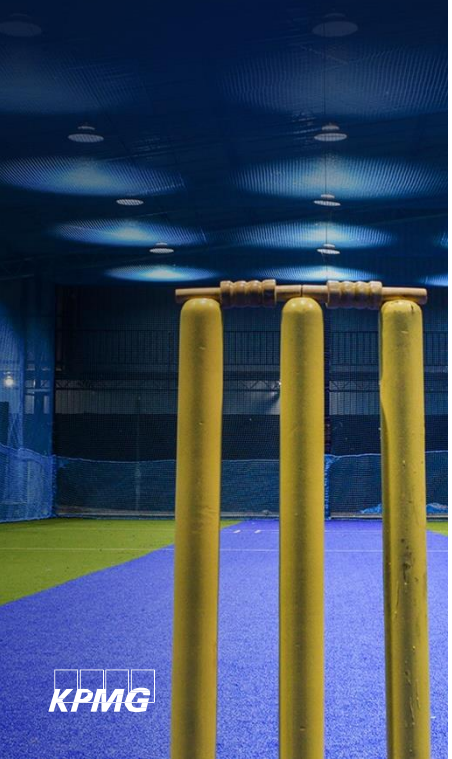
Automation and tools

- Establish toolsets for quick data acquisition
- Automated security tools for initiating initial response measures
- Identify scenario for digital imaging

Threat intel and playbooks

- Source required information related to threat adversary and ability to drive threat hunt missions
- Playbook for various types of incidents covering technology, platforms and services

Being a winner: adopt the right strategy



Organisations are accelerating their preparedness to cyber response as they develop trust and transparency in the service offerings, by leveraging the digital ecosystem.

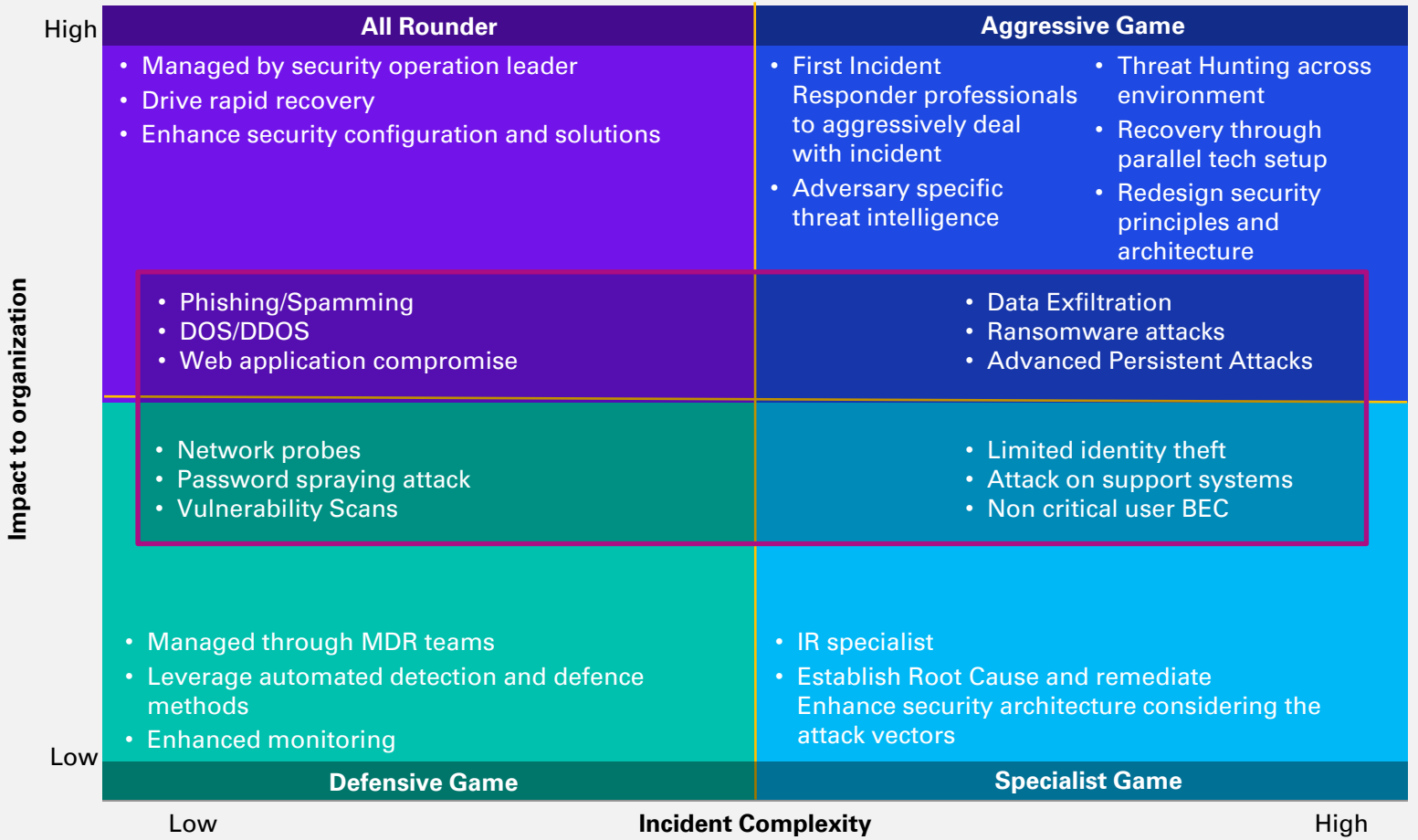
Readiness strategies to prepare for the game

Being a winner: adopt the right strategy

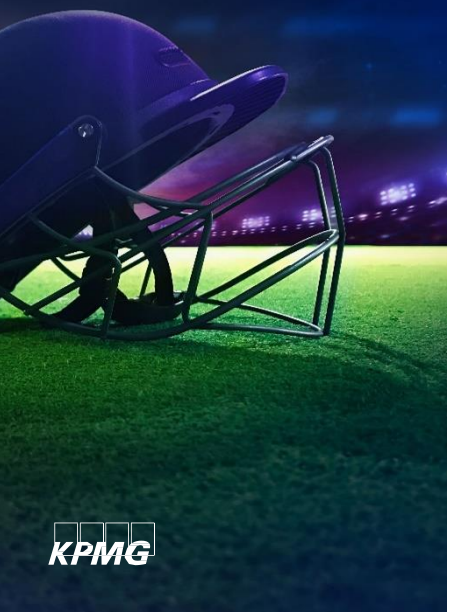
"One size fits all" approach isn't a prudent method, specifically considering the diverse set of threat vectors. Specific strategies need to be taken upon to improve preparedness and recover rapidly, based on complexity of the attack and associated impact to the organisation.

Simultaneously, there is an increased requirement from regulatory authorities on reporting cyber incidents and having the right approach shall enable organisations in fulfilling these obligations.

Deploy right strategy



How KPMG in India can help



KPMG in India helps organisations to create a resilient and trusted digital world — even in the face of evolving threats. Our cyber security professionals offer a multidisciplinary view of risk, helping to carry security throughout the organisation and get an edge with secure and trusted technology.

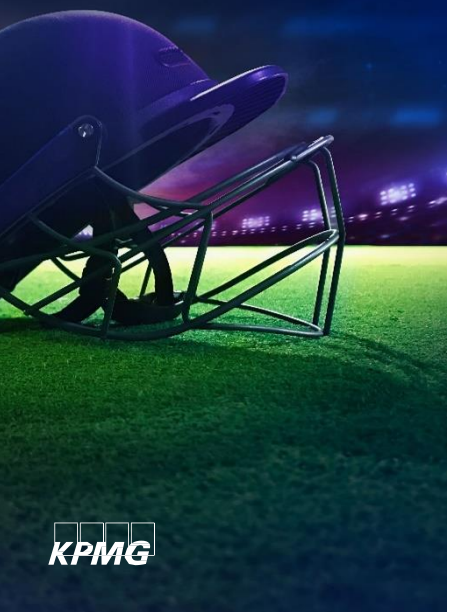
No matter where you are on your cyber security journey, KPMG firms have expertise across the continuum — from the boardroom to the data centre. In addition to assessing your cyber security and aligning it to your business priorities, we can help you develop advanced solutions, assist with implementing them, advise on monitoring ongoing risks and help you respond effectively to cyber incidents.

KPMG firms bring the uncommon combination of technological expertise, deep business knowledge and creative professionals who are passionate about enabling you to protect and build your business. We will help you create a trusted digital world, so you can push the limits of what's possible.

We help organisations in "pre-incident readiness journey", "incident investigation" to "post-incident" analysis. Our services are structured to quickly enhance organisation's cyber response maturity to help them emerge as winner in this ongoing game.

Readiness		Response		Remediation
Table Top simulation	Cyber Response Maturity Assessment	First Incident Responder	Threat Hunting	Compromise assessment
Playbook	Threat Advisory	Cyber Response and Analysis	Incident Reporting	Remediation Advice
Communica-tion Plan	Crisis Plan	Breach Response	IR Retainer	Continuous Monitoring

How KPMG in India can help



KPMG named a ‘Leader’ for Worldwide Incident Readiness Services by IDC MarketScape

The IDC MarketScape report recognises KPMG for being the leader in global incident readiness capabilities and taking a comprehensive approach to cyber incidents through its integrated cyber practice. The report calls out KPMG’s range of incident readiness and response services including the ability to provide direction on cyber insurance, and exercises for clients to train and test their response capabilities.

Based on its analysis of 14 organisations that offer incident readiness services across the globe, the IDC MarketScape report states that, “firms of all sizes that desire to work with a global incident readiness provider with strong digital forensic capabilities should consider KPMG.”

Notes

Notes

KPMG in India contacts:

Akhilesh Tuteja
Global Head - Cyber Security

Atul Gupta
Partner and Head - Cyber Security India
Lead - Digital Trust

Sony Anthony
Partner - Digital Trust

B.V Raghavendra
Partner - Digital Trust

Chandra Prakash
Partner - Digital Trust

Manish Tembhurkar
Associate Partner - Digital Trust

kpmg.com/in

Follow us on:

kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.