KPMG

SAPPHIRE CONNECT
A Division Of Sapphire Human Solutions Pvt. Ltd

Cyber risk and resilience

Mitigating risks and business impact

August, 2021

home.kpmg/in

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Preface

COVID-19 has completely changed the way we work, projects which probably took years have been driven through in weeks. We have seen companies that have taken security risks that they might never have accepted under any other circumstances.

Organised crime groups have been ruthless and entrepreneurial in exploiting fear, uncertainty and doubt over COVID-19. They have been repurposing phishing and attack infrastructure to build COVID-19 fake websites and scams. Nation states themselves have adapted their own cyber espionage tactics.

It has been noted in the recent past that ransomwares are more likely on a network which is connected via end-points of employees who are working from home. Further, the ransomware attack itself has shifted to more targeted and effective exploitation models. With double extortion attacks involving stealing of data which is common and at the same time, greater efforts to locate and encrypt online backups.

Cyber security risk has increased, at least in the short term

The risk teams in financial firms have become increasingly concerned about just how many security waivers were granted in the rapid response to COVID-19. In particular, insider threats are worrying them — from call-centre workers working from home stealing customer card details, to investment traders colluding absence from the watchful eye of their supervisors, to a high level of churn and redundancies as firms come under stress and state support packages draw to a close.

For many firms, distress is on the horizon as demand declines, supply chains are disrupted, and the cost of debt Increases in these challenging market conditions. For sectors such as aviation, oil and gas, conventional retail and hospitality — the impact may be extreme — leading to aggressive cost reduction, restructuring and liquidation. In others, business models are changing faster than expected to embrace digital channels, cloud services and embed home working — the latter with an eye on associated cost savings from property footprint reduction.

This paper was inspired by the panel discussions held at the Cyber Risk and Resilience Summit 2020 where KPMG in India was the Knowledge Partner and we would like to thank the esteemed panelists for their views on cyber risk and resilience.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG in India foreword

The new paradigm of work in 2020 has set in motion a couple of areas with additional focus for multiple stakeholders.

Cyber response to resilience and cyber insurance to an organisation, zero trust security and cloud shifts to the network and privacy to an organisation, its employees and clients.

Cyber response to resilience: There are many great lessons around resilience from COVID-19. It has forced companies to rethink business models to deal with changes in working patterns, customer demand and supply arrangements. Companies have a clearer idea of who and what matters to their businesses, whether described as critical business processes or key individuals. They have been forced to invoke (or create) crisis management arrangements and to do so with pace and agility. It has also raised questions around aspects like a) Are we protecting the right areas – should we question our assumptions? b) Is my cyber security strategy aligned to Business goals and lastly how do we improve our resilience and response to a cyber attack?

On the network front, Zero Trust has been around for decades, it dictates that only authenticated and authorised users, devices, workloads can access applications and data. It is rooted with the principle of "never trust, always verify". Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control. This however did not get the push it required as users operated in safe virtual networks within an organisation's local area network.

However, today with most of our workforce operating from homes, it is prudent that organisations adopt Zero Trust to enhance security. On the scale and availability side, cloud environments have provided that much needed access from anywhere. it is to be noted that not too many organisations have a well-defined cloud strategy that encompasses security and privacy especially when specific risks such as identify theft, data security, cloud misconfigurations and malware in the cloud are increasing exponentially.

Regulations are on full throttle as well. India's data privacy and protection legal framework is about to take a quantum leap in the form of the Personal Data Protection Bill 2019, the challenge is that most organisations do not have a basic understanding of the data they collect, let alone the reasons and purposes of such collection.

Lastly, cyber insurance is gaining prominence. Themes in abundance have emerged targeting organisations irrespective of the security mechanisms implemented or irrespective of how mature the current security posture is. It is therefore imminent for organisations to adopt a cyber insurance policy however large or small it is.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Sapphire Connect's foreword

The COVID19 pandemic ushered in a new normal in the corporate world. Prior to the COVID19 pandemic, organisations across the globe had numerous security checks in place, allowing them to secure their critical and sensitive data. At the onset of the COVID19 pandemic, security leaders and experts found themselves in unchartered waters, and with growing business demands requiring them to re-work their security strategy in the least possible time.

As the business world evolves to accommodate the new normal brought in by COVID19, cyber security now finds itself part of the organisational strategy. The shift had already occurred, COVID19 just expedited it further, in terms of the strategies employed, in terms of the technologies deployed, evolution of law and policies, in terms of the culture that is built within the organisation, all revolving around establishing and maintaining a secure cyberspace.

In this ever changing and ever evolving landscape, 'Threat Actors' did not seem to lose steam, but rather took on the crisis brought on by the COVID19 in their stride, increasing the number of theme-based attacks, especially COVID19 based themed attacks. Keeping abreast with this dynamic change is the key to ensuring your critical data is secure and continues to remain secure.

Considering the dynamic shift brought on by the COVID19 pandemic, Sapphire Connect's Cyber Risk & Resilience Summit at its core aimed at being a premier knowledge sharing platform for cyber security leaders and experts. The summit witnessed deliberation and best practice sharing among security leaders on how to further secure the cyberspace.

Our endeavor at Sapphire Connect has been to highlight current challenges and to bring to light their solutions. Through this Whitepaper we bring forth the deliberations from Cyber Risk & Resilience Summit 2020 for a larger audience to benefit from.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Table of contents

01 Cyber response to resilience 08

02 Zero trust security - The preventive approach 12

03 An overview on cyber insurance 16

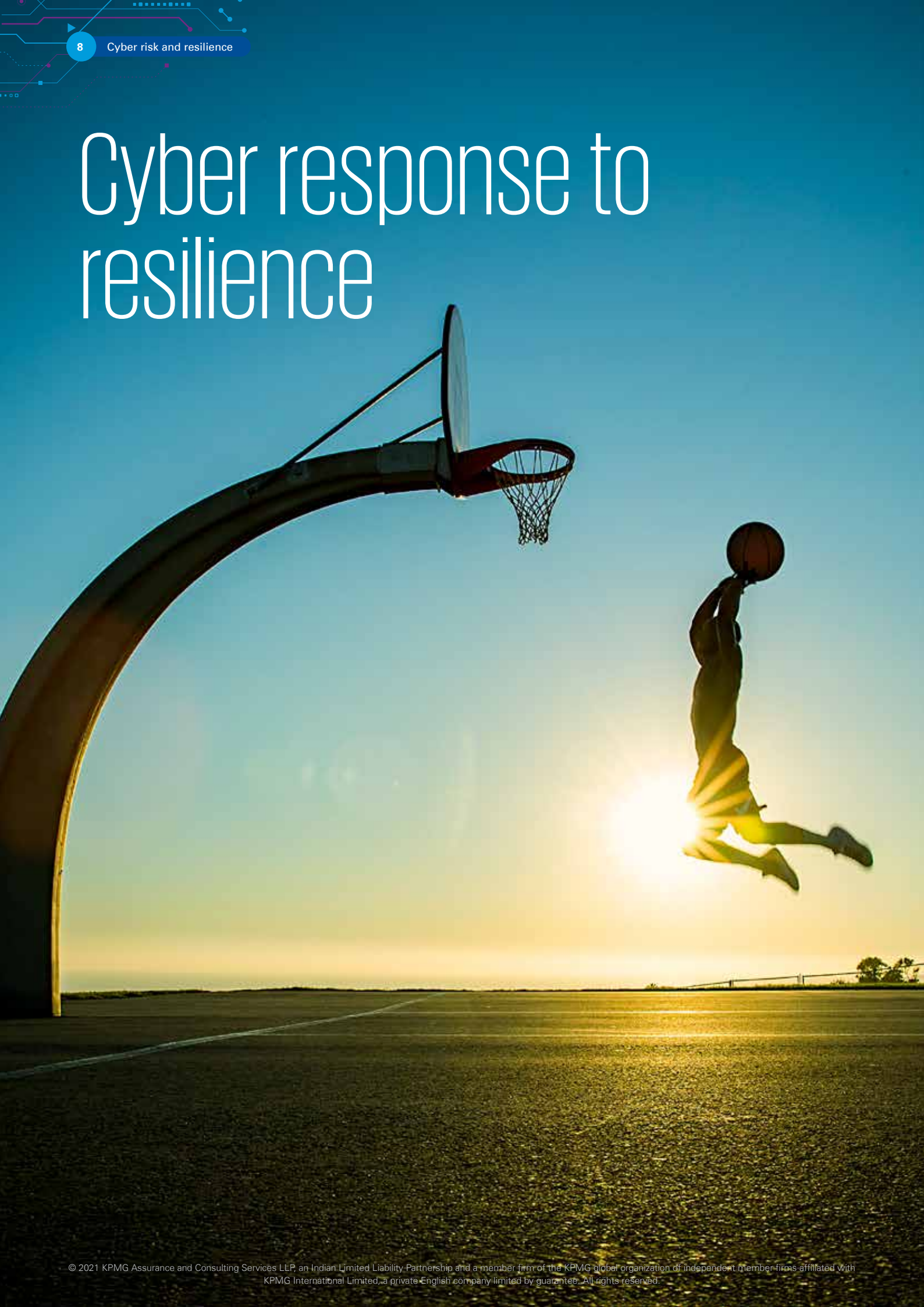
04 Privacy in the age of constant connectivity! 20

05 Cloud security 22

06 In conclusion 24

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Cyber response to resilience



© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

An overview

Already in the grip of tectonic changes driven via social media, increasing consumer mobility, cloud and analytics, businesses were pushed to the brink of breaking point this year, by the challenges brought on by the pandemic. Faced with either shutting shop, or to innovate their way around this situation, we saw many businesses adapt to these changes wholeheartedly. This has led to a completely new working paradigm seeking to exploit the potential proffered by the new digital economy and transform services offered to their customers and employees. The fact that this also drove internal efficiencies and cost saving was an added incentive.

Unfortunately, this change has also been embraced by the cyber criminals who are now presented with an expanded attack fabric. The only way cyber security departments would be able to respond is if their teams can operate at or exceeding the speed at which the adversaries operate. They would need to work collectively across the organisation – creating new collaborative partnerships with the business and becoming a key business enabler and not a support function.

Are we protecting the right areas - should we question our assumptions?

The pandemic and its associated changes have forced businesses to change tactically. This change is also semi-permanent. In the light of this, cyber security and the associated response plans need to relook at its outlay – in terms of people, technology and investment.

Traditional business continuity assumptions are being challenged. Can we continue to rely on our third-party incident responders, archival services and data centres to always function as normal? Having all the elements in a supply chain affected, used to be a 'out of design scenario' and this is now a reality that needs to be planned for.

We have seen regulation shift from preventing breaches and incidents (eg: penalties under the GDPR) to making sure organisations are able to deliver commitments made to stakeholders (eg: operating resilience requirements in the banking industry) during an ongoing attack. This makes incident response mindset change from a 'identify, detect and respond' to a 'keeping the lights on' one.

Finally, this year has also seen nation states perpetuating cyber-attacks on many industries to serve economic and geo-political agendas. This will force governments to undertake resilience planning at the sector level against nation state threats. Cyber response teams will then need to offer higher levels of cooperation, trust, transparency while working with the regulators and law enforcement. It will become even more important to also work with suppliers and competitors to ensure ecosystems less prone to failure.

Back to the basics - align the cyber security strategy to business goals

If anything, the pandemic has demonstrated the disconnect between the business perception of the value of technology and the cyber view of the risks that come with its adoption. These will align only if the identification of these risk scenarios is led by the business teams. Security needs to be an end to end priority across the organisation. To do this, it is necessary to establish an ongoing dialogue between the security organisation and the rest of the enterprise. This will help to drive synchronisation between security and the business in terms of strategic and operational planning. Ultimately security needs to move away from being perceived as an 'Information Technology' led function.

Most organisations have spent large sums of money over the last 10 to 15 years on 'IT security'. In these times, while there is a need to strengthen cyber security and response ability, the cyber team also needs to face the reality that it needs to do so without increasing the cost. The only way it can do this is by focussing on a new risk-based model focused on lowering costs by putting the right people in the right roles and to embrace technology as a part of its response function.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

A new team for the new reality

Security teams are increasingly moving to a three-line defence model. Security processes and controls embedded into the business teams form the first line of defence. The second line would be the traditional security policy, standard and guideline creators within the organisation. The third line of defence is the audit and review function. Traditionally, the second and third lines of defence have been the strong suits of cyber security teams. However, finding the right people in the first line is becoming key.

The first line of defence becomes effective only if the responsibilities and tasks related to cyber security are linked to the annual performance targets. There should be a clear line of sight to the daily activities of cyber security monitoring and response within LOD1

The second line of defence should be more of an IT risk team developing design quality, resilience and response policies and standards and report back to the board. The challenge is that in most organisations, cyber security teams tend to have two sets of professionals working on two ends of the security continuum. One set has the old school security architects who have decades of experience under their belt but haven't quite embraced the changes brought in by mobility and the cloud. The other is the leading-edge security professional – well versed on the latest technology and happy to promote and enable these while embedding security by design and at scale. Getting these two sets of professionals on the same page within LOD2 should be a priority.

Security and response professionals need to be able to 'shift left' along the product development/ acquisition methodology in order to push controls as early as possible in order to deliver maximum value and protection to internal and external customers.

What should organisations do to improve resilience and response to cyber-attacks?

First, they would need to understand that the risk landscape has changed. Both the threats to their assets and the assets themselves are now different. The organisation would need to understand risk scenarios need to be in place, and what controls are most relevant. The organisation's digital environment may have grown significantly over the pandemic as part of measures to transition to remote working. This needs to be identified. Once this has been done, the security team needs to review the controls of new and old infrastructure alike and understand if they are compliant with the policy, and to the organisation's risk appetite. The activities that are needed to close these gaps in order to mitigate the risks posed should be mapped and tracked to completion.

Second, organisations would need to work out a more efficient cyber security response and resilience approach. This may need cyber security teams to start automating their cyber and risk management processes. Threat intelligence can be leveraged across multiple functions such as fraud and financial crime. Playbooks and tooling must be synergised to respond at speed to the changing cyber threat landscape and patterns of attack. They will have to introduce engineering approaches — such as secure by design and privacy by design — that are intended to introduce security into the daily mindset of the DevOps team as they craft new applications and services. Organisations should enable security incident and event management (SIEM) tooling to cater to new working modes. Work out newer ways to manage the containment of malware when immediate access to an endpoint is not guaranteed.

Finally, having got the right skills and teams in place it will be important to communicate the connection between business enablement, business resilience and information protection. Doing this makes security everyone's business and allows for it to be a part of operations.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Zero trust security - the preventive approach

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Not too long ago, an office visit was like entering a castle. The organisation's data was managed within the enterprise and the security tools deployed helped in monitoring and protecting everything that was going in and out of the premise. The basic assumption was that we could trust the environment to a certain degree.

Post COVID, we no longer must enter an office building for work. Companies have enabled work from home wherein employees connect to the internet or via VPN channels to exchange enterprise data using hotspots, home broadband connections via shared internet via wireless home routers. The routers are further shared with family members, flat mates who tend to click on suspicious links and attachments.

There has been an exponential increase in the number of COVID 19 based theme attacks. A large number of companies, irrespective of size and having advanced cyber maturity processes and technologies, have become targets to ransom wares and data exfiltration.

Clearly, it is now the time for a new security paradigm. An environment where we Never Trust, But Always Verify. In simpler words, a security state of mind where no device, no user, no workload, no application should be trusted and a one of the many solutions to achieve this is adoption of Zero Trust.

Zero Trust is a security concept that requires all users, even those inside the organisation's enterprise network, to be authenticated, authorised, and continuously validating security configuration and posture, before being granted or keeping access to applications and data. This concept is not new, it has been around for more than 15 years, and its adoption has gained a lot of traction due to the current ways of working post COVID.

Zero trust acceptances involve building a Zero Trust Architecture and its robust implementation; it focuses on the following key areas:

Micro-segmentation

Micro-segmentation provides the capability to control workloads in a data centre or a multi-cloud environment with granular policy controls and restricts the spread of lateral threats. It provides complete control of traffic within and between segments.

Network segmentation is not new, and traditionally, network firewalls and access lists within virtual LANs were deployed to implement segmentation with static IPs and subnets. However, there are challenges and limitations to this approach, including the inability to segment and protect cloud workloads which has increased exponentially in the recent past.

Software-defined micro-segmentation has made granular segmentation at the host level a reality. A software-defined framework also allows segmentation of workloads in hybrid multi-cloud environments, enabling security teams to maintain a consistent security posture across the entire network.

This ability to define security policies at a granular, host level makes it possible for enterprises to implement zero-trust security regardless of whether the workloads/ applications are on premise or on the cloud.

Multi-factor authentication

Multi-factor authentication (MFA) is used to ensure that digital users are who they say they are by requiring that they provide at least two pieces of evidence to prove their identity. Further, each piece of evidence must come from a different source: something they know like passwords, something they have like tokens or something they are like finger-print readers.

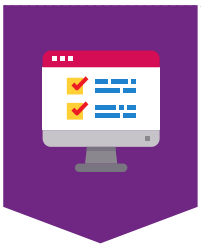
© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Application Context

Application Context filtering in firewalls or context-based access control (CBAC) are features on newer generation firewalls, which intelligently filter both TCP and UDP packets based on application layer protocol session information from either side of the firewall via deep packet inspection.

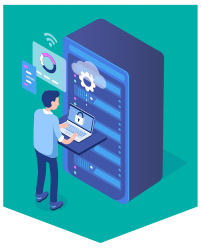
Enhancing identity and access management

Regardless of location all resources must be accessed securely. Further, it is to be assumed that all the traffic is a threat, there should be a team that inspects, verifies and authorises traffic to be secure. In real world situations most traffic is encrypted on external networks and being extended to internal networks. However, cyber criminals can easily detect un-encrypted data and therefore Zero Trust adoption will ensure security professionals while protecting external data on internet, will extend the same principle to internal networks and data.



Implementing the principle of least privilege

A robust implementation of Zero Trust means adoption and implementation of principle of least privilege (POLP) by strictly enforcing access control. It also refers to a security concept of providing user, a program or a process with minimum levels of access or minimum level of permissions to conduct job functions. A mature implementation and enforcement will minimise the temptation for people to access protected resources.



Validate all endpoints, workloads and server infrastructure

In addition to users, it is also a must that for a robust Zero Trust environment, an organisation should ensure all the endpoints and associated workloads are validated as well.

Log and analyse all security events

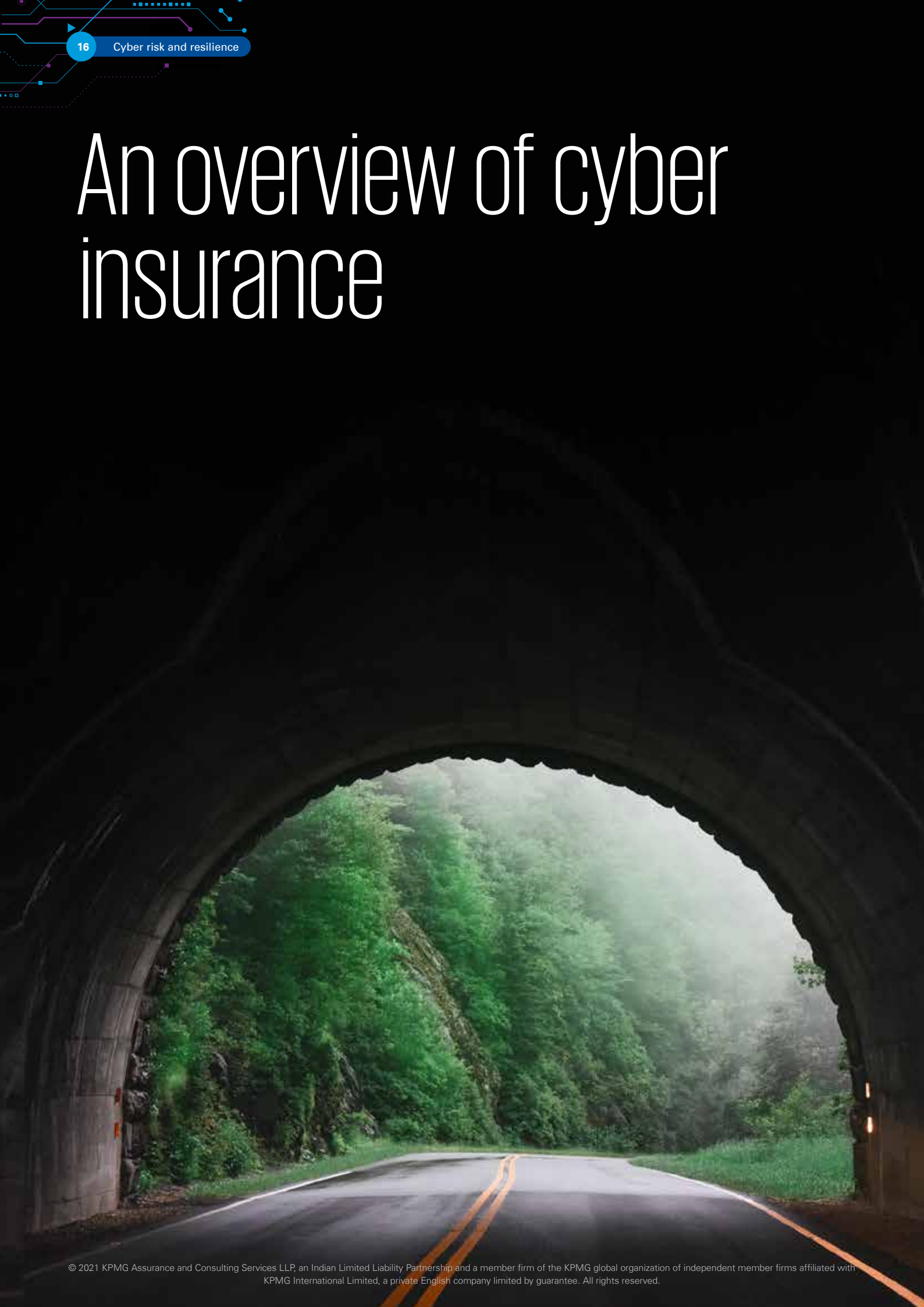
Zero Trust promotes the idea that you must be monitoring traffic as well as logging it for significant view of the network. Many security professionals do log internal network traffic, but that approach is passive and does not provide the real-time protection capabilities necessary in this new threat environment. In Zero Trust, someone will assert their Digital Identity and then we will allow them access to a resource based upon that assertion.

In conclusion, Zero Trust flips the previous thought process of "trust but verify" into "verify and never trust."

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

An overview of cyber insurance



© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

A paradigm shift

In recent times, we witnessed the impact of technology in re-defining the new 'normal' by enabling organisations to carry out day-to-day operations through remote working model amidst the pandemic. Working from home due to the current scale and complexity involved has its own set of challenges from a cyber security standpoint. Cyber criminals are exploiting this opportunity to hack into organisations, exfiltrate data, cause network disruption, etc. which has paved the way for cyber insurance to play a major role to mitigate losses due to cyber incidents and data breaches.

Introduction to cyber insurance

Cyber Insurance Policy is a risk transfer mechanism used by organisations to protect themselves from losses and expenses arising due to cyber-attacks. A typical cyber-attack could range from network interruption to data breach to phishing incident etc.

Some of the typical inclusions of a cyber insurance policy are:

- **Business interruption costs**
- **Forensic investigation costs**
- **Administrative fines**
- **Cyber extortion expenses**
- **Breach notification costs**
- **Legal expenses**

And few typical exclusions are:

- **Fraudulent act or willful violation**
- **Mechanical or electrical failures**
- **Bodily injury**
- **Property damage**
- **Loss of Intellectual Property (IP)**
- **Loss due to cyber terrorism/war**

Market outlook

Cyber insurance is gaining a lot of traction in the recent past, and there has been a significant increase in its adoption levels by organisations to cover themselves from losses arising due to cyber-attacks.

The global cyber insurance market is estimated to exceed USD20- billion by 2025 post Covid-19. In India, there has been an increase in the cyber insurance policies issued over the last year[1]. This volume is expected to increase as cyber security is a boardroom agenda across businesses due to the evolving cyber threat landscape. In countries like Australia, United Kingdom, USA etc. they have re-insurance pools which are extending to cover the losses associated with cyber terrorism.

Typical challenges in policy procurement

While most insurance products are based on decades of aggregated and actuarial data, assessing cyber risks and pricing cyber insurance products has been a little challenging because of the evolving cyber landscape and lack of statistically credible historical data for actuaries to work with. Organisations are also facing challenges to quantify the cyber risks and decide on a suitable cyber insurance cover.

1. Cybersecurity Insurance Market, MARKETSANDMARKETS, October, 2020

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Regulatory watch on cyber insurance

The Insurance Regulatory and Development Authority of India (IRDAI) had set up a nine member panel to explore possibility of a basic standard cyber liability insurance product structure. This working group in brief performed the following:

- Studied various statutory provisions on information and cyber security
- Examined various types of incidents involving cyber security in the recent past and possible insurance coverage strategies for those
- Examined the cyber liability insurance covers available in the Indian market and in other developed jurisdictions
- Explored the possibility of developing standard coverages, exclusions and optional extensions for various categories.

In many countries, the Central Banks have published new cybersecurity requirements as part of the risk management module which has mandated cyber insurance policies to be obtained. Additionally, across Europe, Latin America, etc. insurability of regulatory fines have been adopted.

What should organisations do?

- **Understand your cyber risk posture –** Organisations should undergo a cyber risk assessment to understand their cyber risk profile. The assessment should cover their scale of operations and business portfolios across geographies, regulatory and statutory obligations, third party environment, cyber incident history and information security and data privacy practices.
- **Identify the right policy –** Organisations must quantify their cyber risks to identify the right cyber insurance policy with regard to cover, inclusions, exclusions, first and third party cover, etc.
- **Periodically re-evaluate –** In a dynamically evolving landscape, cyber risks are constantly increasing and hence it is imperative to periodically re-assess the cyber posture of the organisation and accordingly revisit the cyber insurance policy.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Privacy in the age of constant connectivity!

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Impact of coronavirus and industry response

The coronavirus pandemic has resulted in an unprecedented paradigm shift among companies and people. There has been a change in the way people look at connectivity and communication. For example, the discretionary jet setting lifestyle of the yore has now been completely replaced with remote conferencing. What was unheard of before the pandemic has become the new normal. Even the biggest of the companies weren't initially prepared for this. It is now widely accepted that previously overlooked concerns related to data security and confidentiality have now come to the forefront.

So how are companies and consumers responding to these concerns?

First, there has been an increasing trend of organisations adopting new designations like Chief Trust Officer and Data Ethics Officer. These designations come with the responsibility of establishing policies, procedures and frameworks to ensure protection of employee and customer data. Both traditional industries like automobile and new age industries like digital entertainment platforms are paying attention to the concerns of data privacy.

Second, there is also an increasing awareness about the rights and responsibilities of individuals and companies in their day to day life when they are handling data of their customers or clients.

Third, starting from remote conferencing tools to secure work from home systems to data leakage prevention protocols, the companies are now beginning to adopt the right technologies which have made them frugal and effective at the same time. This has reiterated that necessity is the mother of innovation.

Key concern areas

So, what are the key concern areas where data privacy is still a concern?

First, there are concerns of violation of personal space and "Super Surveillance" by employers. This is due to the high amount of penetration of work into our homes and excessive monitoring of employees by the organisations.

Second, it is to be noted that in India, there hasn't been any practical implementation of the data privacy law which has been tabled and there is a lackadaisical nature among people in India when it pertains to their data privacy. Unlike in the Western countries, data privacy isn't being given the attention it deserves in our public discourse.

Third, there isn't an available pool of non-personal data for startups to leverage upon for their R&D purposes. But the practical challenge is on the level of anonymisation required to be performed on this non-personal data to ensure that it isn't misused by anyone.

Fourth, the legal conundrums due to the ambiguity and inconsistency in enforcement of privacy laws in different countries. Certain countries don't have any laws on privacy at all. This raises several legal challenges especially when companies process data pertaining to overseas citizens.

Addressing the key concerns

So how can the above key concerns be addressed?

One, while "Super Surveillance" of employees is a possibility, it requires huge investment from the companies. Instead of investing in "Super Surveillance", the companies should focus on adequate cyber security.

Two, it is imperative to evangelise the mindset of privacy among Indians. An awareness is required on the various rights which help us protect our personal data and on the various responsibility that we must ensure other's personal data is protected too.

Third, the concerns on the misuse of non-personal data can be reduced if the anonymisation of such data is done as per generally accepted risk assessments of the data being used. The established companies should come together and create a pool of such risk assessed anonymised non-personal data for startups to leverage upon.

Fourth, there should be uniformity in Data Privacy laws to ensure protection of personal data in any country it is processed. The lawmakers in the respective countries should abide by the established laws and adjudicate any legal challenges amicably and fairly.

In conclusion

While there are many challenges, companies should try to stay ahead of the curve by leveraging technology to address concerns of the people. They should work to build trust with their customers. But trust is a two-way street where the companies should provide the technologies, the platform and capabilities to customers where customers could trust them, and the companies trust their customers as well.

Law makers across the world should also do their part by bringing in consistent data privacy regulations for companies to abide by so that they can establish physical, technical, and administrative safeguards to ensure confidentiality customer and employee data. These safeguards would require to be effective in detecting and stopping unauthorised access to data.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Cloud security

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Adapt to survive

Digital transformation has been at the back of mind of organisations for long, however the Covid-19 pandemic has really pushed organisations to adapt and adopt digital ways of working and reaching out to customers. Organisations across the spectrum of industries from Information Technology to hospitality and education have found newer ways of working and engaging with customers. Those who have been able to adapt faster have a better chance of surviving and emerging stronger through the pandemic. And at the foundations of the digital push sits "cloud" being able to provide the flexibility, scale, reliability and speed of response required for these organisations to adapt faster.

The adoption of cloud has fundamentally shifted security context within the organisation. Traditional organisational boundaries defined by the perimeter is no longer valid as applications and data move beyond these boundaries into an extended enterprise that is no longer under the organisation's exclusive control. There have been a spate of cyber attacks on cloud environments that have brought forth risks such as identify theft, data security, cloud misconfigurations and malware in the cloud to the forefront.

Defining a strategy for cloud security

Organisations need to define a strategy for cloud security that aligns with business security requirements and helps in mitigation of associated security risks. The key elements of the strategy include:

- Developing a framework for cloud security can bring structure and consistency to dealing with security within the lifecycle of cloud adoption and operations
- Aligning the framework with leading standards like NIST, CSA CCM and ISO 27017 can help in adoption of good practices followed globally
- Identification of key risks considering the assets to be protected (applications, data, middleware, infrastructure) process supporting the governance of assets and people managing the processes
- Design and implementation of appropriate controls to protect, detect, respond and recover to cyber threats in the cloud
- Periodic evaluation of the design and operating effectiveness of controls and reporting thereof helps in measuring the current cloud security posture and planning for continuous improvement.

A holistic view of security

Due to complexity of existing environments, organisations rarely look at a big bang approach to cloud migrations. This leaves them with a mix of on premise and cloud and in many cases multi-cloud environments. It becomes imperative to look at security in holistically considering the hybrid scenario. Key factors of which include:

- Defining a security architecture for the hybrid environment
- Deployment/migration of workloads on to cloud should take into consideration application integrations/dependencies with on-prem/other cloud environments
- Identity and access management becomes key as the cloud environment moves beyond existing perimeters
- Data security and encryption take a hot seat with due considerations for key lifecycle management. Technologies like CASB can help in putting policies around data access and help the organisation in monitoring who has accessed data
- Basic hygiene factors such as patch management and anti-malware protection remain as important in cloud as it is on-prem
- Adoption of Zero Trust principles can help in making sure that end users and end points are authenticated and authorised before gaining access to cloud resources
- Monitoring by design helps in faster detection and response to security threats and aids in compliance with standards and regulations.

Challenges to securing cloud

A majority of the security breaches that have happened in the cloud are on account of security misconfigurations. Another major cause of incidents in the cloud is inappropriate control design due to lack of understanding of shared responsibility model. Managing, monitoring and securing the cloud environment requires completely different skillsets and this necessitates huge investments from organisations in retraining existing resources on cloud and/or hiring appropriate staff that can help in the implementation of the cloud security strategy.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

In conclusion

While the pandemic has pushed many organisations to move to cloud, the adoption is only going to increase as more organisations start to see the benefits. As the journey to cloud leaps forward, organisations need to look at a structured approach towards cloud security taking into consideration people, process and technology aspects. Additionally, security should be viewed holistically across the hybrid environment.

Acknowledgements

Analysis and content:

- Aditya Ghosh
- Bhumika Verma
- Iqra Bhat
- Mayuran Palanisamy
- Merril Cherian
- Ram S
- Rupak Nagarajan
- Sathya Siva Chandan Gorthi
- Sricharan Saripalli
- Sony Anthony

Brand and design:

- Nisha Fernandes
- Rasesh Gajjar
- Sameer Hattangadi

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMG in India contacts:

Atul Gupta
Partner and Head
Digital Trust
India Cyber Security Lead
T: +91 124 307 4134
E: atulgupta@kpmg.com

Sony Anthony
Partner
Digital Trust – Cyber Security
T: +91 80306 54353
E: santhony@kpmg.com

Merril Cherian
Partner
Digital Trust – Cyber Security
T: +91 80683 35524
E: mcherian@kpmg.com

Mayuran Palanisamy
Partner
Digital Trust- Cyber Security
T: +91 96000 57046
E: mpalanisamy@kpmg.com

Sricharan Saripalli
Associate Partner
Digital Trust – Cyber Security
T: +91 80306 54549
E: ssaripalli@kpmg.com

home.kpmg/in

Follow us on:
home.kpmg/in/socialmedia

Sapphire Connect contacts:

Rishi Kapoor
Associate Partner & Business Head
T: +91 22 6901 3000 (Extn:13)
E: rishi@sapphirehs.com

Ruark Jacob
Content Producer
T: +91 22 6901 3000
E: ruark.j@sapphirehs.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The views and opinions expressed herein are those of the third-party, and do not necessarily represent the views and opinions of KPMG in India.

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.

© 2021 KPMG Assurance and Consulting Services LLP, an Indian Limited Liability Partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is for e-communication only. (004_THL0521_RG)