Indian Tech 2.0 – Digital Platforms, Cloud, AI and Cybersecurity

Abstract

During the first two decades of the 21st Century, India became the global hub for IT outsourcing as Western companies off-shored their information technology requirements to leading consultancy firms such as TCS, Wipro and Infosys. India is now in the cusp of a new technology renaissance as global forces such as business digitisation, the migration of computing onto cloud platforms, the development of artificial intelligence as a business tool and the increased demands for cyber security, are now driving a resurgence in higher margin IT services and strategic consulting.

This paper explores the sources of competitive advantage that cloud platform service providers - offering artificial intelligence solutions - are currently building plus the sustainability of this newly emerging trend and the opportunities for Indian IT firms. The paper also considers how - by broadening the attack face for malicious activities – cloud-based AI is creating opportunities for Indian IT firms to develop high margin cyber security and cyber resilient software products.

Keywords: AI, cloud computing, cyber security, digital platforms.

Why is AI Cloud Computing a new source of competitive advantage?

When a company decides to migrate its data onto a cloud platform – in preference over an on-premise strategy – there are two types of value that are created. The first involves cost savings that result from higher productivity and lower technology costs per unit. However, this is what Barney (1995) referred to as a threshold rather than a distinctive capability that was necessary to satisfy minimum customer requirements. This was merely an essential requirement that justified an organisation's presence in the marketplace. It was not a core capability (Leonard, 1995) nor a was it a source of sustainable competitive advantage (Porter, 1985). However, the second source of value involves business model innovation and it is made possible through the use of artificial intelligence which can create tangible market advantages for the leading AI cloud platforms such as Google Cloud Vertex AI, Microsoft Azure AI, the AWS AI services portfolio, Alibaba Cloud and IBM Watson. Rather than pursuing low margin cost leadership strategies, it is now possible for these companies to achieve higher margin broad differentiation advantages (Porter, 1985).

According to Gartner (2022), the artificial intelligence platform market is predicted to grow at a CAGR of 32.48% from 2022 to 2029. Meanwhile, a global research survey by McKinsey (2021) revealed that a key differentiator of outperformance by cloud companies was the adoption of artificial intelligence. The AI-enabled cloud platforms outperformed the non-AI enabled companies by achieving higher profits. It found that 64% of the high performing company workloads ran AI on public or hybrid cloud, compared with 44 percent at other companies.

AI makes cloud computing considerably more effective for a number of important reasons. AI cloud combines AI hardware and software (including open-source software) to deliver AI software-as-a-service (AIaaS) on hybrid cloud infrastructure giving companies access to both AI and a broad range of AI capabilities. AI cloud democratises AI by making it more accessible. It achieves this by lowering adoption costs and facilitating co-creation and innovation. The *Bain Technology Report 2021: The New Technology Economy* (Tuck, 2021) also stated that rapid innovation in artificial intelligence was believed to have democratised AI and created opportunities for all businesses to use it as a competitive advantage.

Cloud platforms create a multiplier effect for AI adoption which in turn, makes cloud computing significantly more effective. Therefore, AI and the cloud feed-off one-another. AI enhances the quality of decision-making but also benefits from the cloud's flexibility, agility and ability to scale by increasing the scope and sphere of influence of artificial intelligence. This starts with the user-enterprise and then expands outwards into the broader marketplace or ecosystem as niche' companies (Iansiti & Levien, 2004) build applications for the platform.

Advantages and Disadvantages of AI Cloud

AI cloud therefore provides a range of valuable benefits. These include transformed IT infrastructures where automation of workload tasks using AI is accelerated. Seamless, unlimited data access is also achieved. Better data mining applications and analytics advantages are also important. Cost reductions (through improved productivity), cloud security automation and better, more timely decision making and predictability are additional benefits from AI cloud adoption leading to more prescriptive solutions.

There are inevitably weaknesses within the AI cloud systems and these include connectivity concerns. For example, cloud-based machine learning systems need to have consistent Internet connectivity. This is because the Internet is used to send raw data to the cloud service and then recover processed data. Poor Internet access can therefore hinder any advantages to be gained from the use of cloud-based machine learning algorithms. Meanwhile, although processing data in the cloud is faster than on-premise computing, a time lag occurs between initial data transmission to the cloud and when it is received. This can be a problem when prediction speed is of primary importance.

Data privacy is another concern. Since AI applications need large amounts of data - such as consumer and vendor information – this can be anonymised. However, in many instances, knowing who the data refers to makes it more valuable which raises issues around ethics and data governance.

The Platform Stack

The leading AI cloud companies are the world's largest platforms. In the US these include Amazon Web Services (AWS), Microsoft Azure and Google Cloud. In China, Alibaba Cloud and Tencent Cloud dominate the online enterprise landscape. These platform companies are configured differently to traditional linear businesses (Choudary, 2015). They are multi-sided and operate as networks upon which technology ecosystems are anchored (Moore, 1993, Iansiti & Levien, 2004). They are data-rich and they have sophisticated technology infrastructures and broad network marketplaces. Research by MIT into platform configurations (Choudary, 2015) revealed that all platforms consisted of three layers which were arranged in the form of a vertical stack illustrated in Figure 1 below.

While platforms function across these three layers, the level of differentiation or the degree to which each layer dominates over the other two may vary due to specialisation. Where the platform is strong in all three layers this is known as "filling-out the stack" (Choudary, 2015).

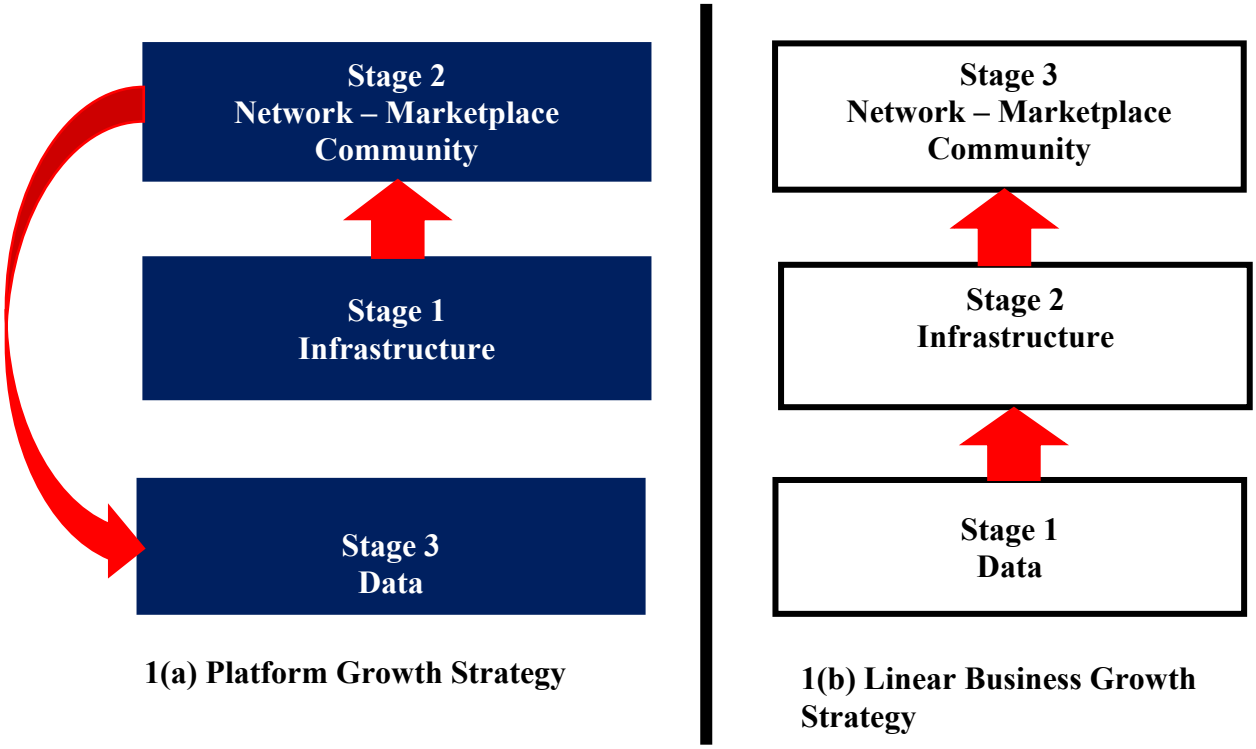

Figure 1. The Platform Stack – Platform vs. Linear Growth Strategies

The leading AI cloud companies (mentioned earlier) dominate all three layers of the stack. When building their platforms from scratch, the large Internet firms developed the infrastructure layer first (Figure 1(a). Stage 1). This consisted of the tools, services and rules that enabled interaction to take place. The next stage (Figure 1(a), Stage 2) was the development the network-market community where users interacted with the platform which generated large amounts of data

through network effects. Over time, this led to the filling out of the data layer (Figure 1(a), Stage 3) which was essential for big data analytics (see Figure 1(a) Platform Growth Strategy).

In order to respond to the threat of platform disruption, linear businesses are having to digitise and 'datafy' (Lycett, 2013) and become technology companies in their own right. However, these traditional businesses (often with on-premise computing systems) need to adopt a different approach when building a platform capability from scratch. A traditional business can acquire an existing platform, build its own platform or form a partnership with an established platform company, such as one of the large cloud computing firms. The chapter focuses on the latter, where the traditional business leverages the platform capabilities of a cloud provider by integrating with its platform ecosystem.

In order to achieve this, the firm needs to start at the data layer first (Figure 1(b), Stage 1) by ensuring datafication (Cukier & Mayer-Schoenberger, 2013) and digitisation has been undertaken and the data is of a good quality. These firms also need to restructure their internal systems to be more data-porous with internal application programming interfaces (APIs) and remove the silos that prevent cross-communication (Choudary, 2015).

The next stage is to leverage the infrastructure of an existing technology platform (Figure 1(b), Stage 2). Where AI cloud is concerned, the company may choose to integrate with an existing cloud platform and migrate its data accordingly. Where the company seeks to adopt a marketplace model it can then exploit some of the benefits of the network-market community layer (Figure 1(b), Stage 3) and become a member of the platform's broader ecosystem (see Figure 1(b) Linear Business Growth Strategy).

Amazon (USA) and Alibaba (China) are examples of companies that have built large entrepreneurial ecosystems by creating platform marketplaces where companies of all sizes can trade globally (Walton, 2022). Firms are able to establish digital store fronts as well as having their orders fulfilled by the platform which can provide a broad range of logistics functions. The data gathered by the platform is then used to provide big data analytics and AI driven cloud services for the companies that trade through the platforms. This is known as the "grid" approach (Lee, 2018) where artificial intelligence is delivered to traditional businesses as a service (AIaaS).

This enables these cloud companies to democratise AI by making it more accessible to SMEs and creates opportunities for all businesses to use it as a competitive advantage, not just an elite strategic group (Porter, 1980). This model has now been copied in India by Reliance Industries and Tata. Reliance Industries is developing a platform model using its Jio telecoms infrastructure. This is being linked to the firm's nationwide retail network to form Jio Mart. Facebook's 200 million WhatsApp users have also been given access to the platform in a bid to

drive “traffic” and monetise India’s small businesses through the development of online payment networks and e-commerce capabilities. The Tata Group, meanwhile, is developing a “super app” that aggregates the conglomerates wide range of business products and services onto a single software platform (Walton, 2022). The “super-app” is a mobile/web application that provides multiple services including payment and financial transaction processing and a marketplace with one-stop shop characteristics. These developments have obvious implications for cloud security and the resulting increase in the size of cyber-attack face.

Moreover, as AI cloud companies become increasingly pervasive across markets and industries and as their technology ecosystems increase in size, this will inevitably create issues relating to Internet connectivity and increased opportunities for distributed denial-of-service (DDOS) as more businesses (Cukier & Mayer-Schoenberger, 2013) connect to the platform infrastructures and as AI and data management becomes more open and democratised. However, these trends pose a number of opportunities for Indian technology companies to develop and implement new high margin cybersecurity and cyber resilience software products.

Threats to AI cloud companies and the Digital ecosystem

AI cloud platforms are now a dominant force in the digital world and at the centre of digital ecosystems. Platforms are disrupting every sector, whether it is commercial, government, education, finance or health. The core drivers of AI cloud companies’ growth are: the internet and digitisation; cloud computing; smart phones and apps and search on social media. This reliance on the internet and cloud computing brings organisations a number of challenges with data privacy and security. Cyber attacks and breaches are some of the biggest threats to these cloud-based companies. Even the most prestigious companies such as Facebook, Twitter and LinkedIn are vulnerable to these data breaches and attacks (Troup 2017).

It becomes imperative for these AI cloud companies to focus on secure systems and risk management to mitigate cyber crimes and protect their businesses. Although, a lot of attention is paid to securing systems from a technological perspective, cyber criminals in recent times are becoming more specialised and use deceptive techniques to carry out the attacks. These can have serious consequences to the organisation resulting in not only financial impacts and disruption to operations, but also a significant impact on reputational loss and legal consequences.

Digital security risk management and strategies are therefore vital for platform organisations to aid them in their readiness to detect, prevent, contain and respond to evolving threats in the digital environment. In the next section we will look at the cyber threat landscape, the types of threats for organisations and some measures that cloud-based companies can adopt to mitigate the attacks and protect their organisation, data and people.

Cyber Threat Landscape

In the last couple of years, since the pandemic, the world has witnessed a rapid increase of cybercrime and a burgeoning cybercrime economy. While in the past attackers had to develop sophisticated technology for cyber-attacks, in recent times cyber criminals simply rely on social engineering techniques to launch an attack. The increase in remote working has had a subsequent increase in the number of cyber-attacks, for example since the pandemic 81% of global organisations have experienced increased cyber threats. Furthermore, 79% of organisations experienced downtime due to cybersecurity risks (McAfee Enterprise and Fireeye, 2021).

The pandemic created a new model of working which has paved the way for malicious adversaries to look for novel methods to cause cyberattacks and breaches. Most security incidents have a human element and attackers are exploiting this potential to trick individuals in enabling their cybercrimes.

Social Engineering

Social Engineering, the most prolific means of obtaining sensitive information that is of use to an attacker is emerging as one of the most challenging cyber security threats in the contemporary age. Social engineering is the practice of taking advantage of human weaknesses through manipulation to accomplish a malicious goal (Aldawood and Skinner, 2018).

This usually involves manipulating legitimate users to induce them to carry out some specific action to divulge confidential information or valuable assets and normally requires no large amount of technical knowledge (Svehla, Sedinić and Pauk, 2016). The attackers using social engineering techniques target the victims based on several factors based on the amount of sensitive data that they could possibly get.

They may employ a set of attack strategies, from bulk phishing emails that deliver malicious software (malware) to scareware in order to manipulate people to reveal sensitive information (Klimburg-Witjes, and Wentland, 2021). There are many types of social engineering techniques that social engineers employ to compromise systems, to exploit people and steal information. Some of the types of attacks (itgovernance, 2022) are highlighted in Table 1 below:

Phishing:	Phishing attacks exploit human error to harvest credentials or spread malware, usually via infected email attachments or links to malicious websites.
Angler phishing:	Phishing attacks carried out via spoof customer service accounts on social media.
Ransomware:	A malware designed to deny a user or organisation access to files on their computer by encrypting the files and demanding a ransom payment for the decryption key.
Pharming:	Redirecting web traffic from legitimate sites to malicious clones.
Baiting:	Enticing victims into inadvertently compromising their security, for example, by offering free giveaways or distributing infected devices.
Scareware:	A form of malicious software – usually in the form of a pop-up that warns that your security software is out of date or that malicious content has been detected on your machine – that fools victims into visiting malicious websites or buying worthless products.
Pretexting:	The con artist gains a victim's trust, typically by creating a backstory that makes them sound trustworthy.
Diversion theft:	Offline diversion thefts involve intercepting deliveries by persuading couriers to go to the wrong location. Online, they involve stealing confidential information by convincing victims to send it to the wrong recipient.
Honey trap:	Attackers pretend to be romantically or sexually interested in the victim to persuade them to yield sensitive information or money.
Tailgating:	A physical security attack that involves an attacker following someone into a secure or restricted area, for instance, while claiming to have mislaid their pass.
Vishing/voice phishing:	A form of targeted social engineering attack that uses the phone. Types of vishing attacks include recorded messages telling recipients their bank accounts have been compromised. Victims are then prompted to enter their details via their phone's keypad, giving them access to their accounts.

419/Nigerian prince/advance fee scams:	These cons involve scammers asking victims to supply their bank details or a fee to help them transfer money out of their country. They originated in Nigeria, and the number 419 refers to the section of Nigeria's Criminal Code that bans the practice.
Water-holing/watering hole:	Watering hole attacks work by infecting websites that a target group is known to frequent. For instance, 2017's NotPetya infection – believed to be a politically motivated attack against Ukraine – infected a Ukrainian government website and then spread through the country's infrastructure.

Table 1: Attack Strategies

Social engineering can happen in one step or as part of a multi-layered tailored attack that will almost be indistinguishable from genuine interactions. Perpetrators will begin with investigating the victims, gather background information and identify potential entry points or weakest links to then launch their attack. They then gain the victim's trust and carry out the actions required for them to gain the sensitive information or access to critical assets.

The Attack Cycle

The social engineering attack process was first described by Kevin Mitnick who described it as an attack cycle of four phases (Mitnick and Simon, 2002) as outlined in Table 2 below:

1	Research: Gather information about the target. There is emphasis on the quality of the information collected which is subsequently utilised in succeeding phases and is of crucial importance in making the attack successful.
2	Developing Rapport and Trust: Different types of social engineering techniques are deployed in this phase to gain the victim's trusts.
3	Exploiting Trust: By manipulating human behaviour the attackers exploit the trust gained and stealthily acquire the desired information.
4	Utilise Information: This final phase is also referred to as "cashing in", the information gained gathered from the previous phases of the victim is used for launching the attack. The attackers then remove all traces of their attack and close the interactions.

Table 2: The Attack Cycle

Social engineering techniques and subsequent attacks are especially dangerous as they rely on manipulating human behavioural traits and preys on human psychology, rather than technical vulnerabilities. Hence predicting these mistakes by users or employees are harder for an organisation and identifying technical solutions to guard against these attacks are limited.

The economics of social engineering cybercrime services

In 2020, the social media platform Twitter was victim to a social engineering attack where hackers targeted the accounts of celebrities such as Elon Musk, Bill Gates, former US President Obama and then democratic nominee Joe Biden. The hackers used the company's customer support services to gain access to the accounts, they utilised this temporary access to solicit cryptocurrency payments from the hacked accounts' followers. This highlighted the widespread attacks using social engineering techniques (Polak, 2020). Twitter as a response ascertained that their networks were not the vulnerability but the hackers "misled certain employees" and "exploited human vulnerabilities" (Twitter, 2020). This highlights the increasing attacks on platforms as a result of social engineering breaches.

Ransomware attacks have exponentially increased since the pandemic, Cybersecurity Ventures (2020) predict that a business will fall victim to ransomware every 11 seconds. Previously cybercriminals had to develop all the technology for their attacks. The high profits that have resulted from ransomware attacks have now fuelled a new business model where hackers rely on a mature supply chain and 'purchase' specialised cybercrime kits and services.

Ransomware as a Service (RaaS) is a business model between ransomware operators and affiliates where the operators sell or lease compact, easily deployable, and scalable malware toolkits to launch the ransomware attacks (Baker, 2022). Operators use similar marketing and sales tactics that legitimate businesses employ on the regular web, to promote and sell RaaS on the dark web.

RaaS kits allow even amateur threat actors who may lack the skills or techniques to develop their own ransomware variants to purchase the services. There are different models available for these nontechnical cybercriminals to choose from the services the operators provide, who will supply the ransomware, recovery services, and payment services. The most common RaaS revenue models (Baker, 2022) are:

- Monthly subscription (for a fixed fee)
- Affiliate programs (same as the monthly subscription model but with a percent of profits)
- One -time fee with no sharing of the profits
- Purely based on profit-sharing

Most of these cybercrime markets are global in nature for example a buyer in Brazil can obtain phishing kits from a seller in Pakistan, domains from the United States, victim leads from Nigeria, and proxies from Romania (Microsoft, 2021).

Phishing

Phishing is the most common types of social engineering techniques where attackers attempt to steal personal or sensitive information by tricking victims into clicking links or directing them to

a fraudulent website. Whilst emails are the most common methods of phishing, attackers may also use other means such as phone calls, text messages or other methods of communication, including social media (NCSC, 2022). Attacks can install malware (such as ransomware), sabotage systems, or steal intellectual property and money.

Malware

Malicious software, or malware, describes any malicious program used by cybercriminals, hacktivists and nation states that is intended to steal sensitive data, disrupt operations and is harmful to systems. Malware is designed to steal, encrypt or delete data and can be in the form of executable code, scripts, active content or other software variants. Malware can even spy on a system's activity without knowledge or permission and may possess varied methods to infect machines and propagate themselves. Malware remains a dangerous and consistent threat and its success has spawned a host of improved detection and prevention technologies (CERT-UK,2016).

Malware can have damaging impacts on individuals and organisations, once they are installed they can infect devices and work towards the attackers' goals. Systems normally slow down as a result of malware, providing remote control for an attacker to use the infected machines. They then gain access to the network or unsuspecting targets and steal the sensitive information.

Phish kits on the dark web

The anonymity of the dark web providers 'phishers' to buy kits from the technically skilled phish kit authors. The phishers obtain the required infrastructure components such as a server, a domain to host the imitation site, and an email account or other endpoint to receive victim information. Once the infrastructure is assembled, they just chose their prey and "stick their poles in the water", the whole process is designed to be as easy as possible by the authors (Microsoft, 2021).

AI based cloud systems can be attacked

Adversaries use 'artificial intelligence attack' to manipulate AI based cloud systems in order to alter behaviour to serve a malicious end goal. These artificial intelligence attacks represent an emerging and systematic vulnerability with the potential to have significant effects on these companies (Comiter, 2019).

Attackers use various types of exploratory attacks against ML models to cause an integrity violation. These attackers may have not necessarily have any specific knowledge of the inner workings of the ML model but instead create changes by submitting inputs and observing the corresponding system output. This threat model is common to many AI systems hosted as a cloud service or on a consumer device (Microsoft, 2021). The other types of attacks on ML models include:

- *Evasion attack:* Attacker modifies the query in a way that causes a model misclassification.
- *Poisoning attack:* Attacker contaminates the training phase of ML systems to get intended result. The attacker wants to misclassify specific examples to cause specific actions to be taken or omitted
- Membership inference: Attacker can infer if a given data record was part of the model's training dataset or not.
- Model stealing: Attacker is able to recover the model through carefully crafted queries

How AI Cloud Companies can prevent attacks

Every aspect of our living is now intrinsically intertwined with some aspects of cloud companies. Cyberattacks and threats are the biggest challenge these companies face and also the general population. On the one hand these cloud companies invest in innovation and on the other must focus constantly on managing the risks associated with the digital transformations and advancement. Cyber breaches which required immense technological knowledge and expertise are no longer essential as attackers simply focus on human psychology and weaknesses. They merely use specialised deceptive techniques targeting individuals to gain access to systems or sensitive information. The trends of these attack patterns have significant impact on cloud companies resulting not only in financial losses and disruptions to operations but can also result in significant reputational damage.

As the frequency and sophistication of cyber threats are increasing, cloud companies have to develop a cyber-resilience strategy to prepare for a wide range of contingencies. Companies must promote cyber hygiene practices to promote a secure environment. Some of the actions they must adopt include:

Multifactor Authentication (MFA)

Multifactor authentication enhances security by requiring users to identify themselves by more than just a username and password. This makes it harder for bad actors to use brute force attacks, stolen credentials or phishing methods to gain access. Companies must ensure the MFA is authorised on all available data points, service and data classifications.

Least privilege access

Companies must apply the principle of least privilege that restricts access rights for users and accounts. This predominantly limits users to only those resources that are absolutely required. Enforcing least privilege is a best practice that prevents attackers from spreading across the network and limits user access with just-in-time and just enough-access (JIT/JEA). This is instrumental in reducing security risk and minimising business disruption that may result from errors or malicious intent.

Keep up to date

To mitigate the risk of software vulnerabilities and from being exploited, all the organization's devices, software infrastructure, and applications must be kept up to date. Endpoint management solutions allow policies to be pushed to machines for correct configuration and ensure systems are running the latest versions.

Utilise antimalware

Malware attacks can be stopped by installing and enabling antimalware solutions on endpoints and devices. Companies must utilise cloud-connected antimalware services for the most current and accurate detection capabilities.

Protect data

Companies must take account of where sensitive data is stored and all those who have access. It is vital to implement information protection best practices such as applying sensitivity labels and data loss prevention policies. If a breach does occur, it's critical that security teams know where the most sensitive data is stored and accessed and ensure that there are enough back-ups and business continuity is warranted.

Conclusion

The cloud infrastructure market continues to grow at an exponential rate. During 2021, $50 billion worth of new business was added with the market reaching $178 billion from $129 billion in 2020, an increase of 36%. The big three technology platforms — Amazon, Microsoft and Google — continue to grow at exponential rates. Microsoft and Google are growing fastest at 45% while Amazon is growing at just under 40% (Miller, 2022). Meanwhile, in China, the year-on-year growth in cloud computing was 49.7%, the highest growth rate in all regions of the world with Alibaba Cloud, Huawei Cloud, Tencent Cloud and Baidu AI leading the way (China Internet Watch, 2022).

As the leading technology platforms increase their market share in the fast-growing cloud computing market, there are significant downside risks. With the size of the cyber-attack-face increasing, due to home working and the digitisation and datafication of traditional business (Lycett, 2013) and the movement of more data into the cloud, there is a threat to further growth if the required protections are not adopted. This raises the bar for technology companies and the need for even more sophisticated artificial intelligence to off-set the increasing intensity of cyber-attacks. This also serves to increase the gap between AI cloud services and non-AI cloud. As the level of sophistication and size of attacks grows, the AI-cloud providers are in a much stronger position to increase market share and sustainable competitive advantage (Porter 1980; 1985). Both of these scenarios provide opportunities for Indian IT firms. The delivery of AI as a service

(AIaaS) via cloud platforms will require a new range of high margin analytics services whilst the growing attack face resulting from this growth will raise the bar for increased cybersecurity support.

References

Aldawood, H. and G. Skinner (2018). *Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review.* IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), . Wollongong, NSW, Australia.

Baker, K. (2022). *Ransomware as a Service (RAAS) Explained* [online] available from https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Barney, J.B. (1995). Looking inside for competitive advantage. *Academy of Management Perspectives,* 9(4). Published Online: 1 November, 1995. https://doi.org/10.5465/ame.1995.9512032192

CERT-UK Report, National Cyber Security Centre (2016). *CERT-UK Annual Report* 2015/16 [online]. available from https://www.ncsc.gov.uk/news/cert-uk-annual-report-201516

China Internet Watch (2022) *China cloud computing market in 2021; top 4 have 80% market share.* https://www.chinainternetwatch.com/30820/cloud-infrastructure-services/#:~:text=The%20overall%20market%20size%20of%20China's%20public%20cloud%20services%20reached,more%20than%2010.5%25%20by%202024.

Choudary, S.P. (2015). *Platform Scale: How a new breed of start-ups is building large empires with minimum investment.* Platform Thinking Labs.

Comiter, M. (2019). *Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It* [online] available from https://www.belfercenter.org/publication/AttackingAI#toc-1-0-0

Cukier, K. & Mayer-Schoenberger, V. (2013). The Rise of Big Data. *Foreign Affairs*, 28–40. May-June, 2013.

Cybersecurity Ventures (2020). *Who's Buying And Selling Ransomware Kits On The Dark Web* [online] available from < https://cybersecurityventures.com/whos-buying-and-selling-ransomware-kits-on-the-dark-web/>

Downes, L. & Nunes, P.F. (2013). Big Bang Disruption. *Harvard Business Review.* March, 2013.

Ducci, F. (2020). *Natural Monopolies in Digital Platform Markets.* Cambridge University Press.

Gartner (2022). *Top Strategic Technology Trends for 2022* https://www.gartner.com/en/information-technology/insights/top-technology-trends/top-technology-trends-ebook

Iansiti, M. & Levien, R. (2004). *The Keystone Advantage: What the New Dynamics of Business Ecosystems Mean for Strategy, Innovation and Sustainability.* Harvard Business Review Press.

IT Governance (2022). *What is Social Engineering?* | Techniques & Prevention [online] available from https://www.itgovernance.co.uk/social-engineering-attacks

Klimburg-Witjes, N. and Wentland, A. (2021). 'Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses', *Science, Technology, & Human Values*, 46(6), pp. 1316–1339. doi: 10.1177/0162243921992844.

Leonard, D. (1995). *Wellsprings of Knowledge: Building and Sustaining the Sources of Innovation.* Harvard Business School Press.

Lee, K-F. (2018) *AI Super-Powers: China, Silicon Valley and the New World Order.* New York, Houghton Mifflin Harcourt.

Lycett, M. (2013). 'Datafication:' making sense of (big) data in a complex world. *European Journal of Information Systems,* 22: 381-386.

McAfee Enterprise and FireEye (2021). *A Look Ahead To 2022: McAfee Enterprise & FireEye Predict Top Cyber Threats* [online] available from < https://www.fireeye.com/company/press-releases/2021/look-ahead-to-2022-mcafee-enterprise-fireeye-predict-top-cyber-threats.html>

McKinsey (2021). *The state of AI in 2021.* December 8, 2021. https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/global-survey-the-state-of-ai-in-2021

Microsoft (2021). *Microsoft Digital Defense Report* [online] available from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

Mitnick K. D. and Simon W. L. (2002). *The art of deception: controlling the human element of security,* W. Publishing., Ed. Indianapolis: Wiley Publishing.
NCSC (2022) *Phishing attacks: defending your organisation* [online] available from https://www.ncsc.gov.uk/guidance/phishing

Miller, R. (2022) Cloud infrastructure market soared to $178B in 2021, growing $49B in one year. *Tech Crunch*. https://guce.techcrunch.com/copyConsent?sessionId=3_cc-session_9f2a671a-74d4-4f41-8b64-26dc50b2bda5&lang=en-US

Moore, J. (1993). *The Death of Competition: Leadership & Strategy in the Age of Business Ecosystems.* Harper Business.

Polak, N (2020). The Twitter Hack Shows a Major Cybersecurity Vulnerability: Employees. *Slate Magazine*, July 21. Accessed January 30, 2021. https://slate.com/technology/2020/07/twitter-hack-human-weakness.html.

Porter, M. E. (1985). *The Competitive Advantage: Creating and Sustaining Superior Performance.* Free Press.

Porter, M. E. (1980). *Competitive Strategy.* Free Press.

Svehla, Z. L Sedinić, I. and Pauk, L. (2016). *Going white hat: Security check by hacking employees using social engineering techniques,* in Proc. 39th Int. Conv. Information and Communication Technology, Electronics and Microelectronics (MIPRO '16), Opatija, Croatia, pp. 1419–1422.

Troup, E. (2017). *Platforms are increasingly key to cybersecurity* https://inform.tmforum.org/features-and-analysis/2017/05/platforms-increasingly-key-cybersecurity/ Imperva (2021) Social Engineering [online] available from < https://www.imperva.com/learn/application-security/social-engineering-attack/>

Tuck, A. (2021). *The Bain Technology Report 2021: The New Technology Economy.* Bain & Company. November 03, 2021. https://aimagazine.com/ai-applications/bain-technology-report-2021-new-technology-economy

Twitter (2020). *An Update on Our Security Incident and What We Know so Far.* July 30. Accessed January 30, 2021. https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html.

Walton, N. (2022). Digital Platforms as Entrepreneurial Ecosystems and Drivers of Born-Global SMEs in Emerging Economies, in: *International Entrepreneurship and in Emerging Markets: Contexts, Behaviours and Successful Entry*. Jafari-Sadeghi and Dana, L-P. (eds.). Routledge Publishing.