



## **CFO Perspectives**

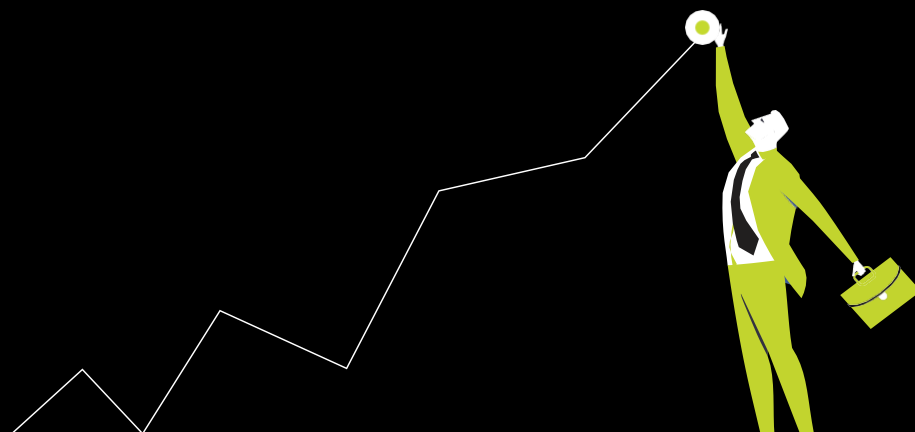
India | CFO Newsletter | November 2020

For private circulation only

# CFO Speaks



**Mr. Piyush Gupta**  
Group CFO and CEO,  
Strategic Investments,  
HT Media Ltd.



**1 During the COVID-19 pandemic and lockdown phases, how deeply has the media industry been impacted, especially with printed newspapers not reaching consumers (and most of them having moved towards digital), and loss in advertising revenues?**

We are still navigating through the challenges and it is far from over for us. Many societies are not allowing newspaper deliveries till date, and as a result, subscription has gone down. Just like the travel and hospitality industry, the print media industry has also been affected. During the first lockdown phase in March 2020, we lost around 80 percent of print subscription business and that had a deep impact on our revenues. Currently, our subscription is back to 70-75 percent, which is not close to the normal business scenario. We see a major fall-out in English subscription due to increasing COVID cases in the metro cities and restrictions imposed by the societies. However, we have seen an increase in Hindi subscription in the last few months.

Certainly, we have been losing advertisement revenues due to less subscription and also, because companies have significantly cut their marketing expenses. The recent festive season (Diwali) was good where we saw advertisement revenues coming back to 60-65 percent of normal, however, it was far away from the festive season business we do in normal years. Advertisements from FMCG business are coming back with time, but Real Estate is not seeing any signs of recovery and their challenges have led to a decline in advertisement revenues coming from the sector.

Needless to say, the pandemic has disrupted the print media. Digital too has impacted the business, and people have changed their preferences, with quite a few customers moving to digital newspapers. Having said that, we will have to now look for new opportunities per the changing customer preferences.

**2. What do you think are the current challenges for the media industry and how soon will the industry return to previous levels? Will some things change forever (like digital)?**

We will not come to pre-COVID levels any time soon. It is important to understand that consumer preference and the business model are now changing. Until now, the advertisements used to subsidise the cost of news, and technically, it used to reach the readers free of cost. Going forward, I don't think the credible news industry can sustain itself solely on advertisement revenues, and I personally feel that in the coming times, readers will have to pay for credible news. As a result, subscription costs will go up, as advertisements can support only a certain percentage of the cost incurred.

The business and industry are continuously evolving, and things are in perpetual transition. Digital has been there for years, and people have transitioned before too. The only thing that has happened during the pandemic is that digital transition has been fast-tracked. Yes, many people have moved to digital during the pandemic and digital is here to stay. That is why we say, business models will change. We cannot have free digital news forever and

we need to start charging for news on digital platforms too. Further, we will have to customise our offerings based on customers preferences, and the readers will receive and pay for news items of their interest areas only. We have seen that many media houses in the western world have started charging for digital news, and people have accepted it as the new norm for quite a few years now. This is bound to happen in India too, and COVID-19 pandemic has just accelerated the entire transformation process.

**3. Technology revolution is transforming the business and industry today. How important you think is the role of technology in the media industry and how are you planning to ride on it in the coming future?**

Technology has been supporting the media sector for a very long time. We have invested in many technology products in our company too. It is essential to follow readers' changing preferences and offer them our services in the way they prefer, and now we see that the consumers are moving towards digital. Thus, we are fast-tracking many of our technological interventions to see how best we can bring a richer experience for our readers. We have the advantage of our strong balance sheet and thus, we can finance our own ambitions. We did face challenging times in the past few months, but we do not have any liquidity issues and we are investing in digital assets which will start giving us healthy returns once the business returns to normal. Sometimes, it gets tough to evaluate and track these digital investments because of the nature of valuations in technology businesses. Hence, we focus more on solving real problems of our consumers and satisfying their requirements by providing credible news at regular intervals.

**4. Your company has done a few acquisitions in the last fiscal year and this year too (like buying stakes in Next Media Works and News Corp). As a CFO, what strategic advantages you think these investments will bring to your organisation?**

At the time we acquired Next Media Works, radio was a value business on the stock market. We have been in the FM industry for 13 years now. However, the radio business got impacted in the wake of the COVID-19 pandemic, and the impact was more than the print media business, since the companies did not have marketing budgets and advertisement revenues fell down. Thus, due to the current pandemic, it did not yield us the desired results. Investing in News Corp was a good opportunity for us, as prices came down sharply during the pandemic and we did the acquisition at a lower price than what we had planned earlier. I feel, we have acquired a good asset, and when the world becomes normal, we can monetise it well. The business should have better synergies in the near future, especially for our Mint newspaper.

The media industry has been in a transformation phase for a decade now, and we are also in the process of transforming. We have invested in FM and digital, which has given us good returns. Further, once we get ourselves completely right with the digital transformation bit, backed with credible news, we will certainly enhance the experience for readers. Going forward, these newly acquired businesses will create a lot of opportunities for us in the long run. The journey will take time, but once we have loyal readers supporting us and understanding the value we bring to them, the business will certainly benefit.

**5. Lastly, as a CFO:**

**i. What was the most challenging decision you had to take during the pandemic?**

We did not have liquidity issues, but still I feel 'liquidity management' was a time-consuming activity, and it required a lot of attention and detailing. Till date, it consumes a lot of time while looking at balance sheets and operational expenses, and we do not know how long this pandemic scenario will last. We also took some tough decisions on cutting operational costs to ensure business efficiency. In addition, we started working on our transformation journey for the next two years. For example, we are working on picking new assets which will help us when the market returns to normal. However, during these tough times, our treasury business has outperformed. It has improved with RBI intervention, reduced repo rate, and subsequent policy measures from the Government.

**ii. What would be your top three priorities as we enter to the "new normal"?**

As we enter the new normal, my top three priorities will be:

- Conserving cash
- Strategising new business and kickstarting growth
- Ensuring the right mix and match of the above two priorities

**iii. What was your personal learning during these tough times?**

Personally, I feel that the toughest of human spirits has been tested during this pandemic. The human spirit is much stronger than what we had thought. People have been on streets to run the show despite the pandemic, and this is really fascinating. It helps us come out stronger and more determined than ever before.



# Expert views

## Will 2020 redefine the cybersecurity ecosystem for the Banking industry?

The year 2020 has been quite challenging for Indian banks when it comes to cybersecurity. After the onset of the COVID-19 crisis, banking operations disrupted severely as banks struggled to provide uninterrupted services to their clients during various stages of lockdowns. In the following months, they accelerated their digital transition efforts (such as digital banking and remote access to employees) to ensure contactless business operations. With a surge in digitisation, banks also witnessed a spike in cyberattacks as cybercriminals found new opportunities and vulnerabilities.

With a new norm ushering in since the COVID-19 crisis, banks will have to keep a foot on the accelerator, and continue with digital transformation to sustain and thrive during and after the pandemic. This will also mean banks are likely to continue to experience rising financial frauds as digital attacks surface increasingly. Rising cyber threats after COVID-19 pose serious concerns for Indian banks and the Reserve Bank of India (RBI). What makes the challenge acute is that different banks are currently at varying stages of digital transformation and cybersecurity maturity levels determined by their past investments, budget allocation, and size in terms of customer outreach and service offerings. To cope with the challenges associated with COVID-19, bank executives will have to embrace new digitisation and cybersecurity norms, and meet business requirements, irrespective of the cybersecurity maturity levels of their banks.

## Cyber-related challenges: part and parcel of digitisation

Banks' foremost agenda in boardrooms has been the digitisation of voluminous confidential data and banking processes (not limited to payments). This urgency has put the spotlight on digital technologies, such as cloud, Artificial Intelligence (AI), analytics, Internet of Things (IoT), and Machine Learning (ML). With technology transformation, confidential information will be saved in remote servers and made ubiquitous. Higher digitisation and remote operations will lead to increased vulnerabilities and open up opportunities for cybercriminals, exposing banks to breaches or hacking. Cybercrimes can be multifaceted; here are a few examples:

- **Cloning of digital identities:** Involves manipulating existing audio, photos, and videos that look real and can cause ethical and legal concerns
- **Malware contagion:** Purposely designed software to cause damage to a network, computer, or server without the owner's knowledge
- **Advanced persistent threats:** Where an infiltrator or unauthorised user enters a bank's systems or network undetected and remains there for an extended time period with the intention to steal financial and personal data, cyber-money laundering, ATM, and credit card frauds
- **Social engineering:** Includes phishing and other malicious actions accomplished through interactions and psychological manipulations that trick users to perform security mistakes or give away information





## Tackling the cybersecurity challenge will be key

To stay relevant and competitive, banks will have to meet stakeholder expectations while preventing threats and adhering to regulatory requirements, by improving their cyber-defence efforts. As banks increasingly focus on moving resources on digital platforms, they should expect higher and more sophisticated attacks. These attacks will shift from in-house devices to those hosted on digital platforms accessed by different stakeholders, and directly target end-users' computing environments. Banks will have to proactively tackle cyber risks from various aspects of security – data, application, identity, infrastructure, and cloud – as well as administer end-user education and regulatory compliances. They have to constantly address security gaps, plan a security roadmap, assess and benchmark best practices, and make strategic investment decisions in cybersecurity core domains in line with business needs and risk appetite. Therefore, banks must build a robust security threat-monitoring mechanism by implementing “state-of-the-art” solutions.

Banks can mitigate cyber risks by adopting the below recommended seven-step approaches:

- **Prioritising cybersecurity assessment**
  - A continuous threat assessment using a risk-based approach
  - Cybersecurity maturity assessment
  - Bridging the gaps
  - Integrating cyber risk assessment with fraud risk and financial crime reporting
- **Securing remote access control**
  - Enabling server-based computing and digital workspaces
  - Deploying zero clients and thin clients
  - Reviewing remote connectivity solutions and security governance
  - Deploying advanced and robust authentication and authorisation
  - Deciding on the scope of services that need secured access
- **Tightening access to third-party services**
  - Prioritising access to services for alliance partners and vendors, as well their availability
  - Restricting or controlling their access to the core infrastructure
  - Exploring the possibility of modifying contractual agreements to monitor third-party access to banking infrastructure

- **Contracting or outsourcing cybersecurity capabilities**

- Dealing with shortages of cybersecurity professionals using leading-edge services of third-party security providers
- Considering outsourcing a myriad of cybersecurity functions, such as security operations and insider-threat detection (including threat hunting and threat intelligence)

- **Adopting advanced technology solutions and tools**

- Creating many lines of defence at different levels in the security ecosystem
- Adopting defence options for threat intelligence and response capabilities, such as zero-trust architecture, advanced endpoint security systems, and augment cybersecurity with AI

- **Raising awareness through training**

- Introducing formal training programmes on cyber threats, and cybersecurity practices for employees
- Involving different methods to educate employees
- Developing cybersecurity culture at every level and viewing it as a continuous process

- **Bolstering security through threat identification and response competencies**

- Integrating a modern and evolving security infrastructure while digitising
- Embedding security, confidentiality, and policy checks into their DevOps decisions and actions

## Cyber challenges for tomorrow

Banks will possibly adopt technologies such as mobile, cloud, remote access, and IoT, not out of choice but out of the need to sustain business during the pandemic and thrive thereafter. Such transformative digitisation will also result in an increased attack surface. For bank executives, the focus will be on achieving business goals even as they recalibrate strategies to address the ever-evolving cyber risks. Thus, banks will have to prioritise and invest in cyber defence to create an agile and resilient infrastructure of the future. Such an infrastructure will address the current cybersecurity risks and prepare itself for cyber challenges of the future. However, for that to happen, the initiative has to come from bank executives and board members who set goals and allocate budget. Accelerating cyber capabilities to match the speed of digital transformation will require executive attention, prioritisation, budget, resources, and governance. Only the leadership can drive such a change. Banks' leaders will decide the degree of agility, pace of change in infrastructure, and collaborative efforts required towards building cybersecurity of the future.

To read or download the complete article, please [click here](#).

# About Deloitte's CFO Programme

The CFO Programme brings together a multi-disciplinary team of Deloitte leaders and subject matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The programme harnesses our organisation's broad capabilities to deliver forward thinking and fresh insights for every stage of a CFO's career – helping CFOs manage the complexities of their roles,

tackle their company's most compelling challenges, and adapt to strategic shifts in the market.

For any feedback, suggestions, or additional information, please write to us at [incfo@deloitte.com](mailto:incfo@deloitte.com)





Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

This communication prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP) contains an interview by Mr. Piyush Gupta in his individual capacity. This material (including any information contained in it) is intended to provide general information on particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information herein is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect you or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

©2020 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited

**This is a private communication and not transferable.**

Click [here](#) to unsubscribe.