CFO Perspectives
CFO Speaks

Mr. Rajesh Gopinathan
Chief Financial Officer
Tata Consultancy Services Ltd

1. **Given the changing technology environment, what in your opinion, are the key emerging digital trends that would impact the business in next 2 years?**

   First and the foremost is the general digital world which has accelerated the trend of technology in any industry. The level of technology has moved from service enablement of industries to now provide differentiation and customization. The second important aspect is sequence of digitization. Digitization has moved up multiple levels from within the company systems to interface backward (with suppliers), to interface forward (with customers), to now customer to customer interface. Social media has become an important platform for decision making for consumers. Given this, the need of business to connect with consumer through social media has increased significantly. In this probabilistic world, tolerance for ambiguity should be higher and need to constantly change plans would be greater. Businesses currently are at a point of perpetual disruption. Technology is replacing manual interventions, the processes and tools including finance need to unwind transactional control and work as enablers for business growth. The investments and returns are to be looked from a different lens now. The pool of

investments and returns need to be collectively evaluated rather than matching of standalone investments and returns.

2. **Technology companies are being constantly confronted with increasing exposure to cyber risks. What steps should an organization such as yours take to counter these risks?**
   With the increasing technology use and digitization, there is no doubt that the exposure to cyber risks have increased. Digitization is the need of the hour and no company can avoid it. It is important for organizations to have robust compliance systems in place. Having said that, organizations need to have high risk tolerance with strong vigilance systems. The one common platform or interlinked systems increases efficiency but at the same time increases threats. Multiple level of fault triggers are required to be placed in systems to avoid failures. Analytics, specifically the predictive analytics, would be the key to manage these risks effectively.

3. **Dealing with millennials is a challenge and an opportunity – especially in the age of Gen Y and "liquid workforce". What strategy should a CFO adopt to convert this challenge into an opportunity?**
   Getting the right mix of people in a workforce is a challenge. The key to motivate entry level Gen Y is to offer the growth and a structured career path. The clear visibility of career path along with the realistic expectations is important to attract and retain talent in the current environment. For the mid- level workforce, it is important for an organization to communicate and equip workforce with the new skill sets and expose them to more business oriented roles. The role of a CFO entails communicating regularly with his team and align them with the organizations goals. The way to manage the challenge is to constantly offer the opportunities to learn and grow at different levels of the business.

4. **Being a global organization in the rapidly changing environment, regulatory compliance has become a greater challenge. How do you ensure that regulatory compliances are effectively managed?**
   Regulatory compliances are there to stay and constantly change. Presence in multiple countries means managing different compliance requirements and a high compliance risk for organization like us. The number of jurisdictions do increase the number of compliance transactions but the simplicity of business

model is an enabler in managing these risks effectively. Fully integrated systems along with the single governance model has been our way to tackle the multi-dimensional challenges in this space. The risk monitoring has to be strong and seamless to avoid faults affecting our systems.

5. **With the constant changes in global environment coupled with policy changes in the country, the role of a CFO has expanded multi-fold. What are the key challenges you face as a CFO and what would be the top 3 priorities for your finance team for FY2016-17?**
   The role of finance is expanding but at the same time focus is changing. The key challenge a CFO is facing currently, is to align the finance teams with the businesses to help them achieve growth. It is important for finance professionals to become business partner and act as a catalyst. Finance needs to work closely with business and unwind the transactional control to reduce bottlenecks in the system. The second important key is to manage multiple internal and external stakeholders. A CFO needs to see business challenges in a positive way and help business in creating value by proactive & transparent communication and build trust with the business. The third challenge is to manage risks. With the current environment, business risks are constantly changing and increasing and it is important to minimize or manage these business risks by increasing controls and decreasing manual interventions. There is a great need of predictive analytics for the effective risk management. As a whole CFO needs to release the transactional control and work with business for strategic growth.

Expert Views

Cybersecurity: The role of a CFO

"As the world is increasingly interconnected, everyone shares the responsibility of securing cyberspace."
— Newton Lee, Counterterrorism and Cybersecurity: Total Information Awareness

Introduction
Cyber risk is among the most complex and rapidly evolving issues companies must contend with. With the increasingly omnipresent nature of mobile technology, cloud computing, and social media, reports on major breaches of intellectual property, customer data

and proprietary information, and of damages to organizational IT infrastructures, have also become increasingly common. As a result, this has made cyber risk a high priority on the agenda of management, boards of directors and audit committees.

As a key part of the management team, the CFO has the primary job of funding, enabling and executing the organization's business strategy and ensuring business decisions are grounded in solid financial criteria. This involves financial assessment of overall risks affecting the organization. As part of the risk assessment exercise, the CFO is often expected to assess cybersecurity risks, align cybersecurity strategy with business strategy and get buy-in from the board on necessary cybersecurity investments.

A comprehensive cybersecurity plan also requires an appropriate culture and tone at the top. These encompass an awareness of the importance of security extending from the C-suite to the professionals in each function, since breaches can occur at any level and in any department.

What is the role of a CFO?

Effective cybersecurity governance and management is the product of multiple layers of defense. CFO should ensure that business understands the need for effectiveness of cybersecurity controls.

1. **Governance & management:** Companies that are good at managing information security risks typically assign responsibility for governance of their cybersecurity program to the highest levels of the organization. Management has ownership, responsibility and accountability for assessing, controlling and mitigating cybersecurity threats. As part of the management team, CFO should ensure that the cybersecurity risks are appropriately identified, their criticality and financial liabilities assessed, and mitigation and remediation strategies are appropriate invested in.

2. **Support to risk management and compliance functions:** Risk management functions facilitate and monitor the implementation of effective cyber risk management practices by management, and help risk owners in reporting adequate risk-related information up and down the firm. The most common impediment to developing an enterprise-wide cybersecurity strategy is a lack of understanding of cyber risks and potential impacts of a breach. Establishing cyber security awareness and developing comprehensive cyber security strategy thus becomes

a key responsibility of the CFO supported by Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

3. **Enabling collaboration:** As stated earlier, cybersecurity is a collaborative effort. Companies that manage cybersecurity well have collaborative groups working together. CFO is in a unique position to demand collaboration from business, with the following contributions from each:

    - Business should hold accountability and ownership for data protection. They should continually be involved in and review the risk assessments and audit findings, and approve policy and program changes in line with changing cyber security requirements.
    - IT has ownership of, implements and manages the cybersecurity tools, such as the firewalls, antivirus software, password controls, mobile device management, etc.
    - Legal partners in terms of consultation, and they approve the various cybersecurity policies that are implemented. They also report on compliance for any legal or regulatory obligations.
    - Talent is involved in communicating to, and training the organization, in partnership with IT. And they also approve, and are consulted in terms of policies, because they own a significant portion of employee information.

CFO should work closely with the CIO, the CISO and the various teams to help implement the strategic objectives of the organization's cybersecurity program. This involves the preparation and implementation of cybersecurity policies and procedures, which may be required by law, as well as incident response plans, which are a best practice in any event. The collaborative effort should also produce metrics that the audit committee/ board can use to evaluate cybersecurity effectiveness.

Conclusion

Cybersecurity is, thus, a business issue that exceeds the boundaries of IT, and needs to be managed with as much discipline as financial processes. Both the technical nature of the threat and the amount of attention cybersecurity demands calls for the entire management involvement.

Yet, organizations have acknowledged a lack of expertise on cybersecurity issues. To bridge this, undivided attention is required from the CFO to implement and oversee effective cybersecurity

program. To be effective and well-balanced, cyber-defense must be secure, vigilant, and resilient.

About Deloitte's CFO Program
The CFO Program brings together a multidisciplinary team of Deloitte leaders and subject matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The Program harnesses our organization'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 more information feedback or suggestions, please write to us at: **incfo@deloitte.com**

Deloitte makes an impact that matters