The 11th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 10th -11th 2016

CIO, RESPONSIBILITIES AND CHALLENGES

SHERAZ Azhar Ali

Pakistan Armed Forces

Abstract:
Chief information officer (CIO) is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. In simple words he is bridge between the management and technology. The chief information officer at one organization could have an entirely different set of responsibilities from the CIO of any other organization keeping in view the tasks and roles. However, in all the cases, the job of CIO's is to innovate, collaborate, balance the IT budget and motivate IT staff.
Key words: CIO, Manager, responsibilities, challenges.

1. Introduction

Chief information officer (CIO) is a job title commonly given to the most senior executive in an enterprise responsible for the information technology and computer systems that support enterprise goals. In simple words he is bridge between the management and technology. The chief information officer at one organization could have an entirely different set of responsibilities from the CIO of any other organization keeping in view the tasks and roles. However, in all the cases, the job of CIO's is to innovate, collaborate, balance the IT budget and motivate IT staff. Generally, the CIO reports to the chief executive officer, chief operating officer or chief financial officer. CIOs work closely with their IT staff and recent studies show there is a benefit in strengthening the CIO-CMO (chief marketing officer) relationship. According to IBM's Global C-suite Study, which was published in 2014, companies at which the CEO, CIO and CMO work more closely together than with other C-level executives tend to outperform competitors. The CIO also has a close relationship with the chief financial officer (CFO) -- in fact, that's the strongest relationship between CIOs and other C-level execs, according to IBM. After the CFO, the CIO has close relationships with the CEO, CMO, chief supply chain officer (CSCO) and the chief human resources officer (CHRO). In military organizations, they report to the commanding officer.

2. The evolving role of the CIO

The CIO role traces its lineage to the late 1950s and 1960s when businesses began to incorporate computing into business operations. According to authors Jeanne W. Ross and David F. Feeny in their 1999 study, "The Evolving Role of the CIO", first-generation IT leaders were typically senior or middle managers in what businesses called the electronic data processing department or, later, the information systems (IS) department. The report, published by the MIT Sloan School of Management, refers to this time period as the *mainframe era*, an interval spanning roughly from the 1960s to the early 1980s and so named for the mainframe computers procured by enterprises to, among other large

computing tasks, automate back office processes. According to Ross and Feeny, these data processing/ IS managers of the mainframe era were rarely involved in determining the enterprise's IT strategy (let alone business strategy), preferring to let the dominant vendor (usually IBM) set the course. The main responsibility of these early IS managers was to deliver new IT systems on time and on budget and run existing systems with "a high level of reliability".

In the mid-1980s, the CIO role was primarily a technical job. As the storage, transmittal and analysis of electronic information became more important to industries of all types, CIOs have come to be viewed as key contributors to formulating strategic goals. In many companies, CIOs report directly to the Chief Executive Officer (CEO), and at some companies, the CIO sits on the executive board. An important component of the CIO role is *to educate executive management and employees on the business value and risk IT systems of an enterprise*.

As a result of their increased strategic responsibilities, CIOs in large organizations typically will delegate the oversight of day-to-day IT operations to a technology deputy, Chief Technical Officer (CTO), and rely on a team of specialists to manage specific areas of IT. In a 2015 survey of 2,810 CIOs by the consultancy Gartner Inc., nearly half of CIOs globally said they have a "Chief Operating/ Technical Officer of IT" in place who performs this function. The authors of the Gartner report, "Global Perspectives on Flipping to Digital Leadership: The 2015 CIO Agenda," note, however, that the title of the role "varies enormously" as does the prevalence of this structure geographically and by industry. For example, 60% of CIOs in Asia have a COO/ CTO of IT, according to the Gartner polling, compared to only 34% of CIOs in North America.

CIO is a difficult job. And to perform this job efficiently, CIO must have proficiency in establishing IT services framework and IT security policies, ability to recruit/ direct IT staff members, aptitude for customer engagement analysis and mastery at establishing strategic service provider partnerships alongwith the skills for project management and budget management.

The Need For CIOs.

In other businesses, CIOs form a key part of any business that utilizes technology and data. In recent times, it has been identified that an understanding of just business or just IT is not sufficient. CIOs are needed for the management of IT resources as well as the “planning of ICT including policy and practice development, planning, budgeting, resourcing and training”. In addition to this, CIOs are becoming increasingly important in calculating how to increase profits via the use of ICT frameworks, as well as the vital role of reducing expenditure and limiting damage by setting up controls and planning for possible disasters. Computer weekly magazine highlights that “53% of IT leaders report a shortage of people with high-level personal skills” in the workplace. In this way, CIOs are needed to decrease the gulf between roles carried out by both IT professionals and non-IT professionals in businesses in order to set up effective and working relationships.

Here I will give an example from my own field regarding evolution of technology and CIOs. In military, there are a lot of presentations required to be delivered at different levels. Initially presentations were prepared in good hand and delivered on “Paper Charts”. Then came the era of “Computers” and “View Graph”; transparencies were prepared and view graphs were utilized for presentations. A need was felt to have some technical expert in the unit to look after these computers and view graphs. And then came the era of “VPS” and “Power Point”, which totally changed the concept of presentations from very simple black and white to more interesting and colorful. With the induction of VPS and power point, status and importance of technical expert was further raised in the units. With the passage of time need was felt to shift to “Paper Free Environment” and utilize modern

gadgets for communication and planning purposes. A separate branch, "IT Branch" was raised in the army and specialist cadre of officers (Information, Communication and Technical Officers (ICTO)) with the requisite qualifications were inducted with the mandate to install "Office Automation System" in the Army so as to provide paper free regime. In the first step all correspondence was shifted to computers centrally linked with intranet of army. In second phase "Planning" aspect was also added to the system and now we can plan any operation on the computers without needing huge maps and operational rooms with reduced time and fewer efforts. The topmost boss of this organization is called "Director General IT" but it has the same roll and duties which are performed by CIO.

2. Roles and responsibilities

1. Roles and Responsibilities Assigned to CIOs.

The Chief Information Officer of an organization is responsible for a number of roles which as follows:

a. Advice and Assistance to Senior Managers. Provide advice and assistance to senior managers on IT acquisition and management. He is the linchpin between management and IT.

b. CIO as Business Leader. The CIO must fulfill the role of business leader. As a CIO must make executive decisions regarding things such as the purchase of IT equipment from suppliers or the creation of new systems, they are therefore responsible for leading and directing the workforce of their specific organization.

c. Organizational Skills. The CIO is 'required to have strong organizational skills'. This is particularly relevant for a Chief Information Officer of an organization who must balance roles in order to gain a competitive advantage and keep the best interests of the organization's employees.

d. Recruitment of Staff. CIOs also have the responsibility of recruiting, so it is important that they take on the best employees to complete the jobs the company needs fulfilling.

e. Development of IT Architecture. Develop, maintain, and facilitate implementation of a sound and integrated IT architecture. CIOs are directly required to map out both the ICT strategy and ICT policy of an organization. The ICT strategy covers future proofing, procurement, and the external and internal standards laid out by an organization. Similarly, the CIO must write up the ICT policy, detailing how ICT is utilized and applied. Both are needed for the protection of the organization in the short and long term and the process of strategizing for the future.

f. Managing all IRM Resources. Promote effective and efficient design and operation of all major IRM processes for the agency, including improvements to work processes.

2. CIO has following duties:

(1) To assess requirements for personnel regarding knowledge and skills needed to achieve performance goals that have been established for IRM.

(2) To assess extent to which all managers at the agency meet those requirements

(3) To develop strategies and specific plans for hiring and training

(4) To report to the Division head on progress made in improving IRM capability.

3. Competence Areas for CIO. Federal Council for CIOs have defined following 10 competence areas for CIOs:-

a. Policy. CIO is the linchpin between Company and IT. He should be competent enough to understand company's vision and goals to formulate IT policy, Enterprise Architecture, for the company.

b. Strategic Planning. CIO deals with almost all the departments and is involved in all planning processes of the company. Therefore, he must have broad vision and thinking mind to articulate strategic plan for IT in support of operational plans.

c. Performance and Result Based Management. Being at top managerial post and IT head of the company, CIO must be competent enough to ensure performance and result based

management in the IT department. He may have long-term goals but he must be delivering result based short term objectives to keep his and his under command team relevance with the company.

d. Process Improvement. Technology is changing at the rapid pace, therefore, CIO must keep himself updated and busy with the continuous process improvement to increase the profit of the company.

e. Capital Planning and Investment. Being the chief of a department, CIO have to run his department, plan for infrastructure improvements and hiring of specialists, therefore, he must have good skills in capital planning and investments.

f. Leadership Management. Today's IT environment is different and to run his department effectively, CIO must have good leadership traits. Some of the traits which must be included in the personality of CIO are:

(1) Must always be self aware.

(2) Should always continue to learn and grow.

(3) Must have ability to work through other people and delegate responsibilities.

(4) Must have good communication skills.

(5) Must be authentic and decisive.

(6) Should be adept at problem solving.

(7) Must have sense of humor and integrity.

(8) And must create collaborative and safe-to-fail environment in their departments.

g. Technology Assessment. CIOs must have good eye to assess the changing technology and need for it in their company.

h. Security. Now everything is related with the provision of data through IT, therefore, CIOs must be very sensitive to the security aspects of their departments.

i. Architecture. They should be good in Enterprise Architecture skills to provide workable IT framework for the company.

j. Acquisition. They must have good acquisition skills to buy latest, effective and economical technology for their departments.

4. Challenges Faced by CIOs. Challenges being faced by CIOs are enumerated below:-

a. Managing or Replacing Legacy Systems. It is extremely difficult to accept and adapt change. As an IT leader, CIO is likely to work with people
from all departments and walks of life. The first challenge for any CIO is to clearly articulate and master his communication skills to brief and convince all stakeholders about importance of IT and his portfolio. He should be able to convince all stakeholders to adapt to the latest changes and replacing the old system with the changing technology.

b. To Create And Manage Change. Once the stakeholders are convinced that the world of technology is changing at a blinding pace and there is a need to go for change from old legacy system to IT, than CIO must take it as a challenge to adapt to new technology and keep him abreast with the changes all the time. Whether it's mastering cloud computing, big data or IT outsourcing, it seems like there is never a break from learning. Changing the posture of the IT function from an operational necessity to a strategic element is the highest priority here. The ability to create change in the corporation's operating and business processes, for both efficiency and competitiveness, is also commonly sought. Business process reengineering and continuous process improvements are on the minds of many CEOs, especially in tougher economic conditions.

c. Having a Solid Knowledge of Business and Industry. If CIO focus specifically on the technology without knowing what the business objectives are, they are not going to be in the best position to know how best to leverage technology. They really need to understand the business problem the company is trying to solve to be able to recommend how the technology can be leveraged. When you spot a trend, it's tempting to jump on the tech bandwagon. This is the natural instinct of good technical people. The successful CIO will first build a compelling business case before recommending an investment in latest-and-greatest technology.

d. Obtaining Adequate Funding for IT Programs and Projects. A CIO has to be effective at building effective relationships in support of IT initiatives with agency senior executives (Agency Head, CFO, Etc.) and getting people onboard with his vision and solutions. CIOs need to be able to articulate the value proposition of any given project and align various people, departments and vendors around a common goal to obtain adequate funds for the IT programs and projects.

e. Formulating or Implementing an Enterprise Architecture (EA). CIO is the main architecture of IT plan in the company. To architect, he has to have a firm grip on the company vision, goals and long/ short term objectives. Only then he will be able to provide an Enterprise Architecture for the company and ensure it's implementation. This is the most important challenge for the CIO.

f. Hiring, Developing and Retaining Skilled Professionals. After conceiving the enterprise architecture, one of the most important challenge for the CIO is to recognize, secure and retain good people to implement his architecture. It's impossible for a CIO to know and understand everything within the range and scope of technology. Accordingly, high marks be given to CIO candidates who hire people who are smarter than they are and spontaneously promote and substantiate their prowess in this area.

g. Simplifying Business Processes to Maximize the Benefit of Technology. It is a fact that technology can simplify business processes to improve performance, drive efficiency, save costs and ultimately become more effective for the profitable business. Ongoing pressure to cut costs year after year and innovate and integrate new technologies for the business profit is another challenge which is encountered by CIO.

h. Aligning IT and Organizational Mission Goals. This challenge is always a cornerstone of the CIO. To complement organization with technology, CIO must understand the vision of the company. Only than specific facets of technology, such as ERP, Web infrastructure, e-commerce, CRM, sales-force automation, data warehousing and so on, can be integrated with the business and benefits could be accrued from them.

i. Creating Data Interoperability Across Agencies. CIO is the person who is dealing with almost all departments of the company. He has to ensure that accurate and timely data is available to all sections of the company to increase efficiency and reduce time and cost.

j. Developing Agency-wide IT Accountability. As the head of ICT, CIO is responsible for the IT audit and accountability. He has to keep himself abreast with his under command team all the time to avoid and mis-management in IT.

k. Balancing Information Sharing and Security/ Privacy Requirements.There is a very delicate and hairline difference between information sharing and compromising with the security / privacy of clients. Therefore, CIOs must have a good vision about the affairs of the company so as to strike balance and not to offend customers, clients and senior management.

5. Risks involved. Cyber space is expanding all the time and technology is integrated with everything. Information Technology is complicate, dynamic, polymorphic and evolving all the time. Once you shift your business to technology, it means that you are open to all and there are chances of cyber attack, i.e, hackers leaking/ stealing your important data or due to some reason incapacitate you for a certain period of time. We have the example of "Estonia Cyber Attack 2007", when they were under cyber attack from Russia and their all important departments went "Off Line". One can imagine the amount of confusion and chaos in the government machinery of Estonia during that period. Since there is only one cyber space, therefore, no one can have sovereignty in their business if they are using the technology through cyber space. To further understand the types of risk involved using technology through cyber space, it is important to understand "Types of Cyber Attacks" and they are as follows:

a. Information theft. This is done to get important data regarding functioning of a company or state. At lower level it may be to steal your important R&D (Research and Development) formulas and at state level it may the important strategies, decisions or secrets of state.

b. Information flow disruption. Like the example of Estonia Cyber Attack 2007 already discussed above, hackers may cause disruption to the flow of information to your company or state and paralyze your system of functioning at critical timings. This may cause your company or state to dilemma of in-activity and irreparable losses.

c. Information manipulation There is a possibility that hackers may enter into your system of functioning and manipulate the data to provide you with wrong information at critical junctures. This may affect the decision making process at various levels and jeopardize your business at lower level and policies at state level.

6. Keeping in view the Cyber Space and Types of Cyber Attacks as discussed above, risks encountered by CIOs of different companies can be categorized in three main categories, 1st is Financial and Recruitment Aspects, 2nd is Software and Technological Aspects and 3rd is Security Aspects. All are discussed as under:-

a. Financial and Recruitment Aspects. Being the top manager of IT, CIO must fulfill the role of business leader. He has to make executive decisions regarding things such as the purchase of IT equipment from suppliers or the creation of new systems along with hiring and retaining of capable staff. They are, therefore, responsible for leading and directing the workforce of their specific organization to run the infrastructure. Risks involved in this aspect are as under:-

(1) Maintenance of Finances. Being the business leader of IT, CIO has a lot of funds at his disposal to erect IT infrastructure. Risk of pilferage in finances or selection of wrong IT equipment by CIO can't be ruled out.

(2) Recruitment and Retention of Professionals. Being a new field, professional personnel are very difficult to be found. And if found, are difficult to be retained. Being the Chief Selector of IT personnel, huge responsibility lies upon CIO to recruit suitable staff for his department, organize required training cadres for the staff and ensure their retention through appropriate packages / rewards.

(3) Development of Policy and Strategy. Stream lining and development of IT policy and strategy in lines with the CEO's business vision and mission is another important task of CIO. To avoid the risk of failure he has to minutely understand the "Business Vision" of CEO to frame IT policy/ Strategy. Any clash or contradiction between IT policy and business vision may have serious implication on the overall business process of the company.

b. Software and Technological Aspects. Risks involved in this aspect have been amply covered above under "Types of Cyber Attacks", however, to put more emphases following is re-iterated:-

(1) Cyber Attacks.Since there is only one cyber space which is open to all, therefore, breach of firewalls and threat of hackers getting into the system and stealing or compromising important information / data regarding the company policies can't be ruled out. It is the major risk which is encountered by CIOs in the present times.

(2) Technical Breakdowns. Technical breakdowns in the shape of power failure, technology failure and malfunctioning of software may compromise the complete project. CIOs have to face this risk all the times and have to prepare themselves to respond to any technical breakdown in the shortest possible time.

c. Information Sharing Vs Security/ Privacy. Since CIO is responsible to integrate all the departments of company, therefore, he deals with almost everyone. In the discharge of his duties, he has to maintain and ensure difference between information sharing and security/ privacy. There is a risk involved that while integrating different stakeholders, aspect of security / privacy may be compromised while providing information to different stakeholders.

7. Suggested Response to the Risks Encountered by CIOs. Being dynamic and evolving nature of IT, defense against cyber attacks may not be possible as of today as defender may not see the same attack twice. However, chances of cyber attack may be minimized by ensuring following suggested security measures:-

a. Have Designated CISO(Chief Information Security Officer). Have a dedicated and efficient CISO to look after the security aspects of IT only.

b. Change Passwords Frequently. Ensure secrecy and frequently changing of passwords in your company.

c. Share information on need to know basis.

d. Cyber Security Seminars. Hold "Cyber Security Seminars" in your company on regular basis.

e. CERT. Constitute a "CERT" (Computer Emergency Response Team) for managing the crisis during some technical failure or cyber attack in some cases. CISO may the head of CERT.

f. Duplicate Storage of Data. If possible, have duplicate storage of data at different location so that incase data is compromised at one location it is available at other location and working efficiency of the company is not affected during this period.

g. Security Clearance of IT Staff. Must carryout regular security clearance of IT staff designated on important IT tasks through a reliable security agency.

4. Conclusion

So we can conclude that with the fast evolution of technology, where every business has a need for some sort of IT support or service. That fact is a reflection of the value of what technology can do to improve performance, drive efficiency, save costs and ultimately to become more effective. There is a compulsion rather than a need to convert to IT environment. To have effective ICT regime, we need competent CIOs to have strategic alliance between IT equipment and goals / objectives set by CEO. So at the end we can summarize following take home facts:-

a. Every business will require an IT setup, hence will require a senior ranking IT manager.

b. IT manager, CIO, must have intimate knowledge of business along with substantial IT knowledge to become the bridge between business operations and IT setups.

c. Being operating in the same cyber space business IT of a company is open to cyber attacks from anyone.

d. Being complicate, dynamic, polymorphic and evolving nature of IT, defense against cyber attacks may not be possible as of today as defender may not see the same attack twice.

e. Adoption of security measures may reduce the chances of cyber attacks but can't eliminate them.

f. Composition of "CERT" (Computer Emergency Response Team) may prove fruitful in managing the crisis during some technical failure or cyber attack in some cases.

g. Since we moving fast towards "Artificial Intelligence", therefore, it is most likely that CIO may be considered to be the most important appointment after CEO and may be designated the role of Deputy CEO.

References:

[1] Chief Information Officer, Wikipedia.
[2] 16 Traits of Great IT Leaders By Rich Hein.
[3] Top 10 Qualities Executives are looking for in a CIO by Mark Polansky.
[4] 6 Skills, Habits and Traits of Successful CIOs by Rich Hein.
[5] Top ten leadership qualities of successful CIOs by By Karen Kidd.
[6] Cyber Security Seminar by "**Kenneth Geers"** at DRESMARA with effect from 27 – 28 October 2016