

4 Reasons Why CIO's Lose Their Jobs

Silverton Consulting, Inc. StorInt™ Briefing



Introduction

The CIO is a very demanding position. If it's not out of control projects, technology failures, or tightening budgets taking up their time, something equally troublesome will emerge. As a result, many CIOs have come to expect a reduced incumbency, handling all this IT chaos, chance, and circumstance.

Every year or so some CIO very publicly loses their job. Often job dismissals can be predicted. Aside from outright illegality or being close to exiting executives during regime change, most discharges result from failure to perform position duties. Nevertheless, the **four examples below** all have some steps that can be taken to help avoid the pitfalls that lead to shortened job tenure.

1. Security breaches

First and foremost, security failures seem to occur almost monthly. For instance, recently several thousand account credentials were posted online, ten million credit cards were compromised and backup tapes with millions of social security numbers were stolen, all that just within the last twelve months.

The fact is most large server networks have significant vulnerabilities from un-patched servers to inadequate passwords and everything in-between. It only really takes one exposure and a determined foe for a serious security breach. Currently, one's human resources are just as likely to lead to a security lapse as system vulnerabilities.

So who is to blame? Sometimes it's backup vendors at fault. But often it's just inadequate training, leaving system administrators who fail to secure servers properly or engineers who develop insecure software. Nonetheless, in large security breakdowns, the CIO is always held responsible. The most recent example of CIO job loss for security breach would be Utah's Department of Health CIO but only a few are publicized. ¹

2. Project boondoggles

The next most recurring reason for CIO termination is large project failures. These significant IT projects, outsourced or internal, never seem to complete or if they do, fail to deliver on promised functionality. They may range from a few million-dollar application alterations to billion-dollar system rewrites to replace software that evolved over decades. Not all such failures receive publicity, many get cancelled long before completion and are rarely known outside an organization. But all of them incur significant expenditures before being scrapped.

¹ May 15, 2012 Government Technology

Frequently, the bigger the project, the higher the likelihood of failure and outsourcing sometimes makes it worse. Large projects fail for a number of reasons such as, significant cost escalation, inadequate project management and underestimating technology or other risk factors.

Often the fault lies with a number of people, for instance project management, system architects and software developers to name just a few. Also, accountability can cut across internal and external organizations involved in any project. However, the CIO normally gets blamed for all such catastrophes. CIO terminations for project failures generate plenty of press, as these mostly involve government organizations, e.g., the recent resignation of UK's NHS CIO. ²

3. Availability failures

Another periodic reason cited for CIO sacking is disaster recovery (DR) failures. Disasters are encountered for many reasons but the problem occurs when IT cannot recover critical services in a timely fashion.

There are many issues in most recovery failures. More often than not, DR plans exist but just haven't been updated. Occasionally, IT encounters unanticipated failures. These usually result in ad hoc recovery plans designed and executed in the moment, but also may result in outright recovery failure.

A few groups must share responsibility for DR failures, starting with BC/DR teams, operations staff and last but not least, facilities. CEO conversations about mission critical system being down are especially trying and often unduly spotlight IT actions alone. Oftentimes, the CIO always seems to receive most of the heat for such availability outages. Instances of CIO firing for availability failures are rarely publicized but one older study indicated that the number two reason for CIO dismissal was inability to recover from disasters. ³

4. System collapse

Another infrequent occurrence of service loss is due to system failures. This time outages occur not because of disasters but due to the inability to scale system performance. The company finally gets lucky or rather, worked hard enough to hit the right social wave, and generates more activity than ever believed possible. As a result, one's well-designed systems, servers or networking seriously slow down or worse yet, seize up and stop operating from the massive overload. Recovery from such events is seldom fast enough to salvage the situation.

² June 11, 2011, ComputerWorld UK

³ August 1997, CIO magazine

With the rise of social media, viral advertisements have become an irregular occurrence. But corporate promotions ultimately depend on data center applications and IT systems all have some sort of designed in limits. When they perform outside these boundaries, results are unpredictable.

The guilty exist throughout the enterprise. Marketing and/or sales devised the promotion, seeded social media and hoped for the best. System architects and sometimes implementers were well aware of what the application could and couldn't support. In any event, the CIO is ultimately held accountable for such outages but it's just as likely a matter of chance that led the system to give out. CIO termination for system outages are infrequently publicized but one example is Bursa Malaysia Bhd CIO's resignation following technical failures in their trading system. ⁴

What CIOs can do to remain employed

Again, CIO positions are very precarious at best. Nonetheless, there are certain remedies that can be used to lengthen one's tenure on the job.

If data privacy is important, increase security to match

To combat cyber attacks takes a concerted, methodical long-term effort. As such, proper information security is a multi-faceted endeavor that includes activities such as keeping systems patched/updated, changing passwords frequently and training personnel on information security. Implementing firewalls, data encryption and monitoring system/user activity won't suffice alone. Also, contracting outside services to test IT security can help. As always, security policies and procedures must be developed and maintained in conjunction with application evolution and new system deployments.

When failures occur and they will policies must be enforced consistently throughout an organization, regardless of who's at fault. Allocating time and effort to all the aforementioned security solutions is good but training is paramount. Eventually, security must become yet another ongoing daily IT activity that must be mastered just like system maintenance, backups and facilities management. Only then will one's data center start to be secure.

⁴ July 19, 2008, New Strait Times

Large, complex projects are inherently risky, mitigation is essential

To manage risks, large projects must be split up into smaller deliverables. Also the riskiest aspects of new projects need to be scheduled first, not last. Professional project management helps but the whole project needs to develop a deep understanding of what's being changed, what's not and where pitfalls lie. Finally, there are many reasons to outsource but one problem with doing so is that external manpower seldom knows as much as internal resources.

CIO's must assign a project czar. This person needs to have enough technical depth to understand the project's key risks but also sufficient leadership skills to manage and monitor it effectively. Next, hold periodic, in-depth reviews with the czar and their team. These reviews should be correlated with stage gates, if not more often. Include outsiders to try to attain an independent assessment of the project. Ultimately, CIOs must keep close tabs on large projects, that way if needed, directions can be changed quickly before costs become excessive.

Disasters happen, understand the risk and plan for recovery

Facilities together with IT staff must periodically and methodically go through all the risks of potential natural/man-made outages. Through this process they can assign probabilities and devise actionable recovery plans for most of them. With the highest risks addressed, some of the less probable ones should be safeguarded as well. Next, outsourcing portions of DR activities can sometimes help. Having hot, warm or cold sites available can minimize alternate site equipment worries. Lastly, DR plans should be maintained often but must be updated and tested whenever applications or systems change.

First, CIO's must fund the development and maintenance of data center DR plans for critical systems. Also, they should institute some form of systems change management that can help to insure that DR plans are updated as applications evolve. Finally, CIOs need to devote adequate resources to periodically test DR plans and correct them when problems occur.

Design services to scale, where needed

It's almost impossible to predict with any likelihood which if any promotion will go viral. However, system scale-ability issues seldom arise without some warning. So, tracking and trending daily system activity across data centers and service vendors can be used to see one's weaknesses. Once identified, creating infrastructure that can scale quickly can be accomplished today using compute cloud or service provider solutions. Perhaps someday soon, software will be available that can help to scale applications across private and public cloud services as well.

Often the CIO or their staff have visibility into high profile promotions and should be able to predict which systems will be impacted. Armed with this knowledge, it's only prudent to have additional resources available to handle the potential load. But in the long run, recognizing susceptible systems and funding scale-able revisions for them is the only real fix to this problem.

Summary

The CIO position is inherently hazardous. However, with a little foresight and concerted activity to address security exposures, large project risk, disaster recovery, and scaling issues, one can avoid the most likely situations that lead to shortened tenure. Yet, there are many circumstances outside the realm of a CIO's responsibilities and sometimes these may impede productive pursuits. Nevertheless, IT success or failure often depends on actions directly under their control and as such, with proper care CIO's should be able to enjoy a long and productive employment.

Silverton Consulting, Inc. is a Storage, Strategy & Systems consulting services company, based in the USA offering products and services to the data storage community. Ray Lucchesi is the President and Founder of Silverton Consulting.