HOW TO DO YOUR JOB AND STAY OUT OF JAIL

AS CIOS GAIN MORE RESPONSIBILITIES, THEY ALSO ATTRACT MORE PERSONAL RISK.

BY **JAMES FRANCIS** | PHOTO: **123RF.COM**

As a CIO, what are the risks you face on a personal level? What liabilities are waiting in the wings in case things go wrong? What are the dark horses and swans that should keep you awake at night?

These turn out to be very broad questions. As business technologies embed themselves deeper and wider across companies, overlapping with different functions, departments and strategies, CIO roles have become more complicated and unpredictable. The job of a CIO is continually being redefined around the purpose of the business they serve, which means there's no answer for everything.

But there are a few things CIOs should consider if they want to make sure legal action, fines and even jail time don't cross their career paths.

THE BIG PICTURE

In all likelihood, a CIO occupies a high-powered position in a company, namely through seats on the board or directorships. These are where they must be most careful, says Paul Esselaar of Esselaar Attorneys.

"The risk of personal liability in terms of a company is a very real one. If I was a CIO, that would be my steady worry."

A CIO is likely in the firing line if the company misbehaves. For example, if two directors are found to cook the books, the other directors can be held accountable as well. Yet CIOs are often saddled with job specifications that don't take this into account. Esselaar says it happens often: a job spec will not give CIOs enough room for general oversight.

"If a CIO's job description does not allow for a portion of that job to be oversight and training on company-wide issues, that's a big red flag. That means the job expects them to spend 100% of their time as a CIO. As a director, you can't do that. It introduces major personal liability."

One highly visible example is the failure of Aurora Empowerment Systems, where the directors were fined R1.5 billion for the death of the company. Even if some of those directors may not have been involved, they are liable.

FINGERS IN PIES

Combine the responsibilities of high-level leadership positions with the mutually exclusive role technology plays in business and it's clear CIOs really need to have a tie to all the other business areas. Fortunately, that plays in both directions: in many cases, direct liability can land on other leaders. The CEO is most often the target if things go bad, with arguably the CFO and COO in tow. Those individuals rely heavily on technology and the CIO to make sure their backs are covered as far as governance and legislation are concerned. CIOs should leverage this to build strong channels of communication with different departments.

Lack of clarity and communication is a big issue, says Esselaar: "Perspectives differ between departments. They may want quick implementation, but not the necessary failsafes. They just want it immediately and don't wait for factors such as business continuity."

Such lapses can cause serious governance gaps, which can lead to direct liability. Staying on the same page is crucial if the CIO role is also a key leadership role.

DON'T LAZE ON LEGISLATION

Compliance is a hotspot for legal trouble. The King III framework uniquely spends an entire chapter (chapter 5) on IT governance. But compliance duties extend beyond that: RICA, FICA and ECTA are all examples of acts that rely on technology to implement properly.

> "IF A CIO'S JOB DESCRIPTION DOES NOT ALLOW FOR A PORTION OF THAT JOB TO BE OVERSIGHT AND TRAINING ON COMPANY-WIDE ISSUES, THAT'S A BIG RED FLAG."
>
> **Paul Esselaar**, Esselaar Attorneys

But the most overarching piece of legislation to arrive is PoPI (Protection of Personal Information Act). Very few companies and sectors are exempt from PoPI and anything from customer to employee information falls under it. It is very important that CIOs and other leaders pay close attention to the relationships PoPI and other acts create, says Dr Peter Tobin, director of Peter Tobin Consultancy, which helps companies manage governance and compliance.

"Let's say an employee's e-mail is intercepted by their manager without consent. That's actually a violation unless it was stipulated in the employee contract. Another example is the risk from suppliers: do your suppliers have access to sensitive company and personal information? If their actions result in a breach or some other compromise, who is liable? Don't assume it will be on them. CIOs must realise that the contracts and policies of their company will dictate those outcomes."

In the same vein, CIOs can't assume their companies have their backs. Define where internal liability starts and ends. Acts such as PoPI expect companies to have created a single policy view, and assessed risks both inside and outside, then adjusted policy and contracts to mitigate those.

"CIOs should be able to implement policy and training. They need to speak a different language and be part of interdepartmental cooperation."

But there's a big silver lining here, adds Tobin. If implementing acts like PoPI is seen as a cost exercise, it will likely be underfunded. But approach compliance as a competitive advantage and it will be easier to get the budget and support for implementation.

"PoPI is actually 20 years in the making and lags behind European privacy legislation. If your company wants to do business in Europe, it needs to meet those standards. So this can be a positive: how does compliance make a company more competitive and attractive? Legal action and fines are not the biggest threats. When the UK telco group, TalkTalk, was hit by multiple breaches, the real damage came from their falling stock value and losing thousands of customers."

Compliance is a journey and will vary based on the sector and size of a company. So spin it into a positive business strategy and use that to your advantage. Create a generally positive culture around compliance and a lot of personal liability concerns can fall to the wayside.