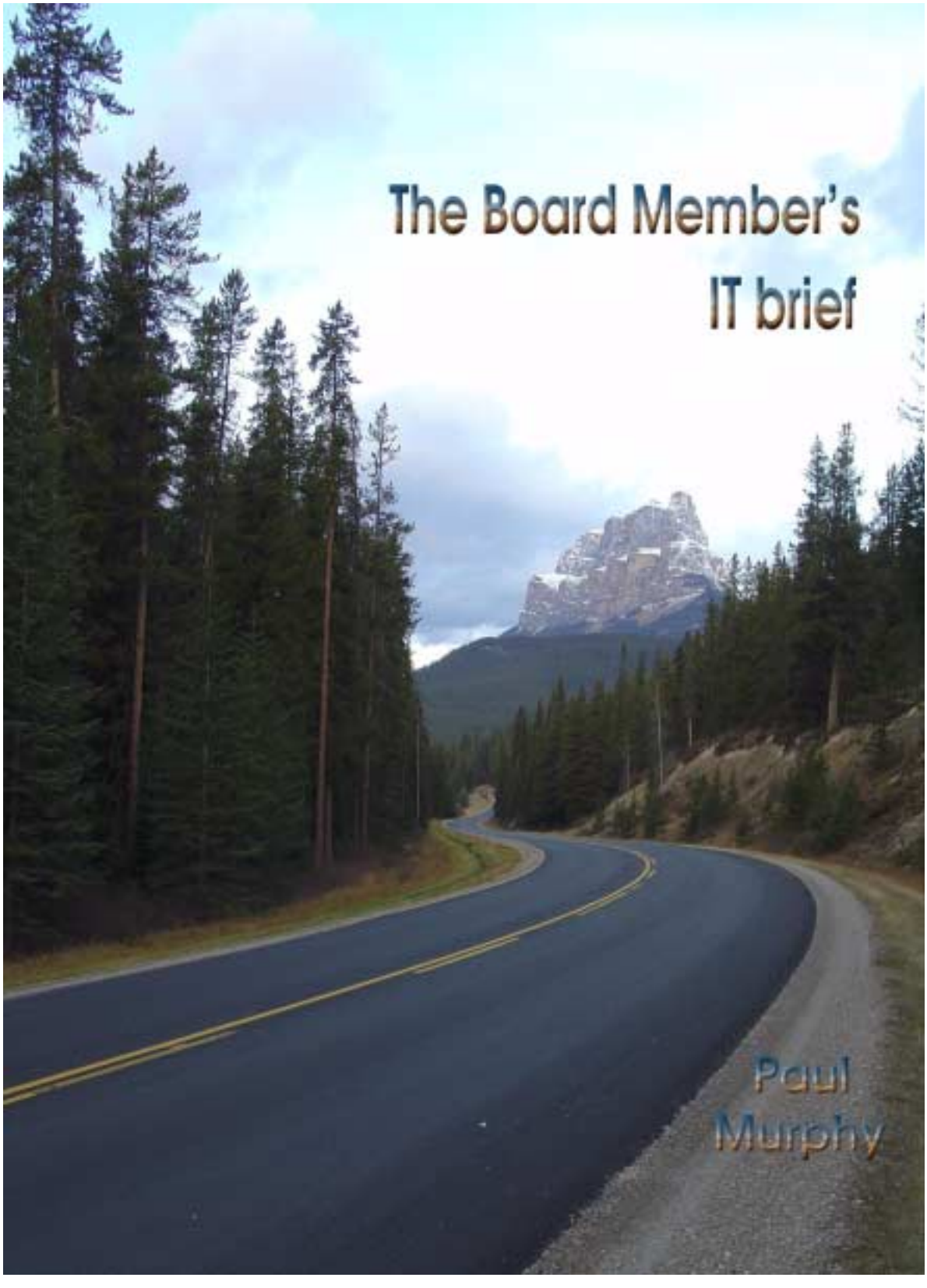
The Board Member's
IT brief
Paul
Murphy

The Boardmember's IT Brief

Paul Murphy

murph@winface.com

The board Member's IT Brief

By Paul Murphy

First Edition: Oct. 2006 . Printed in the United States.

ISBN 0-9689004-0-3

Notice

By necessity, given the nature of the thing as a book of opinion and criticism, this book names names, discusses prices, and gives my opinions on the performance and value of various products. Obviously:

1. all brand names, product names, web site names, and related materials as used in this book are, or may be taken as, trade names, service marks, trademarks, or registered trademarks of their respective owners; and,
2. while every precaution has been taken in the preparation of this book neither the publisher nor the author assumes any legal responsibility for errors or omissions, or for damages arising from the use or distribution of the ideas and/or information, contained herein.

Contents

1 Introduction 1

2 Two Key Concepts 3

2.1 Information Integrity 3

2.1.1 One term, many meanings 3
2.1.2 “The real deal” is found in Shannon’s Model 4
2.1.3 An Example 5
2.2 Information Architectures 6

2.2.1 The consequences of culture 13
2.2.2 There’s no such thing as a pure play 14

3 Evaluating IT Proposals 19

3.0.1 Special Financing 27
3.0.1.1 Mergers and acquisitions 27
3.0.1.2 Business and purchase opportunities 29
3.0.2 Large IT Project Proposals 31
3.0.2.1 And, furthermore 36
3.1 Strategic IT Plan 37

4 Hiring Systems Management 41

4.1 Rule Zero: alignment 41

4.2 Rule One: For Unix: hire a leader; for others: hire a manager 44

4.3 Rule Two: Buy Techies with Trust and Freedom, not dollars . 46

5 Questions 51

5.1 Topic one: disaster avoidance 53

5.1.1 Mainframe and Client-Server Architectures 54
5.1.2 Unix Architectures 56
5.2 Topic Two: Maintaining Information Integrity 57

5.2.1 Mainframe and Client-Server Architectures 57
5.2.2 Unix Architectures 59
5.3 Topic Three: Personal Role 59

5.4 Topic Four: relationships 60

5.4.1 Mainframe and Client-Server Architectures 60
5.4.2 Unix Architecture 61

Chapter 0 : Introduction

The audience for this book is the board member or senior executive who occasionally has to vote yeah or nay on information systems related decisions.

Readers are envisaged as non technical, facing decisions in a governance context, and willing to spend some time getting those decisions right.

Brief is the senior management companion to two other decision guides:

1. The Unix Guide to Defenestration is intended for information technology [IT] professionals. The guide's focus is doing the systems job right by choosing the right people, the right tools, and the right processes, to efficiently deliver high quality systems services.

2. Business Information Technology: Foundations, Infrastructure and Culture, is intended for students and non technical employees who need to work effectively with technical staff. BIT's focus is on helping readers understand the cultural and organizational backgrounds driving technical people to the decisions they want employers and colleagues to ratify.

Brief has four main sections:

1. **Chapter one introduces two critical "conceptual complexes" -** terms that are widely used in IT but whose meanings are little understood and become subject to hot dispute among members of the key IT communities when explored.

2. **Chapter Two focuses on Evaluating IT Proposals**. It looks at the major kinds of IT decisions board members face, and focuses on helping readers recognize and understand the "tells" that distinguish certain losers from possible winners.

3 **Chapter Three: focuses on hiring systems management.** It looks at the problem of who to trust in the context of hiring a CIO and helps readers assess the impact a candidate's ideas and behaviors are likely to have if set loose in their organizations; and,

4 **Chapter Four** discusses some key questions your IT management should be able to answer to your satisfaction.

Chapter 1
Two Key Concepts

1.1 Information Integrity

1.1.1 One term, many meanings

When PC users talk about “information integrity” they’re generally using the phrase as a $10 replacement for the word “security” - itself a term that has a unique meaning in their segment of the IT industry. Specifically, the PC community has a long history of susceptibility to data theft and software failure, either caused internally or through an outside agent such as a thief or a network hacker. As a result “security” to them refers mainly to measures taken to counter or diminish such attacks.

Thus PC software intended to prevent thieves from recovering data on stolen gear, to keep hackers out of networks, or to scan incoming e-mail for attack code is all described as “security” software in private and often as part of an “information integrity assurance” program in meetings with bosses.

In the IBM mainframe and Unix environments, where PC style security concerns are a non issue, “security” usually refers to physical security - ensuring that locked doors are locked and back up tapes aren’t lost.

Although members from all three groups will sometimes use the term “information integrity” when considering compliance issues such as those associated with the American Sarbanes-Oxley act or, more recently, the civil discovery rules, this isn’t (yet) very common. Instead these issues tend to be discussed as compliance or audit rules with some linkage to the “security” concept in the mainframe and Unix worlds, but very little of that in the PC world.

That prior board or committee authorization is the time to separate the strategic decisions from the merely tactical.

Rule 0: Tactical decisions aren't worth your time

For a decision to be strategic, and therefore worth board time, it must have real organizational consequences.

Decisions to do more or less of something the organization is already doing routinely represent tactical choices, as do decisions to change suppliers or methods within an existing architecture. As such they're in management's purview, not yours.

Thus if you find management repeatedly bringing you decisions on things like changing suppliers for standardized IT services like PC help desk support, you should ask yourself whether there might not be some deeper governance issue at work.

A lot of volunteer agencies, for example, have grown large enough to maintain professional management while retaining the appearance of volunteerism at the board and fund raising levels. In these, bombarding the board with essentially pointless brand A versus brand B decisions is often management's easiest way of ensuring the board's irrelevance with respect to the real strategic decisions driving the organization - decisions they're inappropriately abrogating to themselves.

Rule 1: it's easier to criticize than propose, but some risks are worth taking and some worthless proposals contain gems

Before any board level IT decision comes up you should receive an advance information packet describing the objectives, recommended methods, and expected costs of both the decision management prefers and at least the do nothing alternative.

In evaluating those it's important to start from a negative perspective while looking for things you can support in the proposal. This sounds conflicted, but it's what I call "Rule 1" and reflects a simple but brutal truth: most IT proposals are deeply flawed, and it's just far more efficient, and less frustrating, to weed those out early. At the same time, however, even the worst proposals often contain gems - low risk things of real potential value to the organization.

Equally importantly, I think there's a responsibility to sometimes say "Yes." That may seem odd, but one of the problems with IT governance is that simply saying "No" to everything, especially if you lose most votes, will eventually earn you a reputation as a tremendously effective judge of IT

IT management - but remember that the more people there are between your CIO and the actual job, the more disconnected he'll be from the reality of your organization's systems operation.

Leadership, in contrast, grows from the bottom up. As the IT organization develops some people take more and more responsibility and build teams of their own. As a result what you'll see in a leadership situation is a CIO who remains, no matter what the size of the organization, connected to the technology, the job, and his people.

Be aware, when looking at a candidate that there are quite a lot of people who talk the talk, but don't walk the walk.

In particular the reality is that almost every major IT shop has some Unixmachines, and so most CIO candidates can claim Unix experience even though they not only have no idea how to run it, but the certainties they do have will raise your IT costs while reducing the quality of IT service your organization gets.

So how do you tell the 1-5% of good guys from the 95 -99% of bad guys? You have to get that from talking to their former colleagues, from looking carefully at what they've achieved, and from your own gut instinct after talking to them.

In my experience, however, there are two "tells" that should trigger concern on your part - these are not absolutes, of course, merely more often right than wrong:

1. IT executives who see the hardware and software, and not their own technical staff, as the key IT resource tend to be winners in their own careers and losers for you; and,
2. People who refer to Unix use in terms of boxes and without reference to software and purpose are denigrating both the technologies and the people who use them. Thus someone who claims to have had responsibility for multiple Sun boxes is more likely to be a fraud than someone who claims past responsibility for Oracle on Solaris.

3.3 Rule Two: Buy Techies with Trust and Freedom, not dollars

The biggest problem you will face in hiring a good CIO is that, in systems, failure succeeds and success fails.

The Board Member's IT Brief

This IT Briefing is intended for busy, largely non technical, members of the board for organizations facing information systems related decisions.

The book's goal is to equip readers working at the governance level to ask the right questions and to judge, with a reasonable liklihood of getting it right, whether an IT project, proposal, strategy, or hiring is on the whole more likely to harm the organization than help it.

It is assumed, throughout*Brief*, that the board should consider those IT decisions likely to have strategic consequences. As a result specific guidance is provided for determining what is, or isn't, strategic, for evaluating senior IT managers, on when to call for professional, third party, assistance in IT decision making, and on arriving at yea or nay verdicts on specific projects or proposals brought forward by management.

Brief is largely non technical, introducing only two IT related technical concepts - those of "information integrity" and "information architecture."

There are two companion volumes.
***T**he Unix Guide to Defenestration* (Defen, 240pp) is aimed at helping IT professionals make strategic and technical decisions and assumes a highly technical audience.

In contrast *Business Information Technology: Foundations, Infrastructure and Culture* (BIT, 448pp) focuses mainly on understanding IT behavior and is aimed at helping non technical middle and junior managers called to contribute to IT decision making understand the history, terminology, and beliefs driving typical managerial and professional decision making in IT.

ISBN 0-9689004-0-2
52995
9 780968 900406

US $50.00
Cdn $65.00

Get current updates and join discussion forums at winface.com