Abstract
This paper examines the current state of IT benchmarking, and the problem with using these conventional models to benchmark Information Security environments. A framework is presented as a starting point for further development to obtain a fully-fledged, operational Information Security benchmark offering that will ascertain what companies are spending on Information Security and determine whether there is a correlation between the level of Information Security, cost and effectiveness. It will furthermore determine whether there is an “optimal” percentage of IT budget that should be spent on Information Security, and whether there is alignment between spent and a secure environment. When this benchmark model is fully developed and populated, companies will be able to use it to benchmark the cost-efficiency of their Information Security environment against others to find out how they compare, and to identify areas on which they should focus their effort to improve efficiencies.

1. Introduction
1.1 What is IT Benchmarking?
The first benchmarking study was conducted within the manufacturing environment, and evolved from the work done by R.C. Camp at Xerox, which was documented in his 1989 book titled “Benchmarking” [2].

Benchmarking has since increased in popularity, and companies are striving to improve by comparing themselves against other organisations within the same industry, either nationally or globally. What started initially as business-type comparative metrics (for example Dollar per barrel of oil produced), has since extended into the IT sphere, and IT organisations are challenged by CEO’s and Finance Directors to demonstrate their cost-efficiency and whether they are delivering value for money to the business. In order to understand what benchmarking is and to clarify what activities are involved, a number of definitions have been evaluated.

“The Benchmarking Network” [5] defines benchmarking as being “a performance measurement tool used in conjunction with improvement initiatives to measure comparative operating performance and identify Best Practices”. (According to their web-site, “The Benchmarking Network TM” is an organisation of experienced Benchmarking specialists solely dedicated to using Benchmarking to develop value-based opportunities for corporations worldwide.)

A benchmarking specialist from “The Benchmarking Network”, Michael Spendolini [5], defines benchmarking as: “... a continuous, systematic process for evaluating the products, services, and work processes of organisations that are recognized as representing best practices for the purpose of organisational improvement.”

One of the best definitions of IT benchmarking that is also applicable to the IT industry, is the one created by former Xerox CEO, David Kearns in the early 1980s [2]:

“Benchmarking is the continuous process of measuring products, services, and practices against the toughest competitors or those companies recognized as industry leaders”.

Webster’s Dictionary describes the word “benchmark” as "a point of reference from which measurements may be made; something that serves as a standard by which others may be measured.”

Derek Slater [3] defines benchmarking as “comparing corporate products and practices with the world’s best and then borrowing the work processes that will help close the gaps.”

Taking all these definitions into account, one can summarise “Benchmarking” as being the search for industry best practices that can direct an organisation into obtaining improved or even superior performance. It is the ongoing process of identification of best practices, the measurement of oneself against those practices, and the implementation thereof to improve performance. It should be viewed as basically an objective-setting and continuous process – it is not static and is very seldom adding value to a company if conducted as a once-off exercise.

IT Benchmarking uses the same principles, but focuses on IT issues and IT cost components, often expressed in IT terms (for example “Dollar per network access point”), but often also expressed in relation to the broader organisation, for instance “IT Budget as a percentage of company turnover”. Using the previous example of “Dollar per barrel of oil produced”, IT now has to report on its contribution to that as well, i.e. what is the IT cost per barrel of oil produced.

1.2 Why Benchmark
“Keep on the lookout for novel and interesting ideas that others have used successfully. Your idea has to be original only in its adaptation to the problem you’re currently working on.” (Thomas Edison)

There are many reasons why companies engage in benchmarking studies, but the most important reasons are as follows:
Understand current environment and obtain a “stake in the ground”

Benchmarking quite often assists companies in obtaining an understanding their current environments, and to develop a base of knowledge that can be used as a departure point to navigate the
organisation towards better efficiencies and improved effectiveness. The old saying “if you don’t know where you are going, any road will take you there” is the essence of why a lot of companies initiate benchmark projects. Even more so the adage “if you don’t know where you are, a map won’t help you!”. It is also used as a quantitative baseline for sourcing decisions, and to identify which areas qualify to be outsourced to an external service provider.

**IT planning – justify new investments or changes in spending levels**

Benchmarking is a strategic planning tool to be used in establishing a common IT vision for the company and setting of two to three year goals. It is also instrumental in identifying critical short term actions required to achieve the goals, and to compile an operating plan. Companies quite often conduct benchmarking studies to determine whether they should downsize, right-size or source their IT environment, or parts thereof. It is also used to identify “low-hanging fruit” or areas (be it costs or functions) that are under- or over-performing and on which a company should focus on when developing short term improvement plans.

**Continuous improvement – track and monitor performance**

The continuous drive towards improving IT quality is one of the key reasons for the increasing awareness (and participation) of IT executives in IT benchmarking projects. One of the best reasons to benchmark regularly is to establish a performance baseline upon which improvements can be made and measured. But if benchmarking is not conducted on a regular basis, it can happen that the best practices implemented initially after the first benchmark exercise has been completed, are no longer deemed to be competitive in subsequent years. Peer companies have also improve their processes, costs, etc., and if not benchmarked against revised and improved peer groups, what used to be considered as “best practice” will lag considerably if not continually updated.

**User / business satisfaction**

One of the key aspects that should to be assessed during benchmarking is the ability of an organisation’s IT group to satisfy user requirements and to meet their demands and deadlines of the business. Customer and Business Satisfaction surveys or benchmarks should be conducted, at least annually, to determine levels of end-user satisfaction and to identify areas that need to be improved. It is important to determine the business’ perspective of the IT department and to measure the responsiveness of the IT group in terms of user and business requests. Benchmarks can also be conducted to determine business requirements and to measure IT’s performance and service delivery against those requirements.

**Objective and unemotional analysis**

When an IT function faces problems or needs to be redesigned or re-engineered to provide better results, the steps that have to be taken can quite often be very disruptive to the organisation. In order to ensure that IT decisions are taken on solid facts and based on best practice norms, as much subjectivity and emotions need to be removed from the process as possible. Benchmarking brings facts to the decision-making process, and provides an objective evaluation of a current situation. Benchmarking is extremely helpful in removing emotion from a decision, and is therefore an effective cure for ‘denial’ problems. Decisions do not become clouded with personalities or politics. Most importantly, it helps to understand what needs to be changed and why.

**Contractual Obligations (i.e. evaluate outsourcing deals)**

Most outsourcing contracts now incorporate a “benchmarking clause” that stipulates the obligation a service provider has in terms of regular benchmark studies using a mutually-agreed, independent and reputable benchmarking company. The objective is to provide a sanity check on whether the prices and service levels are market-related, and to use the benchmark output to develop action plans that will ensure improved efficiencies or service delivery. Benchmarking is used more and more often to ensure transparent governance of outsourcing contracts and to assist with arbitration and disputes in outsourcing deals.

### 1.3 Traditional IT Benchmarking Models

**IT Benchmarking offerings are available from a range of service providers and consulting firms, but the major international benchmark players are Gartner, Compass, Quantimetrix (for applications) and The Hackett Group. Other computer economics reports and once-off surveys of a particular benchmark topic are also conducted and published by companies such as Forrester, CIO Insight and various IT publications.**

**IT Benchmark services are conventionally offered in terms of technology areas or IT “towers”, such as Networking, Mainframe, IT Help Desk, etc. Depending on the benchmark vendor, the model used for data collection will consist of different elements, but generally speaking, they are grouped as follows: hardware costs, software costs, personnel (internal staff) costs, facilities and occupancy costs, outsourcer (service provider) costs, service level metrics and implemented processes and best practices. The latter two are not direct cost elements, but both have a very real and direct impact on the cost-efficiency of an IT environment.**

The more stringent the service levels required by the business, the higher the operational cost will be. For example, the price difference between 99.5% WAN availability and 99.9% WAN availability can be up to 25% due to extra redundancy required.

On the other hand, the implementation and adoption of best practices and improved processes should result in a reduction of operational costs, even though there will be an initial spike in expenditure due to implementation costs.

The area on the left hand side of Figure 1 lists the typical traditional IT benchmarking models that are currently available from leading benchmark vendors. Each of these areas will have a set of metrics that are generated to indicate an organisation’s levels of cost-efficiency. For instance, Dollar per desktop or end-user, Dollar per Help Desk call, Dollar per Function Point developed, etc.

Each of the IT benchmarking elements illustrated in Figure 1 consists of one or more Security components. The problem with using traditional or conventional benchmarking models to benchmark Information Security, is that the security components are all hidden within the other elements, and no single, coherent framework or model exists that will enable the entire Information Security environment to be benchmarked. This is indicated in the question mark in Figure 1.
Hardware Costs  
Software Costs  
Personnel Costs  
Facilities & Occupancy Costs  
Service Providers  
Service Levels  
Processes

Figure 1: Traditional IT benchmarking models

There is in effect, a “hidden” information security cost in each of the metrics produced. For example, it is not evident what the information security cost or contribution is in the metric “Dollar per desktop supported”. The results provided are rolled-up, consolidated metrics, which makes in-depth analysis of information security cost profiles very difficult, if not impossible.

A real need exists for an Information Security benchmark model that will elevate all the information security components into a transparent and manageable cost framework.

The IT Security Benchmarking Association [6], a division of The Benchmarking Network, provides a security benchmark service, but it only focuses on analysing and improving business processes in IT security. The Benchmarking Network [5] utilise a network model whereby they conduct organised benchmark research, based on a range of special interest group topics. Potential customers can add their names to a benchmarking topic, and will be contacted if other organisations are interested in conducting a similar study. They focus largely on industry benchmarks (e.g. Healthcare and Accounting & Finance), with a limited range of IT benchmark offerings.

Using the Analytic Hierarchy Process (AHP) to evaluate information security investments [1] greatly assist in making the best informed decisions on how to invest in information security. But it does not provide a tool or methodology with which money already spent, ongoing operational expenses and processes and service levels in place, can be benchmarked against other organisations.

2. BENCHMARK METHODOLOGY

The processes used by benchmarking service providers and within organisations differ in terms of the number of steps included in the benchmarking exercises. Some organisations use a four-step benchmarking process while others use a six, seven, eight or twelve step process, or some other variation. However, most companies employ a common approach that helps them to plan the project, collect and analyse the data, develop insights, and implement improvement actions.

The methodology depicted in Figure 2 is a derivative of the most commonly observed benchmarking processes used for IT environments. It consists of five steps, namely:

- Step 2: Plan
- Step 3: Execute
- Step 4: Analyse
- Step 5: Act

Each of the process steps consists of a number of activities – every one key in the success of the benchmark exercise. The first two steps, namely Initiate and Plan, are the most critical phases of any benchmark project. If these two steps are not conducted thoroughly and on a very detailed basis, it will jeopardise the rest of the project, and will not have final acceptance by the sponsor.

The data gathering step normally takes much longer than originally anticipated, and the project plan should cater to take this into account. The implementation phase is the most important stage of the benchmarking project and should receive adequate time and effort to ensure successful improvement in performance. If no implementation actions are taken, the benchmark project would have been a waste of time, resources and money, and would render no improvement to the environment.

3. PROPOSED INFORMATION SECURITY BENCHMARK FRAMEWORK

The proposed Information Security benchmark model will consist of an agreed set of data points that are to be collected and compared. This will be referred to as the benchmark “chart of accounts” and will ensure that all studies are conducted using a uniform model, resulting in fair results that are directly comparable to peer organisations (i.e. “apple-to-apple” comparisons).

The model will provide for direct costs, as well as other “soft issues” such as the effect of non-delivery, risk, legislative impact, downtime due to security breaches, etc. The direct cost components will cater for Information Security expenditure in hardware, software, internal staff, external service providers, facilities and occupancy. Figure 3 illustrates the chart of accounts that will be used for the proposed Information Security benchmark model. The arrows represent the Security components (traditionally found within each of the IT Benchmark Elements as
illustrated in Figure 1) that are now consolidated into this Information Security benchmark framework.

The cost information that will be gathered will consist of annualised operational costs. This will ensure that spikes in capital expenditure are smoothed out over the project or asset life cycle. Capital expenditure will be represented as annual depreciation costs (in the case of large projects that are amortised) or expensed costs (in the case of smaller software purchases which are written off in the year of acquisition).

- Normalised (especially when companies from different geographies are compared – a measure similar to the “Big Mac” index must be used to ensure level playing fields)
- Statistically reliable and auditable
- Appropriate measurements of the right Information Security components
- Quantifiable calculations and comparisons
- Easy to understand and not open to different interpretations
- Consist of actionable, practical recommendations and improvement plans

4. CONCLUDING COMMENTS

Although there are still practical modeling issues that need to be refined and configured before this model can be used in practice, it does provide a benchmark framework that will, when fully developed, determine the cost-efficiency, and to a lesser extent, the cost-effectiveness, of an Information Security environment. There are areas, in particular the “soft issues” that needs to be defined in more detail, and there are aspects such as the impact of service levels and best practice implementation that must still be qualified - the impact thereof on efficiency and expenditure also needs to be determined and quantified. Further development of this framework will focus on ensuring the benchmark model is practical, comprehensive, fair and can be implemented by and used within organizations regardless of industry or geography.

5. REFERENCES


Figure 3: Proposed Information Security Benchmark Model

The most difficult area to benchmark is the intangible or indirect cost area. Although this can represent a large percentage of the total Information Security costs, it is not always accepted by executive or board members as reflective of an organisation’s spending patterns. It is very difficult to (a) identify and (b) quantify these “soft” costs, and it is therefore often ignored by the business. The model will make provision for both direct and indirect costs, but will also, should companies choose to, provide comparative analysis based on direct costs only.

In addition to the use of uniform consensus models and chart of accounts, the metrics produced by the benchmark studies, must also adhere to the following characteristics:

- Objective and unbiased comparisons