USING IT BENCHMARKING PRINCIPLES TO DESIGN AN INFORMATION SECURITY BENCHMARK MODEL

L. McManus* and J.H.P. Eloff**

Information & Computer Security Architectures (ICSA) Research Group, Department of Computer Science, University of Pretoria

* leoniem@mcmanus.co.za; Telephone: 082-904-3773
** eloff@cs.up.ac.za; Telephone: 012 420-3035

ABSTRACT

This paper examines the current state of IT benchmarking and the problem of using conventional IT benchmarking 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 model. This model will determine what money companies are spending on Information Security and whether there is a correlation between the level of Information Security, cost and effectiveness. Once this model has been fully developed and populated, companies will be able to use it as a benchmark tool to determine the cost efficiency of their information security environments. One of the key outputs of this model will be a list of possible areas or actions that companies should focus on in order to improve Information Security efficiencies.

KEY WORDS

Information Security benchmark, IT benchmarking models, benchmark methodology, cost efficiency, benchmark components.

USING IT BENCHMARKING PRINCIPLES TO DESIGN AN INFORMATION SECURITY BENCHMARK MODEL

1 INTRODUCTION

The purpose of this article is to discuss the current IT benchmarking models that are available to companies that wish to benchmark a portion or all of their IT components. It identifies gaps that exist when attempting to use conventional models to benchmark Information Security environments. The article also discusses how these concepts and methodologies can be used and adapted to focus more specifically on Information Security benchmarks, and a skeleton Information Security Model is proposed as a basis for future research and development.

The first section of the paper focuses on an introduction to IT benchmarking and provides an overview of the types of benchmarking available, approaches to benchmarking and reasons why companies initiate benchmarking projects. The remainder of the paper is structured as follows: section 2 provides a high-level methodology for the implementation of an Information Security benchmark framework, and the third section elaborates on the framework itself, explaining which components should be included in such a benchmark model. The paper concludes with a summary that highlights the potential impact of an Information Security Benchmarking tool.

1.1 What is IT Benchmarking?

The first benchmarking study was conducted within the manufacturing environment, and evolved from the work done by Camp (1989). 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 CEOs 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 in general is and to clarify the activities that are involved, a number of definitions have been evaluated.

"The Benchmarking Network" (2006) 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 ™" is an organisation of experienced Benchmarking specialists solely dedicated to using Benchmarking to develop value-based opportunities for corporations worldwide.)*

Spendolini (1992) 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."

Merriam-Webster's Online Dictionary (2006) 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 or judged; a standardized problem or test that serves as a basis for evaluation or comparison."

Slater (1997) 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."

Considering all these definitions, “benchmarking” can be summarised as being the search for industry best practices that can direct an organisation towards obtaining improved or even superior performance. It is the ongoing process of identifying best practices, the measurement of oneself against those practices, and the implementation of such practices to improve performance. It should be viewed as a basic yet continuous process of setting objectives – it is not static and very seldom adds 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”). However, often it is 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 Approaches to Benchmarking

In 2003, the Consortium for Excellence in Higher Education at Sheffield Hallam University published a paper in which they discussed the following seven main approaches to benchmarking:

- **Strategic Benchmarking.** Used where organisations seek to improve their overall performance by focusing on specific strategies or business processes. The key driver is the enhancement of the organisation’s strategic direction and goals and benchmarking will be carried out within the context of the development of core business strategies.
- **Performance or Competitive Benchmarking.** Performance measures, such as market share, retention rates and costs are used to compare an organisation against similar organisations, business units or divisions.
- **Process Benchmarking.** This type of benchmark focuses specifically on business or operational processes within an organisation. Examples are supply chain, procurement, student enrolment, etc.
- **Functional and Generic Benchmarking.** Functional or generic benchmarking involves partnerships of organisations drawn from different sectors that wish to improve some specific activity (for example knowledge management).
- **External Benchmarking.** This type of benchmarking enables a comparison of the organisation’s functions and key processes against good practice organisations. The key driver can be the search for improvement or breakthrough opportunities in business processes.
- **Internal Good Practice Benchmarking.** This is achieved by establishing organisation-wide good practice through the comparison of internal activities or operations. The key driver is the sharing of good practice in cross-cutting activities. This can be done in the context of business planning, as specific process improvement projects can be prioritised and results be compared across business units to identify internal “best-in-class” exemplars.
- **International Benchmarking.** Benchmarking can be undertaken either on a national or international level.

The relationship between the different types of benchmarking, according to Sheffield Hallam University (2003), is illustrated in Figure 1.

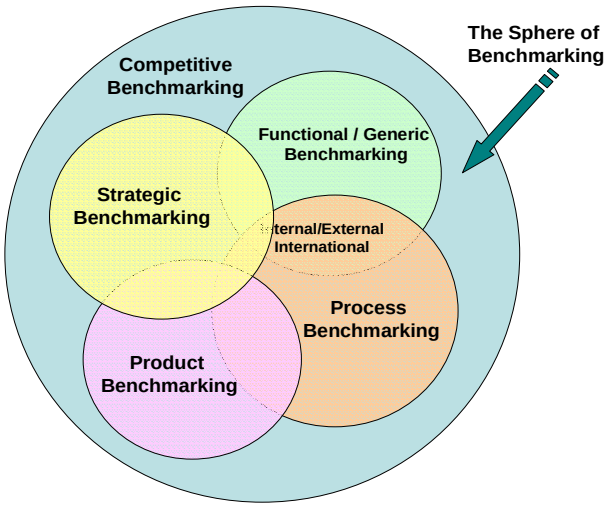

Figure 1: Relationships between different types of Benchmarking

The "performance" and "external" benchmarking approaches are of particular relevance to Information Security. They focus specifically on performance issues and metrics such as cost and outward-focused comparisons, which will be of key importance when measuring Information Security efficiencies. "Functional" benchmarking will also be of key importance when analysing an organisation's information security architecture, procedures, processes and other functional elements within the Information Security sphere.

1.3 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 A. Edison)

There are many reasons why companies engage in benchmarking studies, but the main reasons mentioned by Camp (1989) and Spendolini (1992) are not complete or current. The most important reasons, gained from these two authors, but augmented with more recent and practical experience obtained through IT benchmarking projects conducted within the South African IT industry, are as follows:

- **Understand current environment and obtain a "stake in the ground"**

Benchmarking quite often assists companies in obtaining an understanding of their current environments and in developing 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 many companies initiate benchmark projects. Even more applicable is the adage "If you don't know where you are, a map won't help you!" Benchmarking is used as a quantitative baseline for sourcing decisions, and to identify the specific areas that qualify for being 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 the setting of two-year to three-year goals. It is also instrumental in identifying critical short-term actions required to achieve such goals, and to compile an operating plan. Companies quite often conduct benchmarking studies to determine whether they should downsize, right-size or outsource 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 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 most common reasons cited by companies that conduct regular benchmark studies is to establish a performance baseline upon which improvements can be made and measured. If benchmarking is not conducted on a regular basis, it may happen that the best practices initially implemented will no longer be deemed competitive in subsequent years. Peer companies will also have improved their processes, costs, etc., and if IT services are not benchmarked against revised and improved peer groups, what once used to be considered as "best practice", will lag behind considerably if not updated continually.

- **User / Business satisfaction**

One of the key aspects that should be assessed during benchmarking is the ability of an organisation's IT group to satisfy user requirements and meet their demands as well as the 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 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 the IT group'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, subjectivity and emotions need to be removed as far as possible from the process. Benchmarking does just this, as it brings facts to the decision-making process and provides an objective evaluation of the current situation. Benchmarking is extremely helpful in removing emotion from a decision and therefore serves as an effective cure for 'denial' problems. Decisions do not become clouded with personalities or politics. Most importantly, it helps the organisation 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 (Gartner, 2006). 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 of 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.

- **Specific IT disciplines**

There can be a requirement whereby organisations would like to benchmark specific IT disciplines such as Information Security, Architecture, Processes (for example ITIL), Governance and CoBIT. These disciplines extend across IT towers or boundaries, and should be benchmarked in totality.

1.4 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 (2006), Compass (2006), Quantimetrics (2006) - which specifically focus on applications benchmarks - and The Hackett Group (2006). Other computer economics reports and once-off surveys of a particular benchmark topic are also conducted 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 data 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. They should therefore always be taken into account when benchmark studies are conducted. 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 (Wide Area Network) 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 2 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, key comparative metrics include Rand per desktop or end-user, Rand per Help Desk call, Rand per Function Point developed, and Rand per Internet user.

Each of the IT benchmarking elements illustrated in Figure 2 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 problem is indicated by the question mark in Figure 2.

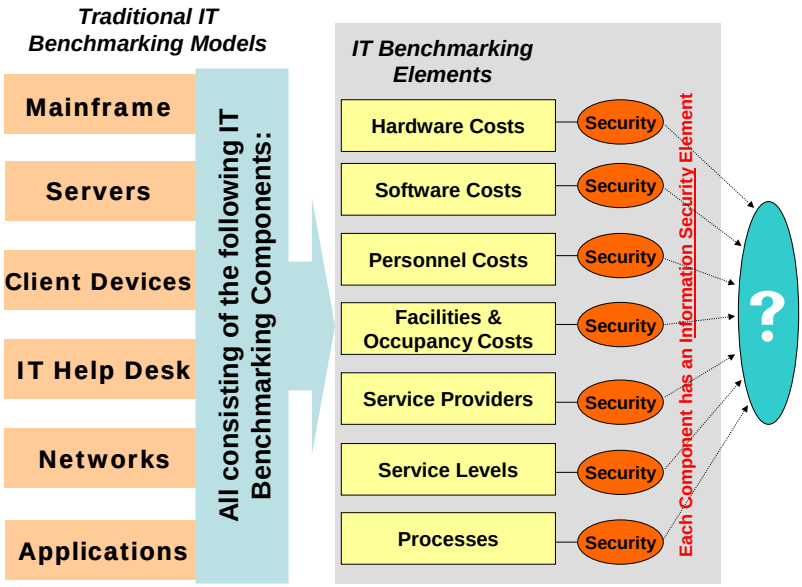

Figure 2: Traditional IT benchmarking models

2 BENCHMARK METHODOLOGY

The methodology used by benchmarking service providers and within organisations differs 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 (Sheffield, 2003). 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 proposed benchmark methodology depicted in Figure 3 is a derivative of the most commonly observed benchmarking processes used for IT environments. It consists of the following five steps:

- Step 1: Initiate
- Step 2: Plan
- Step 3: Execute
- Step 4: Analyse
- Step 5: Act

Each of the methodology steps consists of a number of activities or sub-processes, and all these activities are integral and key to 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, the rest of the project will be jeopardised and it will not achieve final acceptance by the sponsor. The "Execute" phase (Step 3) involves all data-gathering and validation activities and normally takes much longer than originally anticipated. When planning for a benchmark project, it is recommended that the project plan caters for an overrun during this step. The implementation phase (Step 5) is extremely important and should receive adequate time and effort to ensure successful implementation of recommendations that will result in performance improvements. If no implementation actions are taken, the benchmark project will have been a waste of time, resources and money, as it will yield no improvement to the organisation.

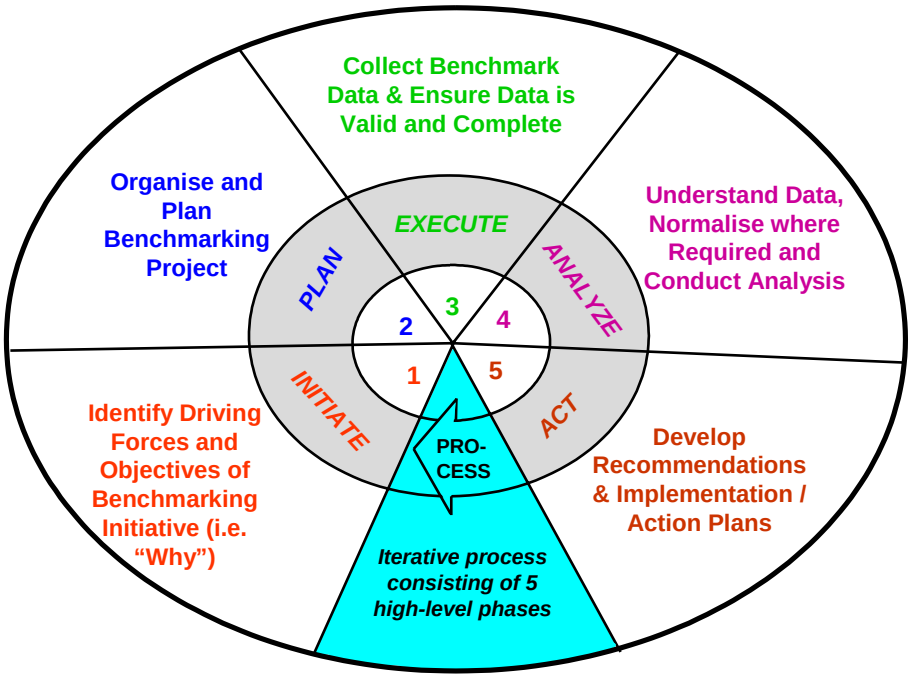

Figure 3: High-level Benchmark Methodology

3 PROPOSED INFORMATION SECURITY BENCHMARK MODEL

From the illustration of traditional IT benchmarking models in Figure 2 it is evident that there is a "hidden" information security cost in each of the IT areas being benchmarked, and therefore in each of the benchmark metrics produced. For example, when conducting traditional benchmarks, it is not evident what the information security cost or contribution is in the metric "Rand per desktop supported". Does it include information security costs such as anti-virus software, authentication, firewalls, single sign-on applications, or does it merely reflect the hardware and software costs of providing a desktop service to the end-user? The results provided by current, traditional benchmarks are consolidated and summarised per IT area, and no in-depth analyses or comparisons of Information Security profiles can be conducted using such an approach.

A real need exists for an Information Security benchmark model that will integrate all the Information Security components into a transparent and manageable cost framework. (Examples of these components are provided in Figure 3 later in this article.)

Although the IT Security Benchmarking Association (ISBA, 2006), a division of The Benchmarking Network, provides a security benchmark service, it only focuses on analysing and improving business processes in IT security. The Benchmarking Network (2006) 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, as well as Accounting and Finance), with a limited range of IT benchmark offerings.

Using the Analytic Hierarchy Process (AHP) to evaluate information security investments (Bodin, 2005) greatly assist in making the best-informed decisions on how to invest in Information Security. However, it does not provide a methodology with which money already spent, ongoing operational expenses and processes and service levels in place, can be benchmarked against other organisations.

An Information Security benchmark model is therefore proposed that consists of an agreed set of data points that are to be collected and compared against other Information Security environments of similar size and scope. 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 among peer organisations.

The model provides for direct costs, as well as for other "soft issues" such as the effect of non-delivery, risk, legislative impact, and downtime due to security breeches. The direct cost components will cater for Information Security expenditure in hardware, software, internal staff, external service providers, facilities and occupancy. The proposed model will also take into account the effect lower or more stringent service levels have on costs. Figure 4 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 2) that are now consolidated into this Information Security benchmark framework.

The cost of information to be gathered includes annualised operational costs, i.e. costs included in a company's operational IT budget such as licensing fees, maintenance charges, support charges, total cost-to-company personnel costs, etc. This will ensure that spikes in capital expenditure are smoothed out over the life span of a project or assets. In the case of large IT projects that have been amortised, the impact of capital expenditure will be taken into account by means of annualised depreciation costs. Software purchases that are expensed during the year of purchase will be included as an annualised operational expense for that particular year.

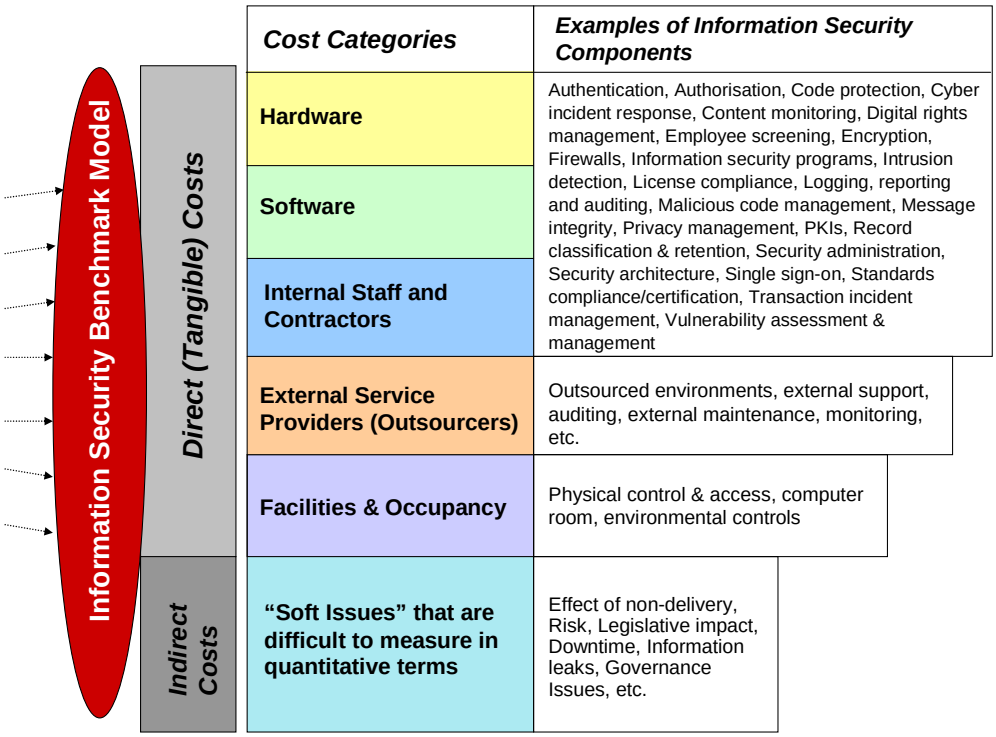

Figure 4: Information Security Components

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 they are therefore often ignored by the business. The model makes provision for both direct and indirect costs and – should companies prefer it – will also provide comparative analysis based on direct costs only.

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

- Information Security benchmark comparisons must be **objective and unbiased**, i.e. they must not be performed by someone who will benefit directly and financially from the results.
- Costs, especially salaries, must be **normalised** before comparing against companies from different geographical regions. This normalisation, which uses a measure similar to the "Big Mac" index must be used to ensure level playing fields – without it, results will be skewed and will always favour geographies with lower cost-of-living indices. Average remuneration costs for Information Security professionals in South Africa will be used as a basis for the normalisation of non-SA personnel costs.
- Results and metrics must be **reliable and auditable**. Although benchmarking is not an exact science, and will not always be statistically accurate (for instance, the sample group is much smaller than would be required for 99% statistical accuracy), it must provide defendable results that can be trusted, and it must be able to track all Information Security components used in the benchmark study with relevant documentation and audit trails.
- **Appropriate Information Security components** must be used for measurement purposes. It does not make sense to measure costs of components that cannot be found in most Information Security environments, or to use a process that cannot be repeated in other organisations. A comprehensive set of data components must be included to provide a model that accurately reflects an organisation's Information Security environment – only benchmarking a small percentage of components will not provide accurate results.

- **Quantifiable calculations and comparisons.** All calculations and analytical measurements must be quantifiable, except in the case of indirect, "soft" issues that are often estimates. This must then be clearly indicated and all assumptions with regard to cost analyses must be documented.
- Results and recommendations must be **easy to understand** and not open to different interpretations. Metrics must be quantified or at least qualified with appropriate explanations or proof of where differences in benchmark results exist.
- Output must consist of **actionable, practical recommendations** and improvement plans. Although there are instances where this will not be feasible or practical, Information Security benchmark projects should always consist of a list of actions that are recommended to improve the environment and to get closer to "best practice" standards. Recommendations must not be "fuzzy", but must consist of action plans that can be implemented in a methodical and practical manner within the organisations that have been benchmarked.

The view of a combined Information Security benchmark model, based not on the conventional towers of IT benchmarking, but more specifically on the components of Information Security, is reflected in Figure 5.

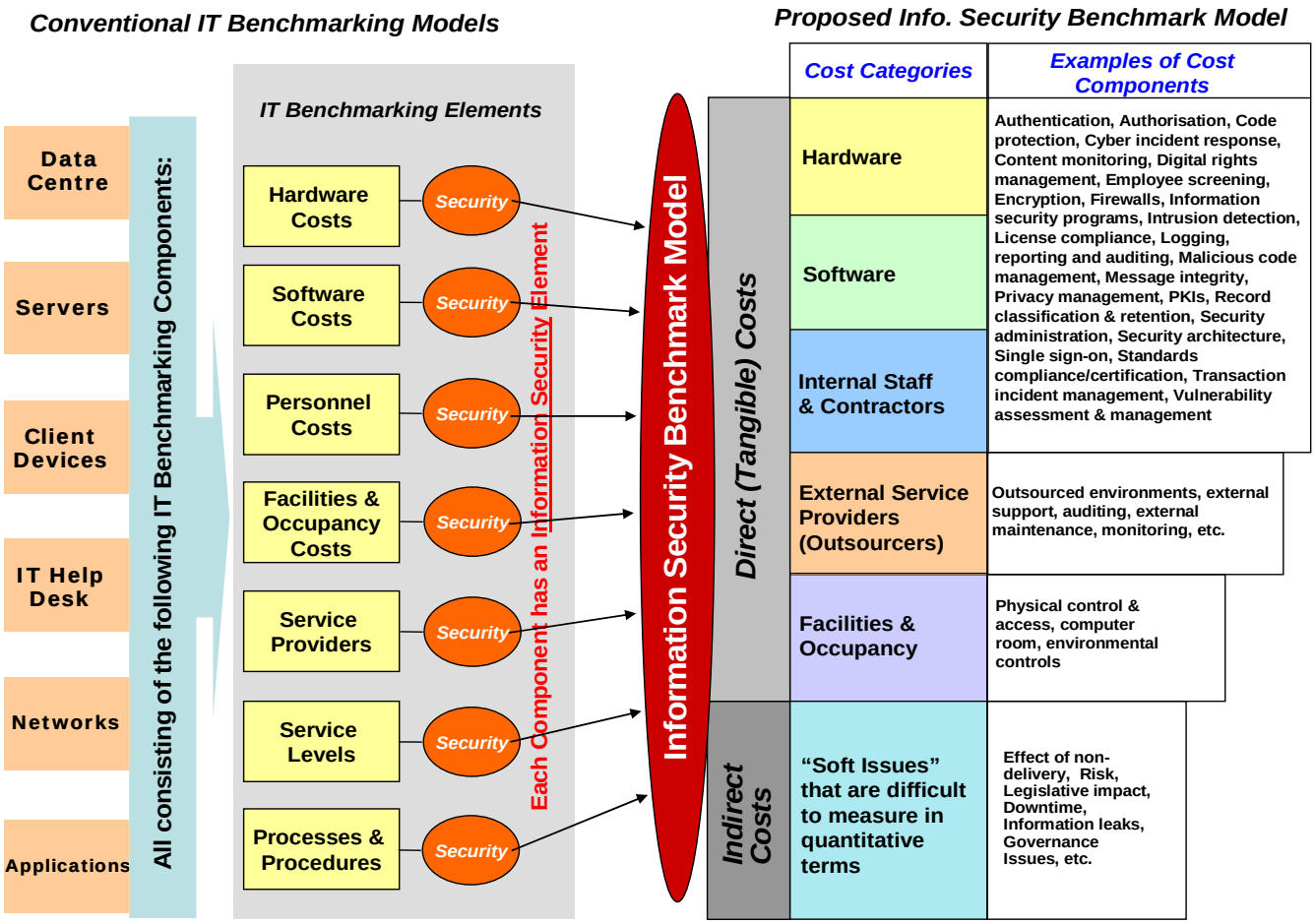

Figure 5: Proposed Information Security Benchmark Model

4 CONCLUDING COMMENTS

Although there are still practical modelling 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. Certain areas, in particular the "soft issues", need to be researched and defined in greater detail, and aspects such as the impact of service levels and best practice implementation must still be qualified – their impact on efficiency and expenditure also needs to be determined and quantified. Further development of this framework will focus on ensuring that the benchmark model is practical, comprehensive and fair, and that it can be implemented by and used within organisations to assess their Information Security environments, regardless of industry or geography.

5 REFERENCES

Bodin, L.D., Gordon, L.A., & Loeb, M.P. (2005, February). Evaluating Information Security Investments using the Analytic Hierarchy Process. *Communications of the ACM*, 48 **(2)**, 79-83.

Camp, R.C. (1989). *Benchmarking: The Search for Industry Best Practices that Lead to Superior Performance*. Milwaukee: ASQC Press.

Compass Management Consulting (2006). Accessed April, 24, 2006, at http://www.compassmc.com.

Gartner Inc. (2006). Accessed April, 24, 2006, at http://www.gartner.com.

ITSBA. (2006). Information Technology Security Benchmarking Association. Accessed April, 24, 2006, at http://www.itsba.com.

Merriam-Webster Online Dictionary. (2006). Accessed April, 24, 2006, at http://www.webster.com.

Consortium for Excellence in Higher Education. (2003). *Benchmarking Methods and Experiences.* Sheffield: Sheffield Hallam University.

Slater, D. (1997, November 15). Is benchmarking worth the bother? *CIO Magazine.*

Spendolini, M. J. (1992). *The Benchmarking Book.* AMACOM.

The Benchmarking Network. (2006). Accessed April, 24, 2006, at http://www.benchmarkingnetwork.com.

The Hackett Group. (2006). Accessed April, 24, 2006, at http://www.thehackettgroup.com.

Quantimetrics. (2006). Accessed April, 24, 2006, at http://www.quantimetrics.net.