الجامعة البريطانية في دبي

The British University in Dubai

A Framework for Designing A Data Center

إطار لتصميم مركز البيانات

by

MALIK MOHAMMED ABDULMALIK ALI

A dissertation submitted in fulfilment

of the requirements for the degree of

MSc INFORMATION TECHNOLOGY MANAGEMENT

at

The British University in Dubai

Dr. Cornelius Ncube
October 2017

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

Malik Ali .

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

Abstract

The role of information has changed drastically during the past century. The advent of information technologies has reshaped most of the operations and processed in nearly every sphere or area. Businesses, governments, non-profits, and many other organizations of different kind faced the major challenge: it was mandatory to adapt to the upcoming changes, implementing technologies that were supposed to allow to collect, process, and store huge volumes of data, generated within new reality. The need in data centers has emerged. Modern data center is a complex system that includes networking, hardware, software, and organizational solutions, targeted at achieving highest effectiveness, protection from inside and outside threat, and provision of adequate redundancy. The major task of a data center built for a business, government facility, or non-profit organization is interruptible and continuous access to information stored in it. Therefore, appropriate policies and techniques must be utilized during the process of planning, building, and maintaining of data center. They are carefully reviewed in this research. To achieve the best possible result, extensive review of the relevant literature was performed to distill the best practices in the industry. Pitfalls and gaps were explored as well to develop the best and well-optimized approaches to the data center creation process. It has been decomposed to the following blocks that were thoroughly assessed: physical characteristics of an appropriate location site, basics and advancements in the networking technologies, hardware and software solutions, organizational issues, threats, and security assurance measures. Additionally, the relevant conclusions were drawn to be used for the development of recommendations.

Keywords: data center, networking, hardware, software, organizational solutions, policies, practices.

نبذة مختصرة

لقد تغير دور المعلومات بشكل كبير خلال القرن الماضي. وقد أعاد ظهور تكنولوجيات المعلومات معظم العمليات وتمت معالجتها في كل مجال أو منطقة تقريبا. واجهت الشركات والحكومات والمؤسسات غير الربحية والعديد من المنظمات الأخرى من مختلف الأنواع التحدي الرئيسي: كان من الضروري التكيف مع التغييرات القادمة ، وتطبيق التقنيات التي كان من المفترض أن تسمح بجمع ومعالجة وتخزين كميات هائلة من البيانات. ولدت ضمن واقع جديد و ظهرت الحاجة لمراكز البيانات. يعد مركز البيانات الحديث نظامًا معقدًا حيث انه يشمل الشبكات والأجهزة والبرمجيات والحلول التنظيمية التي تهدف لتحقيق أعلى مستوى من الفعالية والحماية من التهديدات الداخلية والخارجية وتوفير التكرار المناسب. إن المهمة الرئيسية لمركز بيانات تم تصميمه لمنشأة تجارية أو منشأة حكومية أو منظمة غير ربحية قابلة للمقاطعة والوصول المستمر إلى المعلومات المخزنة بها. لذلك ، يجب استخدام السياسات والتقنيات المناسبة أثناء عملية تخطيط وبناء وصيانة مركز البيانات. و هذا ما تم مراجعته بعناية في هذا البحث. ولتحقيق أفضل النتائج الممكنة ، تم إجراء مراجعة شاملة للأدبيات ذات الصلة من أجل استخلاص أفضل الممارسات في الصناعة. تم استكشاف مطبات وثغرات أيضا لتطوير أفضل المناهج الأمثل لعملية إنشاء مركز البيانات. وقد تحلل إلى الكتل التالية التي تم تقييمها بدقة: الخصائص الفيزيائية للموقع المناسب ، والأساسيات والتقدم في تكنولوجيات الربط الشبكي ، وحلول الأجهزة والبرمجيات ، والمسائل التنظيمية ، والتهديدات ، وتدابير ضمان الأمن. بالإضافة إلى ذلك ، تم استخلاص الاستنتاجات ذات الصلة لاستخدامها في تطوير التوصيات.

الكلمات الرئيسية: مركز البيانات ، الشبكات ، الأجهزة ، البرامج ، الحلول التنظيمية ، السياسات ، الممارسات.

ACKNOWLEDGEMENT

I would first like to thank my thesis advisor Dr. Cornelius Ncube and the entire Faculty of Engineering & Information Technology at the British University in Dubai.

I must also express my very profound gratitude to my parents and to my wife for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Table of Contents

Table of Figures

Tables

Chapter 1: Introduction

The modern society and its scientific achievements created a new dimension of the humankind existence. Computers were invented for scientific and military use in the second half of the 20th century. Eventually, computer became very useful in every aspect of modern life like business, medicine, education, or entertainment, and it was the next and quite logical step to connect computers with each other. The first computer networks were created. Were a group of computers and devices connected with communication channels based on wires and/or wireless technologies to allow users share resources with each other. Thus, the value of information as a product grew drastically when first networks were developed in 70th of the past century (Leiner et al. 2009). Then the problem of storing and securing the information these networks became real. The need in creating data centers has emerged.

Recent research presented concept of information sharing and data through exchange presupposes placing it somewhere online. It is necessary because of the need to have access to information twenty-four-seven. Data centers have emerged as the most convenient and optimal solution of this issue. According to the definition, provided by TechTarget.com (2010), data center is a “centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business.” Depending on the business or company size, the approach of storing the data varies. Company sizes are identified based on its number of employees as well as the size of data, applications or knowledge that belongs to it. Based on these information, companies are categorized into small to medium companies, large companies, government authorities\entities and international organizations. In most cases, depending upon the size of the company, company stakeholders and its IT managers decide where to store their data. But when it comes to Government authorities, international organizations and enterprises of higher scale the majority decide to build their own datacenter in their Head Quarter buildings instead of contracting with 3rd party data center service providers due to data security, authorization and control reasons. Therefore, this inhouse data center effective development, planning and buildup becomes the responsibility of those organizations IT management.

The key problem is the establishment of the effective structure that would resolve the problems of energy efficiency, sufficient redundancy, and, of course, protection of any sensitive information. Therefore, it is highly important to possess knowledge about the mentioned and other processes in the course of data center creation. This research is aimed at exploring the best practices allowing to build contemporary, state-of-the-art data center. More specifically, the research is going to analyze planning procedure, the responsibilities that each department has when data center is operational, evaluate the necessary data center components such as server infrastructure, network, storage infrastructures, security architecture, assess the categories of potential attacks on data centers, and explore real-life implementation of data center building process.

1.1 Rationale for the Study

Datacenters can resolve the major problem of the modern world – leak of information. Contemporary information channels are developed enough to transfer terabytes of unprocessed data. However, information becomes knowledge when it is stored, analyzed, and provided according to secure transfer appropriate request. Datacenters facilitate the process of data storing, analysis, and retrieval. The research is going to develop a framework that will be a guide for IT management (of Government authorities, international organizations and enterprises of higher scale) that outlines all needed processes, activities and documentations o build and protect their own organization’s data center.

1.2 Research Questions

The study is going to analyze the following questions and provide recommendations regarding their effective resolution:

- How can IT management identify the suitable data center building processes?
- How can IT management identify data center's components below?
    - ➢ requirements gathering (functional and non-functional requirements)
    - ➢ purchase of IT equipment, cost
    - ➢ data center backup
    - ➢ operation team SLA
    - ➢ organization of the reliable and robust security system
    - ➢ establishment of the appropriate service units
    - ➢ exploration of the best currently exploited practices.

1.3 Statement of the Problem

Modern data centers have complex structure, multilevel security system, significant maintenance costs, and personnel that must be aware of the variety of peculiarities regarding the maintenance and development of such units. Although, there are many different methods of creating a data center for different kinds of needs. It makes the process of data center planning and development to be rather complicated and long process. Not all companies and interested parties can hire high-class specialists and their teams to perform mentioned operations.

1.4 Limitations of the Study

The available literature is going to be explored to find the gaps in the available knowledge that makes the processes to establish the data center less efficient and time consuming. The limited scope, as well as inability to access as many leaders of the market as possible are the potential limitations of the study.

1.5 Research Structure

The research is organized as follows to present information clearly and logically: Introduction section that includes Background (information about the current state of things in the area), Rationale for the Study (reasons to develop the research), Research Questions (exact issues to be resolved using the research), Statement of the Problem (problematic area to be covered by the research), Limitations of the Study (sufficient gaps in the existing knowledge about the target area), Literature Review (detailed overview of the available literature regarding the development, creation, and securing data centers), Methodology (methods used to obtain, process, and analyze the collected data).

Chapter 2: Literature Review

2.1 Overview

Data centers are built to store information. It is the main asset of any organization big enough to consider building a data center to cover the need in quick and efficient processing of business and any relevant information. Therefore, the issue of security is one of the most critical during this process. There are several options for an organization to acquire a data center: become the client for some company that specializes on such services (IBM, Amazon, etc.); utilize cloud based services (that, however, belong to some third party as well); or build one (Hinkle 2010; FastPCNet.net 2010). The third option is the most appropriate for the large companies as the secureness of information is the top priority. It means that only domestic specialists can have access to databases of a data center – other parties are involved into this process on the limited basis only.

2.2 Planning

Every data center is built according to organization's requirements so in the most cases they differ from each other significantly. However, there is a certain procedure similar for all projects. Thus, conceptually, data center building process includes the following steps: planning, reference designs, cost analysis and design, which includes the process of data center designing itself and site selection (Hinkle 2010). The following figure called Data Center Life Cycle (Figure 1) presents it:

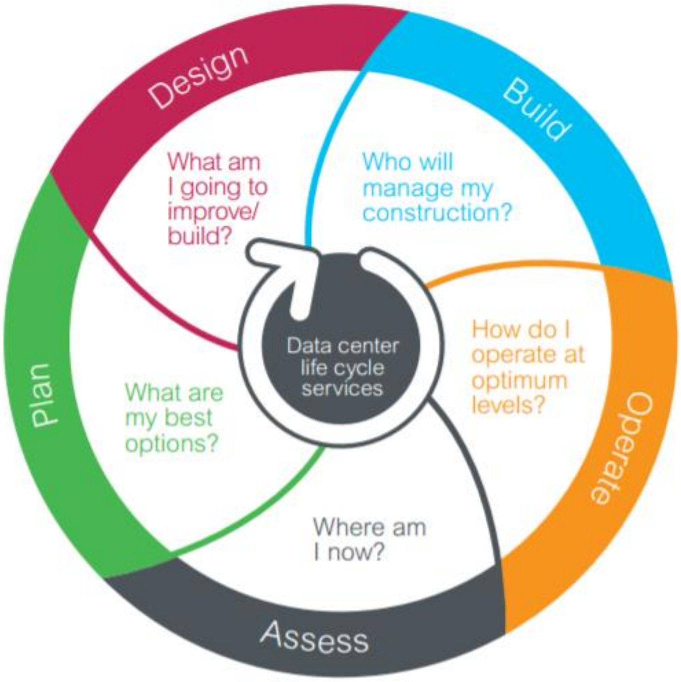
Design
Build
Operate
Assess
Plan
What am I going to improve/ build?
Who will manage my construction?
How do I operate at optimum levels?
Where am I now?
What are my best options?
Data center life cycle services

Figure 1 Data Center Life Cycle

Each stage is utterly important as it develops the necessary background for the successful implementation of the next ones. Thus, step 1 is to identify key parameters of the project to be able to control the budget and general architecture of the system (FastPCNet.net 2010). It is critical at this stage to shape a business need and then work on the determination of the project parameters.

They should be based on the following factors: criticality, density, capacity, growth, budget and efficiency (Smith 2013; Schneider Electric 2016). Step 2 is to develop a concept of the future system. In other words, it is necessary to choose a reference design of data center. This step includes the review of previous factors and adding several new ones such as reputation of the potential suppliers (vendors) and issues with logistics that may emerge in the future (Smith 2013; Schneider Electric 2016). Step 3 of the Planning stage is to merge together the constraints that technical design will have and preferences of the system users and other stakeholders.

This step is too important to avoid or perform it superficially since all next steps will be based on this final draft of the concept (Hinkle, 2010). Step 4 is the determination of requirements important during the implementation process. This procedure usually involves collection of various standards, process requirements, deadlines, and assignments of resources. Additionally, such information as best practices in the area, regulatory compliance standards, and many others is collected (Smith 2013; Schneider Electric 2016). The task of this step is the development of strict rules that should be followed. Finally, Step 5 is assessment of the previous stages to identify any gaps and potential problems that can emerge. It is one of the most important steps in the data center development cycle as it allows to control the quality of the previous work.

It is important to develop the correct, clear, and cost-efficient plan to build a data center that would fit the needs of customer (Beazley 2005). The physical processes will be evaluated using the theoretical and practical background, developed from the appropriate reputable and credible sources. Then, the following components and processes of the mentioned plan will be explored: cost of the data center development, requirements gathering (functional and non-functional requirements) that would comprise the core of data center functionality and usability, the purchase of the required IT equipment (choice, rationale, recommendations), vendor management, issues in the area of data center backups, operation team SLA and the required procedures, review of the organization of reliable and robust security system, establishment of the appropriate service units, and exploration of the best currently exploited practices.

The best way to achieve this is to apply tools and methods, used in business continuity planning. The University of Massachusetts (2009) defines business continuity planning as "the process of identifying critical data systems and business functions, analyzing the risks of disruption to the data systems and business functions, determining the probability of a disruption occurring and then developing business resumption plans (BRP's) to enable those systems and functions to be resumed in the event of a disruption.” In other words, it is the process of identifying the most important and valuable business processes and finding weak spots to eliminate these mitigate their negative influence on the business system’s integrity.

A sustainable continuous business could be created on the appropriate base of material and non-material assets and supported by the everlasting evolutionary changes according to the external and internal influential factors. Other approaches might be successful as well; however, the chances are substantially lower. Many important and influential factors affect the sustainable position and development of any company on a market (Arief & Besnard 2005). Financial situation in a company or organization, of course, is one of the keys to success. The qualification of personnel affects the overall position too. The appropriate managerial, strategic, and tactical decisions allow any company to move forward (Beazley 2005). However, the business data is the main asset for any company or organization of all times. Information and its correct interpretation play a crucial role in the process of the strategic planning and development of the future products, services, etc.

Government’s involvement in business and manufacturing might more likely bring a negative impact on companies’ production (Arief & Besnard 2005). The reason is in control of the carbon emissions and other measures that government facilities implement to mitigate the negative influence of production on the environment. Data centers are among the major consumers of electricity, so their carbon footprint is significant as well to be considered by the mentioned facilities. However, if there is no control at all, some companies might work without caring about carbon emission at all. Implementing rigid quota of carbon emission can slow down the process of manufacturing, as it would often be a restrictive circumstance. Instead, the government can stimulate companies to use the most effective technology in relation to the issue. In that case, the government would not restrict companies but encourage them to improve their strategies (Arief & Besnard 2005). As a result, the data center industry will develop, and carbon emissions would be minimized.

The importance of the data stored in a company's data center is conditioned by the unique experience and peculiarities of the information use in the past. Information from common and accessible sources becomes valuable after it was used for certain goals in order to achieve the particular results (Beazley 2005). Data must be saved from being damaged or destroyed by any means necessary in order to protect the existing achievements of a company and give a chance for the successful future (Beazley 2005).

2.2.1 Threats to Organizations' Data Centers

The threats to the business data and other sensitive information stored in a data center's storages can be divided into two major groups, such as internal and external factors (Beazley 2005). If the first group could be controlled and the aftereffects could be mitigated or even eliminated by timely countermeasures, the second group is not that easy to predicts or prevent.

2.2.1.1 Internal Threats

The internal factors consist of the usual processes of personnel rotation, inevitable aging and turnover of the most experienced employees, transfer of the employees within the industry. They can be controlled, mitigated, or eliminated using the following approaches: appropriate policies regulating employee-company relationships; wise HR policy; and development of the strong corporate culture (Beazley 2005). Any negative outcomes caused by personnel rotation can be controlled by implementing corporate culture and its strong principles across the entire organization. Turnover can be mitigated by experienced HR department. Finally, dangers posed by transfers of the employees within the industry can be eliminated by the disclosure agreements signed by employees that leave a company

2.2.1.2 External Threats

The external factors are as follows: natural disasters, intentional and unintentional damage of the data storages (sabotage and recklessness by employees), industrial espionage, etc. A natural disaster, beyond any doubts, is the most unpredictable (in a matter of long-term prognosis) and devastating external factor that can harm the integrity of any data center and information it stores (Arief & Besnard 2005). It is utterly necessary to develop a plan that should presuppose a complex of measures, including hardware, backup, and organizational measures (Beazley 2005). To be able to create it, it is important to understand each dimension deep enough to be aware of all of its capabilities, opportunities, and limitations.

Hardware solutions are the most well-known part of the plan for most of the companies. It means that different data storages already have developed system of hardware and software tools for the timely and reliable backing up of the data arrays. In case of the natural disaster, the data that is stored on the data servers might not be damaged at all, since it must be doubled previously (Kaieteur Institute for Knowledge Management (KIKM) 2005). This is the case, when more precaution measures do not look excessive. Therefore, the data storages should be placed in the protected and safe places and the number of these places should be more than one (Kaieteur Institute for Knowledge Management (KIKM 2005). It is highly important to perform routine backup procedures and maintain additional storages elsewhere (another location, another branch of a company, etc.) to be sure that data will not be lost due to some natural disaster or other unpredicted situation.

Backup measures, in addition to the hardware solutions, are well known as well. Different backup programs should collect all relevant and important data into the above-mentioned hardware storages (Kaieteur Institute for Knowledge Management (KIKM) 2005). The best ones do it on the real-time basis, so it is necessary to implement as many of these programs as possible into the important business processes. It will allow mitigating the significant aftereffects of the natural disaster and save as much relevant information as possible (University of Massachusetts 2009). In the case of possibility of highly sensitive data loss due to a natural disaster or any other external factor, a company should implement double backup procedures (copying of information to the two different servers in distant locations, for instance).

Organizational solutions are the most difficult part of the plan. All the data stored on the servers' hard drives becomes static and irrelevant very quickly. People are the most valuable sources of information that can be called up-to-date and relevant. Therefore, the following measures should be taken to preserve as much of this information as possible (Beazley 2005). The experienced employees should be encouraged to share their knowledge with newcomers to distribute the "storages" of it and increase the effectiveness of work. In this case, if some part of the experienced personnel could be lost in the natural disaster, other employees could proceed with deep understanding of their spheres (Beazley 2005). It is also highly important to re-check the contracts with other data centers who are backing up the target data center to be sure that all obligations will be performed according to the goals, set by the organization's IT management. These measures could help to protect the unique company's knowledge from the negative consequences of the natural disaster.

2.3 Organization's Facilities Department Responsibility

2.3.1 Place and Facility Structure

Another name for these data centers is the server farm, while the computer room is also used. Regardless of the name, this is the place where all operations and management of servers are performed (Bullock 2009). Any data center includes four major components. Firstly, such element as white space is simply a raised floor that is typically measured in square feet. Even if data centers do not have such a floor, white space is still applied to the environment (Smith 2013; Schneider Electric 2016). Secondly, support infrastructure implies all additional space and necessary equipment that ensure the functioning of data centers.

These include power transformers, UPS, air conditioners and distribution systems, chillers, and many other elements (Bullock 2009). For example, a high-density data center might have so much support infrastructure that the white space will require several times less space for its operations, which should be considered while planning data center (Mills 2006; Smith 2013; Schneider Electric 2016). Thirdly, IT hardware, such as servers and their racks, cables, various network gear, and so on, is used to deliver the DC services to the client (Bullock 2009). Finally, all systems need appropriate maintenance, operation, improvements, and repairs if needed, which is the duty of the operations personnel. Many companies have the staff from IT departments and facility support groups to share the responsibility for operations (Avelar, Azevedo, & French 2012). When a data center operates at its maximum capacity, all efforts are applied to maintain its reliability as well as efficient work of all its systems. IT systems. All servers and devices, be it network or storage, require proper maintenance and regular upgrades (Mills 2006). Specifically, the latest updates for operating systems, applications, or patches are essential for the proper functioning of the entire system, while its system resources must work to their full capacity.

2.3.2 Physical Security, Power and Cooling

Since all supporting systems of any data center are usually heavily loaded, they also require a timely monitoring of their operations and upgrade when required. Thus, uninterrupted power distribution and the use of backup generators as well as cooling and proper humidification of air are essential for the work of data centers (Smith 2013; Schneider Electric 2016). The failure of a device or application, or network connection presents risks to the critical operations of the system. In some cases, the smallest issue in the system might be the reason of a cascade failure of other parts of the system. Thus, eCommerce checkout uses the following program utilities: control of inventory, accounting, credit cards processing, and the variety of others (Mills 2006; Bullock 2009). If one of these components stops working, the entire system will fail. Moreover, the specifics of modern applications lie in their significant dependence on connections or other devices. For a data center to have a maximum uptime, all its systems must be constantly monitored.

The existing complications related to power availability and cooling, as well as extra space is possible to address quickly in the case of optimization of the existing facility (Mills 2006). This implies that the center's overall load can be reduced by using server virtualization and enhancing the facility's efficiency. For example, modern technologies can allow the conservation of approximately 70% of power that is necessary for the cooling and humidification of the environment in the data center (Bullock 2009). Among these technologies are ultrasonic humidification and variable frequency drive units. In combination with modern IT systems, such technologies will enable many data centers to use their resources properly, enhance their capacity, and reduce the overhead of facilities.

In large data centers, such a system enables to have an uninterrupted monitoring of all processes and operations such as power, temperature, cooling, and so on (Mills 2006). A common practice of managing data centers and other IT facilities is to outsource them to the companies, specializing in providing corresponding services. If optimization does not help solve the problem of efficiency, moving the data center is an option (Bullock 2009). Such a move is recommended when the upgrade capacity of the data center is depleted. Thus, it will be necessary to assess the needs and select a site for the new data center. After all calculations and assessments, the existing facility will have to be relocated to a new building (Smith 2013; Schneider Electric 2016). Outsourcing is another alternative to creating a new facility, and it offers two options such as collocation and cloud computing.

Thus, collocation implies that the data center is moved to a facility, which is managed by a provider of appropriate services, but the space is shared with other companies. Modern business models of collocation services are quite versatile, so before choosing any of them, it is recommended to check the agreement terms and make sure that they adhere to the needs of the facility, regardless of their term (Mills 2006). Moreover, flexibility must always be considered when choosing a collocation option since the evolution of the data center is important. The second option is cloud computing. Certain applications that have their specified niche have used shared computing extensively lately (Bullock 2009). Cloud computing is characterized by the quality in service delivery, but some concerns regarding compliance and security prevent it from being deployed by enterprises to the full. Nevertheless, this option is beneficial for those who need to reduce their startup costs and initial expenses.

The task of data centers is the provision of resources for the consumption by end users, but the operations of data centers themselves depend on three groups, namely IT and facilities as well as finance (Bullock 2009). Moreover, each of these groups has its responsibilities. Thus, the IT specialists are responsible for decision-making concerning specific systems or their applications.

They are required to support the operations of end users (Mills 2006). The second group that manages the work of data center is facilities, and its responsibility is physical space. In other words, the group ensures proper operations of all systems as well as their maintenance (Bullock 2009). Consequently, the facilities group will know how efficient data center is overall, how much power it consumes, and how loaded it is. Finally, the operations from financial sphere that are related to data center activities appear to be the duty of the financial unit. It deals with capital expenditures spent on the such processes as upgrade or purchase of additional or necessary assets.

All three mentioned groups face some challenges, and the biggest of them is the nature of a data center (Mills 2006). Thus, it is quite difficult to make data center operate at its optimal range or even come close to it. Typically, a data center has the 10-year life cycle or longer, but its design must be flexible enough to fit the changing requirements to power density or occupancy, which must be done in a quick manner (Mills 2006). Moreover, such aspects as power, space, cooling, and network capabilities must be flexible as well. If the mentioned aspects operate at their limit capacity, the organization will face the necessity to optimize them by expanding current ones or establishing new facilities

2.3.3 Energy Efficiency ("Green" Data Centers)

A data center is considered green when it operates with the minimal impact on the environment while its energy efficiency is at maximum. Thus, its mechanical and electrical equipment as well as various servers and network devices are used with the utmost efficiency. Corporations build green data centers because they want to optimize electricity costs that can be rather high sometimes (Bullock 2009). Consequently, operating expenses on the IT infrastructure are reduced with the usage of green technologies in building data centers. At the same time, the federal government also drives the interest to using such technologies. Furthermore, the U.S. Environmental Protection

Agency (EPA) presented an extensive report that analyzed the trends of energy use and costs in data centers of the USA (Mills 2006). This report also explained current and emerging opportunities that would allow the improvement of energy efficiency in this sphere. Finally, the EPA recommended pursuing such opportunities on the scale of the entire country and implementing various incentive- and information-based programs (Avelar, Azevedo, & French, 2012). The EPA report names two areas in data centers where electricity is consumed the most. Thus, support infrastructure requires 50% of all power, while general servers need 34%.

The energy efficiency of data centers and servers has been significantly improved since this report came out. The increase of density for blade servers enables raising their computation capacity significantly (Avelar, Azevedo, & French, 2012). With server virtualization, organizations can reduce the number of supported servers. Finally, EnergyStar servers offer various options for the use in the private and public server, which enables the reduction of energy consumption by 34% when running general servers (Mills 2006). At the same time, a data center's support infrastructure presents a great range of opportunities for saving in the future. Therefore, combining best saving practices and improving these facilities by introducing ultrasonic humidification or finetuning the airflow in data centers can lead to the reduction of IT load by 30%.

Google's data centers can be used as the example of the best practices used in the area in assuring PUE. The company monitors and calculates its full fleet of data centers all around the world and it does this not only during colder seasons but also throughout the year. Doing calculations, the company counts all sources of overhead (Google Data Centers, n.d.b). The PUE metric is provided by The Green Grid Association - the union of utility companies, facility architects, technology providers, policy maker, and finally users with the goal to raise the resource efficiency of information technology in data centers all around the world.

If the industry continues to grow as it is expected, the use of energy by data centers and related emissions of greenhouse gases will increase too (Avelar, Azevedo, & French, 2012). The experts of the industry find it difficult to publish calculations of the potential growth rate, but the 2020 report of the SMART, which is one of the most respected studies, provides forecast that data center emissions will continue to increase by 7% per year until 2020 (Natural Resources Defense Council, 2014). While the number of researches, predicting that societal carbon emissions will significantly reduce, increases, data centers continue to bring the real and increasing influence on climate.

2.4 Data Center Components

2.4.1 Server Infrastructure

Any data center requires appropriate servers to be installed according to the needs of the customer or users. Therefore, a typical data center usually includes blade servers and rack servers: 1U, 2U, and 4U rack-optimized solutions are combined with blade servers and, sometimes, even stand-alone tower chassis. Modern operational environment requires flexibility that, in turn, presupposes hyper converged infrastructure (HCI) systems use (Robinson 2017). Additionally, solutions that support access to the cloud services are also required as many modern enterprises utilize mixed approach to data management.

The choice of servers in each case is determined by the requirements gathering procedure that is based on the following structure (Bullock 2009). Firstly, it is required to determine an operating system or systems that servers will exploited (Windows environment, Linux, etc.). Secondly, infrastructure influences the choice of servers as well. Location, place, relevant infrastructural solutions, and other factors condition the choice of hardware to the future server room. Thirdly, virtualization support is considered. Scaling and cloud services are important to be well weighed during the procedure of choosing servers and other hardware. Finally, and fourthly, energy efficiency is one of the critical factors that should be considered during the process of choosing servers for a data center.

2.4.1.1 Domain Naming Servers

Directories can be very different in regard to the stored information (Bullock 2009). One directory services were designed to support only certain few types of information, such as telephone directory or domain name system (DNS). Telephone directory, for example, stores names and telephone numbers. DNS these items are domain names and IP addresses. Other directory services, such as the one, used by network operating systems (NOS), are supposed to manage the items (nods) used by the operating system. Users, computers, printers and other resources to share can be named as these resources.

Directory services, in general, are called services for naming. They map the network resources names to the network addresses that correspond to these names (Mills 2006). According to such approach there is no need for a user to memorize the physical address of a resource in the network. Name, mapped to the requested resource, will easily locate it. The scheme of work is rather simple and transparent (Smith 2013; Schneider Electric 2016). Such examples of directory services can be provided to give an understanding of what these services are: domain name system (DNS), Red Hat Directory Server, Apache Directory Server, Active Directory, Open Directory, OpenLDAP and others (Mills 2006). According to the concepts, described above, these directory services should be implemented in every operating system to provide such necessary and useful services.

2.4.1.2 Active Directory Servers

Windows-based operating systems use Active Directory as directory service (Bullock 2009). Apple Open Directory is used in the operational systems from Apple, Inc., like Mac OS X and Mac OS X Server. Rad Hat Directory Servers is implemented in Rad Hat Enterprise Linux (Mills

2006). Various Unix and Linux-based operating systems use eDirectory as directory service. This directory service has evolved from the previously known Novell Directory Services (NDS).

The implementation of Active Directory in Windows-based operational systems is based on the presentation of any information as an object. Literally, everything in the system is an object for Active Directory and these objects fall into two categories: Resources and security principals (Bullock 2009). The first category consists of printers and all other physical resources of the system. The second category includes users, accounts and groups, available in the system. Every object has its unique name that identifies it and a set of attributes that describes this object (Mills 2006). Thus, the administrator can easily determine policies of access to different objects and users can find and use any resource of the system, using only name as identification.

Open Directory, used in Apple's operational systems, has a structure different from Active Directory and is based on modular Directory Services system (Bullock 2009). Mac OS X, in general, hosts Open Directory Domain and this domain is paired with Open Directory Password Server that gives access to the resources in the network according to the permissions, set by the administrator (Bullock 2009). Novell eDirectory, which is often used in Unix and Linux-based operational systems, is a hierarchical, object oriented database that uses the dynamic rights inheritance. Such approach allows global and specific access control of the assets at the same time.

There are many advantages of using directory services in the network operating systems (NOS) (Smith 2013; Schneider Electric 2016). Directory services greatly simplify the usage of network resources since users do not need to understand the specifics and topology of the network, they do not need to find out and remember the names of network resources, such as printers or network storages of information (Mills 2006). Users do not have to log in to several servers to get access to the resources that this server has. All these points of interest in the network are available for users in very simple and transparent way. Another advantage is in the simplicity of administrating such network or computer (Mills 2006). The system administrator has a clear image of what is going on in the system, what users and groups are present in the system or in the network. Thus, this administrator can restrict or give access to various resources for different users very quickly and easily (Bullock 2009).

The disadvantages of directory services are present as well. However, work at improving existing services never stops to remove the narrow places in their overall implementation. Various operating systems like Windows-based, Unix and Linux-based and Apple's, have their own standards, so their effective work with each other is limited by standards restrictions (Bullock 2009). Usually, directory services are structurally flat file databases, which puts certain restrictions to the size of the database. A big database works rather slowly and can cause overall reduce of system or network efficiency. All these disadvantages can be resolved, using more open standards in the industry, which is definitely in the plans of leading developers of applications that provide directory services.

Directory services are very useful for the personal computers' operational systems as well as for networks of different range (Bullock 2009). They make the process of getting access to the resources on the computer or on the network computers mush simpler. Administrating of network and computers is far more convenient and simple using directory services (Mills 2006). The further development of these technologies should eliminate the current disadvantages of the directory services and make them even more useful for end users.

2.4.1.3 Access Management & Authentication Rules

Architecture of data center's software layer is utterly important to be developed according to the highest standards of the industry. Directory service is only the part of the mentioned infrastructure that, however, plays very important role in the proper functioning of a data center. The software system that stores various information, organizes and gives access to it is usually called a directory service (Bullock 2009). The main concept of directory service can be described as the storage of different types of information that corresponds to one item, like name in the network, for example.

As for the alternatives for directory services, relational databases could become one, but they have number of restrictions that might not allow using relational databases as the replacement of directory services (Mills 2006). Among these restrictions are: information in directory is read more often that written, which, by-turn, makes such features of database, like rollback, and others, related to the transactions, less important; data in the directory can be excessive in case it helps performance (Bullock 2009). These peculiarities make directory services more useful for administering information and resources in the networks and computers.

Any system can crash sometimes, and it is inevitable. Various reasons might cause such a crash. Directory services are not an exception and they crash too. That is why such options as backups of databases to several storages are made to prevent the data loss (Bullock 2009). The incorrect information, stored in the directory services database, due to the corruption of the hardware or malicious software can paralyze work of a single computer or entire network. Thus, these databases usually can be restored from several places, if all security measures were performed correctly (Smith 2013; Schneider Electric 2016). The administrator can restore the database from the backup server, which can be located in the same network and must be highly protected from the possible malfunctions of hardware and software (Bullock 2009). This data can be restored from external data carriers, to which it can be backed up simultaneously. The information, corrupted in the directory service database on some server of the network could be restored from the global catalog servers and operations master servers, which keep full replica of all objects within the domain (Mills 2006).

2.4.2 Network Infrastructure

The major purpose of any contemporary data center and its networking component is to accommodate various users with the workloads necessary to fulfill their requests. This is the case when servers perform as components providing users with the required services (Bullock 2009). Modern data center networking infrastructure is based on the two different approaches. Thus, a conventional (used prior to the emergence of cloud computing and the related services) network of a data center includes the following components: servers, switches, routers, controllers, gateways, and clients. The following figure presents it schematically:

Resources of such network have common system of mapping using network standards and conventional technologies. It means that the network utilizes Internet Protocol (IP), Ethernet, and variety of other technologies related to this area (Bullock 2009): Layer 3 IP addressing, TCP/IP, MAC addressed, and many others. Issues, caused by the limitations of these basic technologies usually resolved using additional protocols such as Virtual Extensible Local Area Network (VXLAN), OpenFlow, and others. The following figure demonstrates the networking scheme that conventional data centers usually exploit:

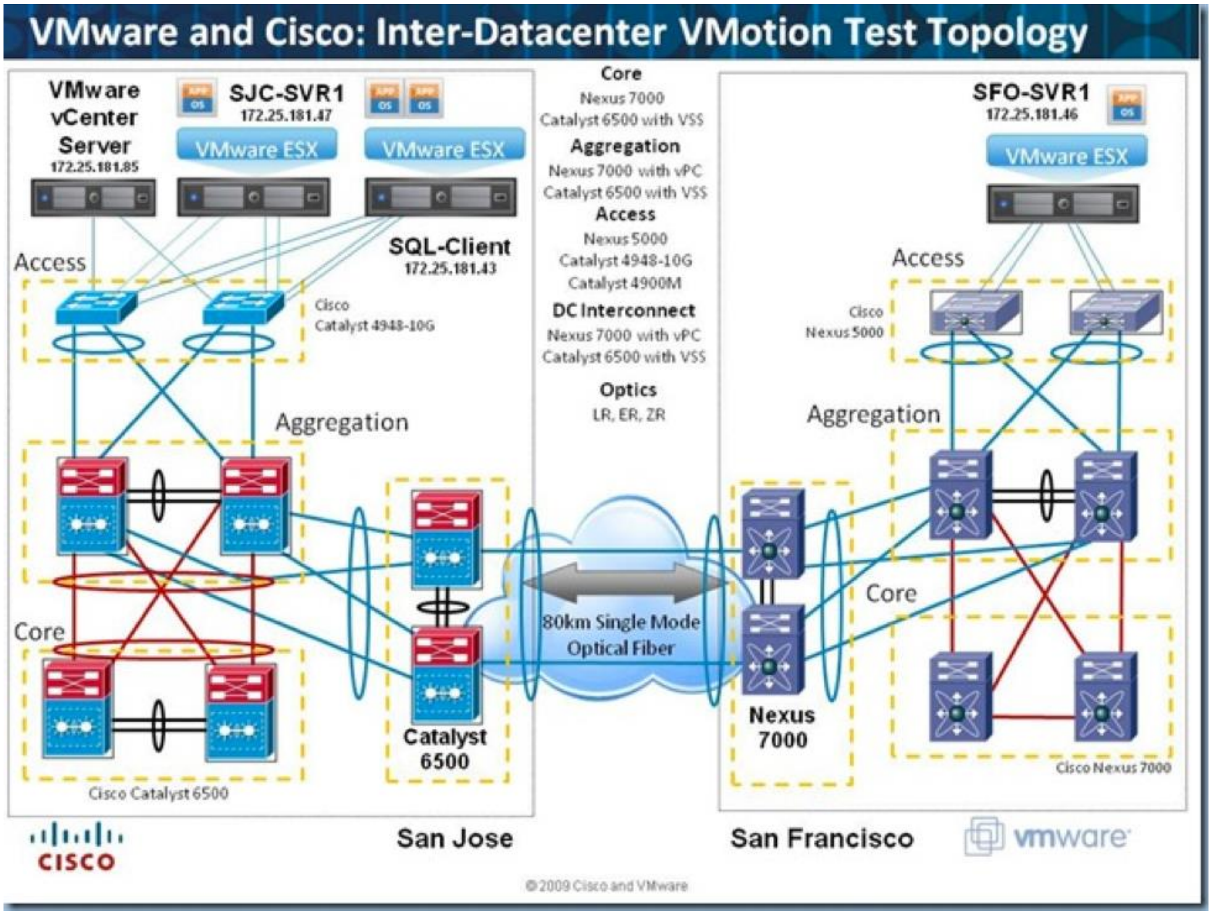

Figure 2. Networking Resources, Hardware, and Software of a Data Center Network (SDX Central 2016)

The second approach to building a data center network is the use of software-defined network (SDN) (SDX Central 2016). It is applied when the load is conditioned by dynamic workflows changes. The need to accommodate resources with users more efficiently emerges. When such approach is used, the workflow is divided into the following categories: the documents (media) that clients used (the data plane), and the data transmitted to servers regarding the procedures of processing the mentioned documents' or media (the control plane) (Bullock 2009). Therefore, a special SDN controller is exploited to adjust the workload according to the current mapping of data plane.

Storage space is usually allocated according to the needs of data center user that are determined by the peak load that has been recorded during previous session of data transfer. It means that when user exploits data server storages, the controller records highest load to reserve space for the next potential data processing procedure (SDX Central 2016). If space is not sufficient, new peak is recorded. Unused space is allocated for another user in the end of session. Business requirements usually determine the average space required for allocation. Scalability of storage space can be achieved using modular systems and redundant server racks' installment (Bullock 2009). The same procedure should be performed for backup and restore procedures. The main principle of assuring safe scalability of data center storages is provision of available and planned (+50%, +80%, +100%, etc.) scalability by the appropriate backup space (Bullock 2009). Redundancy is welcomed in this case.

It should be noted that modern datacenters are less attached to physical limitations and geographical constraints these days. In other words, a data center can have distributed network bond together by the specialized devices (routers, for example) and work as whole effectively (SDX Central 2016). However, it creates certain problems for assuring the data security, including physical protection of servers. Conventional data centers become less popular as various cloud-based infrastructures provide more convenient services (Bullock 2009). Modern businesses prefer switching to "software-as-a-service" paradigm of performing business operations that require data centers (SDX Central 2016). Cloud platform is much more popular these days than data centers with numerous servers and complex networking structures.

The evolution of cloud implied that networks became virtual, which presupposed that physical processors were not linked to the provided services. Consumers associate cloud computing with storage space of varied capacity where they can store their photos, documents, and so on (SDX Central 2016). However, virtualization enabled the creation of cloud data centers in the sense consumers perceive them. In other words, virtual components have enabled unlinking addressable files in distributed file systems from their physical storage (Bullock 2009). These file systems can include a great multitude of volumes that are spread over many domains. These components are managed by SDN controllers of large networks (SDX Central 2016). At the same time, small ones, which are usually enterprise networks, are run by virtual ones where file systems are pooled together by workload orchestrators.

With the further disaggregation of data center networking, it is no longer correct to talk about 'center' itself as this notion gains a more abstract meaning (SDX Central 2016; Bullock 2009). Specifically, 'center' no longer means a physical place where the management and operation of all assets are performed. Instead, this can be an array of IT resources that can be accessed in many ways when a business owns it or on a lease/subscription basis.

2.4.3 Storage Infrastructure

A data center is a complex system that has multilevel architecture. Specialized software and operating system establish the link between the hardware storage and the requirements that users have. The major task of data centers software is to provide meaningful information according to the requests of a company's employees or other authorized users (IT personnel, for example) (Mills 2006).

2.4.3.1 Storage Area Network

Storage area network is the specialized network, whose main purpose is to provide and facilitate data transfer between computer systems and storage elements. Thus, a common SAN consists of the following layers: communication infrastructure (physical layer) and management of the connections, storage elements, and computer systems (logical layer). According to Tate et al. (2006), "SAN is a specialized, high-speed network attaching servers and storage devices and, for this reason, it is sometimes referred to as "the network behind the servers." As for the SAN components, fibre channels dominate as the connectivity channels using which most of the SANs are built (Barker & Massiglia 2002). They use FICON as the standard protocol for z/OS systems, and such standard protocol for open systems as FCP. Figure 3 illustrates components used in most SANs:

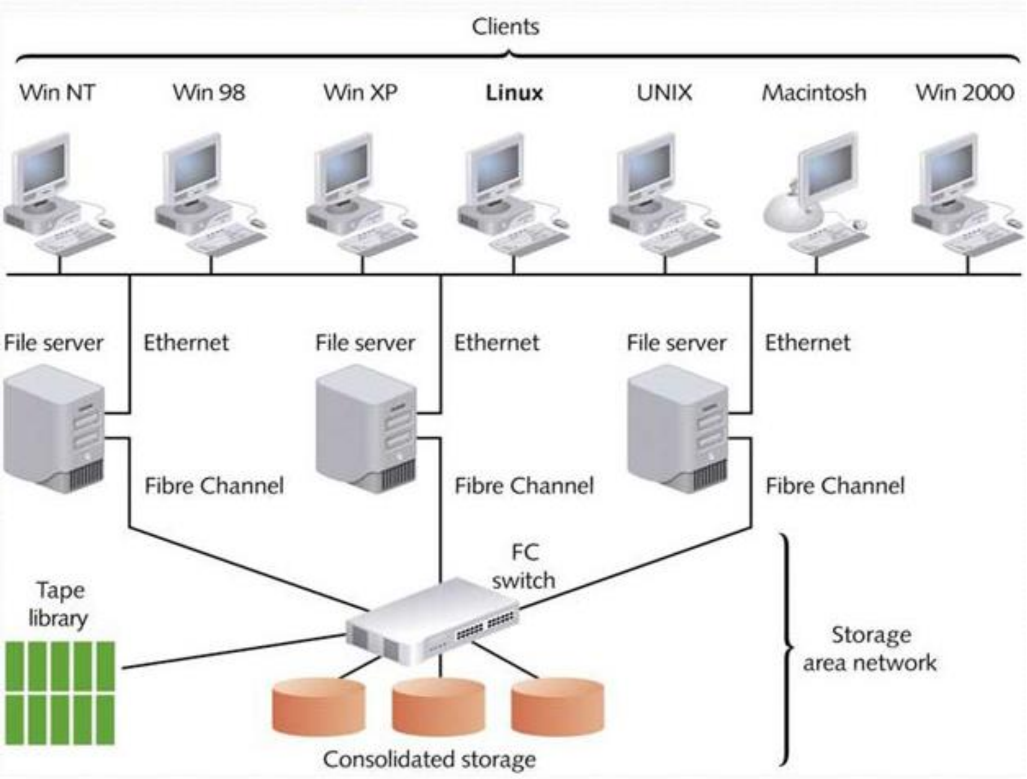

Figure 3 SAN Components (Dean 2005)

SAN is aimed to provide business (and any other customer, if needed) with high-speed, large capacity solution to store and retrieve information for any possible needs. Therefore, the main benefits of SAN are as follows, considering its business orientation mostly: simplification of infrastructure, management of information lifecycle, and assuring continuity of business. Typical SAN provides business with such components as storage (disk systems – JOBD and RAID; and tape systems - tape drives, tape autoloaders, and tape libraries), connectivity (speeds from 1 Gbps to 10 Gbps using Ethernet, fibre channel, and SCSI interfaces), and servers (mainframes, UNIX-, Windows- based, and others) (Tate et al. 2006).

SAN is the solution that is usually used for solving large-scale issues in the companies of big size. Therefore, SAN should be applied in large companies to servers as the storage for information. Small or middle-sized companies can apply this solution as well. However, the price of the average SAN is way above acceptable line of expenditures of middle-sized business, not to mention small companies (Barker & Massiglia 2002). In addition, the capabilities of SAN in most cases are designed to serve large-scale companies and their application in smaller businesses would be unwise considering the inability of such business to load the capacities of SAN in full. Referring to the advantages, assured for a business by common SAN solution, we can outline disadvantages as well. The cost and complexity are the most obvious issues to consider in case of SAN planned installation. According to Breeding (2002), "IT departments will need to include technical staff with expertise to manage the SAN in addition to those that support existing LANs and wide-area networks (WANs). The fibre optic network and the communications equipment that compose the SAN require significant investment as well."

SAN is designed to assure reliability and zero fault tolerance in its operations. Therefore, there is an obvious need to assure certain level of redundancy in SAN solutions. It means doubling or tripling RAID configurations, multiple controllers and power supplies to be included in each SAN (Breeding, 2002; Tate et al. 2006). Thus, each level of redundancy substantially increases the overall expenditures of the end-user for SAN installation. Among onother issues, the following limitation of SAN can be emphasized. SAN model does not presuppose the attachment of multiple servers to the same device in order to share files directly (Breeding, 2002; Tate et al. 2006; Bird, 2002). A SAN model operates with information, so we can conclude that there are two major requirements to be applied to SAN: reliability and speed of data transfer. We have already discussed the reliability in terms of undertaken steps (doubling and tripling critical components and systems) (Barker & Massiglia 2002). Now, the speed of operations is assured by the technologies used in SAN. The following current and emerging technologies are used in SAN today: Ethernet (up to 10Gbps), SCSI, fibre channel, iSCSI, TOE, etc. (Breeding, 2002; Tate et al. 2006; Bird, 2002).

10 Gbps Ethernet. Ethernet adapters are usually used to connect servers or workstations and serves. It uses the familiar IEEE 802.3 Ethernet media access control (MAC) protocol and its frame format and size. Common topology is a usual bus. This technology is well known and can provide bandwidth up to 10Gbps. However, it is rather unreliable and outdated (Breeding, 2002; Tate et al. 2006; Bird, 2002).

SCSI. The small computer system interface (SCSI) is well known as a parallel interface. The devices supporting SCSI connect to form a terminated bus (such kind of bus is terminated using a terminator). This technology has been known for a long time, has many configuration options for error handling and supports both disconnected and reconnect to devices and multiple initiator requests. The major drawback of the technology is the limitation of cable length (25 meters) and a maximum of 16 devices that can be connected to one SCSI bus.

Fibre channel. It is a serial interface, usually implemented with fiber-optic cable. FC is the primary architecture for the most existing SANs these days. This technology provides high-speed connection, it is reliable, and allows to overcome restrictions of SCSI which is maximum cable length is of 25 meters long allowed. Among the disadvantages, the most obvious one is the cost of such solution for the end-users (Breeding, 2002; Tate et al. 2006; Bird, 2002).

iSCSI. Internet SCSI (iSCSI) is a transport protocol that is able to carry SCSI commands from the source to the target. Therefore, it is a data storage networking protocol that can transport SCSI requests of the standard TCP/IP technology. It is used for both storage and data networks. The main advantage of iSCSI is the elimination of the need to build a second network technology just for storage (Third I/O 2008).

TOE. TCP offload engine or TOE is a technology used in network cards in order to offload processing of TCP/IP stack so that network controller could process the data. The main applications of TOE are gigabit Ethernet and 10 Gigabit Ethernet (Third I/O, 2008). It is also often used to reduce overhead associated with IP storage protocols (iSCSI and NFS) (Breeding, 2002; Tate et al. 2006; Bird, 2002).

2.4.3.2 Network Attached Storage

Network Attached Storage (NAS) is a solution of different kind – it is a LAN-attached file server that utilizes some network protocol to assure file storing and sharing. Usually Network File System (NFS) is used. Typical scheme of NAS is an engine that provides file services (using NFS and CIFS), and one or several devices that store data. NAS can be attached to any network. Breeding (2002) states: “NAS devices embody many characteristics of the classic file server, but are stripped of all software features and hardware components except those related to file sharing.”

NAS can be applied for variety of purposes. According to Breeding (2002), “NAS devices embody many characteristics of the classic file server, but are stripped of all software features and hardware components except those related to file sharing. They include high-performance network interfaces, typically 100 MB/second Ethernet or Gigabit Ethernet (though we do expect to see NAS over Fibre Channel in the near future as well).” As we can see, NAS can be used in any system that requires backup solution and does not need the redundancy provided by SAN (Barker & Massiglia 2002).

NAS has the following features: it is built according to the storage-centric design (server manages the data but NAS provides it); the performance of a typical NAS depends on the purposes it is built for – small, midsize, large business needs; it is less expensive and less sophisticated than SAN (Barker & Massiglia 2002); NAS does not require doubling its systems because of the less sophisticated and complex design and other than SAN purposes of application; “NAS is an ideal solution for serving files stored on the SAN to end users in cases where it would be impractical and expensive to equip end users with Fibre Channel adapters” (Tate et al. 2006).

NAS emulates a network file server, once connected to a network. Among its standard features, HTTP and FTP access can be mentioned. Common NAS can be accessed by the client directly or “can be mounted by application servers” (Breeding, 2002). NASs exploit transparent authentication procedures to provide users with the opportunity to avoid re-creation procedures of user accounts and access control lists.

One of the major limitations of NAS is data backup procedures. NASs do not use the technologies and methods of SAN in order to serve their purpose at lower costs. Therefore, it could be difficult to assure data consistency and assure its safety using NAS (Barker & Massiglia 2002). Despite the capability of some NASs to backup data using inbuilt tools, it does not protect from a system-level failure. In addition, such backup procedure (taking a snapshot of data) can take hours of time.

2.4.4 Security Infrastructure

2.4.4.1 Data Centers Security Architecture

Data center security is one of the core issues that a potential owner of DC should care about (Mills 2006). Factually, secureness of information stored in it is the top priority of any IT department, maintaining and supporting data center of its company. Modern means of communication such as mobile gadgets require access to the secured network to perform operations remotely (Mills 2006).

It adds security issues and requires more thorough and well-thought approach to the development of the data center infrastructure. Various protocols and methods were developed to provide architecture of data centers with the appropriate level of secureness. IBM is one of the pioneers in this area.

IBM has developed the synchronous data link control protocol in order to use it in the systems network architecture (SNA) environment for a reason as well. According to Dong (2007, p. 471), "The DATA LINK CONTROL Layer provides the error-free movement of data between the NETWORK ADDRESSABLE UNITS (NAUs) within a given communication network via the SYNCHRONOUS DATA LINK CONTROL (SDLC) Protocol." SDLC protocol is addressed to a computer communication and it is the protocol of the layer 2 for SNA (Mills 2006). The protocol supports multipoint links and error correction. It is assumed that an SNA header presentation goes right after the presentation of the SDLC header. The protocol was used by IBM mainframe and middle range system. However, there are implementations for many platforms created by many vendors.

Today, SNA and SDLC are used less often. The reason is in the continuous replacement by IP-based protocols. In addition, SDLC is being tunneled through IP more often too (Mills 2006). The protocol operates independently, considering each communications link. SDLC protocol is able to operate on point-to-point multipoint or loop facilities; switched, dedicated, two-wire/four-wired circuits; and it can work with full-duplex and half-duplex load. The most unique characteristic of the protocol is that it is able to mix such stations as half-duplex secondary with full-duplex primary on four-wire circuits (Mills 2006). It provides the opportunity to lower the overall price of dedicated facilities.

The following architecture is utilized in Cisco data centers: threat defense, content security, virtualization security, and secure access. Threat defense refers to the high-performance firewall that can be easily scaled in the case of necessity. Additionally, it includes services that prevent intrusion. Content security is guaranteed by services based on cloud technologies (Mills 2006). This security layer prevents malware intrusions into a protected system. Virtualization security is based on the exploitation of highly-advanced switches with zone-based security, regulated by the appropriate policies that can be set by an administrator or other entity with the appropriate clearance. This layer of defense assures the secureness of data at the level of virtual machines (Mills 2006). Finally, secure access is granted by the special software that provides personnel and remote access parties (smartphones, laptops, etc.) with secured and limited according to the security policies access to the databases of data center.

2.4.4.2 Categories of Potential Attacks on Data Centers

2.4.4.2.1 Technical Imperfection

Technical area secureness of connection is perceived as one of the problems in internet security. Hence, traffic interception to get necessary information can be done through the authentication process. Arief & Besnard (2005) stated that technical imperfection of authorization solutions forms a threat as it facilitates the process of acquiring the authorization data for the third parties. Poor encryption methods that are used to protect websites' databases from hackers' attacks are seen as another major technology related problem. Simple algorithms used to encrypt a database with users' authorization information could be cracked for a relatively minor time, which gives no opportunity to apply any extra emergency measures to protect it.

2.4.4.2.2 Internet Security

Distributed-denial-of-service (DDoS) attack on a server would easily result in collapsing the security system if a group of hackers wants to perform DDoS attack (Arief & Besnard, 2005).

However, and given the fact that users are the weakest spot in the security system, poor password management solutions could provide access to the highly secured system without even breaking into it. Hence, poor password management is not connected with technical solutions (Arief & Besnard, 2005). Users could create trivial or easily predicted/guessed passwords, forget passwords, tell them to the third parties, write them down in order to remember, and make many other mistakes that an IT manager could miss. Therefore, password management that is not user friendly, complicated, and unsecure can be a substantial threat to the security system as well.

2.4.4.2.3 Patch Management

Another threat to data center internet security is patch management; following appropriate maintenance of all software solutions that are present in the IT infrastructure of an organization. Recall that updating Software for software solutions is considered common practice by IT managers (to fix bugs, improve, extend functionality and/or add new useful features), some IT managers might think that patch management is running automatic updates of the software solutions which is not true. The fact that any software needs patches confirms the idea that there are weaknesses in any system that can be used for the unauthorized access by the third parties. It is not that obvious that patch management influences security as much as password management does but it is true. This implies that password management techniques can be used in patch management in order to improve performance and ensure data security. Intrusion detection system (IDS) and intrusion prevention system are the parts of computer and network security system of any organization that wants to keep its information untouched. Intrusion detection, in general, is the process of tracking the possibility of the events that could occur in any computer system or network and processing the events in terms of identifying their nature

2.4.4.3 Detection

Intrusion detection system (IDS) and intrusion prevention system (IPS) are the parts of computer and network security system of any organization that wants to keep its information safe and secure. Intrusion detection, in general, is the process of tracking the possibility of the events that could occur in any computer system or network and processing the events in terms of identifying their nature. The datacenter units that track such incidents and monitor networks are called IDS. In more general meaning, IDS are also added with prevention systems and called either IDS/IPS or IDPS. IDPS of different kind is an important part of nearly every security system in most modern organizations (Scarfone & Mell, 2007). IDS can be a software as well as hardware solution. It includes sensors, console, and central engine to detect such malicious things as viruses, worms, attacks, etc. (Computer Forensics, 2006).

There are several types of intrusion detection techniques and technologies available to an organization. Along with above-mentioned methodologies, the following can be outlined: signature-based, anomaly-based, and stateful protocol analysis. In addition to the previous descriptions, signature-based detection is based on recognition of patterns that can be compared with previously detected threats. For example, the following previously detected signatures can be provided: an attempt to connect via Telnet, using username “root”; an e-mail with subjects of attractive sense (such as “Free pictures!”, “Music free download”, and so on) and attached .exe files, which are well known peculiarities of malware; log entry to operating system with status code value of 645 that means disabling of the host’s auditing (Scarfone & Mell, 2007). Thus, such technique is rather effective in cases when known threats are detected. However, the advancements of networking technologies and a growing number of threats make this technique rather ineffective.

The advancements of networking technologies have provided so-called enthusiasts with numerous tools and capabilities to create viruses, worms, and other similar programs in order to attack computers via any network. For the decades of networking technologies evolution, the following methods of attacks were developed and applied: Denial-of-Service (DOS) attacks, eavesdropping attacks, spoofing attacks, intrusion attacks or User to Root Attacks (U2R), logon abuse attacks, and application-level attacks. DOS attacks are commenced rather often on the Internet and are aimed to harm particular services or companies (Karthikeyan & Indra, 2010). Application-level attacks exploit the weaknesses in the application layer in order to gain access to a system. This type of attacks includes commonly known viruses, Trojans, etc. (Karthikeyan & Indra, 2010; Scarfone & Mell, 2007).

Tenable Nessus. This product is presented by Tenable as the best vulnerability scanner in the industry. It has such features as “high-speed recovery, configuration auditing, asset profiling, sensitive data discovery, and vulnerability analysis” (Nessus.org, 2011). Tenable Nessus can be used throughout an enterprise, regardless of the physical configuration of the networks. An organization has to purchase a ProfessionalFeed subscription to be able to perform network scans for vulnerabilities. The price of each ProfessionalFeed is $1,200 per year.

BackTrack. This product is based on Linux. It is an operating system that includes a variety of tools for digital forensics and penetration testing application. The following categories of tools can be found in BackTrack arsenal: “Information Gathering, Network Mapping, Vulnerability Identification, Web Application Analyses, Radio Network Analyses, Penetration, Privilege Escalation, Maintaining Access, Digital Forensics, Reverse Engineering, and Voice Over IP.” (BackTrack.org, 2011). BackTrack is free of charge however, the price of paid support plans varies.

Metaspolit Express. Finally, this product provides security professionals in enterprises and government agencies with the appropriate opportunities to carry out penetration tests quickly and easily. Metasploit Express adds graphical user interface to the Metasploit Framework that is one of the standard de-facto in the industry of penetration testing tools. The product allows automating many tasks, avoiding custom scripting (smart brute forcing, evidence collection, reporting, etc.) (MetaSploit Express, 2011).

The following operations can be performed, using this tool: discovery of vulnerabilities, testing of penetration opportunities, evidence collection, and cleanup in order to verify system security. Metasploit Express can be combined with NeXpose vulnerability management tools in order to provide IT professionals with realistic scoring of risks. The price of the solution is $3,000 per year/per named-user. As for the limitations of each product, they are as follows. Tenable Nessus – the interface is nothing more but flash based one, accessed via web browser; it does not allow to schedule scans; this product is recommended to be used in small organizations that perform occasional scans only due to the above-mentioned limitation; the admin zone of the interface is not protected anyhow and any users with access to the server can add themselves to the list of allowed users (Nessus.org, 2011).

BackTrack – it is difficult to use the set of tools without the appropriate level of knowledge and skills; it has rather limited documentation that presupposes rather hefty learning curve; and regardless of the fact that it has numerous free toolkits available, low cost support makes the learning curve high and it reflects on productivity; in addition, with tools that are foreign to users, there is serious potential to miss obvious weaknesses (BackTrack.org, 2011).

Metasploit Express – it is the most comprehensive and powerful tool set for penetration testing. However, the price limits its use by businesses only because $3,000 is not the price to pay for domestic penetration tests or occasional small office tests. In addition, Metasploit Express demands rather powerful computers to run because it consumes CPU time rather intensively (MetaSploit Express 2011). Therefore, it is easy to conclude that limitations of each product define its niche on the market. Tenable Nessus can be used by small/home offices due to the particular limitations and rather affordable price. BackTrack is the choice for the professionals of high level because of the level of skills and knowledge, required to use this set of tools. However, it is free (or almost free) of charge so it can be a rather wise solution for any office, considering the situation with IT staff professionalism. Finally, Metasploit Express is powerful, user-friendly, with web-based interface, comprehensive solution for enterprise or governmental use due to its price tag.

The penetration test for a data center should be performed using these three tools as complex system. First, it is necessary to perform vulnerability assessment using Tenable Nessus scanner. Assessment of vulnerabilities will provide only the "map" of possible weak spots in the security system of data center IS. Then, BackTrack arsenal and Metasploit Express tools should be used to perform penetration test, also called "ethical hacking".

Ethical hacking is penetration testing in its best meaning. It is performed by former hackers, so-called "white hats", who apply their abilities, skills, and knowledge for testing various networks in terms of their secureness and ability to resist penetrations (Shavit, 2011). In our case, it is very important to ask one of such specialists to perform penetration testing, using the above-described tools and methods. Thus, combination of rather specific experience and skills would allow penetration-testing team to determine the most possible points of potential security breaches.

2.4.4.4 Penetration Testing and Vulnerability Assessment

The difference between penetration testing and vulnerability assessment is rather obvious: vulnerability assessment allows identifying possible vulnerabilities of a network, while penetration testing is the process of getting actual access to this network, exploiting the above-mentioned vulnerabilities. A vulnerability analysis determines the flaws of the security system in a network. Penetration testing is aimed to evaluate how critical these flaws are and which ones are the most crucial for the network security (iViZSecurity.com, 2009). The process of vulnerability assessment is usually passive. The incoming and outgoing traffic are being analyzed; the entire system is monitored for unusual events and other issues in order to determine possible attacks on the network. Penetration testing, on the contrary, is the process of active network penetration by ethical hackers in order to find security gaps.

The "area of interests" for vulnerability assessment is potential risks, while penetration testing proves crucial potential of these risks becoming problems. The scope of penetration testing is broader and includes validation of security vulnerabilities if necessary. According to iViZSecurity.com (2009), "A Vulnerability Analysis answers the question: "What are the present Vulnerabilities and how do we fix them?" A Penetration Testing simply answers the questions: "Can any External Attacker or Internal Intruder break-in and what can they attain?" More to say, vulnerability analysis is needed to see the entire picture of network secureness. Penetration testing is only a snapshot at each given moment of time. Both procedures are vital for the appropriate security functioning of any network, regardless to the size of an enterprise of governmental organization (iViZSecurity.com, 2009). However, penetration testing should be performed by the appropriate specialists only.

2.4.4.4.1 Vulnerability Assessment Steps

Network inspecting & information gathering are the first steps of vulnerability-assessment process. The IT manager/consultant starts with inspecting the Internet Protocol (IP) addresses, domain names, routers, and open firewall ports. Vulnerabilities existence check on the given systems is conducted and hence a search for a way to gain access to systems deep in the internal network. The IT manager/consultant then will be searching for password files, customer data, and confidential company information, such as payroll files. These tests can be performed through technology attacks or good old social engineering. If a company hires a strong consulting company, its social engineering experts could be able to gain access to its network without launching a single network attack.

2.4.4.4.1 Tools

The vulnerability test is performed using the appropriate vulnerability scanner, like Tenable Nessus, for example. It has to be configured properly, according to the needs of the test and done by the specialists (Securitytube.net, 2011). Configuration has to consider all the peculiarities of the network configuration in order to perform the test with maximum efficiency.

Chapter 3: Proposed Framework

3.1 IT Infrastructure and Change Preparations

The primary task is to determine the activities that should be performed in order to reorganize the large company’s IT system and prepare it for changes. The organization’s IT Management should perform the IT audit that will help reach conclusions regarding useful findings in different departments and offices of the organization. However, the overall situation might still be unsatisfactory. Considering the mess (if any) in the company’s IT structure, the first stage of the task completion should be focused on the following: the unification of methodology and technical standards; the consolidation of data centers and networks; and the standardization of servers’ hardware and platforms (NiBusinessInfo.co.uk).

The centralization of certain IT processes, like the creation of a centralized data center, a common website for the different divisions of the company, etc. should facilitate the maintenance of the IT system, which should positively influence the response time and mitigate the negative aftereffects, caused by downtimes (NiBusinessInfo.co.uk). The second stage is the determination of the areas, in which it could be more appropriate to outsource the IT services that do not fall into the category of strategic ones. Outsourcing of non-strategic IT services should allow cutting the costs and decreasing the number of employees, involved into the company’s IT area. The overall optimization of the IT processes, including non-strategic ones, is utterly important in terms of the development of an appropriate plan.

The implementation should be sequential because of the following reasons: a simultaneous implementation of strategic projects would create problems in different areas such as personnel engagement, funding, etc.; the projects’ functionality could overlap and create additional problems during testing procedures, training of end users, etc.; and the implementation of multiple projects at the same time could interrupt the continuity of business processes of the company.

After the preparation stage, it is advisable to choose the appropriate projects to implement that would give the maximum output for the most optimal cost. The main focus should be on the IT infrastructure since this is the major problem of the entire corporation. Thus, the following projects should be implemented (sequentially): networking, computer hardware and software, data warehouse, messaging system, and website.

3.2 Implementation

Networking. The importance of this project is beyond any doubts, because this is the physical layer for the following standardization of the entire corporate IT system. The main goal of this project is to connect data center devices together as planned, as well as making sure all corporate offices and the data center are both connected on the new network and provide them with opportunity to share information without any obstacles (Mills 2006). The information flows that would provide continuous exchange of the most updated information could improve the overall quality and efficiency of the company's products and work (BusinessLifestyleSolutions.com.au).

Computing hardware and software. This is the next stage of the project that however, could be singled out to the separate subproject, because of its scale. The company's IT systems have too many differences in the numerous offices of the company's global structure. Thus, the hardware and software solution, applied there differ greatly as well (for example, AIX, UNIX, Windows NT, 2000, and others are used simultaneously) (Mills 2006). Therefore, the overall upgrade of the existing systems to the level of hardware and software performance would allow implementation of different sophisticated financial, procurement, customer support, etc. systems in every office of the company without any issues (Kelly 2010; Jeffery, Norton, and Yung 2006).

Data warehouse. The following stage of the IT infrastructure remodeling and improvement project would facilitate access to the data and provide eased adding, editing, storing, and retrieval of different kinds of information (Mills 2006). A centralized database with access from any office of the company would decrease the time needed in decision making and thus, would gain the competitive advantage for the company. In addition, the operational control of the business processes would be facilitated as well, because of the most up-to-date information regarding these processes (BusinessLifestyleSolutions.com.au).

Messaging system. Effective communication is important these days as never before. New messaging system would allow avoiding different problems, such as orders' duplication, lack of operative information in the other departments, customer services, etc. This system also should provide more opportunities for the communication with suppliers in order to mitigate the possible problems with delays, information regarding the actuality of the warehouses, etc. (Kelly 2010; Jeffery, Norton, and Yung 2006).

Website. This is the final stage of the IT infrastructure renewal. Modern business world is not imaginable without the Internet and the opportunities it can provide. It makes the need in the corporate website crucial (Mills 2006). This website would give the following advantages comparing with the existing situation: the opportunity to place orders, review products, and create various enquiries online that automatically would reduce transactions costs; the opportunity to have access regarding the company and its services 24/7, disregard to the current state of the offices (opened/closed); the opportunity to provide users with self-service that would increase the overall customer satisfaction, etc. (Kelly 2010; Jeffery, Norton, and Yung 2006). Overall scheme of building a datacenter will be as follows:

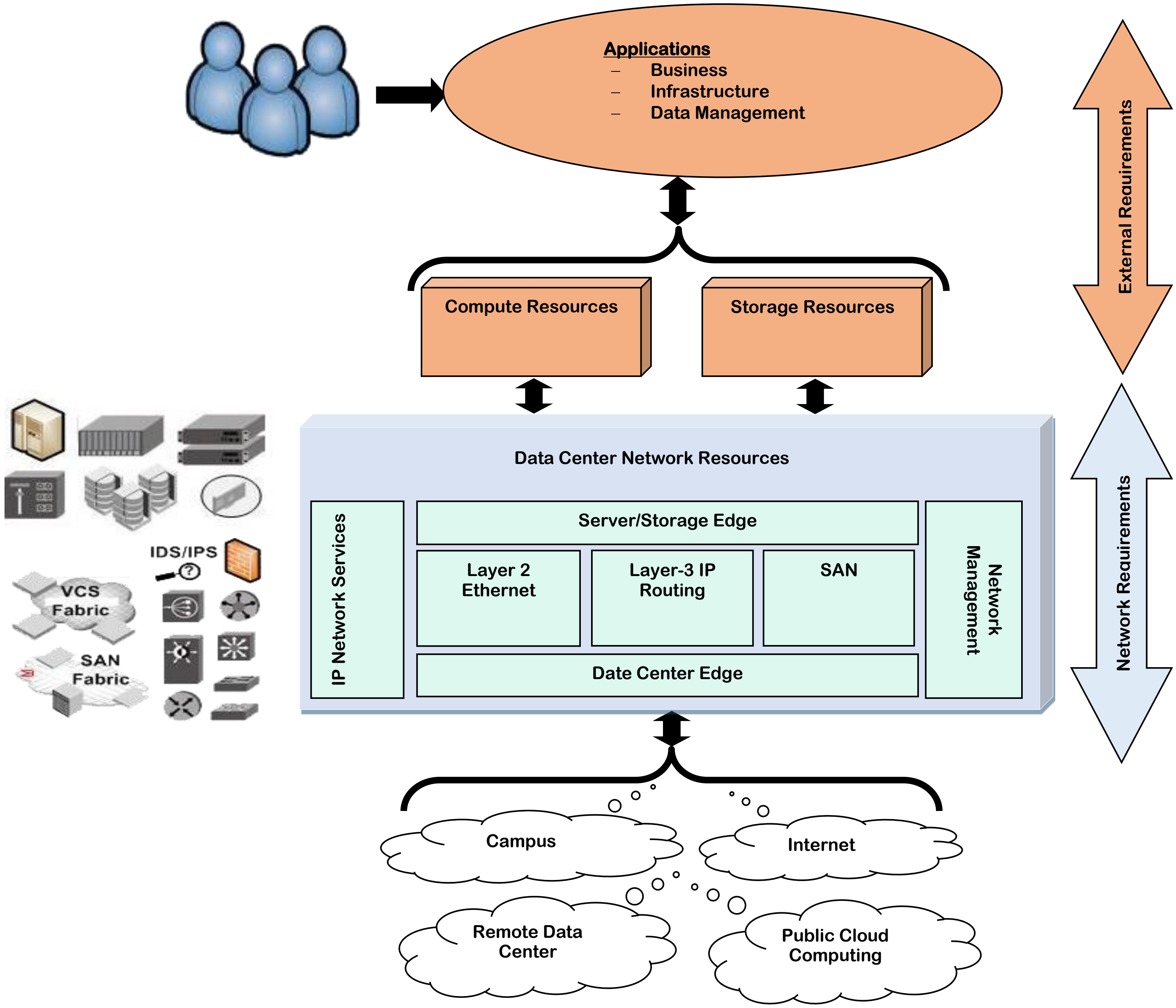

Figure 4. Data Center Scheme

Since the overall plan, the process of its implementation, sequence of the projects' implementation, and their benefits are clear, it is necessary to evaluate these projects in terms of their likelihood to succeed and value to the business (Davis, Fusfeld, Scriven, and Tritle 2001). Any project, especially of such scale as a data center building, requires careful evaluation of potential risks and the value of the implemented functionality to the business. Therefore, there is an utter need in the determination of the mentioned likelihood of success and value according to the typical requirements that a business or organizations has in the process of building of a data center. In order to have some base number to evaluate these projects, we are using the scorecard criteria and numbers established by Davis, Fusfeld, Scriven, and Tritle (2001). They are as follows: likelihood of success - Technical standards: 10%, Skills, capability and training: 10%, Scope and complexity: 25%, Business alignment: 22%, Risk: 21%, and Management capability: 12%; value to the business - Financial return: 30%, Customer and consumer focus: 20%, Supply chain business benefits: 15%, Technology efficiency: 15%, Knowledge advantage: 10%, and Work/life balance: 10% (Kelly 2010; Jeffery, Norton, and Yung 2006).

3.3 Post Implementation, Operational Team SLA

3.3.1 IT Management

3.3.1.1 Service Desk

It is crucial for any company to have developed and well-working service desk system to timely respond to any challenges data center users may face. Only highly-trained specialists along with specialized software must be used in this area (Smith 2013; Schneider Electric 2016). Automation of operations is the major requirement to control, eliminate, and mitigate outcomes that any issue could generate. Service desk in a data center is a must due to the fact that reliance on information stored and processed by it for business and other purposes is overwhelming these days. Only credible and trustworthy suppliers of the specialized software packages should be used regardless of the size and purpose of data center creation (business, non-profit organization, government facility, etc.) (Smith 2013; Schneider Electric 2016).

3.3.1.2 IT Support

IT support unit should be organized as the part of the mentioned service desk department. Creation of such a team will not require high-end specialists (but their presence will be welcomed) since they will resolve less complex and technical issues than their colleagues from service desk subdepartment. The main area of responsibility of IT support will be provision of users with help regarding operations with data center during daily routine (Smith 2013; Schneider Electric 2016). This unit will resolve general problems that most tech illiterate employees usually create for themselves.

3.3.1.3 Network Operation Center

Network operations will be monitored by the specialized team of highly-skilled network professionals. This unit as the sub-unit of IT department will resolve problems related to network infrastructure and related hardware/software solutions (Smith 2013; Schneider Electric 2016). In other words, specialists of network operation center will monitor, maintain, and repair in the case necessity networks utilized by a data center.

3.3.1.4 Security Operation Center

Security of the data center will be assured by the mixed team comprised from the specialists of physical and software protection. It means that physical access to data center facility will be controlled by trained guards, employed by credible security company solutions (Smith 2013; Schneider Electric 2016). This type of protection will be outsourced as third party specialized company will perform these operations much more efficiently and cost-effective than domestic units, organized by a data center owner. At the same time, software security (firewall, rules of authentication, etc.) will be controlled and maintained by domestic IT security professionals of the highest level. They will belong to IT department and report to executives directly solutions (Smith 2013; Schneider Electric 2016).

3.3.1.5 Applications

In-house specialists in software design and engineering will create applications needed by an organization or business to run operations using data center. Proprietary tasks will be completed by these applications. The team will be the subsidiary of IT department. These specialists will provide IT support with any relevant and required data regarding the product they develop and improve (Smith 2013; Schneider Electric 2016). It will allow to organized effective customer support system.

3.3.2 Service Level Agreements

A data center is a complex and multileveled structure that requires sophisticated solutions in many areas (power engineering, networking, software, etc.). However, the major requirement that a well-built data center must meet is redundancy in terms of uptime. In other words, certain service level agreements(SLAs) must be created and approved by all relevant stakeholders (Smith 2013; Schneider Electric 2016). Therefore, to fulfill this requirement, the following components must be included to a typical well-developed SLA: Power, temperature, bandwidth services, and customer support.

Thus, “power” means that data center will meet the requirement of uptime 24/7/365 at 98% level. It means that a good data center is online up to 98% of time. Energy supplier, engineering company assuring power supply to a data center, and relevant hardware/software sub-contractors (or companies they represent) are the parties of this SLA (Smith 2013; Schneider Electric 2016). “Temperature” means that cooling systems must operate appropriately to support high uptime objectives. Appropriate companies and parties that install and support cooling system in a data center are the parties of this SLA.

Them, “bandwidth services” means that a data center can provide users with information provision on a particular speed. In-house departments (networking, software design, and other relevant ones) as well as ISP are the parties of this SLA. Finally, customer support can either in-house or outsourced. In this case, all relevant parties (IT department, service desk, software design as well as third-party support company) are the parties of this SLA (Smith 2013; Schneider Electric 2016).

Chapter 4: Case Study

4.1 Case Study on a Real-Life Implementation

Data centers are required in rather different spheres and areas of application. Public safety and traffic control, for instance, or bus location system are the best candidates for building a data center. Thus, bus location information system (BLIS), for example, is a platform that presents passengers associated information like route, transit, public transit and waiting intervals to bus commuters normally prior to and after transit intervals and helps commuters to make effective decisions when it comes to commuting. It has the following users and functions:

- Commuters are informed of the waiting intervals
- Commuters are informed about remaining distance
- Informs commuters on everything they would want to know about commuting
- Estimate payable costs over a certain distance

Transit control administers transit vehicle flotillas and integrated with other modes and haulage services. This module gets specialized event and synchronized information from traffic control and safety control and sends present transit functional information back to these points. It also gathers and stores precise readership echelons and executes subsequent fare schedule. The module also presents the ability for automated preparation and forecast of public transit activities. It feeds commuters with concurrent travel data, it constantly updates schedules, information to take into account, transfer alternatives and transit roads and fare by way of an information service provider (ISP) and personal information access (PIA).

Parking Control Mechanism: Presents the capacity that offers real-time data on parking fee and accessibility if any, it also permits for parking imbursement without using cash through a multi-user medium, to underpin the recognition, and management of vehicles in need of parking space.

Parking Control Mechanism is closely linked to Transit Control for the function of commuter information. Park and Ride capabilities include VMS on main arterials and throughways before halting into them. VMS indicates whether or not parking space is available and estimate travel interlude to downturn to promote the use such services (Kim, KangSoo, 2001).

- Traffic Control: this is a module that monitors and control traffic flow across a given highway. Events are recognized and confirmed, while event data is presented to safety control, commuters and third-party ISP. Traffic Control module’s prime responsibility is to harmonize traffic data.

- Safety Control: is a module that functions as various emergency terminals underpinning public safety such as police and fire stations, search and free particular disconnects. Gets real-time traffic information from Transit Control is employed to assist the emergency dispatcher in choosing the emergency vehicles and highways that will offer the most immediate feedback (Kim, KangSoo, 2001).

Remote Commuter Support is a module the offers access to commuter information at transit terminals, stops as well as other fixed locations along travel routes as well as main trip generation points including, restaurants, amusement parks and institutions among others. This presents data on schedules and imminent arrival signals (Kim, KangSoo, 2001). This elementary data can be broadened to entail multimodal data such as; traffic situations and commuter plan together with yellow pages information that supports mode and course selection at main trip generation terminus.

External components of the BLIS are as follows:

- GIS
- Sensors
- Antennas
- Terminals
- Pager
- Display Monitors
- Sirens
- Internal Components
- Transit control Application
- Parking Control Mechanism
- Remote Commuter Support
- GPS

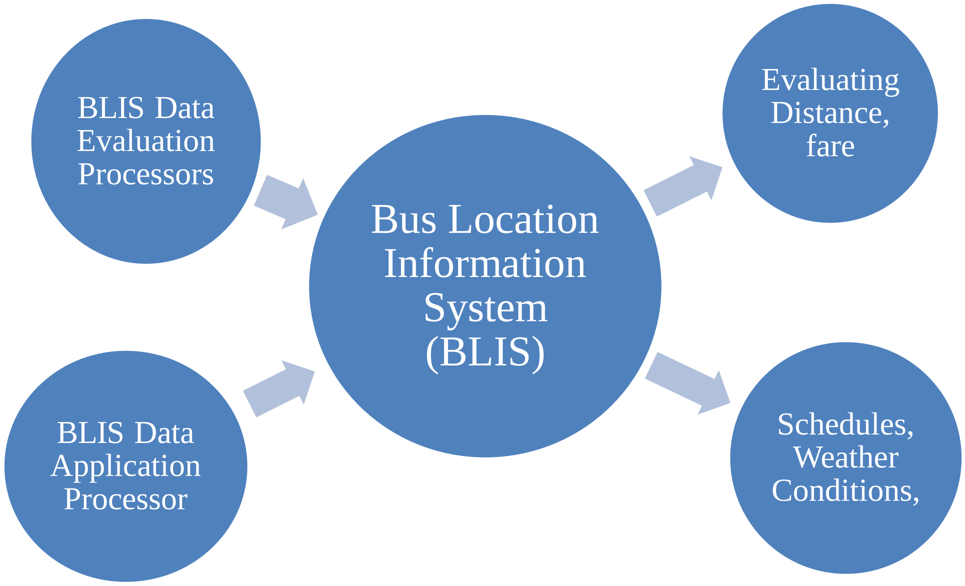
BLIS Data Evaluation Processors
BLIS Data Application Processor
Bus Location Information System (BLIS)
Evaluating Distance, fare
Schedules, Weather Conditions,

Figure 5. Bus Location Information System (BLIS)

BLIS Data Evaluation Processors: Commuters evaluating the remaining distance and decide if it is appropriate to travel from one destination point to the other. BLIS Data Application Processor: Computer system receiving inputs by way of internet and GIS and providing results. BLIS application database contains information with regards to distance, time interval and fare approximates. The ISP gathers, executes, stores and propagate transportation data to system operators as well as the commuting public. The function of the ISP is centered on the delivery of commuters' data to subscribers and the wider public. It also presents the capacity to offer guidelines to commuters by getting origin as well as destination request from travelers, creating a route schedule and sending feedbacks of computed scheduling to commuters. Moreover, the ISP equally underpins specialized route scheduling for vehicle fleets. The ISP is therefore integrated in a dispatch device. Reservation information is relayed by way of Personal Information Access, Remote Traveler Support and several other systems through accessible communication linkages (Kim, KangSoo, 2001).

As mentioned earlier transit control updates transit plans while making synchronized schedules and fares details to information service providers (ISPs). In turn ISPs are in charge of collecting, processing, keeping and disseminating transport data to operators and passengers. This exchange of information can be done through wirelink connections to ISP whereby it is incorporated with information from other transport medium such as train and air to furnish the public with comprehensive and tailored dynamic plans (TCRP, 2003).

Business world also required data centers as the essential component of any IT system these days. This is the scenario of a typical company of large scale that has huge plans and capabilities, but few reasonable people to fulfill these plans (Jeffery, Norton, and Yung 2006). Thus, the company (one of the many), one of the largest subcontractors in the area of medical tools and mechanisms' area (for example), acquired many companies and experienced severe problems in most of the business processes. The problem is connected with inappropriate approach to the information technology area (Jeffery, Norton, and Yung 2006). There are too many numerous standards, systems, databases, etc. that do not have transparent structure, which must be common for the entire corporation. In order to resolve the existing problem, the appropriate plan was developed. It consists of the sequential implementation IT projects that would help to take the situation in the company under control (Schwalbe, 2009).

The scale of the company and the overall confusion in the IT sphere reasons the need in the comprehensive and very precise planning. However, it is very important not to fall into trap of excessiveness. It is not appropriate to include in the plan all possible solutions of numerous company's IT problems (Jeffery, Norton, and Yung 2006). How could we choose the most appropriate programs and systems that should be implemented? What must be included immediately and what can be implemented later if implemented at all? All these questions can get the answers only after the careful evaluation of the situation. The situation with appropriate solutions is explored (as an example) and they are evaluated using scorecard in order to determine the list of solutions to implement and to define the consequence their implementation (Schwalbe, 2009).

4.2 Likelihood of Success

Therefore, we have evaluated the above-described projects, according to these criteria and weights. The results are presented in the Table 1 (Likelihood of success) and Table 2 (value to the business):

Criteria	Projects, %				
	Networking	Computing hardware and software	Data warehouse	Messaging system	Website
Technical standards:	9	7	7	8	10
Skills, capability and training:	4	6	7	5	5
Scope and complexity:	20	20	17	18	24
Business alignment:	21	21	19	20	23
Risk:	9	10	13	8	7
Management capability:	10	5	2	2	5
Total, %:	73	69	65	61	72

Table 1. Likelihood of Success.

Criteria	Projects, %				
	Networking	Computing hardware and software	Data warehouse	Messaging system	Website
Financial return:	9	11	4	19	26
Customer and consumer focus:	11	16	16	16	20
Supply chain business benefits:	16	15	16	15	15
Technology efficiency:	14	16	14	14	14
Knowledge advantage:	7	7	8	8	8
Work/life balance:	1	0	2	3	2
Total, %:	58	65	60	75	85

Table 2. Value to Business.

As we can see from these numbers, the highest possibility of success has networking, the lowest likelihood has the messaging system, the best value to the system has website, and data warehouse can add the lowest value to the system.

The implementation of such kind of project will require expenditures for the following: Salaries and other employment costs; consultancy services; and expenditures for different equipment (hardware, software, etc.) (Mills 2006). Thus, salaries, bonuses, reformatting of units and departments, even termination of the employment contracts in some cases will require extra money. Let us assume the following: 30% of staff who were involved into the processes filling paper of different kind and not directly involved into data management procedures will be dismissed. Therefore, dismissal payoffs will require expenditures (MindTools.com, 2010).

The rest of the employees will be retrained and should receive higher salary, which is costly as well. Consultancy services will be necessary for the entire development process and it will be the second most expensive part of the project. The first part is the reallocation of different equipment, such as server, networking hardware, and, of course the price of new network (Thompson, 2005). Operational costs will include the following: Cost of any legacy conversion; training costs; recruitment costs; and reallocation of any additional equipment. It will be necessary to physically create the data center, etc. Therefore, there will be a necessity to either pay extra money for hiring third party specialists to perform these operations (MindTools.com, 2010). Training of the personnel will be probably the most important part of the entire project implementation activities because if employees are not able to use new network in full, it will be cost ineffective and the project seems rather useless in such case (Thompson, 2005).

Hiring consultants for each department too will require substantial sums at the beginning of systems' functioning to provide all employees with necessary support. These consultants will have short-term contracts but their services will be rather costly (Mills 2006). Additional equipment might be needed to be purchased in case of necessity – mobile devices, like personal digital assistants, or something similar in order to improve overall functionality of new network (MindTools.com, 2010). Finally, additional costs for operations should be planned to cover any emergencies of the training process.

Requirements	**Number x Cost**	**Total Cost**
Development Costs		
Salary		
Network designers	1 x $300	$300
Network administrator	1 x $100	$100
Technicians	1 x $100	$100
Other employees		$500
Cost of equipment		
Project Scope		$100
Project Plan		$200
Project Team Org worksheet		$100
Cost Estimate Worksheet		$50
Consulting Time Estimates		$50
Performance Evaluation		$0
Hardware reallocation		
Computers	2 x $500	$1000
Servers	2 x $500	$1000

UPS	1 x $100	$100
Printer	1 x $200	$200
Laptops	2 x $300	$600
Operational Cost		
Setup costs		
Training	2 x $50	$100
Purchase of any equipment		$0
Overall Cost		**$5,000**

Table 3. summarizes all costs and presents the overall cost:

Work breakdown structure (WBS) is as follows:

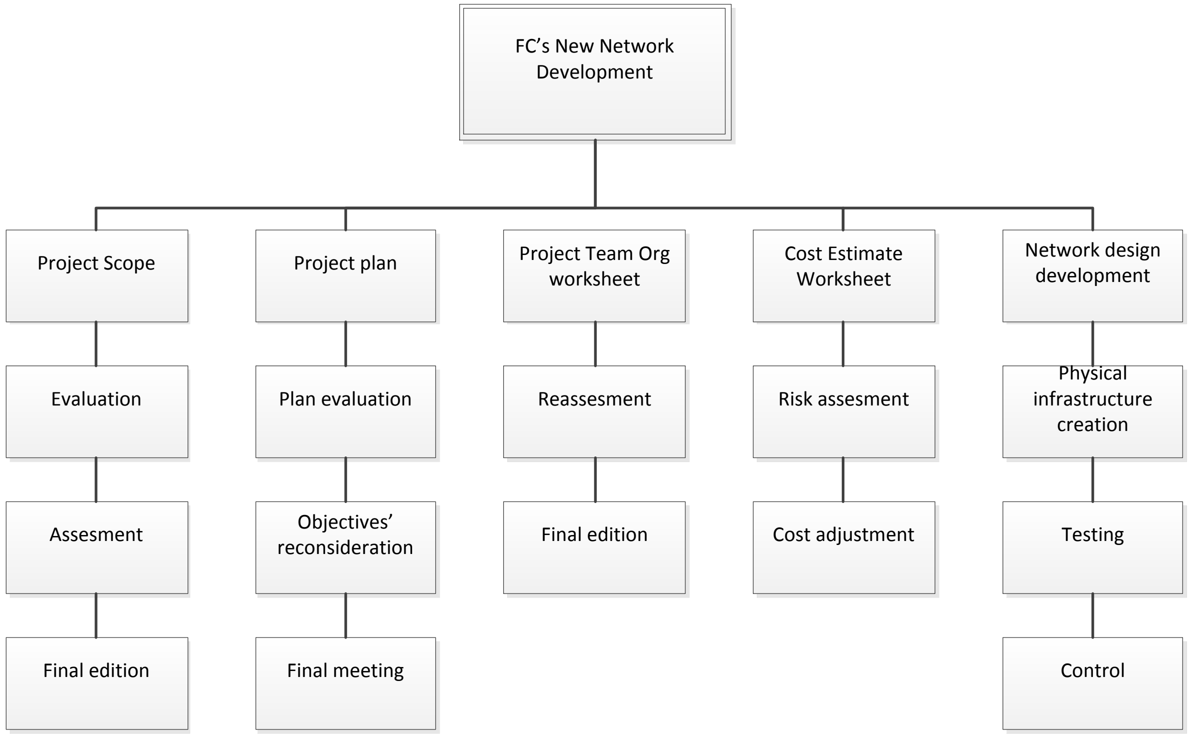

Figure 6. WBS

Cloud computing has been used more often during the last couple of years as the appropriate solution of the enterprise scale. Felten (2009) states that the term "cloud computing" refers to the trend away from services provided by software running on standalone personal computers ("clients"), toward services provided across the Net with data stored in centralized data centers ("servers").” Gmail, Hotmail, Flickr can be named as the examples of such web based services (Felten 2009). The idea of sharing physical resources to provide the clients with computing performance is not new and was realized in the concept of virtualization. According to Johnston Turner (2010), nearly 70% of enterprise datacenters will be virtualized by 2013.

According to this idea, the usage of the hardware and software resources in the cloud should be highly automated and properly managed in order to avoid glitches and slowdowns (Mills 2006). Therefore, the need in the appropriate platform for each cloud computing service is beyond any doubts. Johnston Turner (2010) states, for example, that “the ratio of administrators that manage machines improves only slightly – hovering in the range of about 29 physical servers per administrator versus 33 virtual machines per administrator.” At the same time, the companies “that have aggressively standardized, integrated, and automated physical and virtual system and workload management activities are achieving ratios of 350 - 500 or more servers per administrator.” (Johnston Turner 2010).

The importance of cloud computing management automation can be also outlined by the results of the test, performed by Henderson & Allen (2010). After the testing of three different tools in the public cloud, the authors have concluded that the more system was automated and easy to use, the less operations they had to perform during the test. Since the speed of tasks performing and successful completion plays an important role in the concept of paying for services-on-demand, the more automated management of clouds is beneficial for the clients as well as for the administrators (Henderson & Allen 2010).

As any other technical process, automating cloud computing management process has certain difficulties. The challenges that are usually faced by the administrators of clouds are most likely connected with technical side of the process (Mills 2006). In many cases organizations need to address to different virtualization vendors in order to cover the entire application portfolio. This is the reason why organizations should be flexible during the process of choosing the right vendors. It will allow to avoid vendor lock-in risks and make the work of administrators easier, if some vendor could not provide organization with appropriate services for some reasons (Krishnamsetty 2010).

The administration of visualization must be performed correctly. Otherwise, as Krishnamsetty (2010) states, “if the proper processes and automation are not in place, the virtual infrastructure growth compromises the benefits of virtualization.” Another challenge

that will be faced on this road is the need in the appropriate procurement process (Mills 2006). When the virtualization was not used that widely, the process of application procurement process went through the processes of financial approval, ordering, purchasing, inventorying, installation, and provisioning, which was a rather long process. Thus, in order to achieve advanced performance, organizations need properly organized procurement process to make cloud work efficiently.

According to Krishnamsetty (2010), policy compliance, variety of cloud maintaining tools, and virtual machine sprawl are other challenges to be dealt with. Virtual environments are difficult to audit, so the new virtualization management tools cannot control physical existing physical provisioning tools in full. Despite the fact that users can self-provision, IT should still be able to control and set the policies. The organizations should reduce the number of different management consoles and other similar tools to be able to unify the management system. Finally, since the virtual machines can be created and deployed rather easily, their uncontrolled growth can increase the security risks for the organization, stress the IT management, and increase the cost of cloud usage (Krishnamsetty 2010).

Chapter 5: Conclusion & Recommendations

5.1 Importance of Quality Service Supplier

It is recommended that the average company hires a consulting firm to perform a thorough penetration test for its first analysis. When the company has received the results, and fixed all its vulnerabilities, it should supplement the initial test with periodic (monthly or semi-monthly) vulnerability scans (Harris & Shipley, 2006). In addition, it is recommended to perform an annual penetration test for rapidly changing environments. It is not possible to become aware what might be missed during (re)configuration that could introduce new holes and vulnerabilities into an existing network infrastructure.

Lack of competence in testing toolkits – this risk is one of the most disturbing because after such assessment the resume that “everything is fine” could be false. It can affect the secureness of the network substantially and make it even more vulnerable. Inappropriate choice of the testing toolkit, added to the incompetence of the IT specialists makes the risk of putting security of network in danger of being overestimated is very high. It is possible to avoid this risk only if there is some kind of proof that the chosen toolkit and specialists using it have performed successful tests before (Shavit, 2011; Veracode, Inc., 2011).

5.2 False Knowledge

Already knowing some of the weak areas and scope of the network makes the tests skewed – this risk follows the above-mentioned. The risk means that the assessment of vulnerabilities is performed in incomplete form, knowing that some points are weak and should not be tested before solving this issue. Therefore, the scope of the tests narrows and “complete” vulnerability assessment becomes substantially incomplete. The integrity of every security system is determined by the “strength” of its weakest “chains”. Such inappropriate approach to the vulnerability assessment compromises the secureness of network by default (Shavit, 2011; Veracode, Inc., 2011).

5.3 Inappropriate Responsibility

Inability to migrate responsibility to a third party who is bonded – this risk is rather unconnected with above-mentioned ones. It is more about taking responsibility for the actions that could lead to substantial issues with security in the future. Internal vulnerability assessment would not allow insuring risks related to it (Shavit, 2011; Veracode, Inc., 2011). Only outsourced company can take risks and perform a comprehensive vulnerability assessment procedure. Moreover, only outsourced company will be responsible in case of unexpected security breach and will have to deal with consequences. This risk is one to consider seriously because internal vulnerability assessment does not provide any guarantees that external procedure can give (Shavit, 2011; Veracode, Inc., 2011).

5.4 Legal Considerations & Preparations

If an outside consulting firm is performing the vulnerability assessment of a network, the consultants may ask the company's executives to sign an agreement allowing them to conduct a vulnerability assessment of the network (Harris & Shipley, 2006). Outsourced company will ask to sign the document to protect the consulting firm from anything that may happen during the test. While most tools and checks used today are relatively benign, they have the possibility of corrupting or crashing networks and services. It is important to have this agreement reviewed by organization's in-house legal counsel (Harris & Shipley, 2006).

First, it is important for any company, considering using the services of third-party specialists, to come to the appropriate agreement that should be thoroughly reviewed by legal counsels from both sides (Harris & Shipley, 2006). This agreement will provide solid legal background for further work. Vulnerability assessment is a rather serious procedure in terms of secureness of the company network and it is very important to be sure that contractor will not provide this information to the third parties. Therefore, the agreement should cover all these issues and signed by both sides. Then, the recommendation to collect the information beforehand will save money and time. In addition, these operations can provide some extra information regarding various systems and processes that have been left unnoticed before (Harris & Shipley, 2006). Therefore, it will not be the reason to review the agreement and revise it by the contractor. It means that the client will be ready to any direction of how the situation might develop during the vulnerability assessment.

Vulnerability assessment should be prepared beforehand. Besides speeding up the process, this preparation will also save the money so that the consultants are not billing a company for time they spend gathering information. It is necessary to have all security policies, procedures, network diagrams, and results of internal security assessments ready and available upon request (Harris & Shipley, 2006). This information may be requested by the consultants during the opening meeting, or they may ask for them later. Also during the opening meeting, the consultants will ask a variety of questions about networks to gain better understanding of what they need to do to test them.

5.5 Schedule and Monitoring

After the initial meeting, the consultants will provide a schedule of when the tests will be performed, when they will be completed, and when it should be expected to receive the final report. The procedure can be monitored easily (what the consultants are doing if a company's representative reviews firewall logs and IDS) (Harris & Shipley, 2006). It is highly recommended to monitor their activities to ensure that they perform a thorough test. One common area to watch is to make sure that the consultants check both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports. Many organizations ignore UDP ports and end up leaving some gaping holes in their firewall (Harris & Shipley, 2006). Finally, monitoring of the activities should be performed as well because it provides client with guarantee that the contractor does not perform any actions, not mentioned in the contract. There is a possibility that such actions can be hidden or covered somehow, so the contract should include special section regarding the future issues, related to the inappropriate use of the obtained information.

References

Avelar, V, Azevedo, D, French, A 2012. PUE: A Comprehensive Examination of the Metric. White Paper.

Dong, J 2007. Network Dictionary, Javvin Technologies Inc.

FastPCNet.net (2010). How outsourcing data center operations can boost the business. Retrieved from: http://www.fastpcnet.net/data center.html

Hinkle, J. (2010). Should You Build or Outsource the Data Center? Retrieved from: http://www.data centerknowledge.com/archives/2010/02/05/should-you-build-or-outsource-your-data-center/

TechTarget.com (2010). Data Center. Retrieved from: http://searchdata center.techtarget.com/definition/data-center

BackTrack.org (2011). BackTrack Linux. Retrieved from: https://www.backtrack-linux.org

Harris, K. J., & Shipley, T. G. (2006). Information Technology Security. Retrieved from: http://www.ncirc.gov/documents/public/Info_Technology_Security.pdf

iViZSecurity.com (2009). What is the difference between Vulnerability Assessment and Penetration Testing? Retrieved from: http://www.ivizsecurity.com/blog/penetration-testing/difference-vulnerability-penetration-testing/

MetaSploit Express (2011). MetaSploit Express. Retrieved from: http://www.rapid7.com/store/metasploit/index.jsp

Nessus.org (2011). Nessus Product Overview. Retrieved from: http://www.nessus.org/products/nessus/nessus-product-overview

Securitytube.net (2011). Network Vulnerability Assessment Basics. Retrieved from: http://www.securitytube.net/video/126

Shavit, Y. (2011). Network penetration tools. Retrieved from: http://searchsecuritychannel.techtarget.com/feature/Network-penetration-tools

Veracode, Inc. (2011). What is Penetration Testing? Retrieved from: http://www.veracode.com/security/penetration-testing

Arief, B., & Besnard, D. (2005). Technical and Human Issues in Computer-Based Systems Security. Centre for Software Reliability, School of Computing Science, University of Newcastle upon Tyne. Retrieved from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.1677&rep=rep1&type=pdf

Computer Forensics (2006). Intrusion Detection System. Retrieved from: http://www.computerforensics1.com/intrusion-detection-system.html

Karthikeyan, K. R., & Indra, A. (2010). Intrusion Detection Tools and Techniques – A Survey. International Journal of Computer Theory and Engineering, 2(6), pp. 1793-8201.

Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). Retrieved from: https://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-94-guide-to-intrusion-detection-and-prevention-systems-2007.pdf

Avelar, V., Azevedo, D., & French, A. (Eds.). (2012). PUE: A comprehensive examination of the metric. Retrieved from http://www.thegreengrid.org/~/media/WhitePapers/WP49-PUE%20A%20Comprehensive%20Examination%20of%20the%20Metric_v6.pdf

Google Data Centers. (n.d.a). Efficiency: How others can do it. Retrieved from https://www.google.com/about/datacenters/efficiency/external/

Google Data Centers. (n.d.b). Efficiency: How we do it. Retrieved from

https://www.google.com/about/datacenters/efficiency/internal/index.html#measuring-efficiency

Natural Resources Defense Council. (2014). Data center efficiency assesment. Scaling up energy efficiency across the data center industry: Evaluating key drivers and barriers. Retrieved from https://www.nrdc.org/sites/default/files/data-center-efficiency-assessment-IP.pdf

Schneider Electric 2016. A practical guide to data center planning and design. http://futuredriven.com.au/wp-content/uploads/2017/05/Schneider-Electric-A-practical-guide-to-data-center-planning-and-design.pdf

Smith, G 2013, 8 Steps to Building a Modern Datacenter, https://www.wired.com/insights/2013/06/8-steps-to-building-a-modern-datacenter/

Mills, E 2006, Best Practices for Data Centers: Lessons Learned from Benchmarking 22 Data Centers. ACEEE Summer Study on Energy Efficiency in Buildings 3 http://evanmills.lbl.gov/pubs/pdf/aceee-datacenters.pdf

Bullock, M 2009, Data Center Definition and Solutions, CIO. https://www.cio.com/article/2425545/data-center/data-center-definition-and-solutions.html

Barker, R., & Massiglia, P. (2002). Storage Area Network Essentials. Retrieved from: http://www.snia.org/education/storage_networking_primer/san

Breeding, M. (2002). NAS vs. SAN: Technology Overview. Retrieved from: http://www.librarytechnology.org/ltg-displaytext.pl?RC=9460

Bird, D. (2002). Storage Basics: Storage Area Networks. Retrieved from: http://www.enterprisestorageforum.com/technology/features/article.php/981191/Storage-Basics-Storage-Area-Networks.htm

Tate, J., Lucchese, F., & Moore, R. (2006). Introduction to Storage Area Networks. Retrieved from: www.redbooks.ibm.com/redbooks/pdfs/sg245470.pdf

Third I/O (2008). An Analysis of 8 Gigabit Fibre Channel & 10 Gigabit iSCSI in Terms of Performance, CPU Utilization & Power Consumption. Retrieved form: http://www.thirdio.com/iscsi-fc.pdf

TopTenReviews.com (2011a). 2011 Network Attached Storage Comparisons and Reviews. Retrieved from: http://network-attached-storage-review.toptenreviews.com/

TopTenReviews.com (2011b). Buffalo Technology LinkStation Pro. Retrieved from: http://network-attached-storage-review.toptenreviews.com/buffalo-technology-linkstation-pro-review.html

Beazley, H 2005. Knowledge Continuity: The New Competitive Advantage. <http://www.asaecenter.org/PublicationsResources/EUArticle.cfm?ItemNumber=11836>.

Kaieteur Institute for Knowledge Management (KIKM) 2005. Vital Knowledge Assets Protection Planning Service. 2005. <http://www.kikm.org/assetplanning.pdf>.

University of Massachusetts 2009. Business Continuity and Planning Guidelines. <http://www.massachusetts.edu/policy/buscontplan.html>.

BusinessLifestyleSolutions.com.au. Defining Key Business Objectives and Strategies. 2007. <http://www.businesslifestylesolutions.com.au/Business_Objectives_Strategies.asp>.

NiBusinessInfo.co.uk. Get the Most from IT in Your Business. <http://www.nibusinessinfo.co.uk/bdotg/action/detail?site=191&itemId=1075423034&type=RESOURCES>.

Schwalbe, K. Information Technology Project Management. 2009. Boston, MA: Cengage Learning.

MindTools.com (2010). Cost/Benefit Analysis Retrieved from: http://www.mindtools.com/pages/article/newTED_08.htm

Thompson, A. (2005). Business Feasibility Study Outline. Retrieved from: http://www.rochester.edu/entrepreneurship/pdfs/Business_Feasibility_Study_Outline.pdf

Felten, E 2009, What Economic Forces Drive Cloud Computing? <http://www.freedom-to-tinker.com/blog/felten/what-economic-forces-drive-cloud-computing>.

Henderson, T & Allen, B 2010, Fly the Public Cloud on Autopilot, <http://www.networkworld.com>.

Johnston Turner, M 2010, Automated, Standardized, and Private Cloud Management, <http://research.ebizq.net/detail/RES/1287684633_44.html>.

Krishnamsetty, B 2010, The Challenges of Managing Cloud Virtual Infrastructure, <http://blog.cloupia.com/2010/07/27/the-challenges-of-managing-cloud-virtual-infrastructure/>.

Loh, P 2009, Automating Cloud Services, <http://www.tapinsystems.com/downloads/Automating_Cloud_Services.pdf>.

Otey, M 2010, The Rise of Cloud Computing, <http://www.windowsitpro.com/article/cloud-computing2/The-Rise-of-Cloud-Computing/2.aspx>.

Kim, KangSoo (2001), Stated Preference Design and Analysis (the second phase), The Korea Transport Institute Research, 97-105.

TCRP (2003), "Real-Time Bus Arrival Information Systems", Transportation Research Board, p.10-19.

SDX Central 2016, Data Center Networking Explained, https://www.sdxcentral.com/sdn/network-virtualization/definitions/data-center-networking-explained/

Leiner, BM et al. 2009. A Brief History of the Internet, CCR. doi: http://doi.acm.org/10.1145/1629607.1629613

Jeffery, M, Norton, JF, & Yung, D 2006. MDCM, Inc. (A): IT Strategy Synchronization. http://hbr.org/product/mdcm-inc-a-it-strategy-synchronization/an/KEL170-PDF-ENG

Kelly, C 2010. Information Technology In The MDCM Inc. Company. http://www.articlesbase.com/networking-articles/information-technology-in-the-mdcm-inc-company-2193640.html

Dean, T 2005, Network +guide networks, 4th edn, Cengage Learning, Boston.

Robinson, D 2017, Re-shaping data center servers, DatacenterDynamics, http://www.datacenterdynamics.com/content-tracks/servers-storage/re-shaping-data-center-servers/98197.fullarticle

Davis, J, Fusfeld, A, Scriven, E and Tritle, G 2001, Determining a project's probability of success, Research-Technology Management, vol. 44, no. 3, 2001.