Open Source Security Tools: Market Offers

by

Ali Soheili

a thesis submitted to the Faculty of Graduate Studies and Research

in partial fulfillment of the requirements for the degree of

Master of Applied Science in Technology Innovation Management

Department of Systems and Computer Engineering

Carleton University

Ottawa, Ontario, Canada, K1S 5B6

April 2010

© Copyright 2010, Ali Soheili

Library and Archives
Canada

Published Heritage
Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et
Archives Canada

Direction du
Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file *Votre référence*
ISBN: 978-0-494-68640-9
Our file *Notre référence*
ISBN: 978-0-494-68640-9

NOTICE:

The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protègent cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

■ ♦ ■
Canada

The undersigned recommend to
the Faculty of Graduate Studies and Research
acceptance of the thesis

Open Source Security Tools: Market Offers

submitted by

Ali Soheili

in partial fulfillment of the requirements for
the degree of Master of Applied Science in Technology Innovation Management

Chair, Howard Schwartz, Department of Systems and Computer Engineering

Thesis Supervisor, Douglas King

Carleton University
April 2010

ABSTRACT

An empirically derived quantitative study of 185 firms active in the Open Source Security Tool (OSST) context is presented. Exploratory Factor Analysis techniques are used to extract nine types of market offers using information from the Internet and public websites of the firms. Five of these offer types are unique to OSST and the security concept of OSS: (i) Security Analysis Services; (ii) Monitoring Services; (iii) Confidentiality services; (iv) Authentication, Authorization, and Accountability Services; and (v) Disaster Recovery and Business Continuity Services. The other four offer types are similar to market offers and commercialization strategies that have been identified in previous research. These four offer types are: (i) Support Services; (ii) Product Services; (iii) Hosted Services; and (iv) Project Management Services. The firms have been clustered into three main groups: (i) Consulting Service Providers; (ii) Solution and Product Creators; (iii) Hosted Solution Providers.

ACKNOWLEDGEMENT

Sincere gratitude is hereby extended to my thesis supervisor, Professor Douglas King with his ongoing support and supervision until this thesis structured. Also, I'd like to extend my special thanks to Professor Antonio Bailetti who has provided me constructive guidance and advice in this research process. Other Technology Innovation Management faculty at Carleton University have also provided me great insights and I thank them all.

Also, Mr. Frank Horsfall, the president and founder of EnTeraSec security consulting firm provided me guidance and consultation during this research and I want to thank him for his ongoing support.

Most importantly, this work is dedicated to my wife for her endless inspiration, support and love as well as my parents who always encouraged me in this journey.

TABLE OF CONTENT

ABSTRACT.....	iii
ACKNOWLEDGMENT.....	iv
TABLE OF CONTENT.....	v
LIST OF TABLES.....	ix
LIST OF FIGURES.....	x
1. INTRODUCTION	1
1.1 Research Question	2
1.2 Security in a nutshell.....	3
1.3 OSST.....	7
1.4 Objectives	8
1.5 Deliverables	9
1.6 Contribution.....	9
1.7 Relevance.....	10
1.8 Document Organization.....	11
2. LITERATURE REVIEW	13
2.1 Open Source Software	13
2.1.1 Motivation.....	14
2.1.2 Licenses	15

2.2 OSS adoption and commercialization factors.....	16
2.2.1 Adoption Factors.....	17
2.2.2 Commercialization Factors	19
2.2.2.1 Koenig strategies.....	19
2.2.2.2 Dahlamder Frame Work	21
2.2.2.3 Hecker Model	22
2.2.2.4 Alam Result	23
2.3 OSST Security	23
2.4 Data Analysis.....	25
2.4.1 Factor Analysis Vs. Principal Component Analysis.....	27
2.4.2 Factor Extraction Methods.....	27
2.4.3 Factor Extraction.....	28
2.4.4 Rotation Methods.....	29
2.4.5 Sample Size	29
2.5 Lessons Learned	30
3. RESEARCH METHODOLOGY.....	31
3.1 Research Strategy	31
3.2 Research Design	32

3.3 Research Steps	33
3.4 Sample Creation.....	35
3.5 Keyword Selection.....	36
3.6 Data Acquisition	37
3.7 Data Validation.....	38
4. RESEARCH RESULT.....	40
4.1 Data Analysis.....	40
4.2 Firms Ranking	53
4.3 Validate Result.....	74
5. DISCUSSION OF RESULTS.....	76
5.1 Interpret Factors.....	76
5.2 OSST and OSS market offers compassion	87
5.3 Clustering Factors	91
6. CONCLUSION, LIMITATIONS AND FUTURE RESEARCH SUGGESTIONS.....	98
6.1 Conclusion	98
6.2 Limitations	100
6.3 Future Research Opportunities	101
REFERENCES	103

APPENDICES	111
Appendix- 1: List of OSST companies.....	111
Appendix--2: Initial Keywords.....	115
Appendix- 3: Example Open Source Security Tools.....	117

LIST OF TABLES

TABLE 1: OSS LICENSES	15
TABLE 2- DAHLAMDER FRAMEWORK.....	22
TABLE 3-HECKER FRAMEWORK.....	22
TABLE 4- RESEARCH STEPS	33
TABLE 5- KMO AND BARTLETT’S TEST (SAMPLE 184).....	39
TABLE 7- RESULT OF FACTOR ANALYSIS- KEYWORD LOADINGS (SAMPLE 184)	49
TABLE 8- FACTOR ANALYSIS RESULT OF EACH KEYWORD (SAMPLE 184)	51
TABLE 9- SUM OF SQUARED LOADINGS (SAMPLE 184)	52
TABLE 10- DESCRIPTIVE STATISTICS OF NINE FACTORS.....	53
TABLE 11- COMPANY CODINGS.....	55
TABLE 12- COMPANIES CLASSIFICATION BASED ON FACTORS	60
TABLE 13- FORTUNE 1000 STATISTICAL TESTS	75
TABLE 14- FACTOR INTERPRETATION- OSST MARKET OFFERS	77
TABLE 15- OSS AND OSST MARKET OFFERS COMPARISON	90
TABLE 16- K-MEAN CLUSTER ANALYSIS RESULT.....	93

LIST OF FIGURES

FIGURE 1: KEYWORD SEARCHER TOOL	38
FIGURE 2- SCREE PLOT (SAMPLE 184).....	47
FIGURE 3- PCA CHART RESULT	48
FIGURE 4- FACTORS SCORING CHART	54
FIGURE 5- K-MEAN CLUSTER ANALYSIS PLOT TO DETERMINE NUMBER OF CLUSTERS	92
FIGURE 6- FACTOR CLUSTERED ACCORDING TO K-MEAN CLUSTERING	96

1. INTRODUCTION

Open Source Software (OSS) is a relatively new and evolutionary process of producing software based products and making the source code accessible to the public as opposed to a closed and proprietary approach. OSS is seen as a business model which provides types of flexibility, opportunity and benefits different from those provided by the conventional model (Capek et al., 2005). Firms are incorporating OSS in their market offers through different approaches and create appealing offers to compete. A product or market offer is anything that is offered to the market for attention, acquisition, use, or consumption that might satisfy a want or need (Kotler and Turner , 1995). Baghai et al. (2000) also defined a market offer as the whole package of product and add-ons that creates value to customer. OSS can be classified into different categories. sourceforge.net has classified them into 19 categories such as Database, Education, Internet, etc. Security is one such category and there are many projects that are classified in other categories but provide security related tasks. This research focuses on the vertical market that has been established across Open Source Security related projects that are named Open Source Security Tools (OSST).

Many previous studies have used a qualitative approach to construct or test hypotheses and examine the OSS market offers and commercialization strategies. OSS has been studied as a whole and no previous study on different specialized types of OSS have been found by the researcher. The researcher chose the security types of OSS and

studied them to help gain an understanding of the differences and similarities in commercialization strategies between OSS and OSST in particular. Also, using an empirically driven quantitative method to uncover the key components or factors in OSST commercialization has been a contribution of this research to the OSS knowledgebase. A number of researchers have used Exploratory Factor Analysis of web-content mining to pursue similar quantitative studies. Motivated by the explanatory power of factor analysis, this research uses a keyword Web Search Tool to acquire data from the Internet and the researcher then performed Factor Analysis to extract the underlying differentiating factors for OSST market offers.

In this section a quick introduction of security concepts has been provided to ensure that the reader is aware of the basic concepts underlying these security tools. Also, Appendix-2 summarizes some of the popular OSSTs with a quick discussion on their capabilities.

1.1 Research Question

This research intends to answer the question of what are the different types of market offers from Open Source Security Tools (OSST). Companies are using the phenomenon of Open Source Software in their appealing market offers to enter the competitive market. The fact that the source code is open and anyone can access it has not limited innovative firms and entrepreneurs to create offers based on OSS. This research studies and analyzes the different types of market offers that have been created from Open Source Software that are used for security and privacy purposes.

1.2 Security in a nutshell

Security implies a stable, relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear of disturbance or injury (Fischer, R.J. and Green, G., 2004, p.21). Security has remained relatively unchanged over the past centuries and the recent changes in the concept are the result of advent in technology. When locks and fences were previously protecting buildings and rooms, we now see the state-of-art in sophisticated computers and sensors controlling the access to buildings. High-tech cameras are replacing security guards and computer programs are evolving in securing the perimeter. It is worth mentioning that still the human factor and physical security measures like fences and dead-bolts are used by security professionals. In this remainder of this section, we will cover some of the basic concepts of Information System Security.

Security management addresses the identification of the information assets in an organization. It spells out how organizations manage their security practices and details (Gregg, 2006; Basse, 2003). The four fundamentals that security is based on are: Confidentiality, Integrity, Availability and Accountability (also known as CIAA):

Confidentiality ensures private information is kept secure from unauthorized people. In other words, people who do not have proper security clearance or need to know cannot access the information. Some attacks against confidentiality are sniffing, keystroke monitoring and shoulder surfing.

Integrity means the data is accurate and has not been changed during storage, transmission or any other process without authorization. An example would be a change in a bank balance by adding 0s.

Availability ensures that data is available anytime and anywhere. For example an Internet Service Provider (ISP) needs to ensure that its service is available anytime and customers can access the Internet at all time. A good example of an attack against availability is a Denial of Service (DOS) Attack.

Accountability is another element in the fundamental of security. Some text books and literatures only classify the concepts as CIA and some add accountability to the list. Accountability ensures that the person who changed or consumed information is accountable for his or her act. This can be used to pursue any legal actions and conduct investigations. Impersonating is a good example of attacks against accountability; an attacker would impersonate and try to exploit the victim's vulnerabilities using mechanisms such as spam emails.

Risk management is another security management concept and is described as determining the threats to the organization, analyzing vulnerabilities, defining an acceptable level of risk and implementing the security measures and controls to prevent the vulnerabilities. Risk can be handled in different ways: reduced, transferred (e.g., insurance), accepted to avoid potential cost, or rejected (pretend never exists - not the best way) (Gregg, 2006). The process of analyzing threats, vulnerabilities and level of risks and proposing the security controls is called Threat

Risk Assessment (TRA). Security is often a multi-layered process. Some professionals use an onion layer model to indicate that to obtain a more secure perimeter more layers of security should be implemented. Policies, procedures, standards, baselines and guidelines are used by organizations to ensure that the security controls suggested by risk management are in place and being followed by employees and partners. Examples would be patch management, password protection, and employee screening processes, backup practices and so on. Security controls are also categorized into administrative, technical and physical. Administrative controls are composed of mechanisms to enforce policies, procedures, guidelines and baselines. Technical controls are logical measures used to provide access control and other devices like firewalls, Intrusion detection systems and authentication devices. Physical controls are measures that are implemented to protect the physical perimeter like fences, locks and guards (Fischer & Green, 2005; Gregg, 2006).

Access Control is a key component of security; it helps to keep the perimeter secure from unauthorized individuals. A simple access control mechanism is the user name and password; however, the current access control systems are more sophisticated than simple user name and password. The biometrics attributes incorporate and provide top-notch authentication solutions. The three main concepts of access control are the Identification, Authentication and Authorization. Identification is the process of identifying yourself to an authentication service provider, authentication is the process of determination of the person's identity and authorization is the process of whether a

user has the right to access the requested resources (Gregg, 2006). Accountability is another factor that can be included in this process to ensure a higher level of security.

Monitoring is another component of security. In the context of perimeter security, the primary goal of system and network monitoring is to provide administrators with the awareness of the state of protected environment (Northcutt, S. et al., 2003. p.462). Monitoring helps detect disruption in the availability of systems, changes in performance, unexpected changes and attacks in the process. Tools like Network and Hosts Intrusion Detection Systems (N/HIDS) and prevention system (N/HIPS) are mainly used to pursue the monitoring process.

Cryptography is the science and study of secret writing. It is concerned with the ways in which information can be encoded to prevent disclosures. It is tied closely to two pillars of security: integrity and confidentiality (Gregg, 2006). The history of cryptography is very old: the ancient Hebrews used basic cryptography by replacing letters. The art of cryptography has been implemented in different applications like digital signatures, security certificates, email and data encryption, access control (e.g., encrypted USB keys that allows access to a server) and so on.

Business continuity and Disaster Recovery are two important domains in security. Business Continuity is concerned with assessing risk and determining how a business would respond in a major disruption. On the other hand, Disaster Recovery deals with what is needed to keep the organization running in case of a disaster. For example, in case of a flood, the plan that would indicate the process that should be undertaken to

rescue the organization's resources and bring the process back to normal operation would be summarized in the Disaster Recovery Plan. The processes that would help allow functioning business operations until the full recovery would fit into the Business Continuity plan. Some examples are backups, having duplicate sites (hot, warm or cold sites), multiple data centers, reciprocal agreements and others.

1.3 OSST

For the purposes of this work, Open Source Security Tools are defined as any open source software (or hardware containing embedded open source software) that would be used to provide any types of security. Some of the major categorizations of these tools are as follows:

- Monitoring: Monitor and scan the network for vulnerabilities(e.g. Nessus);
- Antivirus: Keep the computer clean from viruses (e.g. ClamAV);
- Cryptography: Use for encryption purposes (e.g. Cryptology);
- Remote Access: Use to secure remote connections (e.g. Open SSL, Open VPN); and
- Networking : Help to Secure the network (e.g. NMAP, TCPDUMP).

Some of these tools like Snort, Nessus and Open SSL are used in a variety of applications by security professionals in enterprises. A summary of some of these tools with descriptions is provided in Appendix -3.

1.4 Objectives

The main objective of this research is to examine how the specific nature of OSST projects (security) affects the types of market offers by using an Exploratory Factor Analysis approach.

To perform the data analysis of this research, the researcher needed a list of companies that are creating appealing offers from OSST. The researcher was not able to locate any available database that includes these companies, so the lack of such a database was apparent. The researcher performed an extensive search on the publicly available resources through the Internet to create such a database. The website of well known projects like Snort and Nessus and data available on sourceforge.net were used as starting points, and augmented using manual searches to find additional projects. One of the other deliverables of this research is the creation of the list of 205 companies that are directly using OSST in their market offers with their Internet URLs.

The art of this research was the process of identifying the market offers. The important tool that has been created to fulfill the data analysis was the list of keywords: keywords that differentiate different type of market offers within the OSST domain.

Classification of the OSST market offers and a framework for deciding how to enter the competitive market by adopting an OSST project is another unique objective of this research.

Also, the researcher compares the OSST market offers with OSS market offers that have been extracted from previous studies and lists the unique offers available through OSST.

1.5 Deliverables

The research has produced the following deliverables:

- An empirical categorization of OSST market offers;
- A subsample of companies developing specific type of market offers with OSST projects (a list of companies with OSST market offers and their URLs);
- Analysis of factors that differentiate the OSST market offers - clustering of companies based on the factors; and
- List of offers that are unique to OSST.

1.6 Contribution

The research provides following contributions:

- Businesses can use the results to identify and differentiate potential collaborators and/or competitors for products either in their cluster of adjacent cluster;
- Researchers can apply the method to other domains in which market offer information is publicly available on the Internet through the firm's websites; and

- This research identifies OSST market offers and clusters them into three unique groupings that can be used by security companies to create their offers based on OSST.

1.7 Relevance

This research is relevant to three main groups:

- Researchers would be offered an extensive literature review and a new path for research anchored around OSST. Also, the quantitative approach using factor analysis has been used in this research that can provide insights for other researches. Eugene Spafford, director of Purdue University's Center for Education and Research in Information Assurance and Security has stated, "Some of the public domain tools are very well maintained and have many people contributing new tools and patterns. In some senses, they rival commercial tools (Lawton, 2002)."
- Top Management Teams of companies that are adopting OSST for their processes would benefit from this research since this research points at what services and complimentary assets are available with OSST. Mark Cox, senior director of engineering of Red Hat's Open SSL group, added, "Companies running Unix based platforms, such as Linux and Solaris, are likely to use open source tools like Nessus, Snare, and Snort because they were developed and run like Unix (Lawton, 2002)."

- Top Management Teams of companies that are using OSST in their offers and entrepreneurs can benefit from this thesis by learning how other companies are creating offers from OSST and which offers and strategies are more popular. They also can learn about companies that are currently using the OSST in their offers. Buddy Baxter, technical delivery manager for infrastructure needs for EDS's credit-union customers, said, "Just because a product costs a lot does not mean it will be more secure." He said EDS can deploy a security installation using Astaro's software for about 25 percent of the cost of using Check Point Software Technologies' commercial product (Lawton, 2002)."

1.8 Document Organization

The thesis is organized into six chapters. The first chapter includes an introduction and an overview of the research. The second chapter contains a summary of the literature review divided into five streams; Open Source Software, OSS adoption and commercialization and type of offers, Security of OSST, factor analysis, and finally lessons learned. The third chapter describes the research methodology and strategies, research design, research steps, sample creation, keyword selection, data acquisition and data validation. Chapter four covers the research results including: data analysis, firms ranking and data validation. Chapter five contains a discussion of results and includes: factor interpretation, OSST and OSS market offers comparison, and factor

clustering. Finally, the last chapter wraps up the research with conclusions, research limitations and suggestions for future research opportunities.

2. LITERATURE REVIEW

This chapter is organized into five streams. First stream reviews the academic literature on the phenomenon of Open Source Software in detail. The second stream contains the adoption factors of OSS in government and private firms as well as different frameworks and strategies of creating market offers based on OSS. Four frameworks has been studied and used as a benchmark for comparing the final result. The third stream reviews the security aspects of OSST products and whether the OSST is as secure as similar closed source products. The fourth stream provides a review of research methodologies based on factor analysis and how to perform an exploratory factor analysis. Finally, Section 2.5 covers the lessons learned.

2.1 Open Source Software

An Open Source Software is governed by a license that permits anybody to access the source code, modify the software and redistribute it (Alam, 2006). Open Source offers enterprises the opportunity to be more self-reliant through source code modification. It allows incremental project and upgrade schedules, free reign in integration decisions, and direct interaction with open source community (Koenig, 2004). The freedom of selection from border range of vendors and service providers is considered a major advantage of OSS related products as oppose of proprietary solutions.

2.1.1 Motivation

Success of an OSS project depends on the developer motivation. Roberts et al. (2006) explore two types of motivation intrinsic and extrinsic to participate in OSS projects. The intrinsic motivation has been linked to the satisfaction of human needs. In OSS context, the human needs can be satisfied through greater opportunities to express creativity, enjoyment from work and experience sense of satisfaction from accomplishing the work. On the other hand, extrinsic motivation has been linked to incentives that reinforced desired behaviors. This type of motivation is characterized by focusing on incentives and rewards. The commercial interests in OSS have raised this motivation and the examples of companies that are directly and indirectly participating in OSS development are a good indication.

Alam, (2006) categorized developer motivations into two categories; individual motivations and company motivations. Individual motivations are varied; enhancing the programming skills, satisfy own need, showcase their skills, making configurations for own use and learning opportunities. These individuals are communicating through email, newsgroups, Instant Messaging, Source Code management, forums and any other ways. On the other hand, companies and organizations are contributing to OSS project success as well. Some major reasons are; independency from IP and big firms, making money on complementary services, affording innovation, hiring good people, reducing costs, promoting standards and others. Some companies are only benefiting from these projects and some are contributing as well.

2.1.2 Licenses

Hecker, (1998) and Alam, (2006), studied the possible license choices for OSS projects. I am summarizing some of these licenses in the table below; however, the in-depth study of these licenses is not the purpose of this research.

Table 1: OSS Licenses

License	Description
Generalized Public License (GPL)	<ul style="list-style-type: none"> • Use Copyright law to keep the software free • Any work on the software should be released with same license • Most common use of licensing for OSS
GNU Library General Purpose License (LGPL)	<ul style="list-style-type: none"> • More flexible than GPL • A use of LGPL licensed software in a proprietary tool is accepted
Berkeley System Distribution (BSD)	<ul style="list-style-type: none"> • Permits the modified software be licensed as proprietary • Most widely used non-restrictive license (maximum freedom)
Netscape Public License	<ul style="list-style-type: none"> • Can be mixed with free software • Can be modified and used as proprietary • Contains special privileges for the original copyright

License	Description
Mozilla Public License	<ul style="list-style-type: none"> • Can be modified and used as proprietary
Artistic License	<ul style="list-style-type: none"> • Encourages users to make modifications and make it available to public free • Allows the proprietary product invisibly embed the OSS in their solution
Public Domain	<ul style="list-style-type: none"> • No license at all • Anyone can use it with no restriction • The modified version can be licensed by anyone and used as proprietary; however, if it becomes a dominant design then it is no longer an OSS.

Bonaccorsi & Rossi (2003) identified that most companies use software from projects that issue GPL and LGPL licenses.

2.2 OSS adoption and commercialization factors

This stream is divided into two sub-streams; adoption factors and commercialization factors. The need to understand the adoption factors has a direct relation with commercialization since it would help firms to address those needs and try to tailor their solutions to meet adoptions criteria.

2.2.1 Adoption Factors

The adoption factors have some similarities and differences in government vs. private sectors. Dedrick and West (2004) research summarized the adoption of computing platforms based on Linux or other OSS. They have documented a rich set of technological, organizational and environmental factors that influence such decisions.

The technology factors summarized into:

- *Relative advantage*: For example the relative advantage of Linux over Windows.
- *Cost*: For example the cost advantage of Linux (hardware / Software)
- *Reliability*: The trust in performance and services
- *Compatibility*: The decision to adopt an OSS platforms or tools appears to be greatly influenced by the compatibility of new technology with current technologies, skills and tasks.
- *Trial ability*: The ability to try the OSS at a very low cost as oppose of closed source tools.

Organizational factors are summarized into:

- *IT innovation*: Moving quickly when a new technology begins to gain widespread adoption.

- *Centrality of IT*: Willingness to adopt is the strategic importance of IT to the firm's business. For example, for Internet Service Provider, company adopting an OSS in their process is easier than a fast food restaurant.
- *Slack*: Financial and human slacks have been identified in Dedrick and West (2004) research.

Environmental factors are summarized into:

- *Availability of technology skills and service*: Lack of technical support for OSS projects vs. proprietary.
- *Sponsor-driven legitimacy*

The Simon (2005) study identified that OSS is a good fit for government because of interoperability, vendor lock-in and flexibility. Governments consume, manage and produce massive amounts of information. The interoperability delivered by OSS is independent of whether OSS or proprietary is used to implement the standards. A good example is e-government services, which have gained momentum in recent years (Simon, 2005). The other adoption factor is "vendor lock-in", the deployment of a solution would not force governments to take high financial risk. Governments are operating on limited budgets and cannot afford to pay high prices of software solutions. Flexibility of OSS identified as another factor in adoption of OSS by governments.

2.2.2 Commercialization Factors

Open Source offers enterprises the opportunity to be more self-reliant through source code modification. It allows incremental project and upgrade schedules, free reign in integration decisions, and direct interaction with the open source community (Koenig, 2004). Firms are mixing open source approaches with proprietary assets and investments to profit from OSS (Fosfuri et al. 2008). Companies like Red Hat, IBM, HP, and Oracle are using OSS in their products and services and creating an appealing offer compare to proprietary solutions. Different literatures have discussed different strategies, business models and market offers that are created with OSS by firms. I have summarized some of the different approaches in the following pages. Koenig (2004) has identified strategies for OSS commercialization. Dahlamder (2004) created a framework for appropriating return from OSS. Hecker (1998) studied a framework for business models around OSS and Alam (2006) concluded a categorization of OSS market offers.

2.2.2.1 Koenig strategies

Koenig identified seven strategies for competitive advantage from OSS:

1- The optimization strategy:

It's a manifestation of Christensen's law of conservation of modularity. One layer of the software stack is "modular and comfortable" allowing adjacent software layers to

be optimized. The first layer in a commodity and are unprofitable and the second layer would generate profit (Koenig, 2004).

2- The dual license strategy

A software company offers free use of its software with some limitations and a commercial version with full functionality.

3- The support strategy

Its revenue from services (both maintenance and consulting) is used to create the offer. The fact that open source products are downloadable as-is, increases the ability to provide support services on top of that.

4- The consulting strategy

Companies are adding consultation with their offer and charging their customers consulting fees.

5- The patronage strategy

Companies use this strategy to commoditize a particular layer of the software to eliminate competitors that are extracting revenue from that layer and create profit from other layers (clustering, provisioning, security, software management).

6- The hosted strategy

Salesforce.com uses OSS in their Software as a Service (SaaS) offer and provides a Customer Relation Management (CRM) tool and charges users a monthly fee.

7- The embedded strategy

Linux has been used in many customer products such as TIVO and cell phones. One strategy for OSS commercialization is to embed the software into hardware and sell the hardware.

2.2.2.2 Dahlamder Framework

Dahlamder (2004) discussed a framework for analyzing the means of appropriating returns from OSS. The appropriability is defined as the possibility the owner of a resource has to capture a return equal to more than the value created by the recourse (Dahlamder, 2004). The framework is summarized in the below table:

Table 2- Dahlamder Framework

Category	Sub Categories	Explanation of How it works in OSS
Products	Licensing	Licensing the right to use software
	Black Box	Bunching several pieces of OSS in hardware solution
Services	Consultancy	Providing consulting services with OSS
	Education	Offering training courses, certifications and seminars about OSS
	Support	Supporting the OSS projects or the licensed products based on OSS

2.2.2.3 Hecker Model

Hecker (1998) pointed out different business models that can be created by OSS. The findings are summarized in the table below:

Table 3-Hecker Framework

Support Sellers	Revenue comes from media distribution, branding, training, consulting, custom development, licensing fee...
Loss leader	No charge OSS used as a loss leader and commercial software will generate revenue. (e.g. Netscape Communicator product)
Widget Frosting	Use OSS as a driver to enable their hardware and sell the hardware
Accessorizing	OSS used to distribute goods like O'Reilly use OSS to publish books

Service Enabler	OSS help to generate online services (e.g. Amazon)
Brand Licensing	Company charges other companies to use their brand in creating products.
Sell it, Free it	Company product starts as a commercial product and converts to open product when becomes commodity and adds value to newer proprietary products
Software Franchising	A company allows others to use their models.
Hybrid	Any combination of above models.

2.2.2.4 Alam Result

Alam's (2006) research found 6 types of market offers that would complement other frameworks. He summarized the types of offers into; (i) hosting and content services, (ii) training and testing, (iii) support, (iv) subscription, (v) commercial licenses, and (vi) products.

2.3 OSST Security

The debate about open versus closed systems started out in the nineteenth century when Auguste Kerckhofs pointed out the wisdom of assuming that the enemy knew one's cipher system, so the security can only reside in the key that use to cipher and decipher (Anderson,2002). The fact that opening the source code would lead to exploiting vulnerabilities since attackers can access it has been a controversial subject.

The real world is not safe and no matter the source code is open or not an intelligent attacker can exploit it. The fact that a large community of programmers are contributing to the source code of OSS projects would increase the likelihood of better security in OSS compared to closed source products. It considerably lessens the chances for hidden back-door security holes.

The OSS security tools have widely been used by IT security professionals and consultants. Tools like Netfilter, iptables, snort, Open SSL, Nessus are famous tools that have been used in enterprises to provide security and privacy. Lawton (2002) pointed out some pros and cons of OSST projects. Cost and quality are considered as positive points in OSST and support is the disadvantage of OSST.

Hoepman and Jacobs (2008) discussed the security of a system, the exposure of the system and risk associated with that system. The security of a system is an objective measure of the number of its vulnerability and their severity. The exposure of the system is the likelihood of a successful attack and finally, the risk is the combination of likelihood and damage to the assets resulting from it. They have claimed that opening the source code allows independent assessment of the exposure of a system and makes patching bugs easier and more likely. There is a huge difference between openness of the design and openness of the source code. Opening the design may reveal logical error in security in the worst case. Opening the source code gives unfair advantage to attacker to find vulnerability and launch a successful attack. This is considered an uneven battle (Hoepman & Jacobs, 2008).

They also discussed that closed is not so close and attackers can always exploit a vulnerability in the source code. The downside here is only the producer of closed source can release patches for vulnerabilities and many of those patches are released too late. Moreover, open source enables users to evaluate the security by themselves and faster patches will lead to more secure code. Also users can add extra security measures since anybody can contribute. They concluded that in the long run, openness of the source increases the security.

The security of open source based security tools is not in the scope of this research; however, the researcher felt the need to point out some of the debates and literatures regarding this matter. Whether these tools are as secure as proprietary ones or not should be studied more in-depth and even case by case. The fact that many of these tools are widely used in industry by security and IT professionals is a good indication that they are considered secure.

2.4 Data Analysis

Hicks et al. (2006) used web mining techniques to gather data on the commercialization strategies of innovative small high tech firms. They used the company website to extract their data instead of using questionnaires and interviews. The frequencies of the words extracted from websites were obtained and the pattern of occurrence assessed to perform classification.

Lombardi (2006) used this same technique to classify the interaction between Eclipse foundation members and projects. He gathered data from 163 eclipse member organization and used 43 keywords to perform factor analysis. He used a tool called keywordsearcher tool to calculate the frequencies of the keywords and performed a factor analysis to extract the classes of interaction between eclipse members.

Allen (2009) used the same methodology and tools to study the first empirical identification of components of value co-creation. He performed component analysis and used keywordsearcher tool to conclude his research.

Jdue (2009) undertook same steps to accomplish his research in Level One Industrial Automation in choosing network control systems. He performed factor analysis and used the same approach that Allen (2009) and Lombardi (2006) had done in their research.

Data mining from the Internet is good method for research especially for OSS since most of the projects have enough information on the Internet.

Darlington (2007) and Costello & Osborne (2005) discussed the strategy and best practises in Exploratory Factor Analysis (EFA). EFA includes both component analysis and common factor analysis. The purpose of EFA is to discover simple patterns in the patterns of relationship among variables (Darlington, 2007). It has been used in social science and human psychology studies. It is an effective way to build

constructs from large number of gathered data. A successful factor analysis will provide answers to the following 4 questions (Allen, 2009; Darlington, 2007):

- How many different factors are needed to explain the pattern of relationships among these variables?
- What is the nature of those factors?
- How well do the hypothesized factors explain the observed data?
- How much purely random or unique variance does each observed variable include?

2.4.1 Factor Analysis Vs. Principal Component Analysis

The extraction methods in most statistics packages are Principal Component Analysis (PCA) and Factor Analysis. PCA is not the best method to use according to (Costello and Osborn, 2005; Darlington, 2007). Costello and Osborn (2005) recommended Factor Analysis over PCA since PCA considered being a data reduction method that became popular when computing technologies were expensive. Factor Analysis would result in same solution as PCA and avoid the increase of variance by making use of more complex algorithms for today's computers (Jdue, 2009).

2.4.2 Factor Extraction Methods

Costello and Osborn (2005) pointed out more than six factor extraction methods that can be used in Factor Analysis (PCA, un-weighted least squares, generalized squares,

maximum likelihood, principal axis factoring, alpha factoring and image factoring). They also identified the best practices to avoid confusion in choosing the best method. They recommended if data is normally distributed, maximum likelihood is the best choice; however, if data is not normally distributed, the principal factor method also referred to “Principal Axis Factors Or Common Factor Analysis” can be used.

2.4.3 Factor Extraction

PCA seeks a linear combination of variables and variables with maximum variance are extracted. Common Factor Analysis (CFA) and Principal Factor Analysis (PFA) seek the least number of factors that can be used for common variance or correlation. Selecting the number of factors is an important step in factor analysis. The higher the number of factors, the more complex the results will be.

To determine how many factors to extract, different methods have been recommended. Eigenvalue of a given factor is the variance in all variables for that factor. In other words, variables with low eigenvalue can be ignored since they have low contribution. Best practices recommend choosing variables with an eigenvalue over 1. Costello and Osborne recommend the Scree test, which tends to be the most widely available method in all statistical packages. In the Scree test, the graph of eigenvalues is examined and the number of data points above the “break” in the graph becomes the number of factors to retain. In Darlington (2007), use of the Scree test is also

recommended. As an alternative, Darlington (2007) recommends completing a complete factor analysis with various numbers of factors and selecting the one that has the most well-defined structure. Although more time and resource consuming, this will lead to the best results.

2.4.4 Rotation Methods

Rotation makes the output more understandable. By rotating your factors you attempt to find a factor solution that is equal to that obtained in the initial extraction but which has the simplest interpretation.

There are many different types of rotation, but they all try to make your factors highly responsive to a small subset of your items (as opposed to being moderately responsive to a broad set). There are two major categories of rotations, orthogonal rotations, which produce uncorrelated factors, and oblique rotations, which produce correlated factors. The best orthogonal rotation is widely believed to be Varimax (Varimax which is the mainly used method for rotation differentiates original variables by extracted factors, so each variable can be identified by a single factor). Oblique rotations are less distinguishable, with the three most commonly used being Direct Quartimin, Promax, and Harris-Kaiser Orthoblique (DeCoster, 1998).

2.4.5 Sample Size

The rule of thumb for sample size is to have more data (Costello and Osborn, 2005; Darlington, 2007).

2.5 Lessons Learned

The following insights gained from reviewing the literatures:

1. Literatures are available on how companies are integrating OSS in their market offers but not OSST. No single literature differentiated the type of market offers created from OSST.
2. There are very few empirical studies regarding the security of current OSST projects. None of these literatures performed an empirical study on how secure the OSST are compare to proprietary tools.
3. Data mining techniques are a good choice for OSST research, since most OSST projects have a website or enough information on the Internet (esp. Sourceforge.net).
4. Companies are using different strategies like consulting, support, embedding into hardware, dual -licensing and others to create value from OSS.

3. RESEARCH METHODOLOGY

This chapter provides the detailed steps and methods that have been undertaken to complete this research. It is organized into seven sections. Section 3.1 covers the research strategy and methodology. Section 3.2 identifies research design. Section 3.3 discusses the detail steps in this research. Section 3.4 identifies sample creation. Section 3.5 discusses the steps in creating the list of keywords. Section 3.6 covers the data acquisition and finally, Section 3.7 includes the data validation strategy.

3.1 Research Strategy

An approach based on grounded theory as per the descriptive building theory by Christensen and Carlile (2005) has been pursued. The following are the steps that have been used in this research and are structured around the grounded theory approach; however, the researcher did not create any theory or model and the final result is the classification of findings:

1- Observation: In the first step, the researcher has observed the raw data:

- Identify data sources (websites of companies)
- Identify Keywords

2- Classification (Factor Analysis): In this step, researcher has performed a factor analysis on the gathered data:

- Classify & quantify factors
- Cluster companies based on their market offers
- Create a framework & cluster analysis (offer groupings)
- Compare the results with OSS commercialization frameworks studied in the literature review.

The research employed content analysis from company websites as the data mining technique. This approach builds on the earlier keyword based web data mining techniques of Hicks et al. (2008), Lombardi (2008), Allen (2009) and Jdue (2009). Using exploratory factor analysis (EFA) allowed the researcher to identify the underlying dimensions that distinguish various types of OSST market offers from publicly available websites. Dholakia et al. (2000) emphasized that the web's interactive nature creates a totally new communication environment. Instead of the traditional model of one-to-many communication, the Web is a "many-to-many" channel of communication.

3.2 Research Design

The Unit of Analysis in this research is the company's websites which use OSST in their market offer.

There is no specific time period for companies since a large list of companies should be examined. Samples should be as large as possible to obtain the best result. Samples have been drawn from Internet during November 2009 to January 2010. The

detail of how samples have been identified will be discussed in detail in the following sections.

3.3 Research Steps

The table below shows the step-by-step tasks that have been undertaken to fulfil this research. The steps undertaken are similar to the steps that Allen (2009), Jdue (2009) and Lombardi (2008) undertook in their research:

Table 4- Research Steps

No.	Step	Activity
1	Literature Review	<p>Identify the underlying characteristic of OSST:</p> <ul style="list-style-type: none"> I. Select and review academic literatures and books II. Select and review white papers and online sources <p>Define Keywords that can differentiate the market offers and characteristic of security offerings.</p> <p>Build a strategy to create the inventory of companies.</p> <p>Study data mining methods and statistical techniques used to pursue the data analysis:</p> <ul style="list-style-type: none"> I. Google Ajax Search API II. Exploratory Factor Analysis (EFA)
2	Lessons Learned	<p>Develop lessons learned from studying the literature</p> <p>Identify the importance of this research</p>

No.	Step	Activity
3	Sample Creation	Websites: 205 Selection Criteria: <ul style="list-style-type: none"> I. Companies should have an offering related to OSST II. Companies websites should have been over 5 pages in total to avoid outliers in EFA
4	Keyword Selection	Keyword have been selected: <ul style="list-style-type: none"> I. Concepts from literature review II. Concepts from studying 10% of sample websites
5	Data Acquisition	Used Keyword Search Tool (Google Ajax API): <ul style="list-style-type: none"> I. Capture keyword frequency (hit counts) II. Remove redundant/ ubiquitous/rare keywords
6	Data Validation	Adjust keywords (variables) until meet the requirements for factor analysis: <ul style="list-style-type: none"> I. KMO sampling adequacy test > 0.5 II. Bartlett's significance test < 0.05 Iterate steps 5-6 until validity criteria are satisfied
7	Factor Analysis	Use Open Source statistical tool R to extract factors: <ul style="list-style-type: none"> I. Exploratory Factor Analysis II. Maximum likelihood III. Screeplot and eigenvalue IV. Varimax

No.	Step	Activity
8	Firms Ranking	Calculate each firm's factor scores: I. Compare firm's score II. Code companies by factors III. Associate firms and factors
9	Validate Result	Test the final set of keywords with 2007 Fortune 1000 firms.
10	Discuss Results	Interpret factors using keywords loadings: I. Excluded variables with loadings <0.45 II. Avoid cross loadings Comparing result with OSS commercialization frameworks Clustering factors : I. K-mean cluster Analysis
11	Draw Conclusion	Synthesize conclusion and insights and identify limitations and future research opportunities

3.4 Sample Creation

Creating the list of company's websites was the most challenging part of this research since not all the companies that use OSST in their offer are explicitly talking about that project in their website. I have limited myself to companies that directly and indirectly mention that they are using specific OSST in their offer. There are over 1840 OSS security related projects listed in sourceforge.net and I have also located over 100 famous projects and performed a Google search on those projects. Then, I located the companies that are using that project (tool) in their offer and added the

company information into a spreadsheet. Initially 205 companies were identified, during the initial pre-screen 21 companies were deleted:

- 9 URLs have been deleted since the Keyword Search Tool returned zero on the number of pages. The reason was the websites themselves that led the researcher to remove them from the sample list.
- 12 URLs have been deleted since they have returned exactly the same value for each variable.

The list of companies has been reduced to 184 firms from 205. This list has been used to perform the final analysis. Appendix-1 lists the 205 company's URLs.

3.5 Keyword Selection

The development of the list of keywords was the second important step in this research. The keywords are intended to represent many aspects of OSS & OSST market offers to allow the factor analysis detect specific aspects. Keywords were collected through an extensive search on literatures and sample websites. By focusing on literature that discussed types of market offers generated from OSS and studying 10% of the sample companies that have been randomly selected, a set of 35 keywords have been identified. Since Google Ajax Search API would support the "AND" and "OR" logical operation, combination of keywords can be used as one keyword. Below are three examples of keywords that have been identified in the first initial keyword

selection step: (Appendix -2 lists the entire set of keywords that have been initially created)

Hosted OR Hosting

(Technical AND Support) OR maintenance OR(Customer AND support)

OR (technical AND Assistant)

(Incident AND Response) OR monitoring OR (defence AND center) OR

(remote and control)

The combination of keywords with “AND” and “OR” is based on their meaning and usage.

3.6 Data Acquisition

The web search data mining technique has been used to generate the deliverables. This approach is described by Hicks et al. (2006) and Opoku (2005) which use public websites of companies and use keywords to extract results.

The Keyword Searcher tool is used to perform the web search. This tool has been created by Steven Lombardi to support his research into interaction of Eclipse member firms and is based on the Google Ajax search API. It is similar to the IFAPI tool

developed and used by Hicks et al. (2006) to automate their research. The Keyword Searcher Tool has been used by Steve Allen and Amer Jdue as well as other researchers to fulfil different researches. The tool accepts a list of URLs and a list of keywords as a text file and returns a comma separated variable (.csv) output file with the number of occurrence of each keyword and total number of pages in each URL. The Keyword searcher tool interface that has been used is shown in the next figure (Figure-1):

Figure 1: Keyword Searcher Tool

3.7 Data Validation

The data set must meet specific criteria for correlation, sampling adequacy and statistical significance to result in a successful factor analysis (Field, 2005). The following table demonstrates the results of the Kaiser-Meyer-Olkin and Bartlett's test of significance:

Table 5- KMO and Bartlett's test (Sample 184)

Metric		Limit	Result
Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy		>0.5	0.68
Bartlett's test of Sphericity Significance Test	Approx. Chi-Square		1385.9
	df		183
	Sig.	<0.05	< 2.2e-16

Bartlett's test of Sphericity Significance Test and Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy tests are the two main tests that can be used to determine the factorability of a matrix. For the result to be considered statistically valid, the KMO measure of sampling adequacy must be larger than 0.5 and the Bartlett's test of Sphericity Significance Test (Sig) should be smaller than 0.05 to indicate the adequate degree of correlation for factor analysis to converge (Field, 2005; Allen, 2009). The KMO result between 0.6 to 0.7 is a good indication of factorability of the result. If factor analysis is performed, the extracted factors would account for a fairly large amount of variance. The significance calculated in Bartlett's test is almost zero and is much smaller than the limit.

4. RESEARCH RESULT

This chapter includes three sections. Section 4.1 covers data analysis and the details of factor analysis. Section 4.2 identifies the results of factor analysis on the 184 sample companies and ranks the companies based on their factors. Section 4.3 covers the validation of the result against Fortune 1000 companies and the steps that undertook.

4.1 Data Analysis

Common Factor Analysis (CFA) and Principal Component Analysis (PCA) are two approaches that are used by researchers to uncover the dimensions underlying the variation of large sets of data. CFA is preferred over PCA although both produce a reliable result. For the purpose of this research, the researcher has tried both CFA and PCA and CFA produced the cleanest result. The best practices defined by Darlington (2007) and Costello and Osborne (2005) were used to define the factor analysis rules. After running the Keyword Search Tool on 184 firms and 35 keywords, the following steps were undertaken to assure adequate result for factor analysis:

- Five keywords have been dropped since they were identical or returned zero on all websites (100% zero). This indicates that these keywords were not a suitable selection for OSST market offers. The keywords that have been removed are:

Threat risk assessment OR risk analysis

Call center security

Data integrity

Threat risk analysis

Advertisement OR advertise

The following table shows the descriptive statistics of remained 30 keywords:

Table 6- Descriptive Statistics of 30 keywords

Keywords	Min	Max	Mean	STD. Dev	Variance	Median	Norm -ality
Service OR Support	0.670	466.26 5	45.735	38.779	1495.656	44.315	0.559 9
Technical Support OR Customer Support	0	89.908	12.281	16.744	278.860	7.300	0.702
Installation OR Install OR Deployment	0	76.455	18.561	15.116	227.272	14.481	0.921
Planning OR project management OR Configuration	0	78.125	12.650	13.483	180.821	8.989	0.805

Keywords	Min	Max	Mean	STD. Dev	Variance	Median	Norm -ality
Consulting OR Consult OR Consultation	0	101.79 9	16.119	25.353	639.289	4.903	0.658
License OR Copyright OR application OR Product OR appliance	0	100	36.711	24.427	593.463	33.902	0.951
Hosted OR hosting OR host	0	94.736	12.578	16.212	261.401	6.321	0.731
Customization OR Customize	0	53.125	3.525	6.764	45.515	1.447	0.526
Operation Center	0	36.065	0.294	2.762	7.590	0	0.082
Hardening OR Securing OR Protection	0	24.740	1.453	3.244	10.470	0	0.515
Disaster Recovery OR Business Continuity	0	73.333	3.159	9.062	81.677	0.112	0.386

Keywords	Min	Max	Mean	STD. Dev	Variance	Median	Norm -ality
Audit OR Vulnerability Assessment OR Penetration Testing	0	64.179	7.573	13.371	177.832	1.454	0.622
Network Security OR IT Security	0	95.856	9.128	17.859	317.244	1.620	0.561
Voice OR VOIP OR telephony security	0	100	1.884	8.864	78.157	0	0.204
Data Security OR Back up OR data protection	0	63.449	8.586	11.416	129.620	4.351	0.727
Education OR Training OR Course OR certificate OR Seminar	0	100	18.304	20.503	418.124	11.324	0.815
Integrate OR Integration OR Integrating	0	98.076	14.414	18.067	324.665	8.432	0.747

Keywords	Min	Max	Mean	STD. Dev	Variance	Median	Norm -ality
SaaS OR Software as a Service	0	95.454	8.206	15.437	237.008	1.864	0.583
Incident Response OR Defence Center OR Intrusion detection	0	92.168	14.634	16.763	279.482	8.248	0.802
Confidentiality	0	9.302	1.046	1.854	3.420	0.027	0.637
Authentication OR Authorization	0	68.512	5.772	10.582	111.389	1.585	0.580
Access Control OR ACL	0	57.283	2.600	6.962	48.215	0.409	0.388
Encryption	0	83.386	6.860	13.707	186.872	1.166	0.548
Non repudiation	0	8.333	0.169	0.799	0.634	0	0.221
Availability	0	97.590	7.944	11.311	127.255	4.555	0.660
Monitoring OR Monitor	0	100	14.824	19.898	393.793	6.765	0.728
Intrusion detection	0	72.727	3.738	9.690	93.403	0.174	0.432
Penetration testing OR Vulnerability	0	97.435	7.448	16.436	268.690	0.4007	0.518

Keywords	Min	Max	Mean	STD. Dev	Variance	Median	Norm -ality
Network Scanning	0	5.263	0.102	0.575	0.329	0	0.172
SSL Certification OR Certification Authority	0	3.544	0.031	0.291	0.084	0	0.084

- Key words with low Shapiro –Wilk Normality or no variance have been removed. Seven keywords have been removed and the keyword list has been narrowed down to a set of twenty three keywords. The dropped keywords are:

Operation Center

Voice OR VOIP OR Telephony Security

Access Control OR ACL

Non – Repudiation

Intrusion Detection

Network Scanning

SSL Certificate OR Certificate Authority

In the event that the data collected is normally distributed, the maximum likelihood would be used to extract factors. If data is skewed substantially, alpha extraction would be applied to data. Rotation is used to “find the best distribution of factor loadings in terms of meanings of the factors” (Reinard, 2006). The available rotation methods with statistical tools are: Varimax, Quatimax, Equamax, Promax, Direct Oblimin and None. Field 2005 and Reinard 2006 suggested Varimax for factors that may be related, so Varimax rotation has been used in factor analysis to produce an orthogonal set of interoperable dimensions and uncorrelated factors.

The next step in factor analysis is to identify the number of factors to extract. Most of the statistics literature suggests the Kaiser’s criterion method which would select factors with Eigenvalues larger than 1.0 . The other proposed method for determining number of factors to extract is the Screeplot which indicates to select the factors above the point at which the curve bends to form a knee (Darlington, 2008; Field, 2005; Costello & Osborn, 2005; Reinard, 2006).

The following is the Scree plot of the 23 keywords and 184 URLs:

Figure 2- Scree plot (Sample 184)

The Scree plot suggests that 10 factors' eigenvalues are greater than 1.0 and 5 factors are above the knee. The researcher decided to choose the Kaiser's criterion method.

Costello et al. (2005) suggested 0.32 loading as a good rule of thumb to be considered for the minimum loading. Reinard recommends excluding keywords with loading less than 0.6 and cross-loading larger than 0.4 . Allen (2009) used 0.44 as a cut off and minimum loading threshold and Jdue (2009) used 0.32. Since the factor loading are high, I have chosen 0.45. This threshold would remove cross loadings and indicate variables with high loadings. Initially, I performed the PCA and CFA with 10 factors extraction. The below chart shows the result of PCA with 10 components:

Figure 3- PCA chart
result

Factor nine and ten are so close and the CFA with ten factors and “cut off” of 0.45 resulted in removal of Factor 10 (factor 10 highest loading was 0.42). The final result

for CFA was nine factors and the loadings of 0.45 or higher. The following table shows the resulting factors with their associated keywords and loadings:

Table 7- Result of Factor Analysis- Keyword loadings (Sample 184)

Factor 1	Loading
Service OR Support	0.76
Availability	0.76
Technical Support OR Customer Support	0.48
<i>Average</i>	<i>0.66</i>
Factor 2	
Installation OR Install OR Deployment	0.63
License OR Copyright OR application OR Product OR appliance	0.62
Education OR Training OR Course OR certificate OR Seminar	0.54
<i>Average</i>	<i>0.59</i>
Factor 3	
Hosted OR Hosting OR Host	0.96
SaaS Or Software as a Service	0.68
<i>Average</i>	<i>0.82</i>
Factor 4	
Penetration testing OR Vulnerability	0.69
Audit OR Vulnerability Testing OR Penetration Testing	0.68
Network Security OR IT security	0.47
<i>Average</i>	<i>0.61</i>
Factor 5	
Monitoring	0.97
Incident Response OR Defence Center OR Intrusion	0.65

Detection	
<i>Average</i>	<i>0.81</i>
Factor 6	
Confidentiality	0.86
Factor 7	
Authentication Or Authorization	0.67
Encryption	0.48
<i>Average</i>	<i>0.57</i>
Factor 8	
Planning OR project Management Or configuration	0.54
Consulting OR Consult OR Consultation	0.48
Integrate OR Integration OR Integrating	0.45
<i>Average</i>	<i>0.49</i>
Factor 9	
Data Security OR Back up OR data protection	0.90
Disaster Recovery OR Business Continuity	0.47
<i>Average</i>	<i>0.68</i>

Twenty one keywords have been considered in the factor loadings and no cross-loading has been identified. Having no cross loading is a strong result and indicates the solidness of the result. Stevens (2009) recommended that the average loadings higher than 0.6 would be considered reliable factors. All factors have average loading above 0.49, 6 factors have average loading over 0.6 and only three factors (factor 2, factor 7 and factor 8) loadings are below 0.6 but close to border. It's the researcher's decision to accept these factors. I have decided to accept them since the keywords that have been identified in those factors were meaningful and good insights could be

constructed based on them. The following table shows the result of nine factors and loadings of each keyword:

Table 8- Factor Analysis Result of each keyword (Sample 184)

		Factor1	Factor2	Factor3	Factor4	Factor5	Factor6	Factor7	Factor8	Factor9
1	Service OR Support	0.76	0.17	0.165	0.169	0	0	0.156	0.108	0
2	Technical Support OR Customer Support	0.478	0.213	0	0	0	0	0.117	0.183	0
3	Installation OR Install OR Deployment	0.105	0.625	0.198	0	0.147	0	0	0	0
4	Planning OR project management OR Configuration	0.286	0.38	0	0	0	0	0	0.536	0
5	Consulting OR Consult OR Consultation	0	0	0	0	0	0	-0.107	0.479	0
6	License OR Copyright OR application OR Product OR appliance	0.127	0.623	0	0.249	0	0	0	0.143	0
7	Hosted OR hosting OR host	0	0.238	0.964	0	0	0	0	0	0
8	Customization OR Customize	0	0.263	0	-0.179	0	0	0	0.329	0
9	Hardening OR Securing OR Protection	0	0.171	0	0.319	0.125	0.418	0.275	0	0.131
10	Disaster Recovery OR Business Continuity	0.266	0	0	0	0	0.123	-0.133	0.158	0.48
11	Audit OR Vulnerability Assessment OR Penetration Testing	0	0.149	0	0.677	0	0.125	0.213	0.102	0.197
12	Network Security OR IT Security	0.329	0.27	0	0.474	0.102	0	0	-0.202	0
13	Data Security OR Back up OR data protection	0.302	0.103	0.147	0	0	0.152	0.172	0	0.9
14	Education OR Training OR Course OR certificate OR Seminar	0.169	0.545	0	0	0	0.183	0.205	0.164	0
15	Integrate OR Integration OR Integrating	0.372	0.209	0	0	0	0	0.198	0.446	0
16	SaaS OR Software as a Service	0.231	0	0.676	0	0	0	0.306	0	0.12

The following table indicates that 58% of the sample's total variance was explained by the extracted factors. While it is a fairly low percentage, the result was predictable. The keywords are the language of the websites and not all the companies using the same language on their website. The research methodology has been undertaken with previous researchers and they have faced similar low cumulative variance with their factors. For example, Allen (2009) accepts his 4 components with 36.7% cumulative variance.

Table 9- Sum of Squared loadings (Sample 184)

Factors	SS Loading	Proportion Var	Cumulative Var
Factor1	2.43	0.11	0.11
Factor2	1.78	0.08	0.18
Factor3	1.58	0.07	0.25
Factor4	1.52	0.07	0.32
Factor5	1.51	0.07	0.38
Factor6	1.25	0.05	0.44
Factor7	1.14	0.05	0.49
Factor8	1.08	0.05	0.53
Factor9	1.07	0.05	0.58

4.2 Firms Ranking

Each firm's website can be scored based on the factor and loading of the keywords. In order to do so, a matrix of firm's and factors have been calculated and allowed the factors to be ranked in terms of corresponding level of activity found in the sample. Top 25% of each score were most active and has been used to calculate the companies' scoring and coding (Allen, 2009). The following table indicates the descriptive statistics of the nine factors:

Table 10- Descriptive Statistics of nine factors

Factors	Min	Max	Mean	Std
Factor 1	1.540633	648.7456	82.16171	60.74991
Factor 2	2.153978	270.9265	77.71175	47.03639
Factor 3	1.402894	173.2599	33.55232	29.93456
Factor 4	0.211854	189.907	36.85675	31.31856
Factor 5	0	149.0037	29.3768	29.96519
Factor 6	0	80.64778	12.32083	13.06184
Factor 7	-5.1	198.8001	27.91198	25.96036
Factor 8	-7.2718	156.3313	37.65962	27.72896
Factor 9	0	103.7995	13.86671	16.69129

Figure-4 demonstrates that Factor 1 and Factor 2 are dominating with over twice the average scores of other factors. Factor 3, 4, 8 are the respective followers with scores higher than 30%.

Figure 4- Factors Scoring
Chart

The following table shows the 109 companies classified by type of factors. One under each factor means that the company associates with that factor in the manner described by that factor. The coding is based on the association of each factor with each company. For example EnTeraSec associates with factors 4, 8 and 9, so it is coded as “489”. This table would be useful to identify the companies’ different offerings. The offerings are varied and different combinations are used by companies.

Table 11- Company Coding

Company	F1	F2	F3	F4	F5	F6	F7	F8	F9	Code
Fisher Screek	0	0	0	0	0	0	0	1	0	8
Cedvalinfo	0	0	0	0	1	0	0	0	0	5
Open Technology Group	0	1	0	0	0	0	0	0	0	2
CopyLeft Solutions	0	1	0	0	0	0	0	0	0	2
Tag 1 Consulting	0	0	0	0	0	0	0	1	0	8
PC Mech	0	0	1	0	0	0	0	0	0	3
Edgeos	0	0	0	1	0	0	0	0	0	4
EnteraSec	0	0	0	1	0	0	0	1	1	489
Secure Network Inc	0	0	0	0	0	1	0	0	0	6
Arden Group	0	0	0	0	0	0	0	1	1	89
True Digital Security	0	0	0	1	1	0	0	0	0	45
Bit Pusher	0	0	0	0	1	0	0	0	0	5
Agenda	1	1	0	0	0	1	1	1	0	12678
OSSEC	0	0	0	0	1	0	0	0	0	5
Above Security	0	0	0	1	0	1	0	0	0	46
Linalis	0	1	1	0	0	0	1	1	0	2378
Stealth-ISS Group	0	0	0	0	0	1	0	0	1	69
Global System	0	0	0	0	0	0	0	1	0	8

Company	F1	F2	F3	F4	F5	F6	F7	F8	F9	Code
Consulting										
Report Star	0	0	0	0	1	0	0	0	0	5
Essensys	0	0	0	0	1	0	0	0	1	59
Snow doniait	0	0	0	0	1	0	0	0	0	5
Iqbio	0	0	0	0	0	0	0	0	1	9
Spider Tools	0	0	0	0	0	0	0	1	0	8
Cymtec	0	0	0	1	0	0	0	0	0	4
Allegro										
Consulting	0	0	0	0	1	0	0	1	0	58
Voyantinc	0	0	0	0	0	1	0	0	1	69
Open Xtra	0	0	1	0	1	0	0	0	0	35
Clear Bluse										
Security	0	0	0	1	1	0	0	0	0	45
BA	0	0	0	0	0	0	0	1	0	8
WebSense	0	0	0	0	0	0	0	0	1	9
Ground Work										
Open Source	0	0	1	0	1	0	0	0	0	35
bit-axx	0	0	1	0	0	0	0	0	1	39
Netways	0	0	0	0	1	0	0	0	1	59
Palaestra										
Training	0	0	1	0	0	0	0	0	0	3
Anteza	0	0	1	0	0	0	0	1	0	38
OSX	0	0	1	0	0	0	0	0	1	39
TripWire	0	0	0	1	1	1	1	1	1	456789
Koteas	0	0	0	1	0	1	0	0	0	46
Parallels	0	0	1	0	0	0	0	0	0	3
OP5	0	0	0	0	1	0	0	1	0	58
Tachometry	0	0	0	0	0	0	0	1	0	8
Aladdin	0	1	1	1	0	1	1	0	1	23467

Company	F1	F2	F3	F4	F5	F6	F7	F8	F9	Code
BT- Managed Security Solutions	1	1	1	1	1	1	1	0	1	12345679
B-LUC consulting	0	1	1	1	1	1	0	1	0	234568
F5	1	1	0	0	1	1	1	1	1	1256789
Cat Bird	1	1	0	1	1	1	0	0	0	12456
Xroads Networks	0	0	0	0	1	0	0	0	1	59
Terinea	0	0	1	0	0	0	0	0	1	39
Lumension	1	1	0	1	0	1	1	1	1	1246789
Professor Messer	1	1	1	0	1	1	1	0	1	1235679
Guardian Digital	0	0	0	1	1	0	0	0	0	45
Sawmill	1	1	1	1	0	1	1	0	1	1234679
Titus Labs	0	0	0	0	0	1	0	0	0	6
Adventus	0	0	0	0	1	0	0	0	0	5
Astaro	1	1	1	1	0	1	1	0	1	1234679
Auricnet	0	1	0	0	0	0	0	0	1	29
Clear Swift	0	0	0	0	0	1	0	0	0	1
Symmetrix Tech	1	1	1	0	1	0	0	1	0	12358
BorderWare	0	0	0	1	0	0	0	0	0	4
Source Fire	1	0	0	1	0	1	0	0	0	146
Chosen Security	0	0	0	0	0	1	1	0	0	67
Send Mail	1	1	0	1	1	1	1	1	0	1245678
Intersectalliance	1	1	1	1	1	1	1	0	1	12345679
Protocol 6	1	1	0	1	1	0	0	1	0	12458
SupportPro	0	0	1	0	1	0	0	0	1	359
Singlepoint OC	1	0	0	0	1	1	0	1	1	115689
Work Share	0	0	1	0	0	0	1	0	1	379

Company	F1	F2	F3	F4	F5	F6	F7	F8	F9	Code
Solutionary	1	1	0	1	1	1	1	1	1	12456789
Contego	0	0	0	0	1	0	0	0	0	5
NeoNOVA	0	0	1	0	0	0	0	0	0	3
Consol	0	0	0	0	1	0	0	0	0	5
Zenoss	1	1	1	0	1	0	0	1	0	12358
Symtrex	1	1	1	1	1	1	1	0	1	12345679
Phoenix Datacom	1	1	0	1	1	0	0	1	0	12458
FS-Security	0	0	1	0	0	0	0	0	0	3
Iron Port	1	1	1	1	1	1	1	0	1	12345679
Athena-SCS	0	1	0	0	0	1	1	0	0	267
Secnap	1	1	1	1	1	1	1	0	0	1234567
RSA	1	1	1	0	0	1	1	1	1	1236789
Project Open	0	0	0	0	0	0	0	1	0	8
Heidi	0	1	0	0	0	1	1	0	0	267
Alphanet Solution	1	1	1	0	0	1	0	0	1	12369
GeoTrust	0	1	1	0	0	1	1	0	0	2367
Industrial Defender	1	1	1	1	1	1	1	0	0	1234567
Centrify	1	1	1	1	1	1	1	1	1	123456789
EasyRider	1	1	1	1	1	0	0	1	0	123458
Untangle	1	1	0	0	1	1	0	0	0	1256
Visolve	0	1	1	0	1	0	1	1	0	23578
Emergen	1	1	0	0	0	1	0	1	1	12689
Clearly Connected	1	1	0	0	0	0	0	1	1	1289
PGP	1	1	1	1	0	1	1	0	1	1234679
Endian	1	1	0	1	1	1	1	0	0	124567
Savvis	1	0	1	0	1	0	0	0	1	1359

Company	F1	F2	F3	F4	F5	F6	F7	F8	F9	Code
ProofPoint	1	1	1	0	0	1	1	0	1	123679
MiraPoint	1	1	0	0	0	1	1	1	1	126789
Qualys	1	1	1	1	1	1	1	0	1	12345679
Safenet Inc	1	1	1	1	0	1	1	1	1	12346789
Ubuntu	0	1	0	1	0	0	0	0	0	24
Osriver	1	1	0	1	0	0	0	1	0	1248
Saosce	1	0	0	0	1	0	0	1	1	1589
Oakton	1	1	0	0	0	0	0	1	0	128
Computer Revolution	1	1	1	0	0	1	1	1	1	1236789
Consol Consulting Solution	0	0	0	0	1	0	0	1	0	58
Ethereal Soft	0	1	0	0	0	1	1	1	0	2678
Hurricane labs	1	0	1	0	1	0	1	0	0	1357
Hacker Target	0	0	1	1	0	1	0	1	0	3468
Solution First	1	0	1	0	0	0	0	0	1	139
Axiom Networking	1	0	0	0	0	0	0	1	0	18
Barracuda Networks	1	1	1	1	1	1	1	1	1	123456789

The following table (Table-12) demonstrates the companies that are scored as top 25% companies that are associating with each factor:

Table 12- Companies classification based on factors

Factor	Companies	%
Factor 1	Agenda, BT- Managed Security Solutions F5 Cat Bird Lumension Professor Messer Sawmill Astaro Symmetrix Tech Source Fire Send Mail Intersectalliance Protocol 6 Singlepoint OC Solutionary Zenoss Symtrex Phoenix Datacom Iron Port Secnap RSA Alphanet Solution Industrial Defender Centrify	23.9%

Factor	Companies	%
	EasyRider Untangle Emergen Sun Clearly Connected PGP Endian Savvis ProofPoint MiraPoint Qualys Safenet Inc Osriver Saosce Oakton Computer Revolution Hurricane labs Solution First Axiom Networking Barracuda Networks	
Factor 2	Open Technology Group CopyLeft Solutions Agenda Linalis Aladdin BT- Managed Security Solutions B-LUC consulting	26%

Factor	Companies	%
	F5 Cat Bird Lumension Professor Messer Sawmill Astaro Auricnet Symmetrix Tech Send Mail Intersectalliance Protocol 6 Solutionary Zenoss Symtrex Phoenix Datacom Iron Port Athena-SCS Secnap RSA Heidi Alphanet Solution GeoTrust Industrial Defender Centrifify EasyRider Untangle Visolve Emergen	

Factor	Companies	%
	Clearly Connected PGP Endian ProofPoint MiraPoint Qualys Safenet Inc Ubuntu Osriver Oakton Computer Revolution Ethereal Soft Barracuda Networks	
Factor 3	PC Mech Linalis Open Xtra Ground Work Open Source bit-axx Palaestra Training Anteza OSX Parallels Aladdin BT- Managed Security Solutions B-LUC consulting Terinea Professor Messer	23.3%

Factor	Companies	%
	Sawmill Astaro Symmetrix Tech Intersectalliance SupportPro Work Share NeoNOVA Zenoss Symtrex FS-Security Iron Port Secnap RSA Alphanet Solution GeoTrust Industrial Defender Centrify EasyRider Visolve PGP Savvis ProofPoint Qualys Safenet Inc Computer Revolution Hurricane labs Hacker Target Solution First	

Factor	Companies	%
	Barracuda Networks	
Factor 4	Edgeos EnteraSec True Digital Security Above Security Cymtec Clear Bluse Security TripWire Koteas Aladdin BT- Managed Security Solutions B-LUC consulting Cat Bird Lumension Guardian Digital Sawmill Astaro BorderWare Source Fire Send Mail Intersectalliance Protocol 6 Solutionary Symtrex Phoenix Datacom Iron Port Secnap	20.1%

Factor	Companies	%
	Industrial Defender Centrifify EasyRider PGP Endian Qualys Safenet Inc Ubuntu Osriver Hacker Target Barracuda Networks	
Factor 5	Cedvalinfo True Digital Security Bit Pusher OSSEC Report Star Essensys Snow doniait Allegro Consulting Open Xtra Clear Bluse Security Ground Work Open Source Netways TripWire OP5 BT- Managed Security Solutions	26.08%

Factor	Companies	%
	B-LUC consulting F5 Cat Bird Xroads Networks Professor Messer Guardian Digital Adventus Symmetrix Tech Send Mail Intersectalliance Protocol 6 SupportPro Singlepoint OC Solutionary Contego Consol Zenoss Symtrex Phoenix Datacom Iron Port Secnap Industrial Defender Centrify EasyRider Untangle Visolve Endian Savvis	

Factor	Companies	%
	Qualys Saosce Consol Consulting Solution Hurricane labs Barracuda Networks	
Factor 6	Secure Network Inc Agenda Above Security Stealth-ISS Group Voyantinc TripWire Koteas Aladdin BT- Managed Security Solutions B-LUC consulting F5 Cat Bird Lumension Professor Messer Sawmill Titus Labs Astaro Clear Swift Source Fire Chosen Security Send Mail	25%

Factor	Companies	%
	Intersectalliance Singlepoint OC Solutionary Symtrex Iron Port Athena-SCS Secnap RSA Heidi Alphanet Solution GeoTrust Industrial Defender Centrify Untangle Emergen PGP Endian ProofPoint MiraPoint Qualys Safenet Inc Computer Revolution Ethereum Soft Hacker Target Barracuda Networks	
Factor 7	Agenda Linalis TripWire	19.5%

Factor	Companies	%
	Aladdin BT- Managed Security Solutions F5 Lumension Professor Messer Sawmill Astaro Chosen Security Send Mail Intersectalliance Work Share Solutionary Symtrex Iron Port Athena-SCS Secnap RSA Heidi GeoTrust Industrial Defender Centrify Visolve PGP Endian ProofPoint MiraPoint Qualys	

Factor	Companies	%
	Safenet Inc Computer Revolution Ethereum Soft Hurricane labs Barracuda Networks Online WebStat	
Factor 8	Fisher Scream Tag 1 Consulting EnteraSec Arden Group Agenda Linalis Global System Consulting Spider Tools Allegro Consulting BA Anteza TripWire OP5 Tachometry B-LUC consulting F5 Lumension Symmetrix Tech Send Mail Protocol 6 Singlepoint OC	22.8%

Factor	Companies	%
	Solutionary Zenoss Phoenix Datacom RSA Project Open Centrify EasyRider Visolve Emergen Clearly Connected MiraPoint Safenet Inc Osriver Saosce Oakton Computer Revolution Consol Consulting Solution Ethereal Soft Hacker Target Axiom Networking Barracuda Networks	
Factor 9	EnteraSec Arden Group Stealth-ISS Group Essensys Iqbio Voyantinc	23.36%

Factor	Companies	%
	WebSense bit-axx Netways OSX TripWire Aladdin BT- Managed Security Solutions F5 Xroads Networks Terinea Lumension Professor Messer Sawmill Astaro Auricnet Intersectalliance SupportPro Singlepoint OC Work Share Solutionary Symtrex Iron Port RSA Alphanet Solution Centrify Emergen Clearly Connected	

Factor	Companies	%
	PGP	
	Savvis	
	ProofPoint	
	MiraPoint	
	Qualys	
	Safenet Inc	
	Saosce	
	Computer Revolution	
	Solution First	
	Barracuda Networks	

4.3 Validate Result

Hicks et al.(2005) recommends that the researcher should validate their results to ensure that the result was not a pure statistical outcome and have nothing to do with reality. The keywords were the main tools that led to the generation of this result and in order to prove that this set of keywords are meaningful in the open source security context not any ordinary context, the researcher has used the same set of keywords on Fortune 1000 company URLs and calculated the same test results to conclude that the data is not factorable. This is the same strategy that Hicks et al.(2006), Jdue (2009) and Allen (2009) pursued to validate their research. I have used the same list of URLs that Allen and Jdue used in their research validation, so the list is Fortune 1000 that has been created on 2007. Total of 959 URLs were used as the input of Keyword Searcher Tool and the same set of 23 keywords that resulted in our nine factors. The

result returned a huge number of URLs with no hit count for any of the keywords. The output was trimmed and only URLs with at least one variable higher than “0” was kept and rest deleted. This process was necessary since our statistical tool (R) would not accept it otherwise. The final was 131 URLs out of 959 (828 URLs removed). This is a good indication that the keywords are addressing different context and are so rare in Fortune 1000 companies, but I performed the Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy and the Bartlett’s test of Sphericity Significance Test to observe the difference.

Table 13- Fortune 1000 Statistical Tests

Metric		Limit	Result
Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy		>0.5	0.503
Bartlett’s test of Sphericity Significance Test	Approx. Chi-Square		750.7
	df		130
	Sig.	<0.05	< 2.2e-16

The result of KMO sampling adequacy test (Table-13) indicates that even the 131 remaining URLs is not able to be factorized since the result is almost on border. This is a very powerful indication that these keywords are not general and cannot be used on Fortune 1000 companies.

5. DISCUSSION OF RESULTS

This chapter covers three sections. Section 5.1 identifies the factor interoperation. Section 5.2 compares the result of this research to the OSS commercialization frameworks that have been studied in the literature review. Section 5.3 demonstrates the factor clustering based on K-mean clustering.

5.1 Interpret Factors

The following table has summarized the factor interoperation. The factors are interoperated based on initial knowledge about the definition of selected keywords found in company websites and the literature review. For each factor at least 10 companies have been studied in-depth (companies that coded with that factor). This helped the researcher to create a more accurate interpretation of factors. A minimum two keywords have been used for the interoperation of each factor with the exception of Factor 6 that only one keyword had loading over 0.45, so the researcher incorporated two other keywords with loading of 0.41 to describe this factor. Factors are named based on their description and the naming can be biased by the researcher's preference. These factors are identified as the nine different market offer types available through OSST.

Table 14- Factor Interpretation- OSST Market offers

Factor	Name	Keywords	Interpretation
1	Support Services	<p>The following keywords were used by this factor with loading over 0.45:</p> <p>Service OR Support: With 0.76 Loading, these keywords can be interpreted as any service or support that is provided to customers regarding OSST or related products.</p> <p>Availability: With 0.76 loading, these keywords can be interpreted to ensure availability of the client's infrastructure through 24/7 support.</p> <p>Technical support OR customer support: With 0.48 loading, these keywords show the technical related supports for OSST through different types of technical support services.</p>	<p>Companies that are offering support services based on OSST are mainly providing following type of solutions:</p> <p>These companies provide technical support through phone, chat, email, online knowledge base, product updates and firmware and other ways.</p> <p>Companies that are in this category ensure the availability of mission critical infrastructure of their clients by providing them a 24/7 support services and on time updates.</p> <p>Some of these companies are</p>

Factor	Name	Keywords	Interpretation
			embedding the OSST in the new product and provide a technical and customer support for their own specific product. Some integrate the OSST as a solution for their clients and provide support services, as well these companies can be categorized as consulting companies that continue their relationship with their customers through an ongoing support contracts and some of the companies in this category only provide technical support services for OSST.
2	Product Services	<p>The following keywords were used by this factor with loading over 0.45:</p> <p>Installation OR Deployment:</p> <p>With 0.63 loading, these keywords can be interpreted as</p>	Companies that are offering Professional solutions based on OSST are mainly providing following type of solutions:

Factor	Name	Keywords	Interpretation
		<p>services to integrate OSST with companies' infrastructure like policy development, security assessment, security device integration...</p> <p>License OR Commercial OR Product OR Appliance: With 0.62 loading, these keywords mean the offering of OSST as a hardware appliance (embedding OSST into firewall, VPN, USB based authentication keys, content filtering) or software suite (vulnerability management tools, policy compliance tools, web application scanners)</p> <p>Training OR educations: With 0.54 loading, these keywords emphasize the training programs that are delivered by companies on OSST or their products that is based on OSST.</p>	<p>Companies provide different type of services to integrate OSST into client's current infrastructure.</p> <p>Companies use dual licensing approach or embed some of the OSST into one solid hardware appliance / software suite and sell the products with additional services to their clients.</p> <p>Some companies position themselves as specialist in providing training services for OSST. World class training programs for industry certificates as well as on site or in class trainings for system and network administration based on OSST. Different types of training are offers</p>

Factor	Name	Keywords	Interpretation
			from in class trainings for Snort certification to quick on line tutorials for simpler tools that can be used for day to day network administration tasks.
3	Hosted Services	<p>The following keywords were used by this factor with loading over 0.45:</p> <p>Hosted OR Subscription: With 0.96 loading, these keywords can be interpreted as any security related services like monitoring, vulnerability assessment and virus removal that are provided as a service over the internet and generate revenue through subscriptions.</p> <p>SaaS OR Software as a Service: With 0.68 loading, these keywords indicate solutions like virtualization, web hosting and virtual private servers. These services can be provided to consumers of these services or providers like</p>	<p>Companies that are offering Hosted Services based on OSST are mainly providing following type of solutions:</p> <p>Some of these companies are providing IT and security services through internet as a service to their clients. Example of these services are 24/7 automated monitoring of network infrastructure, Online antivirus and antispyware removal, remote vulnerability assessments and</p>

Factor	Name	Keywords	Interpretation
		independent software vendors that are willing to host their software on the clouds.	managed IT services. Some of these services are aimed for cloud service providers like virtualizations, and web hosting.
4	Security Analysis Services	<p>The following keywords were used by this factor with loading over 0.45:</p> <p>Audit OR Vulnerability Assessment: 0.68 loading</p> <p>Penetration testing OR vulnerability: 0.69 loading</p> <p>These keywords can be interpreted as services that are using OSST to identify IT security threats to business and provide solutions to mitigate them. These services can be provided as a hosted service or on-site service. Some specific types of services are log management, vulnerability management, online security</p>	<p>Companies that are offering Security Analysis Services based on OSST are mainly providing following type of solutions:</p> <p>They evaluate security vulnerabilities and propose measurements to mitigate them.</p> <p>They unified different tools and provide a complete security analysis of the client's infrastructure as a hosted / in-house service.</p>

Factor	Name	Keywords	Interpretation
		scans (nmap , nessus...)	Some of these companies provide a platform for vulnerability assessment and penetration testing, so other security consulting companies can use it in their offerings.
5	Monitoring Services	<p>The following keywords were used by this factor with loading over 0.45:</p> <p>Incident Response OR Defence Center: With 0.65 loading, these keywords can be interpreted as offerings that provide incident response solutions for companies that are willing to outsource their security. Usually OSST and proprietary tools would be installed on client's infrastructure (HIDS, NIDS...) and an automated tool, human or a hybrid solution would alert the company in case of an attack. Tools like Snort are</p>	<p>Companies that are offering Monitoring Services based on OSST are mainly providing following type of solutions:</p> <p>Some of these companies outsource the security solutions of their clients by providing them a defence center which monitors their network activity and reports back the result to the monitoring stations and an automated task or human interaction</p>

Factor	Name	Keywords	Interpretation
		<p>great examples that are used in this offering.</p> <p>Monitoring: With loading of 0.97, this keyword can be interpreted as a service that incorporate OSST tools like Nagios and monitor any activity on the network and report the result. These services can be provided as a simple online monitoring tool for small businesses to more sophisticated solution for enterprises with over 10000 nodes.</p>	<p>would perform any further actions.</p> <p>Some of these offerings are created some additions for some OSST monitoring tools like reporting, real time alerting or active response and market their product as a product or service and provide further monitoring services as requested.</p>
6	Confidentiality services	<p>The “Confidentiality” keyword was used with 0.86 loading, “Encryption” Loading was 0.411 and “hardening OR protection” keywords loading was 0.418):</p> <p>These keywords are the indication that some companies are providing encryption services to ensure the confidentiality and integrity of</p>	<p>Companies that are offering Confidentiality Services based on OSST are mainly providing following type of solutions:</p> <p>They provide data integrity and confidentiality through encryption and data storage. Tools like</p>

Factor	Name	Keywords	Interpretation
		data. They secure data storage and provide data encryption solutions to their clients.	PGP, TrueCrypt are some of the examples of OSST that are used in these offering.
7	Authentication, Authorization and Accountability (AAA) Services	<p>The following keyword was used by this factor with loading over 0.45:</p> <p>Authentication OR Authorization: With 0.67 loading, this keyword can be interpreted as any solution that deals with authentication and authorization. Digital Signature, secure Email, security certificate, smart card and tokens, PKI tools.</p> <p>Encryption: With loading of 0.48, this keyword indicates incorporating encryption technology into AAA products.</p>	<p>Companies that are offering AAA Services based on OSST are mainly providing following type of solutions:</p> <p>They use OSST to create solutions that can be implemented into AAA services. Example would be using Open SSL to create Security Certificates or digital signatures, incorporating OSST into smart cards.</p> <p>Some of these companies have created tools for legal activities and investigation</p>

Factor	Name	Keywords	Interpretation
			purposes. Like document comparison.
8	Project Management Services	<p>The following keyword was used by this factor with loading over 0.45:</p> <p>Planning OR Project Management: With loading of 0.54, these keywords are interpreted as any security consulting services that incorporate OSST into implementing security solutions.</p> <p>Consulting OR Consult: With 0.48, these keywords indicates any consulting services.</p> <p>Integrate OR Integration OR Integrating: with loading of 0.45, these keywords indicate integrating OSST into new or current solutions. In other words, some companies help their clients with integration of OSST as a solution.</p>	<p>Companies that are offering Project Management Services based on OSST are mainly providing following type of solutions:</p> <p>Companies using OSST and perform a full or partial project management from planning to deployment and support to secure their clients network and other assets. This can vary from deploying a top notch solution for enterprises or a simple software installation for consumers.</p>
9	Disaster Recovery and	The “ Data Security OR back up ” keywords was used with	Companies that are offering Disaster

Factor	Name	Keywords	Interpretation
	Business Continuity services	<p>0.9 loading, “Disaster Recovery” keyword Loading was 0.47 :</p> <p>These keywords are good indication of offerings that are tailored for securing data and ensure the availability of company’s asset. Online backup storages, offsite backups and data recovery are some of the specific offerings that fit into this category.</p>	<p>Recovery and Business Continuity Services based on OSST are mainly providing following type of solutions:</p> <p>They provide data backups through online (hosted) solutions or in-house services. Some companies provide data storage and some provide expertise. The main goal is to ensure availability of their customer’s data.</p> <p>Some of these offerings are aimed to recover lost or stolen data (e.g. OSST can be incorporated to reveal deleted files).</p> <p>Some companies provide professional services to their clients</p>

Factor	Name	Keywords	Interpretation
			to define disaster recovery plans. These companies are mainly consultants that their main area of expertise is disaster recovery.

5.2 OSST and OSS market offers compassion

Factor interpretation can be used to generate the type of market offers existing within the OSST domain and compare them with the frameworks and taxonomies of OSS commercialization as studied in the literature review. Five of the OSST offers are considered to be unique offerings that are only available in OSST and security related offerings. Nine OSST market offers and comparison to OSS market offers:

- 1- **Support Services:** This offering provides any technical support services on OSST and products that are created based on OSST. Koenig (2004) support strategy, Dahlamder (2004) support category, Hecker (1998) support sellers and Alam (2006) support offerings are the similar offerings that are available on OSS. In other words, in OSST the same support strategy is available to provide technical support that is not available through the community of open source.
- 2- **Product Services:** This offering includes services to integrate OSST into client infrastructure, dual license and embedding into hardware, and training services. Koenig (2004) optimization, patronage and embedded strategies;

Dahlamder (2004) Licensing and Black Box categories,;Hecker (1998) Loss leader and Widget Frosting; and Alam (2006) Commercial Licenses and products and training and testing offerings are the similar offerings on OSS.

- 3- **Hosted Services:** This offer provides SaaS and cloud computing types of offerings with OSST. Koeing (2004) Hosted strategies; Hecker (1998) Service Enabler; and Alam (2006) hosting and content services offerings are the similar offerings on OSS.
- 4- **Security Analysis Services:** This offering provides any security related services like vulnerability assessment, penetration testing and threat risk assessment. This offering is unique in OSST and no similar offerings in general OSS commercialization models have been found.
- 5- **Monitoring Services:** This offering provides defence and monitoring centers that is used to outsource client's security. This offering is unique in OSST and no similar offerings in general OSS commercialization models have been found.
- 6- **Confidentiality Services:** This is another unique offering around OSST that incorporates technologies like encryption to achieve confidentiality and integrity of data. Generally OSS has not any offerings like this and it's classified as an OSST specialized market offer type.
- 7- **AAA Services:** This offer provides security solutions to implement AAA services and it's applicable in securing infrastructure and legal investigations.

This offer is unique for OSST and similar offerings in the general OSS context are not available.

- 8- **Project Management Services:** This offer provides consulting services and implementation of security based projects based on OSST. Koeing (2004) Consulting strategies; Dahlamder (2004) consultancy category; Hecker (1998) Support Sellers; and Alam (2006) support services offerings are the similar offerings in OSS.
- 9- **Disaster Recovery and Business Continuity Services:** This offer provides security related services to recover from a disaster and ensure the continuity of business processes. This offer is unique for OSST and the similar strategies and offerings are not available in the general OSS context. The following table demonstrates the OSS and OSST market offers:

Table 15- OSS and OSST Market Offers comparison

Market Offers	OSS	OSST
Support Services	✓	✓
Product Services	✓	✓
Hosted Services	✓	✓
Security Analysis Services		✓
Monitoring Services		✓
Confidentiality Services		✓
AAA Services		✓
Project Management Services	✓	✓
BC and DR Services		✓

This table illustrates the fact that the specialized vertical subset of OSS projects (OSST) provides more options for companies to create market offers. In other words, firm's can incorporate OSST in their offerings in the ways that is not available with general OSS. Surprisingly, OSST provides you with more options to create market offers like monitoring services or Business Continuity and Disaster Recovery.

5.3 Clustering Factors

The research goal is to find out which factors are used in conjunction with others and can be classified as separate groups. Cluster analysis is one useful method that has been used by researchers in different types of research and use mathematical methods to classify similar objects together. A cluster is a set of entities which are alike, and entities from different clusters are not alike (Rui and Wunsh,2009). Different strategies have been studied to cluster the offerings and K-mean clustering seemed to be the best candidate for our data. Haung (1998) and Macqueen (1967) identified K-means clustering as a good way of clustering large data set by using similarities grouping. K -means clustering algorithm was developed by J. MacQueen (1967) and then by J. A. Hartigan and M. A. Wong around 1975. Simply speaking, K-means clustering is an algorithm to classify or to group your objects based on attributes/features into K number of group. K is positive integer number. The grouping is done by minimizing the sum of squares of distances between data and the corresponding cluster centroid. Thus the purpose of K-mean clustering is to classify the data (Teknomo, 2006).

We have performed cluster analysis on firm's that have been factorized. The list of 109 companies with loading for each factors have been used to perform K-mean clustering. A plot of the within groups sum of squares by number of clusters extracted can help determine the appropriate number of clusters. The researcher looks for a bend in the plot similar to a Scree test in factor analysis (Everitt and Hothorn,

2006, P 251) . The following graph is the plot that indicates the bend between 2 and 3 clusters.

Figure 5- K-mean Cluster Analysis plot to determine number of clusters

The researcher performed both K-mean cluster analyses with 2 and 3 clusters. The result of clustering with 3 clusters was more appealing, so the cluster analysis with three clusters has been performed and factors with the mean higher than average mean of each cluster extracted as the factors that are clustering in each cluster. The following table summarized the k-mean clustering of 100 companies:

Table 16- K-mean Cluster Analysis Result

Cluster	Factors	Name	Interpretation	%
Cluster 1	F4- Security Analysis Services F5- Monitoring Services F8- Project Management Services F2- Product Services F1- Support Services	Consulting Service Providers	<p>The cluster of these companies are providing security analysis services like vulnerability assessment and project management services, They provide support services, training and counselling to their clients and also set up monitoring centers to monitor their client's infrastructure.</p> <p>Companies clustered in this category are mainly providing parliamentary vulnerability assessment of their client's infrastructure and implement the solution and provide future support services as well as trainings and also offer ongoing monitoring services.</p>	17%

Cluster	Factors	Name	Interpretation	%
Cluster 2	F7-Authentication, Authorization and Accountability (AAA) services F8- Confidentiality Services F2- Product Services F1- Support Services	Solution and Product Integrators	This cluster provides solutions (mainly products and appliances) that would provide AAA and confidentiality solutions. They also provide additional services like training, technical support and deployment. The companies in this category are mainly entering the market with a product based on OSST and either market their products with additional services or only sell their professional services.	35.7%

Cluster	Factors	Name	Interpretation	%
Cluster 3	<p>F8- Project Management Services</p> <p>F5- Monitoring services</p> <p>F3- Hosted Services</p> <p>F9- Disaster Recovery and Business Continuity Services</p>	<p>Hosted Solution Providers</p>	<p>This cluster is a very strong indication that the number of companies provide hosted services mainly for disaster recovery and business continuity purposes as well as monitoring and incident response. The SaaS phenomenon are used in their business models and instead of providing an appliance or software, they provide their solutions as a service through Internet. Online storages for backing up data instead of using onsite physical back up mechanism are good example of business continuity product that is offered as a hosted service.</p>	53.2%

The following graph shows the result of k-mean clustering of 109 companies:

Figure 6- Factor clustered according to K-mean clustering

The result indicates that “Hosted Solution Providers” is a popular way of offering the security services. Companies are offering different products and services as an online service to their clients from monitoring to disaster recovery. After hosted solutions, the “Solution and Product Integrators” are in majority. Companies in this category are providing security related products and services like security appliances. The least crowded category is the “Consulting Service Providers”. This is a surprise to the researcher since consulting has always been a crowded market.

Firms can use following result and identify opportunities in their own cluster or adjacent cluster. For example, EnTeraSec which is a security consulting firm in Ottawa is located in Consulting Service Providers cluster which is the least crowded cluster. EnTeraSec can explore opportunities available in other clusters and identify subject matter expert companies as potential collaborators to partner with. For example Open Xtra provides web based monitoring services and is located in Hosted Solution Providers cluster and EnTeraSec is specialized in vulnerability assessment and security consulting. Collaboration of these two companies from different clusters can benefit both companies.

6. CONCLUSION, LIMITATIONS AND FUTURE RESEARCH SUGGESTIONS

This chapter contains three sections. Section 6.1 covers the conclusions of this research. Section 6.2 presents limitations of this research and Section 6.3 concludes the research with future research opportunities.

6.1 Conclusion

Previous research into open source commercialization strategies were qualitative studies. Those early studies as mentioned in the literature review led to the creation of models and frameworks. This research provides an empirically derived approach into categorization of Open Source Security Tools commercialization by analyzing 185 sample firms. Analyzing the vertical market around OSST led to identifying nine underlying factors that differentiate different types of market offers with OSST:

- 1) Support Services
- 2) Product Services
- 3) Hosted Services
- 4) Security Analysis Services
- 5) Monitoring Services
- 6) Confidentiality Services

- 7) Authentication, Authorization and Accountability (AAA) Services
- 8) Project Management Services
- 9) Disaster Recovery and Business Continuity Services

The comparison of OSST market offers and OSS commercialization strategies that have been studied in the literature review identified five unique offerings around OSST: Security Analysis Services, Monitoring Services, Confidentiality Services, AAA Services and Disaster Recovery and Business Continuity Services.

The distribution of factors was varied in the sample companies which indicate that companies are incorporating different strategies in their market offerings. The coding table indicates that a variety of combinations is undertaken with each company; however, factors have been clustered into three different clusters of firms offering similar combinations of OSST market offers:

- 1) Consulting Service Providers- This cluster indicates a range of offerings like project management, support services, vulnerability assessment, monitoring and professional services. Firms in this category mainly provide security consulting services and we named it as consulting service providers.
- 2) Solution and Product Integrators- This cluster indicates the offerings that are addressing AAA and confidentiality solutions in form of a product or service. Firms in this category mainly provide security solutions and products and provide support and professional services as additional add-ons.

- 3) Hosted Solution Providers- This cluster is the most popular cluster and indicates any security services from monitoring to disaster recovery that is provided with a SaaS business model. Project management and consulting is used as a way to implement these solutions for the clients.

While it may be an intuitively compelling proposition, the “hosted solution providers” turns out to be the strongest and most popular approach in commercialization of OSST. The hosting and SaaS approach is a new phenomenon and 53.2% of companies are somehow incorporating this in their market offer. As discussed in the section “Future Work”, to support this clustering and categorization, case studies can be undertaken as well as a longitudinal study of firms can examine how market offers evolve over time especially to SaaS approach.

6.2 Limitations

This research was not without any limitations. Some of them are:

Firstly, the interpretation of factors and developing definitions and names for factors and clusters are subjective and can be influenced by the researcher’s prior knowledge and literature review.

Secondly, the lack of prior research on the same topic was the main reason that led the researcher to use a grounded theory approach. Grounded theory is mainly used for qualitative analysis; however, there is no theory against not using this approach with

quantitative methods. If this topic had been studied before, we could have hypothesized and use this approach to test our hypothesis.

Thirdly, the research was limited in using English language websites and using English keywords. Some of the companies were located in Europe and Other continents and their websites was not in English which lead us to exclude them from our sample list. The ability to use non English websites and keywords could improve the result.

6.3 Future Research Opportunities

The following are the future research opportunities that have been identified by researcher:

1. Develop case studies of the companies in each cluster to verify that firm's market offerings are accurately presented.
2. Perform a longitudinal study of companies to understand the evolution of their offerings through time. As mentioned in the research result, "Hosted Service Providers" is the most popular cluster in these offerings and SaaS is a new concept. A study that would test the evolution of offerings from traditional approaches to more hosted strategies would be a great future research.
3. The OSST market offers has been studied in this research; however, some of these offerings are not limited to open source. There are security related firms that offer similar offerings and are not openly incorporating OSST.

Comparing the results of this research with general security related market offers could provide more insights.

4. The researcher did not study the relationship of market offers and different Open Source Security Projects. The main reason was the fact that not all the firms are talking about the projects they are using in their offerings, so using this methodology and keywords may not be a proper way. A more qualitative approach through interviews and surveys would be extremely helpful to map each project with offerings and even rate the projects based on their usage. This could be helpful for companies that are considering the preliminary research to adopt or incorporate OSST.

REFERENCES

Alam, R. (2006). Open Source Software Project, Market Offer, and Competitive Advantage. Masters Thesis, Technology Innovation Management, Carleton University, Ottawa, Ontario.

Allen, S. (2009). An Empirical Study of components of value co-creation. Masters Thesis, Technology Innovation Management, Carleton University, Ottawa, Ontario.

Anderson, R.J. (2002). Security in open versus closed systems---the Dance of Boltzmann, Coase and Moore. Presented at Open Source Software Economics.

Baase, S. (2003). A gift of fire: social, legal, and ethical issues for computers and the Internet (second edition). Pearson Education, Inc: Saddle River, NJ. ISBN: 0-13-008215-5.

Baghai, M., Coley, C., White, D. (2000). The Alchemy of growth: Practical Insights for building the Enduring Enterprise. Cambridge, Mass: Perseus Publishing.

Berlecon Research. (2002). Floss Final Report- part-3: Basics of Open Source Software Markets & business models. Available at:

http://banners.noticiasdot.com/termometro/boletines/docs/consultoras/floss/2002/FLOSS_Grundlagen.pdf (accessed on Nov/15/2009).

Bezroukov, N. (1999). Open source software development as a special type of academic research (critique of vulgar Raymondism). First Monday 4 (10).

Bonaccorsi, A. Rossi, C. (2003). Why Open Source software can succeed. Research Policy 32(7): 1243–258.

Capek, P.G., Frank, S.P., Gredt, S., Shields, D. (2005), A history of IBM's open-source involvement and strategy, *IBM Systems Journal*, 44(2): 249-257.

Christensen, M.C., Carlile, R. (2005). The cycles of theory building in management research. Research Paper. Version 6.0.

Colquitt, J., Zapata Phelan, C. (2007), "Trends in theory building and theory testing: a five decade study of the academy of management journal," *Academy of Management Journal* 50(6): 1281–1303.

Costello, A.J., Osborne. (2005). Best Practices in Exploratory Factor Analysis: Four Recommendations for Getting the Most from Your Analysis. *Practical Assessment Research & Evaluation*, 10(7):1-9.

Crispin Cowan (2003). Software security for open-source systems. *IEEE J. Security & Privacy*, 1(1):38–45.

Dahlamder, L. (2004). Appropriating the commons: Firms in Open Source Software. Research Paper.

Dahlamder, L. (2007), Penguin in a new suit: a tale of how de novo entrants emerged to harness free and open source software communities, *Industrial and Corporate Change*, 16(5):913-943.

Darlington, R. (2007). Factor Analysis. Available at : <http://www.psych.cornell.edu/Darlington/factor.htm> (accessed on Jan/10/2010).

DeCoster, J. (1998). Overview of Factor Analysis. Available at: <http://www.stat-help.com/index.html>. (accessed on Nov/12/2009).

Dedrick, J., West, J. (2004) "An exploratory study into open source platform adoption." *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, 5-8 Jan, 265 – 274.

Dey, I. (1999), *Grounding grounded theory – Guidelines for qualitative inquiry*, San Diego: Academic Press.

Dick, B. (2005), “Grounded theory: a thumbnail sketch”. Available at: <http://www.scu.edu.au/schools/gcm/ar/arp/grounded.html> (accessed on Mar/17/2010).

Dholakia, R.Miao, Z.Dholakia, N. Fortin,D. (2000). Interactivity and Revisits to Websites:A Theoretical Framework. Available at: <http://ritim.cba.uri.edu/wp/> (accessed on Mar/16/2009).

Edmondson, A. McManus, S. (2007), Methodological fit in management field research, *Academy of Management Review* 32(4): 1155–1179.

Everitt, B.S., Hothorn, T. (2006). *A Handbook of Statistical Analyses Using R*. Tylor and Francis Groups, LLC. ISBN # 978-1-58488-5399-9.

Friel, M,C. (2009). Notes on Factor analysis. Criminal Justice Center. Sam Houston University. Available at: http://www.shsu.edu/~icc_cmfcj_742/stats9.doc (accessed on Mar/10/2010).

Field, A. (2005). *Discovering Statistics Using SPSS*. Second edition. London: Sage Publications.

Fischer, R,J., Green, G. (2004). *Introduction to security* (seventh edition). Boston: Butterworth- Heinemann). ISBN: 0-7506-7600-0.

Fosfuri, A., Giarratana, M.S., Luzzi, A. (2008). The penguin has entered the building: the commercialization of open source software products, *Organization Science*, 19(2): 292-305.

Fox, J. .(2006). *Getting Started With the R Commander*. Available at:<http://socserv.mcmaster.ca/jfox/Misc/Rcmdr/> (accessed on Feb/02/2010).

Garson, D. (2008). Statnotes: Topics in Multivariate Analysis. Available at: <http://www2.chass.ncsu.edu/garson/pa765/statnote.htm> (accessed on Feb/10/2010).

Glaser, B. G. (1992). Basics of grounded theory analysis. Mill Valley, CA: Sociology Press.

Glaser, B. G., Strauss, A. L. (1967). The discovery of grounded theory: Strategies for qualitative research. New York: Aldine.

Gregg, M. (2006). CISSP (Certificate Information System Security Professionals) Exam Cram2. Que Publishing: USA. ISBN: 08-070605-4321.

Greckhamer, T., Misangyi, V., Elms, H. and Lacey, R. (2008), Using qualitative comparative analysis in strategic management research: An examination of combinations of industry, corporate, and business unit effects, *Organizational Research Methods*. 11(4): 695726.

Hars, A., Ou, S.(2002). Working for free? Motivations for participating in open source project. *International Journal of Electronic Commerce*. 6 (3):25-39.

Hecker, F. (1998). Setting up Shop: The business of Open Source Software. Revision 0.8. Available at: <http://hecker.org/writings/setting-up-shop> (accessed on Feb/20/2009).

Hicks, D., Libaers, D., Porter, L., Schoeneck, D. (2006). Identification of the Technology Commercialization Strategies of High-tech Small Firms. *Small Business Research Summary*. Available at: <http://www.sba.gov/advo/research/rs289tot.pdf> (accessed on Mar/04/2009).

Hoepman, J,H., Jacobs, B.(2008). Increased security through open source. *Communications of the ACM* , 50 (1), 79-83. ACM Digital Library.

Huang, Z. (1998). Extensions to the K-means Algorithm for Clustering Large Datasets with Categorical Values. *Data Mining and Knowledge Discovery*. 2: 283-304.

Jdue, A.A. (2009). Level One Industrial Automation: Choosing Network control Systems. Masters Thesis, Technology Innovation Management, Carleton University, Ottawa, Ontario.

Kelle, Udo (2005), "Emergence' vs. 'Forcing' of Empirical Data? A Crucial Problem of 'Grounded Theory' Reconsidered," *Forum: Qualitative Social Research*, 6(2), Art. 27.

Koenig, J. (2004). Seven Open Source business strategies for competitive advantage. Special Report. Riseforth. Inc. ISSUE 15984.

Kotler, P., Turner, R. (1995). Managing products, lines, brands, and packaging, marketing management analysis, planning, implementation and control. Prentice Hall Canada. 420-449.

Krishnamurthy, S. (2002). Cave or Community? An Empirical Examination of 100 Mature Open Source Projects. Research paper.

Lawton, G.(2002). Open Source Security: Opportunity or Oxymoron? *Computer*, 35(3): 18-21.

Lerner, J., Tirole, J. (2000). The simple economics of open source. NBER working papers series. Number: 7600.

Lerner, J., Tirole, J. (2002). The scope of open source licensing. NBER working papers Series. Number: 9363.

Lombardi, A.J.S. (2008). Interactions between Eclipse Foundation Members and Eclipse Projects. Masters Thesis, Technology Innovation Management, Carleton University, Ottawa, Ontario.

Lowry, R. (2005). Computations and Applications of Inferential Statistics. Available at: <http://faculty.vassar.edu/lowry/webtext.html> (accessed on Mar/10/2010).

MacQueen, J. B. (1967). Some Methods for classification and Analysis of Multivariate Observations, Proceedings of 5-th Berkeley Symposium on Mathematical Statistics and Probability, Berkeley, University of California Press, 1:281-297.

Madey, G., Freeh, V., Tynan, R. (2004), Modeling the free/open source software community: a quantitative investigation, in. Free/Open Source Software Development, Idea Group Publishing, 203-220.

McGahan, Anita M. (2007), "Academic research that matters to managers: on zebras, dogs, lemmings, hammers, and turnips," Academy of Management Journal 50(4), 748–753.

Mockus, A., Fielding, R.T., Hersleb, J.D. (2002), Two case studies of open source software development: Apache and Mozilla, ACM Transactions on Software Engineering Methods, 11(3): 309-346.

Northcutt, S., Zeltser, L., Winters, S., Fredrick, K.K., Ritchy, R.W. (2003) Inside Network Perimeter Security: The definitive Guide to firewalls, VPNs, Routers, and Intrusion Detection Systems. New Riders: Indianapolis, Indiana. ISBN: 0-7357-1232-8.

Opoku, R. (2005), Communication of Brand Personality by Some Top Business Schools Online, Licentiate Thesis, Lulea University of Technology, ISSN: 1402-1757.

Pettigrew, A.M., Woodman, R.W., and Cameron, K.S. (2001) "Studying organizational change and development: Challenges for future research," Academy of Management Journal, 44(4): 697-713.

Pisano, G., Verganti, R. (2008). What kind of collaboration is right for you? *Harvard Business Review*, 78-86.

Reinard, J. (2006). *Communication Research Statistics*, Thousand Oaks, CA, Sage Publications.

Raymond, E. (1999). *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. O'Reilly Press. Available at: <http://catb.org/~esr/writings/cathedral-bazaar/> (accessed on Mar/17/2009).

Roberts, J.A., Hann, I., Slaughter, S.A. (2006), Understanding the motivations, participation, and performance of open source software developers: a longitudinal study of the Apache projects, *Management Science*, 52(7): 984-999.

Rui, X., Wunsh, D. (2009). *Clustering*. IEEE Press. ISBN:9780470276808.

Scacchi, W. (2007). Free/Open Source Software Development: Recent Research Results and Emerging opportunities., *Academy of Management Journal*, 459-468.

Schwartz, Martin A. (2008), "The importance of stupidity in scientific research," *Journal of Cell Science*. 121, 1771.

Simon, K.D. (2005). The value of open standards and open-source software in government environments. *IBM Systems Journal*. 44(2):227-238.

Suddaby, R. (2006), "What grounded theory is not?" *Academy of Management Journal*, 49(4): 633-642.

Tanev, S., Xu, A., Bailetti, A., Wilmore, J. (2008) "Open Standards vs. Open Source: a Case of the Open Access Standard," *ISPIM Conference Open Innovation: Creating Products and Services through Collaboration*, Tours, France.

Teknomo, K. (2006). K-mean Clustering Tutorial. Available at:
<http://people.revoledu.com/kardi/tutorial/kMean/index.html> (accessed on
 Mar/18/2010).

Toigo, J.W. (1989). Disaster recovery planning: Managing risk and catastrophe in
 information systems. PRENTICE HALL PUBLISHING, OLD TAPPAN, NJ (USA).

Trochim, B. (2002). Research Methods Knowledge Base. Available at:
<http://www.socialresearchmethods.net/kb/> (accessed on Mar/19/2009).

Tucker, R.L., MacCallum, C.R. (1997). Exploratory Factor Analysis. Available at
 University of North Carolina Public Library. Available at:
<http://www.unc.edu/~rcm/book/factornew.htm> (accessed on Apr/07/2009).

Vanhaverbeke, W., Vrande, V. & Chesbrough, H. (2008), Understanding the
 advantages of open innovation practices in corporate venturing in terms of real options,
 Creativity and Innovation Management, 17(4): 251-258.

Von Hippel, E., von Krogh, G. (2003). Open source software and the 'private
 collective' innovation model: Issues for organization science. Organization Science 14
 (2):209-223.

West, J., Gallagher, S. (2006), Challenges of open innovation: the paradox of firm
 investment in open-source software, R&D Management, 36(3): 319-331.

West, J., Mahoney, S. (2008), The role of participation architecture in growing
 sponsored open source communities, Industry & Innovation, 15(2):145-168.

Witten, B., Landwehr, C., Caloyannides, M. (2001). Does open source improve system
 security? IEEE Software, 18(5): 57-61.

APPENDICES

Appendix- 1: List of OSST companies

The following list is the list of initial 205 companies that have been used in this study (the URL's of companies):

http://www.clearlyconnected.com/	URL1	http://www.abovesecurity.com/	URL103
http://www.untangle.com/	URL2	http://altornetworks.com/	URL104
http://www.alienvault.com/	URL3	http://www.astaro.com/	URL105
http://www.onlinewebstats.com/	URL4	http://bt.counterpane.com/	URL106
http://www.guardiandigital.com/	URL5	http://www2.catbird.com/	URL107
http://www.sourcefire.com/	URL6	http://www.clearbluesecurity.com/	URL108
http://www.eds.com/	URL7	http://www.cymtec.com/	URL109
www.Nagios.com	URL8	http://www.industrialdefender.com/	URL110
http://www.antezeta.com/	URL9	http://www.open.ch/	URL111
http://www.internetofficer.com/	URL10	http://www.optenet.com/	URL112
http://www.untangle.com/	URL11	http://www.savvis.net/	URL113
http://www.vyatta.com/	URL12	http://www.secnap.com/	URL114
http://www.vyatta.com/	URL13	http://www.solutionary.com/	URL115
http://ebox-platform.com/	URL14	http://www.truedigitalsecurity.com/	URL116
http://isak.gplindustries.com/	URL15	http://www.voyantinc.com/	URL117
http://www.securitydistro.com/	URL16	http://www.xroadsnetworks.com/	URL118
http://metasploit.com/	URL17	http://www.sun.com/	URL119
http://www.intersectalliance.com/	URL18	http://www.phoenixdatacom.com/	URL120
http://www.pcmec.com/	URL19	http://www.lumension.com/	URL121
http://www.edgeos.com/	URL20	http://www.aladdin.com/	URL122
http://www.securityfocus.com/	URL21	http://www.altitude.com/	URL123
http://www.sawmill.net/	URL22	http://www.athena-scs.com/	URL124
http://www.mailcleaner.net/	URL23	http://www.borderware.com/	URL125
http://www.onlinewebstats.com/	URL24	http://www.chosensecurity.com/	URL126

http://www.sourcefire.com/	URL25	http://www.clearswift.com/	URL127
http://www.clamwin.com	URL26	http://www.communicate.com/	URL128
http://www.supportpro.com/	URL27	http://www.f5.com/	URL129
http://www.endian.com/	URL28	http://www.gemalto.com/	URL130
http://www.smoothwall.net/	URL29	http://www.geotrust.com/	URL131
http://www.vyatta.com/	URL30	http://www.gi-de.com/	URL132
http://www.fs-security.com/	URL31	http://www.ironport.com/	URL133
http://www.netscantools.com/	URL32	http://www.mirapoint.com/	URL134
http://www.heidi.ie/	URL33	http://www.proofpoint.com/	URL135
http://www.emiic.net/	URL34	http://www.rsa.com/	URL136
http://www.pgp.com/	URL35	http://www.safenet-inc.com/	URL137
http://www.rim.net/	URL36	http://www.sendmail.com/	URL138
http://www.apple.com/	URL37	http://www.signacert.com/	URL139
http://www.opentrust.com/	URL38	http://www.sophos.com/	URL140
http://www.securenetworkinc.com/	URL39	http://www.titus-labs.com/	URL141
http://www.sphorium.com/	URL40	http://www.websense.com/	URL142
http://www.untangleappliances.com/	URL41	http://www.workshare.com/	URL143
http://www.planetsoft.pl/en/	URL42	http://www.enterasec.com/	URL144
https://olex.openlogic.com/	URL43	http://www.qualys.com/	URL145
http://www.nessus.org/	URL44	http://www.visolve.com/	URL146
http://www.groundworkopensource.com/	URL45	http://www.stealth-iss.net/	URL147
http://www.op5.com/	URL46	http://www.findopensourcesupport.com/	URL148
http://www.otg-nc.com/	URL47	http://www.agenda.si/eng/	URL149
http://spidertools.com/	URL48	http://www.acoupleofgurus.com/	URL150
http://www.linobox.com/	URL49	http://www.adamsinfoserv.com/	URL151
http://tag1consulting.com/	URL50	http://www.adventus.lv/en/	URL152
http://www.netways.de/en	URL51	http://www.allegroconsultants.com/	URL153
http://www.easyrider.com/	URL52	http://www.alphanetsolutions.net/	URL154
http://www.bitpusher.com/	URL53	http://www.auricnet.ca/	URL155
http://www.sandboxdev.com/	URL54	http://www.axiomnetworking.ca/	URL156

http://www.nagiossupport.com.au/?page_id=18	URL55	http://consult.btoy1.net/	URL157
http://www.consol.com/	URL56	http://www.ba.be/	URL158
http://www.ardengrp.com/	URL57	http://www.bit-axx.com/	URL159
http://www.fisherscreek.com/	URL58	http://www.bitpusher.com/	URL160
http://www.openextra.co.uk/	URL59	http://www.costeffectivedev.com/	URL161
http://www.digiraticonsulting.com/pub/node/1	URL60	http://www.cedvalinfo.com/en/	URL162
http://www.linalis.com/en/	URL61	http://www.clearbearing.com/	URL163
http://www.parallels.com/	URL62	http://www.consol.de/	URL164
http://www.opensourceexperts.com/	URL63	http://www.contego.net/site/	URL165
http://www.protocol6.com/	URL64	http://www.copyleft.com.pk/	URL166
http://www.symtrex.com/	URL65	http://www.cyberrazor.com/	URL167
http://www.oakton.com.au/	URL66	http://darq.com/	URL168
http://www.elint.eu/	URL67	http://www.djhsolutions.com/	URL169
http://www.strongboxsolutions.com/	URL68	http://www.emergen.biz/	URL170
https://www.securityfocus.com/	URL69	http://www.emuadmin.com/	URL171
http://hackertarget.com/	URL70	http://www.essensys.com/	URL172
http://www.palaestratraining.com/	URL71	http://www.etherealsoft.com/	URL173
http://www.pantek.com/	URL72	http://www.geminitechs.com/	URL174
http://www.mailspect.com/	URL73	http://globalsystemsconsulting.com/	URL175
http://www.computerevolution.net/	URL74	http://www.infostrategie.com/	URL176
http://osx.topicdesk.com/	URL75	http://www.ironmountainfoundry.com/	URL177
http://www.wikidsystems.com/	URL76	http://www.jaymor.com/	URL178
http://www.hurricanelabs.com/	URL77	http://www.koteas.com/	URL179
http://www.onlinebankingsolutions.com/	URL78	http://www.magnifix.com/	URL180
http://www.smoothwall.net/	URL79	http://www.mountaincloud.net/	URL181
http://www.tripwire.com/	URL80	http://www.neonova.net/	URL182
http://www.credativ.co.uk/	URL81	http://www.netstruxure.com/	URL183
http://www.iqbio.eu/eu_en/	URL82	http://www.otg-nc.com/	URL184
http://osuosl.org/	URL83	http://www.openlogic.com/	URL185

http://redmondmediagroup.com/	URL84	http://osriver.com/	URL186
http://www.project-open.com	URL85	http://www.pantek.com/	URL187
http://www.timesys.com/	URL86	http://www.reportstar.net/	URL188
http://eracks.com/	URL87	http://www.revolutionlinux.com/	URL189
http://trolltech.com/	URL88	http://www.rowzuntec.com/	URL190
http://www.ubuntu.com/	URL89	http://www.saosce.com.au/	URL191
http://www.opendns.com/	URL90	http://www.singlepointoc.com/	URL192
http://www.visolve.com/	URL91	http://www.zenoss.com/	URL193
http://www.centrifly.com/	URL92	http://www.willingminds.com/	URL194
http://www.barracudanetworks.com/ns/?L=en_ca	URL93	http://www.turnkeyinternet.net/	URL195
http://www.viscosityvpn.com/	URL94	http://www.trusted.cz/aboutus.en.html	URL196
http://www.nobleprog.co.uk/	URL95	http://www.theuptimegroup.com/	URL197
https://www.professormesser.com/	URL96	http://www.terinea.co.uk/	URL198
http://www.pctech101.com/	URL97	http://www.tachometry.com/	URL199
http://www.ossec.net/	URL98	http://www.syntonic.com.au/	URL200
http://anon.inf.tu-dresden.de/	URL99	http://www.symmetrixtech.com/	URL201
http://babel.sourceforge.net/en/index.php	URL100	http://www.synaq.com/	URL202
http://www.CGI.com	URL101	http://www2.solutionsfirst.com.au/	URL203
http://www.clearlyconnected.com/	URL102	http://www.snowdoniait.com/	URL204
		http://www.singlepointoc.com/	URL205

Appendix--2: Initial Keywords

The following list represents the initial keywords that have been assembled through literature review and studying sample websites:

service OR support OR supports	K1
Technical+support OR maintenance OR customer +support OR technical+assistant	K2
installation OR install OR deployment OR deploy OR implementing OR implement	K3
planning OR project+management OR configuration	K4
consulting OR consult OR consultation	K5
license OR commercial OR copyright OR product OR application OR appliance	K6
hosted OR hosting OR subscription OR subscribe OR host	K7
customization OR customize OR tailor	K8
Operation+center	K9
hardening OR securing OR protection	K10
disaster+recovery OR Business+continuity	K11
audit OR vulnerability+assessment OR penetration+testing	K12
threat+risk+assessment OR risk+ analysis OR TRA OR threat+AND+risk+assessment	K13
network+security OR IT+security	K14
voice+security OR VOIP+ Security OR telephony	K15
data+security OR data+protection OR backup OR backupingup	K16
call+center+security	K17
education OR trainingOR course OR seminar OR certificate OR certification	K18
integration OR integrating OR integrate	K19
SaaS OR software+as+a+service OR subscription OR online+service	K20
incident+response OR monitor OR monitoring OR defence+center OR intrusion+detection	K21

Confidentiality	K22
data+integrity	K23
authentication OR authorization	K24
access+control OR ACL	K25
encryption	K26
non-repudiation	K27
availability	K28
monitoring	K29
intrusion+detection	K30
penetration+testing OR vulnerability	K31
network+scanning	K32
threat+risk+analysis	K33
advertisement+advertise	K34
SSL+certificates OR Certification+authority	K35

Appendix- 3: Example Open Source Security Tools

Thirty eight Open Source Security Tools have been identified. These tools have been identified as tools that are widely used by companies and individuals. These tools have been used to identify the sample list of 205 Open Source Security companies that drove the research. The tools have been categorized based on their usage. A short description regarding the capabilities and functionalities of each one with some of the commercialization strategies that has been mainly extracted from data analysis is given to provide a basic knowledge of these tools.

Monitoring and Vulnerability Assessment:

1. Nagios: <http://www.nagios.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Monitors entire Enterprise IT infrastructure • Sends alert when critical component fails • System Reports • Reports necessary upgrades • Compatible with most distribution of Linux and FreeBSD 	<ul style="list-style-type: none"> • Enterprise – class license (Nagios XI)- Price range : 595 – 1295 \$- Nagios Core OSS (free) • Project management and implementation • Technical Support for Nagios core – around 2495\$/year 	GPL

2. Nessus : <http://www.nessus.org/nessus/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Network Security Vulnerability Scanner • Security monitoring, IT auditing and compliance monitoring • Security Center- asset-based security monitoring (fee based) • Log Correlation Engine (fee based) • Compatible with most popular Operating Systems 	<ul style="list-style-type: none"> • Nessus Hardware and virtual Appliances • Enterprise management with security center • Professional feed subscription (vulnerabilities update...) • Log Correlation Engine (receive log from different gears like IDS...) 	GPL

3. AWStats: <http://awstats.sourceforge.net/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Powerful webserver log file analyzer that generates advanced web, streaming, ftp or mail server statistics, with graphical capabilities • The log analyzer can show: authenticated users, hosts, worms attack, visits... • Work from a command line and works with all operating systems 	<ul style="list-style-type: none"> • Used in Search Engine Optimization • Support, tuning and project management 	GPL

4. Snort: <http://www.snort.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Intrusion Detection System(IDS) and Intrusion Prevention System(IPS) • Compatible with all popular operating Systems 	<ul style="list-style-type: none"> • Customer Support • Software updates • Training and certification • Project Management • Implement into hardware 	GPL (V2)

5. iSAK (Internet Secure Access Kit): <http://isak.gplindustries.com/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Web traffic management platform • Savoir-faire Linux network security solution • Generate statistical Report • Define Web access policies • Antivirus interface: CalmAV, McAfee... • Block or Allow categories of websites 	<ul style="list-style-type: none"> • Technical Support • Professional services 	GPL

6- OSSIM (*Open Source Security Information Management*) :

<http://www.alienvault.com/community.php?section=Home>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • A set of tools for Intrusion detection and prevention • Some of the components: Arpwtach, pads, Nessus, Snort, TcpTrack, Ntop, Nagios... 	<ul style="list-style-type: none"> • Technical Support • Embedding into hardware as an appliance • Training and certificates 	LGPL

7- Honeytrap: <http://honeytrap.carnivore.it/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Observe Attacks against TCP services • Low-interaction honeypot daemon • Compatible with most Linux distribution 	<ul style="list-style-type: none"> • Vulnerability Assessment 	GPL

8- SNARE (System iNtrusion Analysis and Reporting Environment):

<http://www.intersectalliance.com/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Collect audit log data from a variety of operating systems • SNARE agent collects data and sends it to the centralized server • SNARE agents are available as OSS free for download 	<ul style="list-style-type: none"> • InterSect Alliance owned the proprietary server Appliances • Technical Support Services 	GPL

9- Nikto : <http://cirt.net/nikto2>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Web server scanner • Checks for outdated server components • Save reports in plain text, XML, HTML or CSV • Compatible with Linux and Windows 	<ul style="list-style-type: none"> • Online/ hosted Vulnerability Assessment • Consulting • Training 	GPL

Antivirus and AntiSpam:

1. Spam Assassin : <http://spamassassin.apache.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • An Apache project that identify spam signatures • Can be integrated into mail server for email filtering 	<ul style="list-style-type: none"> • Technical Support • Project Management • Consulting 	Apache License 2

2. MailCleaner: <http://www.mailcleaner.net/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Email filtering gateway • Graphical web interface (administration and user Gui) • Installed between Internet and mail server 	<ul style="list-style-type: none"> • Hosting Services (for small to mid-sized companies) • Enterprise solution – updates, support, in-house installation • Embed into hardware as an appliance 	GPL

3. ClamAV and ClamWin : <http://www.clamav.net/> <http://www.clamwin.com/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Anti-virus toolkit for UNIX, designed especially for e-mail scanning on mail gateways • CalmWin- for windows 	<ul style="list-style-type: none"> • Technical Support • Training • Project Management • Consulting 	GPL

4. Moon Secure AV: <http://www.moonsecure.com/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Using ClamAV Engine • Run on Windows (XP, Vista) • Detects Viruses, Trojans and Spywares • Real-time scanner capabilities 	<ul style="list-style-type: none"> • Technical Support and professional Services 	GPL

Firewalls:

1. Vyatta: <http://www.vyatta.com/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Linux-based routing and security distribution • Connect and secure physical infrastructures as well as virtualization and cloud infrastructures 	<ul style="list-style-type: none"> • Proprietary hardware solutions; router, firewall, VPN • Training, subscription, consulting and project management, technical support 	GPL

2. Endian Firewall: <http://www.endian.com/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Stateful packet inspection, application level proxy, Antivirus filtering, Content filtering and a VPN based on OpenVPN • Works with most Linux distribution 	<ul style="list-style-type: none"> • Embedding into hardware • Web-based centralized management for Endian products • Technical Support and Consulting Services 	GPL

3. IPCop: <http://sourceforge.net/apps/trac/ipcop/wiki>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Linux Stateful firewall • Web-based Interface • Home users and SOHO users 	No clear commercialization strategy has been identified	GPL

Files and Data:

1- WinSCP: <http://winscp.net/eng/index.php>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • A Secure FTP client for Windows • Secure File transfer • Support Legacy SCP protocols • Works with Windows infrastructure 	No clear commercialization strategy has been identified	GPL

2- Cyberduck : <http://cyberduck.ch/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • FTP and SFTP • Used in cloud Computing (e.g. Amazon S3) • Worked with Mac 	No clear commercialization strategy has been identified	GPL

3- Eraser: <http://eraser.heidi.ie/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Compatible with Windows • Remove sensitive data by overriding them several times • Worked with external schedulers 	<ul style="list-style-type: none"> • Support • Training 	GPL (V3)

4- The Sleuth Kit: <http://www.sleuthkit.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Recover deleted files • Worked on all Operating Systems • Command line digital investigation tools with a GUI based browser 	<ul style="list-style-type: none"> • Disaster Recovery • Legal and investigation tasks 	GPL

Encryption and Password:

1- PGP: <http://www.pgp.com/> <http://www.pgpi.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Signing, Encrypting and decrypting emails • PGPdisk- encrypt disk partitions • PGPfone- make Secure telephone calls (VOIP) • GNU Privacy guard (GnuPG)- Command Line replacement for PGP (DOS, Unix) 	<ul style="list-style-type: none"> • Embedding into hardware • Technical Support 	GPL

2- TrueCrypt: <http://www.truecrypt.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Disk encryption • Works in Windows, Mac, Linux 	<ul style="list-style-type: none"> • Embedding into hardware 	GPL

3- KeePass: <http://keepass.info/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Generate and keep encrypted passwords (password manager) • Portability- can be carried on USB • Compatible with Windows, Linux, Mac OS 	No clear commercialization strategy has been identified	GPL

4- Password Safe: <http://pwsafe.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Generate and keep encrypted passwords (password manager) • Compatible with Windows 	<ul style="list-style-type: none"> • Dual Licensing – Enterprise version 	Artistic License 2.0

Remote Access:

1- Open SSH: <http://www.openssh.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> Secure remote connection to host Encrypt communication Putty is the windows version : http://www.chiark.greenend.org.uk/~sgtatham/putty/ 	<ul style="list-style-type: none"> Support Consulting Training 	GPL

2- Open VPN: <http://openvpn.net/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> Remote Access and Site-to-site VPN A management interface Compatible with Linux, Windows, Mac... 	<ul style="list-style-type: none"> Project Management Training 	GPL (V2)

3- SSL-Explorer : <http://sourceforge.net/projects/sslexplorer/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Web-based SSL VPN server • Project has now been acquired by Barracuda Networks, Inc. • Compatible with standard Browsers 	<ul style="list-style-type: none"> • Embedding to hardware (VPN appliances) 	GPL

4- StrongSwan : <http://www.strongswan.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • IP-based VPN for Linux • Support IPV6 • Use of X.509 attributes certificates to implement advanced access control schemes based on group memberships 	No clear commercialization strategy has been identified	GPL

Networking:

1- Nmap (Network Mapper): <http://nmap.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Network exploration or security auditing • Used to reveal information like: available hosts on the network, their services, their OS, the firewall info and more • Worked with most popular Operating Systems 	<ul style="list-style-type: none"> • Consulting • Threat Risk Analysis • Vulnerability Assessment • Training 	GPL

2- WireShark: <http://www.wireshark.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Network Protocol Analyzer- Originally named Ethereal, a packet analyzer (sniffer) that allows user to analyze all packets over the Ethernet network • Run on all OS • VOIP analysis • Decryption Support (e.g. IPSec) • Worked with most popular Operating Systems 	<ul style="list-style-type: none"> • Threat Risk Analysis • Vulnerability Assessment 	GPL

3- Bro: <http://bro-ids.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Network Intrusion detection System (Unix Based) that monitor all incoming and outgoing traffic • Custom Scripting Language • Detection can generate logs, reports and execute commands like removing or blocking • Convert snort signature to Bro signature through a tool called snort2bro • Compatible with Linux 	<ul style="list-style-type: none"> • Monitoring services • Vulnerability assessment 	BSD

4-

5- Netcat: <http://netcat.sourceforge.net/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. • Port Scanning capabilities • Reading from and writing network connections using TCP or UDP with network debugging and investigation tool • Compatible with Windows and Linux 	<ul style="list-style-type: none"> • Vulnerability Assessment 	GPL

6- Angry IP Scanner: <http://www.angryip.org/w/Home>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • It scans IP addresses and ports ... • Supporting all platforms 	<ul style="list-style-type: none"> • Vulnerability Assessment • Monitoring • Threat Risk Analysis 	GPL (V2)

7- OSSEC: <http://www.ossec.net/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Host-based Intrusion Detection System. It performs log analysis, file integrity checking, policy monitoring, root kit detection, real-time alerting and active response • Support all Operating Systems • Commercial Support through Trend Micro 	<ul style="list-style-type: none"> • Commercial Support • Training • Monitoring • Consulting 	GPL (V3)

8- TCPDUMP: <http://www.tcpdump.org/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Packet Analyzer that run over command prompt • The windows version called windump also worked with Linux and others • Good for debugging network traffic 	<ul style="list-style-type: none"> • Vulnerability assessment • Threat Risk Analysis • Training 	GPL

9- Kismet: <http://www.kismetwireless.net/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • 802.11 layer2 wireless network detector, sniffer, and intrusion detection system • 802.11b, 802.11g, 802.11a, 802.11n sniffing • Standard PCAP file logging (Wireshark, Tcpdump, etc) • Runtime WEP decoding • Linux, OSX, Windows, and BSD support (devices and drivers permitting) 	<ul style="list-style-type: none"> • Vulnerability Assessment • Threat Risk Analysis 	GPL

Others:

1- TripWire: <http://sourceforge.net/projects/tripwire/>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Monitor and alert specific file and system changes • File Integrity monitoring, compliance policy management, accountability (who changed 	<ul style="list-style-type: none"> • Dual Licensing (enterprise version) • Upgrades and technical support • Log analyzer center 	GPL

what...) <ul style="list-style-type: none"> • Compatible with most Operating Systems 	<ul style="list-style-type: none"> • Data protection... 	
--	--	--

2- Babel: <http://babel.sourceforge.net/en/index.php>

Capabilities	Example of Commercialization Strategies	License
<ul style="list-style-type: none"> • Measure the risk of each asset in a company • Evaluates compliance level • Babel agent gather data through set of questions and answers • Used for threat Risk Analysis, audit, system hardening • Compatible with Linux and Windows 	<ul style="list-style-type: none"> • Threat Risk Analysis • Consulting 	GPL