NPS-AM-17-026

ACQUISITION RESEARCH PROGRAM SPONSORED REPORT SERIES

Freeware Versus Commercial Office Productivity Software

December 2016

LCDR Lindsay R. Anderson, USN

LCDR Shelley Conyers, USN

Thesis Advisors: Dr. Douglas Brinkley, Senior Lecturer
LCDR Matthew Kremer, Military Faculty

Graduate School of Business & Public Policy

Naval Postgraduate School

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

ABSTRACT

In 1998, the Department of Defense (DOD) Enterprise Software Initiative (ESI) was created as an official DOD initiative, sponsored by the DOD chief information officer (CIO) to lead in the establishment and management of enterprise commercial off-the-shelf (COTS) information technology agreements, assets, and policies. This included software products such as Microsoft, Oracle, VMWare, and multiple others. In July 2010, Google announced the launch of Google Apps for Government, adapting Google's widely popular freeware for government agency usage. This study analyzes the proposed benefits of using freeware, specifically Google Apps, in the DOD in relation to reliability, cost, and security. The results of our analysis supported our recommendation to the DOD ESI to begin complete integration of Google Apps within DOD commands.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This research was supported by the Acquisition Research Program. We would like to thank our colleagues from the Naval Postgraduate School Business School who provided insight and expertise that greatly assisted the research.

We would like to thank our writing coach, Carla Hunt, for her assistance with the proper use of commas, active sentences, and cool sticky notes. With your guidance, assistance, and our weekly meetings, we have created a manuscript we can love.

We would also like to show our gratitude to our advisors Dr. Douglas Brinkley and LCDR Matthew Kremer. Thank you both for sharing your pearls of wisdom with us during the course of this research. We are immensely grateful to you both for your comments on our draft version of the manuscript. We would also like to thank three "anonymous" reviewers for their insights.

Lindsay R. Anderson

Special thanks to my wonderful husband, Dennis, for watching our son, Ezra, a growing baby boy, and our crazy dog, Petey, as I lived in the library and on the couch until the sun came up every day. I love you sweetie.

Shelley Conyers

I would like to thank my husband, Andre, and our children, Deandre, Andre Jr., and Aiden. Without their understanding, patience, and support, I would not have been able to successfully complete this project. Thank you and I love you all.

THIS PAGE INTENTIONALLY LEFT BLANK

ABOUT THE AUTHORS

Lindsay R. Anderson, Lieutenant Commander, graduated from the U.S. Naval Academy, Annapolis, MD, in 2005 with a degree in Information Technology. After graduation she served onboard the USS *Enterprise* (CVN 65) as the Wardroom Officer, Stock Control Assistant and Stock Control Officer.. During her second tour she was a Fuels Intern at Manchester Fuel Farm, FISC Bremerton. After the FISC she worked in the Logistics Office at COMLOG WESTPAC. Her fourth tour was onboard USS *Lake Erie (CG 70)* as the Supply Officer and directly following she was hand selected to serve as the Supply Officer on USS Georgia (SSGN 729)(Blue) for the Women in Submarine Program. She married her husband Dennis in May 2012, and they currently have three children: Christin – 17, Dennis Jr. – 16 and Ezra – 1. Lieutenant Commander Anderson reported to Naval Postgraduate School in January 2015 and is currently a student studying Acquisition and Contract Management curriculum. In her free time, LCDR Anderson is the President of the Supply Corps Foundation Monterey Peninsula Chapter. After graduation in December 2016, she will be reporting to the Office of Special Projects in Washington D.C., as a Contracting Officer. Lieutenant Commander Anderson is a qualified Naval Aviation Supply Corps Officer, Surface Warfare Supply Corps Officer and Submarine Supply Corps Officer. Her personal decorations include three Navy and Marine Corps Commendation Medals, three Navy and Marine Corps Achievement Medals and various unit and service awards.

Shelley Conyers, Lieutenant Commander, graduated from Strayer University with a degree in Computer Networking and received her commission in 2005 through Officer Candidate School. She is also a graduate of The Naval War College distance education JPME Phase I program. Lieutenant Commander Conyers reported to Naval Postgraduate School in June 2015 and is currently a student studying the Information Systems Management curriculum. Her sea duty assignments include: Material Officer, Postal Officer, and Disbursing Officer, USS IWO JIMA (LHD 7), Norfolk, Virginia and Stock Control Officer, USS ENTERPRISE (CVN 65), Norfolk, Virginia. Lieutenant Commander Conyers shore duty assignments include: Aviation Support Detachment Officer, ASD Oceana, Virginia Beach, Virginia and Supply Officer at VFA-106 in Virginia Beach, Virginia. Shelley and her husband, Andre, live in Seaside, CA and are the parents of three sons: Deandre-16, Andre Jr.-

6, and Aiden-3. In her free time, LCDR Conyers is the Vice President of the Supply Corps Foundation Monterey Peninsula Chapter and is a running enthusiast who races in several full and half marathons throughout the year. After graduation in December 2016, she will be reporting to the Fleet Logistics Center Jacksonville, as a Contracting Officer. Lieutenant Commander Conyers is a qualified Naval Aviation Supply Corps Officer and Surface Warfare Supply Corps Officer. Her personal decorations include the Navy and Marine Corps Commendation Medal (two awards), Navy and Marine Corps Achievement Medal (four awards), and various unit and service awards.

NPS-AM-17-026

ACQUISITION RESEARCH PROGRAM SPONSORED REPORT SERIES

Freeware Versus Commercial Office Productivity Software

December 2016

LCDR Lindsay R. Anderson, USN

LCDR Shelley Conyers, USN

Thesis Advisors: Dr. Douglas Brinkley, Senior Lecturer
LCDR Matthew Kremer, Military Faculty

Graduate School of Business & Public Policy

Naval Postgraduate School

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization
BPA	Blanket Purchase Agreement
CIO	Chief Information Officer
CMS	Content Management System
COTS	Commercial Off-the-Shelf
DFARS	Defense Federal Acquisition Regulation Supplement
DIACAP	DOD Information Assurance Certification and Accreditation Process
DIARFM	Defense Information Assurance Risk Management Framework
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DON	Department of the Navy
ESI	Enterprise Software Initiative
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FOSS	Free and Open Source Software
FSF	Free Software Foundation
GPEA	Government Paperwork Elimination Act
HIPAA	Health Insurance Portability and Accountability Act of 1996
MBSA	Microsoft Baseline Security Analyzer
NIST	National Institute of Standards and Technology
OSI	Open Source Initiative
PAAS	Platform as a Service
SA	Software Assurance
SAAS	Software as a Service
SASU	Software Assurance-Step Up
SOCOM	Special Operations Command
SWOT	Strengths, Weaknesses, Opportunities, and Threats
WSUS	Windows Server Update Services

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The rapid change of the external environment has required the Department of Defense (DOD) to expand its collaborative efforts with multinational partners, non-government agencies, and civilian companies. To navigate this new and open environment, the DOD can no longer rely on closed productivity systems and outdated file sharing methods. The DOD can breach the generational gap through the exploration and implementation of more accessible freeware products such as Google Apps, while potentially saving $12 billon per year. This chapter presents the background, purpose, research questions, scope, and methodology for an analytical comparison of freeware versus commercial office productivity software.

A. BACKGROUND

The DOD's reliance on technology can be seen everywhere, from the battlefield and sailors launching drones off the flight deck to a base office where a contracting officer utilizes email to award a new contract. The Department of the Navy (DON) spends approximately $190 million per year on a "blanket purchase agreement [BPA] for Microsoft licenses and software assurance (SA)" (Department of Defense Enterprise Software Initiative [DOD ESI], 2015). The BPAs support "the renewal of SA and procurement of new Microsoft brand software licenses with SA, subscriptions, and SA-step up (SASU) for desktop and server-based products" (DOD ESI, 2015). While the DON continues to spend millions on the purchase and support for several versions of Microsoft software, over 35 other government agencies (including nine federal agencies) in 45 states instead use Google Apps as their primary productivity suite, according to Google (Google, 2016). Google's research shows that agencies spend about 50% less per year on their annual licensing costs (Google, 2016). Although Google Apps save agencies an incredible amount of money and the integration for Google Apps is a streamlined process, the Defense Information Assurance Risk Management Framework (DIARMF) and the Federal Risk and Authorization Management Program (FedRAMP) certification have created a roadblock for the DOD's use of Google Apps.

An initiative sponsored by the DOD Chief Information Officer created the DOD Enterprise Software Initiative. DOD ESI is the lead on "the establishment and management

of enterprise Commercial Off the Shelf (COTS) IT agreements, assets, and policies" (DOD Enterprise Software Initiative, 2015). Google's widely popular freeware was adapted for government agency use through the launch of Google Apps for Government (Krishnan, 2010).

B. PURPOSE

This study analyzes the appropriateness of freeware use by the DOD as the primary productivity office suite. We analyze whether freeware is reliable and safe, as well as its potential benefits. We also analyze the proposed benefits of using freeware, specifically Google Docs, in the DOD, in relation to the Federal Acquisition Regulation (FAR) requirements, the DOD Information Assurance Certification and Accreditation Process (DIACAP), and Federal Risk and Authorization Management Program (FedRAMP). Capitalizing on the ease of use and functionality of a SWOT analysis, the results of our SWOT analysis identified potential benefits and recommendations to the DON Enterprise Software Initiative (ESI) for Microsoft and Google.

C. RESEARCH QUESTIONS

- In what instances is it appropriate to use freeware as the primary productivity/mobile office software (i.e., Microsoft Office versus Google Docs)?
- What are the relevant DOD cost savings for freeware integration and cloud computing?
- To what level is freeware supported?
- Are there any significant security threats while using freeware?

D. SCOPE

Instead of spending money on basic office software, the DOD should be able to implement free software, or freeware, to accomplish day-to-day tasks. However, the requirements for software accreditations and certification, due to extra needed security, are so stringent that the DOD is years behind the general public. We found so many benefits to using Google Apps, we worry that we'd sound like a Google commercial. In order to constrain the

scope of this topic, this thesis focuses only the use of Google Apps for DOD use as a potential alternative to Microsoft and do not consider any other freeware.

To produce a win-win outcome, it is important to understand the DOD's software requirements. Additionally, it is equally important to understand the DOD's process of acquiring, certifying, and implementing software suites, whether through the Enterprise Software Initiative or independently.

E. METHODOLOGY

This project compares the traditional and currently used office productivity suite, Microsoft Office, with cloud-based freeware Google Apps. This study is conducted in four stages. In the first stage, we review previous literature on the topic including: journals articles, projects, theses, and other scholarly information pertaining to the traditional software security requirements regulated through DIARMF (DOD, 2014) and cloud computing services regulated through FedRAMP (n.d.-b). Additionally, we explore the differences between open-source software and freeware, as well as some of the vulnerability and reliability challenges that plague the DOD.

Second, we collected information from both major software giants, as well from comparison studies already completed by major corporations and agencies prior to choosing the best productivity software. This stage may have proven to be the most challenging as a number search tool for scholarly and independent opinions was one of the companies in review. Additionally, it is important to note that although there is plenty of information on cloud based systems for both companies the information readily available for Microsoft was lacking. Stage three comprises the analysis of the data, particularly focusing on vulnerabilities, cost, and reliability, while the final stage involves interpreting the results and providing a recommendation on the use of freeware within the DOD.

F. ORGANIZATION OF STUDY

This study comprises five chapters.

- Chapter I—Introduction. This chapter provides background, research questions, scope, methodology, and other introductory items.
- Chapter II—Literature Review. This chapter provides an examination of the available writings in the area of the study. Documents reviewed for this research include information provided by Google and Microsoft, Internet searches on numerous websites, professional analysis reports, and publications with directed studies on Microsoft Office and Google Apps. Our research also includes data collected by reading through DOD instructions and contracts.
- Chapter III—Methodology. This chapter discusses the method used to gather data and the development and reasoning behind the utilized method.
- Chapter IV—Findings. This chapter provides an analysis of the information gathered from the study.
- Chapter V—Conclusions and Recommendations. This chapter provides the conclusions and the recommendations for the Department of Defense (DOD) moving forward with the acquisition and implementation of Google Apps for Government as an everyday productivity suite.

G. SUMMARY

This chapter provided an overview of the body of research contained in the subsequent pages and a brief synopsis of our primary research question: Google Apps (freeware) versus Microsoft Office (traditional productivity suite). It provided the research questions, the scope, and methodology of the research. Finally, it provided a general outline of the paper.

The next chapter discusses details on the documents the researchers reviewed to gain basic knowledge in the area. Documents reviewed for this research include information provided by Google and Microsoft, Internet searches on numerous websites, professional analysis reports, and publications with directed studies on Microsoft Office and Google Apps. We also include in our research, data collected from DOD instructions and contracts.

II. LITERATURE REVIEW

Chapter II provides definitions of freeware, free software, open source software, and cloud computing. It also provides an overview of DOD software acquisition and cost, the effects of the Defense Information Assurance Risk Management Framework (DIARMF), and the Federal Risk and Authorization Management Program (FedRAMP). It also discusses freeware reliability and cyber vulnerabilities and mitigation.

A. DEFINITIONS (FREEWARE, FREE SOFTWARE, OPEN SOURCE SOFTWARE, CLOUD COMPUTING)

Freeware, *free software*, *open source software*, and *cloud computing* are terms used when describing services provided by Microsoft and Google. However, one of the largest problems in both the civilian sectors and the Department of Defense is that these terms are used interchangeably and incorrectly, so our thesis starts by offering accurate definitions as a way to improve overall understanding.

1. Freeware

Freeware is exclusive software that can be used without expense. Some examples of freeware include: Google Apps, Mozilla Firefox, Skype and many others. Although it is free of charge, the proprietor, who maintains all rights, has the ability to control its dispersion and can benefit from it by offering upgraded versions for a fee (Linux Information Project, 2006). The free version of the software may still be available and functional but with limited capabilities and for a limited amount of time. The source code of freeware is generally unavailable to its users; therefore, it cannot be altered and redistributed without the author's authorization (Linux Information Project, 2006).

The license for freeware usually has specific restrictions on when or how it should be utilized. Some examples of such restrictions are non-profit usage, private or personal use, non-military, and academic usage. "Freeware is difficult to manage since there is only one organization responsible for updating the free product" (Linux Information Project, 2006). However, the DOD is more likely to purchase and utilize freeware, such as Google Apps, as software because there is only one organization responsible for updating their product, which, therefore, decreases the risk of security breaches.

2. Free Software

Often confused with freeware, free software has little or no restrictions. Under the software license, free software allows its users access to the source code so they are able to make modifications, as well as have the ability to run the program for a multitude of other purposes (Free Software Foundation, 2016a). *Free software* refers to the user's rights with the source code, not the price. Free software is available for all users to use as needed. Additionally, users are able to sell the software, charge for added services such as warranties or customer support, and redistribute the software free of charge. "Free software is completely different from Google Docs or Microsoft Office whereas users are unable to change, study, or share it" (Linux Information Project, 2006). Within the DOD, cyber vulnerabilities and attacks remain a primary concern of software acquisitions and usage, though the DOD has acknowledged the potential innovations available in free software.

3. Open Source Software

According to the DOD, "open source software is not similar to freeware or free software" (Chief Information Officer, DOD, 2009). Open source software is free, the source code is made readily available to the users, and there is free redistribution (Huger, 2016). It is largely established by volunteer efforts. The holder of the patent offers its users the ability to modify, study, or distribute the software. Open source software provides flexibility and innovation; however, it also means increased security risks and non-uniformity, which can cause compatibility issues later.

4. Cloud Computing

When DOD organizations purchase new hardware, it is preloaded with Microsoft Office and the commands license is applied to that machine. This has become a built in cost for the DOD and does not allowed organizations to have dynamic growth or mobility. Prior to cloud computing, information and services were stored directly on some form of hardware, such as a personal computer, server bank or removable media. The following definition from Grance and Mell provides a thorough explanation of what cloud computing is.

> Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models. (Grance & Mell, 2011, p. 2)

There are five characteristics, three delivery modes and four deployment models that comprise cloud computing. "The five characteristics of cloud computing are: on demand service, ubiquitous network access, location independent resource pooling, rapid elasticity and measure service" (Grance & Mell, 2011, p. 2). These characteristics could be initial measurements guidelines that the DOD could use to determine if the particular freeware in question would be a best fit for any command trying to employ that particular freeware. "The three delivery models of cloud computing are: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS)" (Grance & Mell, 2011, p. 2). Google Apps would define as a SaaS. "The four deployment models of cloud computing include: private cloud, community cloud, public cloud and hybrid cloud" (Grance & Mell, 2011, p. 3). As you will read later on in this thesis, we will discuss why the DOD would need to find a hybrid deployment model more palatable. As the world continues to change at the speed of information sharing, cloud computing has the ability to usher in a new element of interoperability for services and the DOD.

B. DOD SOFTWARE ACQUISITION

As the DOD and other government agencies move into the realm of cloud computing, the DOD has been slow to update its policies and acquisition practices for government usage. Multiple software suites are available for government usage, and each command has access to DOD-wide software blanket purchase agreements (BPAs) for a streamlined acquisition process. The DOD has BPAs with both Microsoft and Google for their Google for Government Apps (Foley, 2013). The acquisition of those items has been labeled as commercial-off-the-shelf (COTS) items by the Federal Acquisition Regulation, but the Defense Federal Acquisition Regulation Supplement (DFARS) went more in depth to align the acquisition of commercial software with the enterprise software agreements established by the DOD Enterprise Software Initiative (ESI):

> Department and agencies shall fulfill requirements for commercial software and related services, such as software maintenance, in accordance with the DOD Enterprise Software Initiative (ESA) (see website at http://www.esi.mil). ESI promotes the use of enterprise software agreements (ESAs) with contractor that allow DOD to obtain favorable terms and pricing for commercial software and related services. ESI does not dictate the products or services to be acquired. (DFARS 208.7402, 2016)

Although the BPA with Google is still in its infancy and has not been released to all components of the DOD, the ability to expand Google's usage to other commands would potentially be easy as a BPA provides commands with a vetted service provider and product (Foley, 2013).

Google for Government does follow the traditional methods for software procurement, but it falls into a new realm for ESI defined as "software as a service" (SaaS). "SaaS is a software application delivery model where a software vendor develops a web-based software application and hosts and operates (either independently or through a third-party) the application for use by its customers over the Internet" (Gil, 2016). This is an important transition, because most of the high fees associated with software acquisition come from licensing and maintenance. GSA noted that its transition from traditional productivity suites to Google for Government would "save more than $15.2 million for the agency" in five years (Google, 2016).

C. DEFENSE INFORMATION ASSURANCE RISK MANAGEMENT FRAMEWORK (DIARMF)

All proprietary software, such as Microsoft Office is certified through DIARMF. All software acquired for DOD, whether commercial or developed, can create multiple security risks to the DOD and national security. The DOD has had multiple iterations for certification and accreditation of its IT systems, including outdated policies like the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and the DOD Information Assurance Certification and Accreditation Process (DIACAP; Marzigliano, 2011). The latest DOD policy for certification and accreditation of IT systems is the DIARMF, more commonly known as RMF. "The purpose of DIARMF is for the DOD to establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the RMF)" (DOD, 2014). The revisions made to DIACAP

not only change nomenclature for key roles and procedures but also "advances the practice of Information Assurance (IA) at DOD and reflects the growing importance of IA within the federal government" (Marzigliano, 2011). "Most employees familiar with DIACAP would hail RMF for the required paradigm shift and making sure the DOD no longer looked at IA as a check in the block for FISMA [Federal Information Security Management Act] compliance" (Marzigliano, 2011). This paradigm shift could take less time as expected once the DOD incorporate its methods and philosophy into current IA training.

Under this new policy, as shown in Figure 1, the DOD is promoting a culture shift for the assessment of information assurance and cybersecurity. Operational resilience, integration, and interoperability are the key tenets of the new policy, which also adopts a common language for federal cybersecurity terminology (Redman, 2016b). Additionally, the DOD's transition to the "National Institute of Standards and Technology (NIST) Special Publication 800–53 Security Control Catalog incorporates security early and continuously within the acquisition life cycle" (Redman, 2016a). RMF promotes a different level of continuous monitoring than its predecessor DIACAP, which could be achieved through the use of continuous security scanning (Marzigliano, 2011).

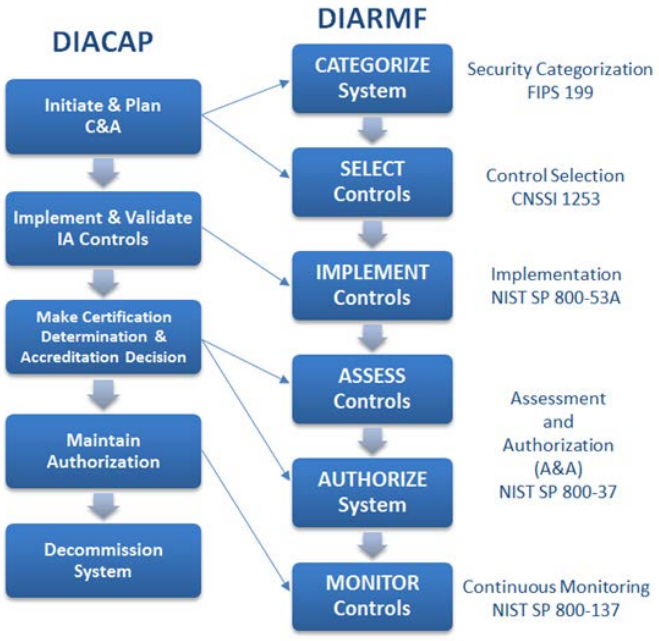


Figure 1. Comparison of DIACAP and DIARMF Processes. Source: Marzigliano (2011).

While RMF will change the certification and accreditation process to an assessment and authorization (A&A) process, thus reducing the total process time, it will also increase cost and effort (Marzigliano, 2011). Security for IT systems will be "baked in and not bolted on" as in the past under the previous DOD Information Assurance policies (Redman, 2016a). Starting the RMF process in the acquisition phase will drive acquisition costs higher in the initial purchase of a new IT system, but then will lower costs later in the IT life cycle, as the continuous monitoring and A&A process are more automated and incorporated into the initial programming (Marzigliano, 2011; Redman, 2016b). Google and Microsoft are both, therefore, required to have their programs approved, monitored, and certified prior to being deployed on DOD computers.

Many companies, like Google have a high number of previous government employees among its ranks, which gives the company an insider perspective on government needs and security risks (Levine, 2014). Microsoft has its own career progression program, that helps veterans and soon to be veterans transition from the military into a job with Microsoft (Microsoft, 2016c). The use of Microsoft Office and has been accredited and authorized through the DIARMF.

D. FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FEDRAMP)

While Microsoft can deliver its productivity suite as a SaaS, through its new cloud based applications, the DOD has relied heavily on preloaded software. In response to Google's primary revival, Google promised to reduce cost and add many benefits to the DOD with its SaaS, Google Apps. To lower overall cloud computing costs for the DOD, Google must certify its application through FedRAMP (n.d.-b). "FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services" (FedRAMP, n.d.-b). "The purpose of FedRAMP is to

- Ensure that cloud systems used by Government entities have adequate safeguards
- Eliminate duplication of effort and reduce risk management costs
- Enable rapid and cost-effective Government procurement of information systems/services" (FedRAMP, n.d.-b).

Google for Government maintains a FedRAMP certification and is accessible on DOD networks (Google, 2016a).

Cloud computing through Google Apps opens the DOD to hundreds of security risks while trying to satisfy the primary customers of the service. In Potter's (2012) thesis, *An Evaluation Methodology for the Usability and Security of Cloud-Based File Sharing Technologies*, he highlighted that "providing usability and maintaining security in IT systems have traditionally been viewed as conflicting goals" (Pp. 80). FedRAMP was developed as a means to create a symbiotic relationship between those two goals. In theory, this would decrease the number of non-malicious insider breaches that Potter also highlighted in his research.

In a Government Accountability Office (GAO) report focused on cloud computing, the GAO (2016) recommended that agencies follow 10 key practices while executing service-level contracts for cloud computing. Of those 10 practices, two involved security. The following are the two security practices recommended by the GAO:

1. Specify metrics the cloud provider must meet in order to show it is meeting the agency's security performance requirements for protecting data (e.g., clearly define who has access to the data and the protections in place to protect the agency's data; GAO, 2016).
2. Specify performance requirements and attributes defining how and when the cloud service provider is to notify the agency when security requirements are not being met (e.g., when there is a data breach; GAO, 2016).

FedRAMP satisfies the GAO suggestions during its three-step process (security assessment, levering and authorization, and ongoing assessment and authorization).

E. FREEWARE, FREE SOFTWARE, AND OPEN SOURCE SOFTWARE RELIABILITY

1. Freeware

Even though FedRAMP would certify the cloud computing aspect of Google, the government has no formal process to address freeware. Google Apps falls under freeware, and the DOD does not have any specific policies addressing the acquisition or use of freeware. According to the Free Software Foundation (FSF), there is no clear definition for freeware because it is a loosely defined category; however, the FSF requires that free

software not be called freeware (Free Software Foundation, 2016a). The most commonly used freeware examples are Microsoft Internet Explorer, Adobe Acrobat Reader, and Skype. Figure 2 demonstrates "the typical relationship between freeware and open source software. According to Rosen, open source software and freeware is not the same thing" (Rosen, 2016). Prior to implementing the use of Google Apps, it would be prudent for the DOD to bridge the gap between its policies on cloud computing and its definition and use of the term *freeware*.

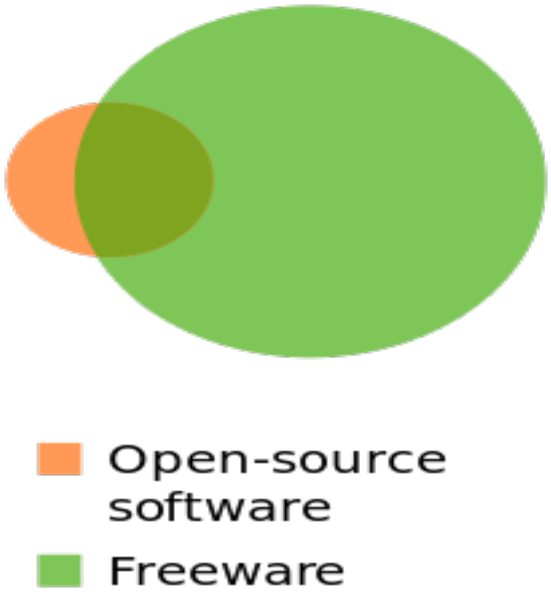
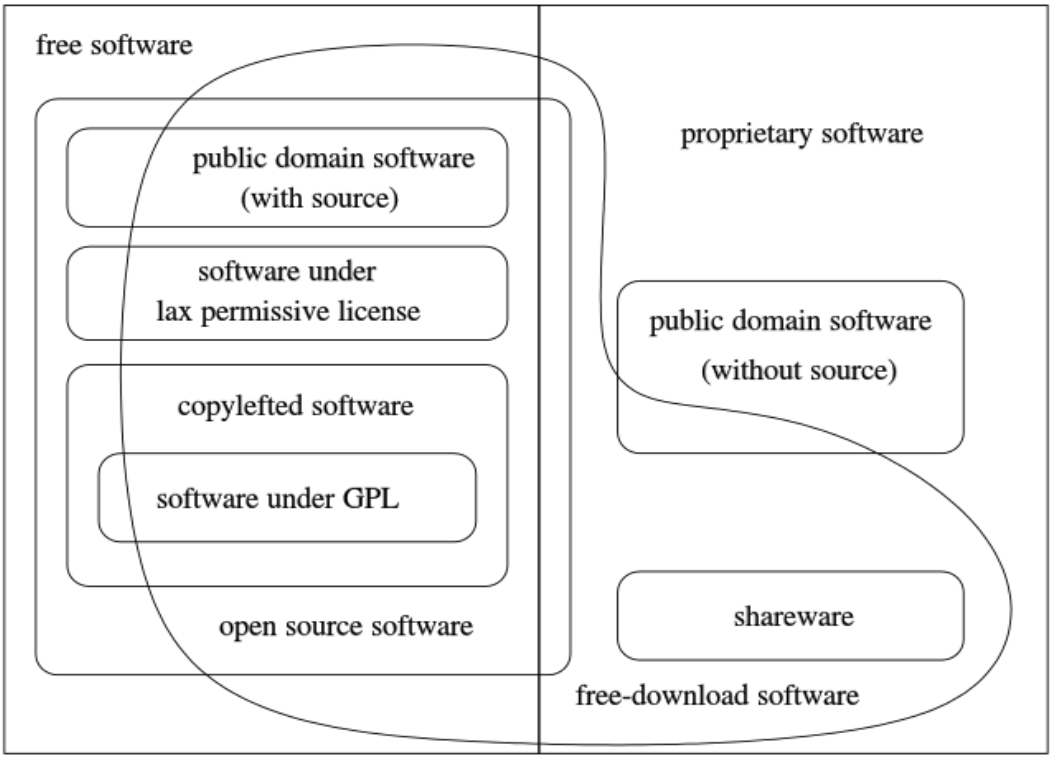


Figure 2. Relation to Other Forms of Software Licensing. Source: Rosen (2010).

2. Free Software

The DOD does have policies dictating the use of free and open software due to its potential security concerns. In contrast with freeware, free software gives a user the liberties to make changes to the code and to copy and distribute the software as needed. Figure 3 defines the categories of free and non-free software, according to the Free Software Foundation. According to Richard Stallman, president of the Free Software Foundation, "Software is considered to be free software if people who receive a copy of the software have these four freedoms" (Free Software Foundation, 2016).

Freedom zero is the freedom to run the program for any purpose. Freedom one is the freedom to study how the program works, and change it to make it do what you wish. Freedom two is the freedom to redistribute and make copies so you can help your neighbor. Freedom three is the freedom to improve the program, and release your improvements (and modified versions in general) to the public, so that the whole community benefits. (Free Software Foundation, 2016)



As defined by the Free Software Foundation. Left: free software, right: proprietary software, encircled: free software.

Figure 3. Categories of Free and Non-Free Software, According to the Free Software Foundation. Source: Free Software Foundation (2016).

According to the Free Software Foundation, free software is said to be more reliable than comparable proprietary software (Free Software Foundation, 2016). In a test conducted from 1990 to 1995 on the reliability of software, commercial software crashed 40% of the time, while free software only crashed 7% of the time (Free Software Foundation, 2016).

3. Open Source Software

The DOD does an adequate job of defining open source software, but it is the operators and users that have made the term synonymous with freeware, although the

meanings are not the same. This poses a problem when defining requirements for acquisition as well as security protocols for the use of Google Apps versus Microsoft Office. According to the FSF, "there is a significant overlap between open source software and free software" (Free Software Foundation, 2016). Open source software has previously been called alternative names such as *free and open source software* (FOSS) (Chief Information Officer, DOD, 2009). "To determine if a particular license is actually an open source software license, legal review is required" (Chief Information Officer, DOD, 2009). "Open Source Initiative (OSI) publishes a list of licenses which have successfully been approved and comply with the open source definition" (Chief Information Officer, DOD, 2009).

According to a Fuzz study conducted in 1995, "there is quantitative data confirming that mature FOSS programs are often more reliable and the reliability of a system was measured by feeding programs random characters and determining which ones resisted crashing and freeze-ups" (Wheeler, 2015). A comparison of the results of the testing shows that "seven commercial systems have an average failure rate of 23%; while Linux has a failure rate of 9% and the GNU utilities have a failure rate of 6%" (Wheeler, 2015). In 2000, a paper titled *An Empirical Study of the Robustness of Windows NT Application Using Random Testing*, researchers discovered Windows NT GUI applications crashed 21% of the time; additionally, it hung 24% of the applications, and crashed or hung all the tested applications (Forrester & Miller, 2002). Although this experiment and test was done a number of years ago, "there is nothing that suggests that proprietary software has become better than FOSS programs" (Wheeler, 2015).

The debate over open source versus closed source has been going on for a very long time. According to a survey done by Open Source Business Conference, "the top four reasons individuals or organizations choose open source software are lower cost, security, no vendor 'lock in,' and better quality" (Guseva, 2009).

These reasons are why proprietary software is becoming less and less necessary. "In 2009, the U.S. White House switched its Content Management System (CMS) from a proprietary system to open source" (Vaughan-Nichols, 2009). It is reported that "98% of enterprise-level companies use open source software offerings in some capacity" (Cabot Technology Solutions Inc., 2016). There is a strong argument that open source software may

be safer since many people can view and edit the code. “A study of the Linux source code has 0.17 bugs per 1,000 lines of code while proprietary software generally scores 20–30 bugs per 1,000 lines” (Delio, 2004).

F. CYBER VULNERABILITY AND MITIGATION

The DOD has an established network, security protocols, and mitigation steps for the use of Microsoft Office in and out of its offices. Although the DOD has fostered a working relationship with Microsoft Office for multiple years, the use of its cloud computing functions and storage through Google Apps is a new player with uncharted security risks and vulnerabilities (Levine, 2014). For years, there have been debates about the security of free software compared to proprietary software. One major argument has been security through obscurity. Users of free software believe that there is security through disclosure. The free software community is more willing to discuss the vulnerabilities of free software because the source code is accessible and anyone can view the code to find possible bugs. Finding free software with hidden spyware is less likely to occur because so many users are inspecting the source code, compared to proprietary software where that software developer is the only one able to view the source code. Since the source code is available in open source software, bugs tend to be fixed immediately, as opposed to commercial software which sometimes takes weeks or months to patch vulnerabilities.

“The DOD uses FOSS in areas of Infrastructure Support, Software Development, Security, and Research” (Sdubois Contributions, 2010). If there was a ban of FOSS for the military, “the military’s security would have immediate, broad, and strong negative impacts on the ability of the DOD to analyze and protect its own network intrusion applications that hostile groups could use to stage cyber-attacks” (The MITRE Corporation, 2003, p. 17).

Three conditions that may limit risks from unintentional vulnerabilities in open source software are that developers have a strong knowledge of security, people are required to review the code, and problems are fixed before the software is deployed (Chief Information Officer, DOD, 2009).

G. CLOUD MIGRATION

In an online article for FedTech Magazine, Phil Goldstien explores the DOD push for cloud computing, including the proposed challenges and hopefully outcomes from this new technology (Goldstein, 2016a). Some highlights from the article include: the use of FedRAMP in software acquisition, culture shifts, cloud migration: theory to reality and security concerns (Goldstein, 2016a). FedRAMP, as mentioned previously in this chapter, requires certification prior for any acquisition of any cloud based service or software. While the DOD is "going all-in on the cloud," there is still a requirement to pick and choose which data should be moved to a cloud and which applications can be moved to the cloud (Goldstein, 2016a). Additionally, as there is a certain level of security required for all DOD applications and data, the debate continues on commercial versus on-premises cloud environments. The DOD's most likely option is a hybrid system, keeping its most secure data under lock and key with on-premises environments. The primary decision factor for this cybersecurity division could mainly rely on the primary mission of each organization and command inside the DOD (Goldstein, 2016a). This article is particular relevant to the thesis as Google's primary cloud storage is commercial cloud environment and based on this article, the DOD is not fully committed to 100% commercial cloud storage.

While Google has obvious advantages the obvious question for the DOD and military use is: how do we get Google Apps to work in isolated and remote places with limited bandwidth? One of the largest challenges for cloud computing and the use of Google Apps in the DOD is the problem of mobility. Limited bandwidth in addition to secure communications can both help and hinder a possible transition from built in software to cloud based Software as a Service (SaaS). These problems are addressed in two papers: "Cloud Computing and Virtual Desktop infrastructures in afloat environments, by Stefan E. Gillette and "Cloud Computing Adoption by Firms" by Mariana Espadanal and Tiago Oliveria. Both papers research and theorize on how to implement cloud computing in large mobile environments. Combining the diffusion of innovations (DOI) theory and technology, organizational and environmental (TOE) framework, Espadanal and Oliveria, identified four factors that are important for the adoption of cloud computing into firms (Espadanal and Oliveria, 2012). These factors included: characteristics innovations, technology, organizational and environmental context. Related to a business modeled, cloud computing can be adopted for firms and large business,

such as the DOD, due to its speed, scalability and cost efficiency. This theory goes hand-in-hand with the conclusion made by Stefan Gillette.

As the DOD makes a move to drive down cost and become more efficient and effective, cloud computing is a front runner for achieving those goals. Stefan concluded that the fleet implementation of cloud computing is only a few steps away and with the continued DOD and Navy partnerships without outside companies and rely on innovations between cloud computing and virtualizations, the DOD will be able to run SaaS and IaaS on afloat commands (Gillette, 2012). If cloud computing can work with afloat commands, then theoretically it can with work with most mobile commands in the DOD. The virtual model that Stefan used to prove his theory, given the right parameters, could be recreated to explore multiple remote environments for not just the Navy, but the other forces as well. Whether the DOD decided to migrate to Microsoft's cloud based application or just completely switch to Google Apps, this test would address the functionality of cloud computing's five characteristics in a DOD environment.

H. SUMMARY

With the use of any available OSS or proprietary software, there is always a chance that malicious code could be embedded into the software. Completely eliminating all risk is impossible. Users should focus on reducing the risk to acceptable levels. The DOD has RMF and FedRAMP to assess acceptable security risk, and measures are in place regarding the acceptance of new IT systems. Newly released RMF should change the way the DOD acquires IT, by creating a bottom-up approach to cybersecurity, and both RMF and FedRAMP rely on continuous monitoring to maximize efficiency, security, and usability. The DOD has the tools to clearly define and create an effective policy for the use of freeware.

The next chapter covers the methodology for this project, including the origin of the research question and which analysis tools the researchers utilized with the data collected.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

Chapter II provided an overview of the body of research contained in this thesis. It provided the research questions, the scope and methodology of the research, and a general outline of the paper. Chapter III examines the data collected and assumptions used to analyze the appropriateness of freeware use by the DOD as the primary office productivity suite. It also categorizes the possible vulnerabilities, cost, and reliability of Google Apps and Microsoft Office productivity suites. This chapter describes the steps we took to decide on the four different analysis tools used to organize the data and why we chose each specific tool. The three tools discussed include SWOT (strength, weaknesses, opportunities, and threats), risk management analysis, and a cost–benefit analysis.

The beginning of our research focused specifically on problems in the DOD acquisition process and the DOD's increased use of technology because of our individual fields of study. At NPS, one of us focused on contracting and acquisition, while the other focused on information technology. We contacted SOCOM and went through multiple iterations of a project topic. The first topic included a discussion on SOCOM's long-term acquisition and the "Make or Buy" decision for IT and software at SOCOM. The initial project proposal was rejected by SOCOM, and we began our search for a different topic.

In the midst of conversation with the Command, Control, Communications, and Computers (USSOCOM AT&L/C4) contracting shop and the Communications Systems (USSOCOM J6), the J6 then directed the topic of the conversation to the use of Google Apps as a productivity software. The term used by the contracting shop to describe Google Apps was "open source software." Once we brought this topic to our thesis advisor and did a bit of initial research, we discovered that the term *open source software* was being improperly used. Google Apps is actually freeware and is in a different category of the typical productive software, such as Microsoft Office. With SOCOM's concurrence on this new project question, we began to examine the process required to acquire software in the DOD and what would be the largest challenges for acquiring and implementing freeware. Upon further research, we discovered the DOD had little literature and few definitions for freeware in any of its instructions and was in the midst of discovery and transitions into cloud computing.

A. DATA COLLECTION PROCEDURE

Gathering unbiased information on both Microsoft and Google was essential to our project research, validation, and recommendations. The scope of this thesis is limited to analyzing the data collected from information provided by Google, Microsoft, Internet searches on numerous websites, professional analysis reports, and publications with directed studies on Microsoft Office and Google Apps. Data collected from DOD instructions and contracts is also included in our research.

We thought the best information would be provided from comparing a government entity that uses Google Apps with SOCOM, which uses Microsoft Office, and what capabilities they expected to gain from the use of Google Apps. We developed questions and contacted a Google representative to ask specific questions about cost, technology, general security protocols, and certification, which is used to certify Google Apps with other government entities. Once research began, we found that there was no real necessity to get additional feedback from SOCOM. We decide to make our project more applicable to multiple commands by focusing on previous company research and comparative analysis conducted on these two productivity software giants.

B. LIST OF ASSUMPTIONS

- SOCOM was trying to find a lower cost in the use of productivity software.
- All DOD software was required to go through DIACAP prior to full contract and implementation.
- Google had not been through DIACAP.
- DOD did not have instructions/regulations pertaining to the use of Internet-based programs.

C. LIST OF LIMITATIONS

- Some variables may have been omitted from data collection and analysis.
- Every command has an individual contract with Microsoft.
- Google Apps for Government is in a test phase with the Army.

- DIACAP was revised and transformed to DIARMF.
- We did not have direct access to Microsoft representative.

D. ANALYSIS TOOLS

Throughout the research process, we tried to decide the best way to answer our research questions, which include discussing the biggest concerns in the acquisition of new software and technology. Three major concerns when acquiring new software in the DOD are vulnerability, cost, and reliability. In order to analyze the advantages and disadvantages of Google Apps versus Microsoft Office, we had to decide on the best tool to analyze our research findings. We used our findings and information provided from our sources, articles, and studies conducted by other outside companies. Our initial thought was to use three SWOT analysis diagrams separated by vulnerabilities SWOT, cost SWOT, and reliability SWOT. Although the SWOT analysis would work well for cost, it would not work well for the other categorizes, and it was difficult to define strengths for vulnerabilities and weaknesses for reliabilities.

Analysis tools that would be best suited to analyze cost would not work as well to analyze the vulnerability and reliability problems of Google Apps and Microsoft Office. Risk management analysis, trade-off analysis, and cost–benefit analysis were some of the other types of analysis tools discussed. We divided each of the three categories into columns and did a pros and cons list of which topics would best be beneficial to our research.

E. CATEGORIZING BY VULNERABILITIES

We decided to analyze the potential vulnerabilities of Google Apps and Microsoft Office using risk management analysis because it was the best way to differentiate the overall likelihood of occurrence combined with its overall consequence.

F. CATEGORIZING BY COST

The cost–benefit analysis tool was the best tool to analyze the cost of Google Apps and Microsoft Office. It gave us the ability to look at the capabilities offered side by side and directly associated them with costs. Using these costs, it was easy to define which company had the advantage in certain categories and which company was at a disadvantage in others.

G. CATEGORIZING BY RELIABILITY

We decided to analyze the reliability of Google Apps and Microsoft Office through trade-off analysis because of the easy identifiable pros and cons for each company. Once a list of pros and cons was created, we were then able to eliminate equally weighted items from each list and ascertain the advantages and disadvantages for each software giant.

H. SUMMARY

Chapter III describes the process by which we collected data and applied those findings to our research questions. It also identifies the assumptions made prior to researching the topic, limitations, and the analysis tools. We decided to categorize the data by vulnerabilities, cost, and reliability.

In the end, we decided to use a SWOT analysis for the initial categorization of our findings and organize our research findings with the use of multiple analysis tools. A SWOT analysis would help us create a list of the pros and cons between Google Apps and Microsoft Office, separated by each company's strengths, weaknesses, opportunities, and threats. A risk management analysis, a cost–benefit analysis, and a trade-off analysis of reliability were utilized to dive deeper into vulnerabilities, cost, and reliability analysis. These methods of analysis are important to create similar categories for comparing each productivity suite. Without thesis categorization, comparing Microsoft to Google would be like comparing apples and oranges. Without the ability to compare similar categories, the DOD cannot buy the best systems for each of its customers at the lowest cost.

Chapter IV discusses the findings based on the information gathered during the data collection process.

IV. FINDINGS

Chapter III described the methodological process by which we collected data regarding Microsoft and Google, as well as software in general and applied those findings to our research questions regarding Microsoft office and Google Apps within DOD. It also identified the assumptions made prior to researching the topic, limitations, and the analysis tools. Chapter IV presents an analysis on the DOD's potential use of Google Apps versus Microsoft Office. The first part of this chapter examines the Strengths, Weaknesses, Opportunities, and Threats (SWOT) of Google Apps and Microsoft Office. The second part identifies the vulnerability, cost, and reliability of using Google Apps and Microsoft Office. We used a SWOT analysis to categorize our findings because it enabled us to create and examine the pros and cons between Google Apps and Microsoft Office in detail, separated by each company's strengths, weaknesses, opportunities, and threats.

A. STRENGTHS, WEAKNESSES, OPPORTUNITIES, THREAT (SWOT) ANALYSIS

Comparing multiple categories in a product selection process helps aid the DOD in choosing the correct productivity suite. Our SWOT analysis presents the findings in an accessible way, incorporating all the main categories of focus into one diagram. An "analytical framework," invented by Edmund P. Learned, C. Roland Christensen, Kenneth Andrews, and William D. Book, "SWOT analysis presents the strengths, weaknesses, opportunities, and threats of a given enterprise" (R.D. Irwin, 1969; Taylor, 2016). SWOT analysis examines internal and external influences and will help the DOD identify the controllable and uncontrollable "forces influencing" Google Apps and Microsoft Office (Taylor, 2016). A SWOT analysis is divided into four columns in which the positive and negative, and internal and external forces don't typically match but will connect in subtle ways (Taylor, 2016). SWOT analysis spotlights crucial aspects involved in the acquisition and usage of a given choice, here Google versus Microsoft for the DOD (Taylor, 2016). Because SWOT identifies both internal and external forces, the DOD's product selection process needs to consider both. Once these forces have been identified, the DOD will be able to capitalize on or mitigate the positive or negative benefits associated with using either product.

B. SWOT ANALYSIS OF GOOGLE APPS

The researchers conducted a SWOT analysis of Google Apps and identified the strengths, weaknesses, opportunities, and threats presented in Figure 4. Initial analysis regarding Google Apps revealed 12 strengths, five opportunities for growth, four major weaknesses, and five significant threats that should be considered if the DOD decides to use Google Apps as its primary office productivity suite.

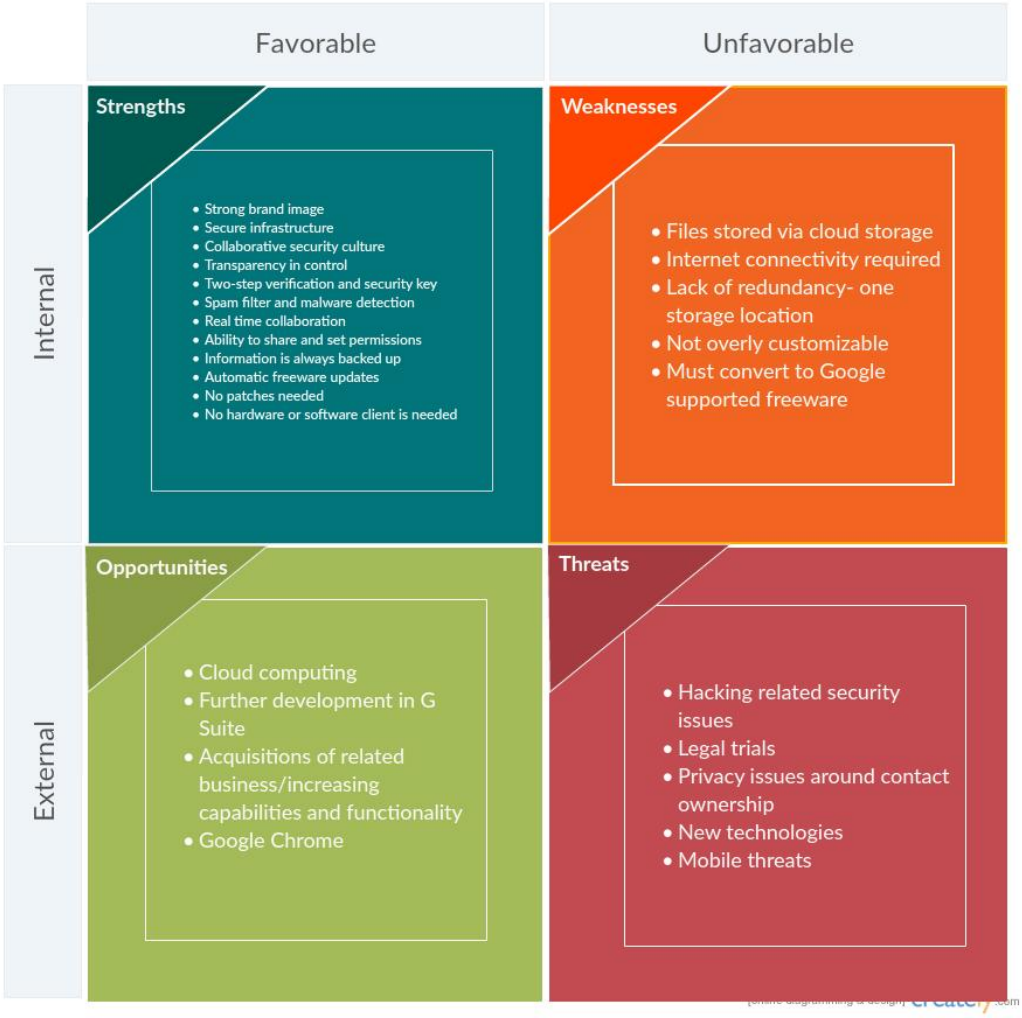


Figure 4. Google Apps SWOT Analysis. Adapted from Thompson (2015).

Of the 12 strengths found for Google, one of the more important internal forces is the strong brand name. The strength of the brand is very important to the DOD since a strong brand name can also be translated into easier acceptance across multiple DOD agencies, the

interagency, and foreign partners. When users hear the name Google, many already feel somewhat comfortable, so asking them to transition may result in a better response than an unheard of software. According to Google, Google Apps is already utilized by government agencies in over 45 states, 66 of the top 100 universities, and over five million businesses (Lardinois, 2012). A significant number of today's government employees have likely previously also used Google's Apps for personal day-to-day functions and would be partially familiar with Google's applications easing the DOD's potential transition.

Google also presents a strength in multiple security measures employed to ensure they maintain a secure infrastructure. The government and DOD's secrets, intentions, and plans are critical to the safety of the public as well as for the safety of government personnel. Therefore, information security and access control is essential for DOD productivity suites. The U.S. Government spends approximately $12 billion a year on cybersecurity (Bryan, 2015). If cyber-attacks continue to increase, it would be reasonable to assume that the budget would increase to meet these new cyber threats. It is beneficial to the DOD that Google's security is so strong that the DOD could redirect some of the money they would use on increased cybersecurity measures towards other programs. We address further strength later in the chapter.

Another strength of Google is transparency in control of and the ability to share and set permissions. Google allows its users to have full control over any documents they create and save (Google, 2016a). At no time will Google ever take over control of a user's file. Users can feel safe knowing that they could save and delete a file as they feel necessary and know that the information is not stored anywhere else. Users also have the right to share files and to set the permissions to give other users access to view or edit their files.

Primary weaknesses identified for Google Apps deal more with a necessary culture shift, a slow shift that the DOD is already making. In 2003, "the Government Paperwork Elimination Act (GPEA), required Federal agencies to submit information or transactions electronically, when practicable, and to maintain records electronically, when practicable" (Office of Management and Budget, 2016). The DOD's conversion to a paperless fighting force is still ongoing, and, with Google's primary storage in a "cloud," data duplication,

access, and retrieval may be harder to control. If the cloud is not maintained within the DOD's agency location, there may be a question of security, redundancy, and reliability.

Another major internal weakness for consideration is compatibility issues. It took the DOD a long time to convert to Microsoft, and DOD still maintains multiple versions of Microsoft to maintain productivity and communicate across various commands. Switching to Google Apps would require conversion of all Microsoft docs to Google compatible versions. Formatting may be lost when converting back and forth between each version, as well as some capabilities while working within Microsoft. As part of a response to this issue, Google does conversion/migration services for your office (Young, 2016). They also provide training to new users. Also, as new workers are hired into the DOD, these younger generations tend to be more familiar with the several technology and productivity suite options offered by Google, which are also available to be tailored to the DOD.

External forces for Google Apps are beyond its control; therefore, the threat of hacking related security issues and Google's acquisitions of related businesses may also be outside the DOD's control. These opportunities and threats can affect the DOD's overall mission and there should be a method of mitigation, particularly for the threats, that would provide increased control to the DOD. This is a primary reason while all cloud based computing must be certified through FedRAMP.

One of the five highlighted Google opportunities that could benefit the DOD as much as it benefits Google are the increasing acquisitions and partnership that Google has with its exceptional growth in the tech market. These partnerships, while promising to produce new innovations for Google, may also produce new innovations for the DOD in multiple fields such as communication, and collaboration. Google recently partnered with PricewaterhouseCoopers to execute its $11 billion defense contract for Electronic Health Records (EHR), providing similar cloud computing capabilities that it will employ if the DOD migrates to a Google Apps productivity suite (Tahir, 2015).

The largest continuing threat to both Google and the DOD are the continued security threats not just from external threats, but also from internal threats. Securing data brings into question responsibility and accountability for the data. Content ownership could cause a rift between Google and the DOD. "The key to privacy protection in the cloud environment is

the strict separation of sensitive data from non-sensitive data followed by the encryption of sensitive elements" (Chen & Zhao, 2012). The three main categories of data include: classified information, controlled unclassified information, and special data categories (Reynolds, 2015). The DOD and the federal government monitor contractors who have access to sensitive and non-sensitive data through specific cybersecurity responsibilities (Reynolds, 2015). These rules and regulations make both the DOD and contractor responsible for data security. "The laws, regulations, and policies that create these requirements are varied, and the protections that must be implemented frequently depend in large part on the nature of the information" (Reynolds, 2015). Google would be responsible and accountable for strict adherence to DOD policies in order to cultivate a budding partnership.

Overall, Google has multiple strengths, weaknesses, opportunities, and threats that could have both positive and negative effects on the DOD infrastructure and organizational productivity. Like Google, Microsoft also has multiple influences that can both assist and diminish the DOD's ultimate goal of effective productivity. The next section covers the SWOT analysis for Microsoft Office and the advantages and disadvantages the DOD would gain from remaining loyal to its productivity suite.

C. MICROSOFT OFFICE SWOT ANALYSIS

The SWOT analysis of Microsoft Office identified the strengths, weaknesses, opportunities, and threats listed in Figure 5. We identified eight prime strengths, six crucial weaknesses, eight considerable threats regarding Microsoft Office and very few opportunities for growth. The DOD currently uses Microsoft Office within most of its agencies, but more than 30 government agencies, including multiple units in the U.S. Army, have already transitioned over to Google Apps (Sullivan, 2013).

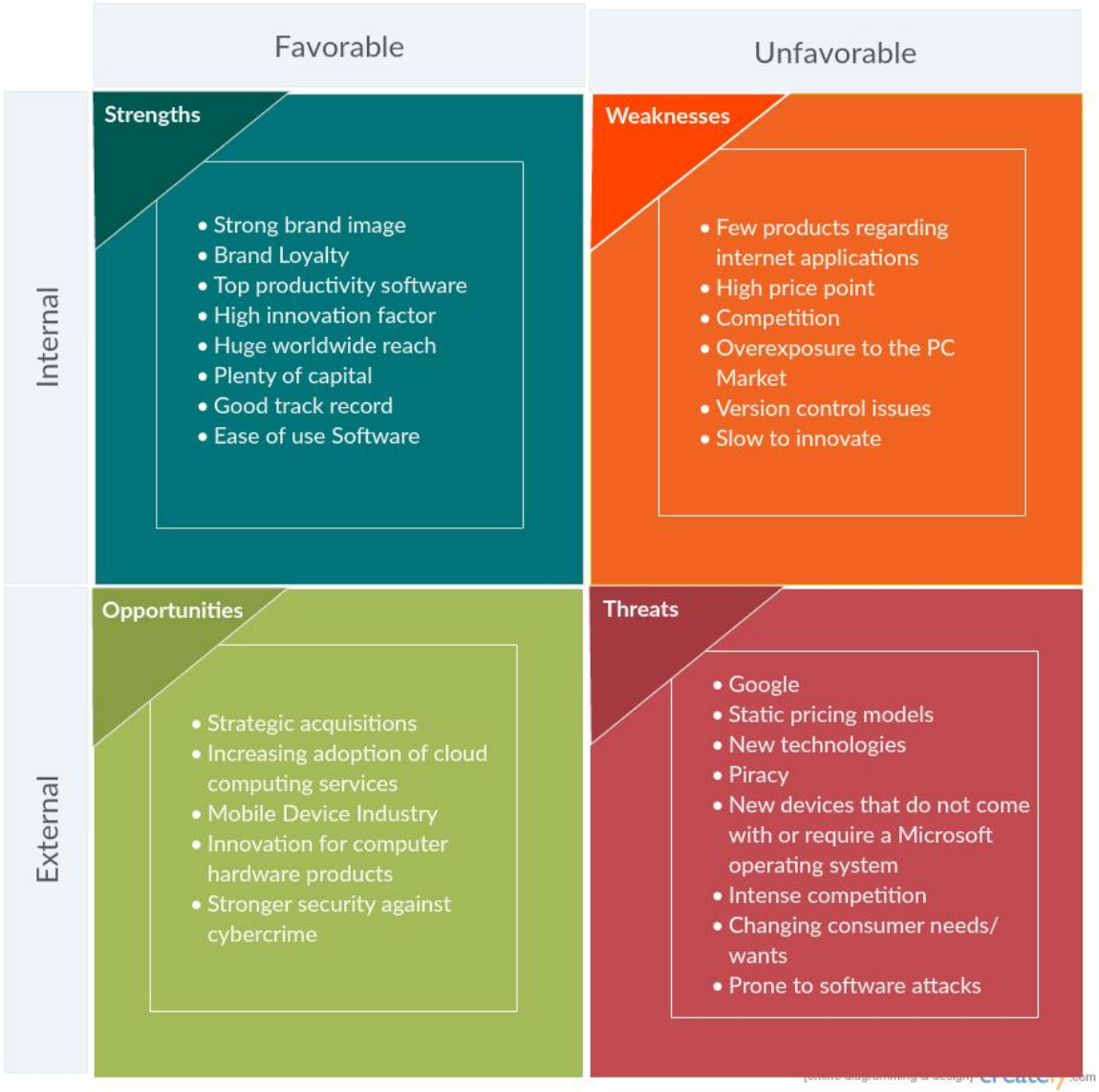


Figure 5. Microsoft Office SWOT Analysis. Adapted from Jurevicius (2013).

Like Google, Microsoft also has a strong brand image and Microsoft has been utilized in the DOD for many years. Due to its longevity, users in the DOD are trained and well-versed on the functions of Microsoft Office. The ease of software use and the productivity functions found in Microsoft Office applications, such as PowerPoint and Excel, are unmatched by any other competitor. The working relationship that Microsoft has built with the DOD is a testament to its good track record and understanding of DOD process. Recently, Microsoft was able to certify some of its cloud based applications "six times faster" through FedRAMP then it takes for most applications in the FedRAMP system

(Goldstein, 2016b). In addition to its large reach within the DOD, Microsoft also has a huge worldwide reach and is a common platform utilized across multiple agencies and nations. In a recent 2016 Microsoft survey, over 1.2 million users in 140 countries and 107 languages use Microsoft Office as a primary productivity suite (Microsoft, 2016).

One of Microsoft's largest weaknesses that not only affects the majority of the population but also the DOD is version control. The DOD spends millions of dollars annually in order to renew the license rights for the multiple versions required to exchange documents within its network (DOD Enterprise Software Initiative, n.d.). Additionally, its high price point, competition, and its overexposure in the PC market could make Microsoft seem like an aging dinosaur with new weaknesses building every day (Dawson, 2009). Indigo Equity Research analysis on Microsoft's profit margins and market strategies show the company does not excel at servicing both the consumer and enterprise market (Ide, 2014).

However, in contrast, using Microsoft products allows the DOD to capitalize on Microsoft's strong brand image and new partnerships and to draw on new tech companies and future innovations. Additionally, through Microsoft's transition to cloud computing services and leveraging of the latest advances in cloud computing, "customers benefit from a comprehensive application platform with deeply integrated services including infrastructure, data services, advanced analytics, and developer tools and services, all provided within a consistent portal experience" (Microsoft, 2016). While some external influences would be helpful in an agreement between the DOD and Microsoft, the threats to Microsoft are also threats to the DOD.

The primary threat to Microsoft and the DOD are the constant software attacks. Already highlighted in the SWOT overview for Google, the DOD spends billions of dollars annually to keep its data secure (Bryan, 2015). While the DOD spends over six billion dollars annually for cyber security, Microsoft plans to spend over one billion dollars per year to keep its tech company and products secure (Bort, 2015). The more money Microsoft spends on its security the less money the DOD will have to spend on keeping the data it houses with Microsoft secure. This in turn creates a win-win situation for both the Microsoft and the DOD as a potential returning customer.

D. COMPARISON OF STRENGTHS, WEAKNESSES, OPPORTUNITIES, AND THREATS

1. STRENGTHS

The comparison of Google Apps and Microsoft Office in Figure 6 shows that, although Google Apps and Microsoft both have a strong brand image, Google Apps is leading in real-time collaboration and the ability to backup data instantly. Data edited in Google Apps is saved and backed up on a Google server as soon as it is typed, compared to Microsoft Office where the user has to decide where and when to save the data. This strength is important to Google Apps users because, if there is a system crash, no data is ever lost. Users could log in to another computer and continue working right where they stopped. In contrast, if there is a computer crash while using Microsoft Office and the data is saved only locally on a hard drive, all data will be lost.

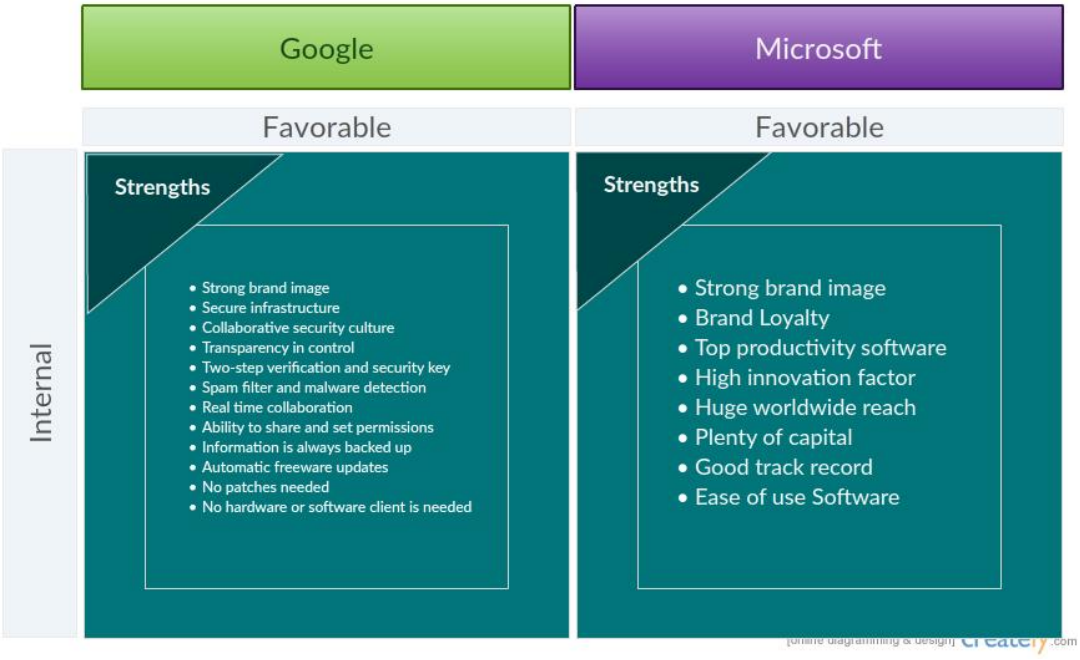


Figure 6. A Comparison of Google Apps and Microsoft Office Strengths. Adapted from Thompson (2015) and Jurevicius (2013).

Other strengths that Google Apps has are "strong encryption and authentication and a secure cloud infrastructure" (Google, 2016a). Google Apps offers an extra layer of security with two factor authentication, which greatly reduces the risk of hackers stealing usernames

and passwords" (Google, 2016d). Google users sign into their account and put in their password; then they will be asked to input a code that is sent via text message as the second step of the verification process. Google Apps automatically updates its patches online compared to Microsoft, where patches are deployed to users and then updated. "Google is recognized as a trusted name and an industry leader in reliable cloud infrastructure" (Google, 2016c). The use of Google Apps reduces infrastructure cost for the DOD since all data would be stored in the cloud. If the DOD continues to use Microsoft Office, there will still be a need to spend money on maintaining local servers that support these files.

The large market share of Microsoft Office products make it somewhat difficult for Google Apps to compete. Microsoft Office is a well-known product worldwide that has been used for years. According to Dave Skowronski, an app developer for Microsoft, only about 20% of users use Microsoft applications to their full potential and Google Apps therefore will not be sufficient for them (McGarvey, 2014). Microsoft has already established a very good baseline with its current number of users from preloaded software, while Google must continue to grow its productivity suite users from its number of everyday search engine users. In a Forbes.com article, Gordon Kelley calls Microsoft the "new Google" and Google the "new Microsoft" highlighting the Microsoft's newest strategies to remain relevant and overpower Google's market domination (Kelley, 2015). His article highlights some of Microsoft's strength in our SWOT, particularly the high innovation factor and plenty of capital Microsoft utilizes. If the DOD realized that most users are not using Microsoft Office to its full potential, then they may be able to save costs by not paying for millions of licenses for the entire Office productivity suite.

2. WEAKNESSES

A comparison of the weaknesses of Google Apps and Microsoft Office in Figure 7 shows that both companies have areas in which they could improve. Google for Government files are all stored in one primary location. There is a lack of redundancy which one may think is a good thing; however, if that Google server crashed, then the data would be lost because the information is not saved anywhere else. An issue like this could cause major problems within the DOD if important data becomes unavailable. Also, since Google relies on an Internet connection to access the files, this may be detrimental to DOD agencies and

military personnel who may be in very isolated areas for periods of time without an Internet connection. Google Apps allows a user to download files and edit them offline; however, this prevents instant collaboration with other users.

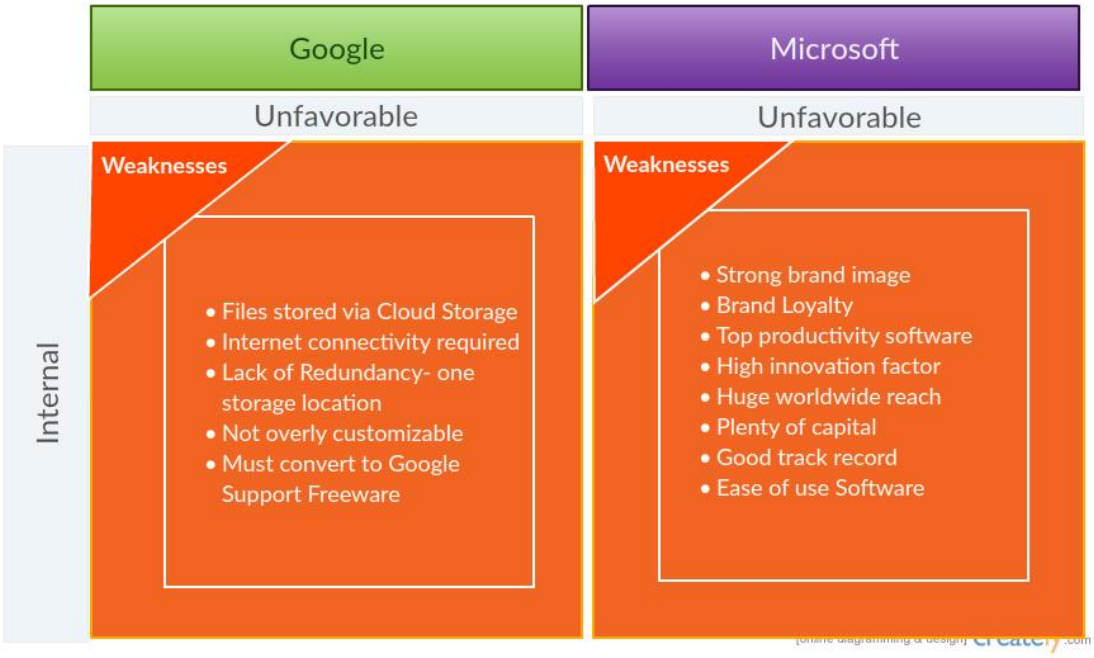


Figure 7. A Comparison of Google Apps and Microsoft Office Weaknesses. Adapted from Thompson (2015) and Jurevicius (2013).

Another weakness of Google is that all old files must be converted to Google Docs in order for the user to make changes to it. For companies who have been around for a very long time, and the DOD, this is not a feasible option. It will take a lot of time and manpower to convert/migrate all existing documents to Google.

One weakness the researchers identified with Microsoft is the high price point at which their product is sold. Until recently, there have not been any viable alternatives of an office productivity suite that provides similar applications. Microsoft has been able to charge the DOD whatever they want to because of the DOD's dependency on their product. Now there is competition in the market with Google Apps. With the increased usability, availability, and functionality of Google Apps, more and more users are switching over to Google. Another weakness is that there is no version control when using Microsoft Office products. At any given DOD agency, there may be multiple versions of Microsoft Office

operating at the same time. This can be confusing to users and can also be very expensive to maintain.

3. OPPORTUNITIES

A comparison of the opportunities inherent in Google Apps and Microsoft Office in Figure 8 identified that both companies have the ability to expand in the area of cloud computing. Google has already done this with Google Apps, which is done solely online with the data saved in the cloud, and will continue to expand in that area. "Google Cloud Platform frees the users up from the overhead of managing infrastructure, provisioning servers, and configuring networks" (Google, 2016a).

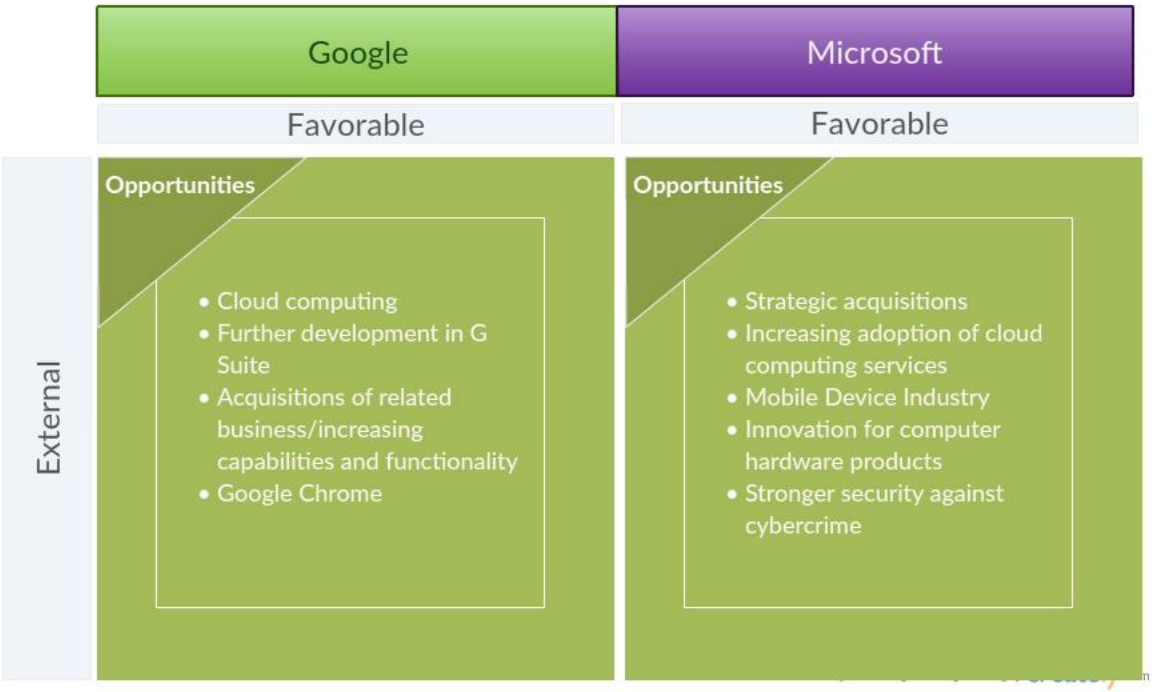


Figure 8. A Comparison of Google Apps and Microsoft Office Opportunities. Adapted from Thompson (2015) and Jurevicius (2013).

The newly developed "G Suite was designed as an entirely cloud-based service from the ground up, so IT departments don't need to spend time and money maintaining any desktop components" (Google, 2016a). The cost savings from hiring less IT personnel could be utilized in another vital area within the DOD. "G Suite users enjoy the same experience across different devices, operating systems and browsers" (Google, 2016a). This

standardization is very important within the DOD. DOD users are more effective and efficient when their work environment looks the same no matter if they are using a laptop, tablet, smartphone, or a different physical location.

The Google Chrome browser was developed to operate in areas where there is low or limited bandwidth (Young, 2016). This feature is critical to the DOD, especially since there are areas of the world where the military operates that may not have a strong Internet connection. Google Chrome has a feature called Data Saver. Utilizing this feature enables the user to use less bandwidth since "the web traffic goes through Google servers before being downloaded to your device; less data gets downloaded to your device, because Google servers compresses it" (Google, 2016f). The Data Saver feature allows users to require less bandwidth in order to view web pages and use Google Apps.

Microsoft's growth in Microsoft Azure Government (Cloud for Government), "increases the agility of federal, state, and local government organizations and partners with hyper scale computing, storage, networking, and identity management services" (Microsoft in Government, 2015). "Azure Government has an ongoing commitment to maintaining the most certifications and attestations for mission-critical government workloads; the data centers meet or exceed the complex and critical requirements for U.S. Federal, Department of Defense, state, and local government" (Microsoft Azure Government, 2016).

4. THREATS

Threats facing both Google and Microsoft are laid out in Figure 9. One common threat amongst both companies is competition with new technologies. Each company creates new technologies and strives to release the newest product first. Google also faces competition from companies like Microsoft, Apple, and Yahoo. Even though competition is a threat to the individual companies, it is a benefit to the DOD. Competition in the market gives the DOD more bargaining power to negotiate the best contract.

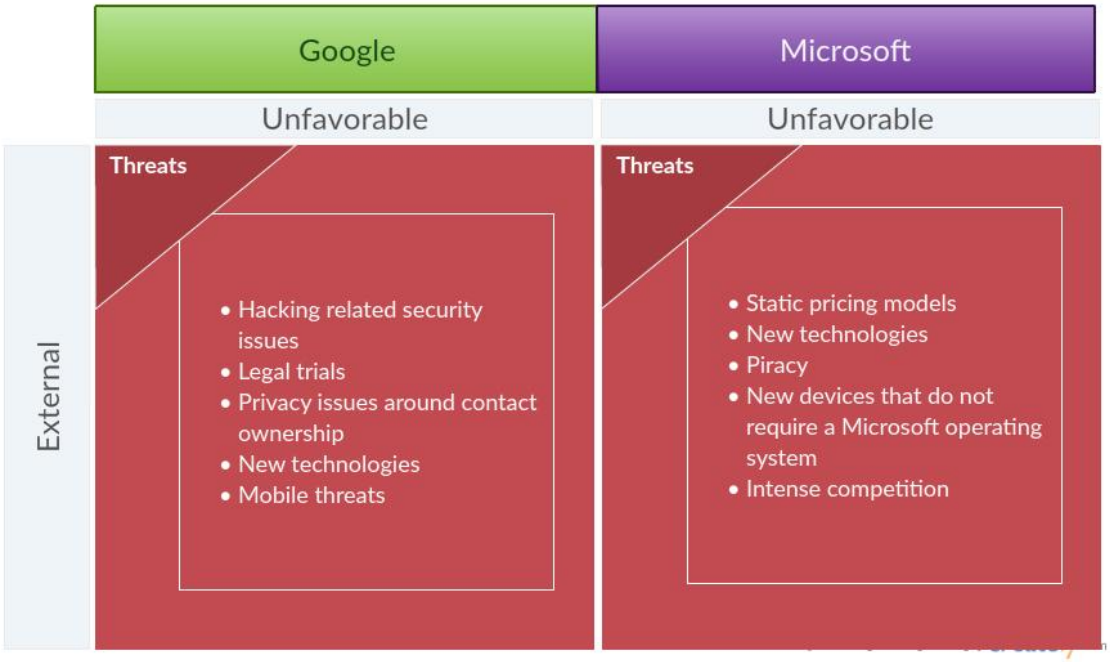


Figure 9. A Comparison of Google Apps and Microsoft Office Threats. Adapted from Thompson (2015) and Jurevicius (2013).

Another threat that Google faces are that more often, users search on alternate third party apps for things like hotels and restaurants instead of going to Google's website. Google does not get paid if the users don't use their website to search for what they need. This threat is increasing each day as individual companies create apps specifically for their products.

Google has faced many legal trials over the years. "Google controls one-third of the global digital ad market and more than 40 percent of the U.S. market" (Levy, 2014). This large control of the ad market has made them the target of antitrust related complaints. Other companies are trying to limit the market share and power of Google to prevent them from becoming a monopoly.

Of the five threats facing Microsoft, new technologies and piracy are becoming a larger problem each day. Microsoft faces intense competition from companies like Google, Apple, and Yahoo who create new technologies that are introduced into the market. This is a major threat because these companies are taking over a portion of the market share. Another threat that faces Microsoft is piracy. Sometimes users pay for Microsoft Office online and may have purchased counterfeit versions of the software. Since this is a real threat that

equates to a lot of money lost by the company, Microsoft is committed to investigate and take action against anyone who sells counterfeit versions of their products.

E. FURTHER ANALYSIS

1. VULNERABILITIES

The crucial information stored, shared, and contained within the DOD creates multiple vulnerability challenges for both Google and Microsoft. Although some pieces of information are smaller than others, aggregated information could mean the life of a soldier/ sailor and citizens and rights they protect. The DOD houses tons of classified information that could be left vulnerable to hackers if the applications used are not safe and protected. Google recognizes that no system is 100% free of vulnerabilities, so they created the Google Vulnerability Reward Program. This program has been running continuously since November 2010, and offers a cash reward ranging from $100 to $20,000 for finding qualifying bugs (Google, 2016e). Some of the vulnerabilities Google is concerned about are "cross-site scripting, cross-site request forgery, mixed-content scripts, authentication or authorization flaws, and server-side code execution bugs" (Google, 2016e). To reduce risks and vulnerabilities, Google's data centers don't include unnecessary software or hardware; they are built and designed for applications (Google, 2016e).

The Chrome Rewards Program is another program which began "in January 2010 to help reward the contributions of security researchers who invest their time and effort in helping Google to make Chrome and Chrome OS more secure" (Google, 2016b). A reward of $100,000 is awarded to anyone who can crack a Chromebook or Chromebox while in guest mode (Google, 2016b). Other vulnerabilities Google is interested in are Sandbox Escape, Renderer Remote Code Execution, Universal XSS (local bypass or equivalent), Information Leak, and Download Protection bypass.

In January 2015, "Google launched the Vulnerability Research Grants Program with the goal of rewarding security researchers that look into the security of Google products and services" (Google, 2016g). The program provides grants to users who conduct research to improve Google's security, services, and features.

Microsoft's approach to vulnerabilities is a little different than Google's in that Microsoft provides security tools and downloads for users. These tools are used to detect, deploy, and prevent vulnerabilities in the system. One tool used for detection is the Microsoft Baseline Security Analyzer (MBSA), which is "an easy-to-use tool that provides a streamlined method to identify missing security updates and common security misconfigurations" (Microsoft, 2016a). Another tool used for deployment is Windows Server Update Services (WSUS), which "enables IT administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system" (Microsoft, 2016a). One of Microsoft's prevention tools is the Malicious Software Removal Tool, which "checks computers for infection, prevalent malicious software, and helps remove the infection if found" (Microsoft, 2016a).

2. COST

One of the main reasons we have conducted this research is to help the DOD become more cost efficient in the use of its service contracts. The Army has been using Google Apps since 2013 in order "to reduce its IT costs while giving troops access to always up to date, web tools for productivity, collaboration and communication" (Sullivan, 2013). However, it was not simple comparing the prices for Google and Microsoft, as Microsoft Office offers multiple features, which you can piece together to make your perfect productivity suite for your office. Derrick Wlodarz, from Betanews.com, has the best comparison parameters for large business enterprises, such as the DOD, which are highlighted in Figure 10 (Wlodarz, 2015). The largest problem with comparing costs between Google and Microsoft is comparing Microsoft's pre-installed software to Google Apps cloud based software. Google Apps direct Microsoft competition is Office 365. Office 365 is Microsoft's cloud-based productivity tool created to compete directly with Google Apps. Additionally, for the purposes of this comparison in cost structure, Google Apps for Work and Google Apps for Work (w/Vault) have the same price structure as Google Apps for Government and Google Apps for Government (w/Vault). Both Google App versions offer the same features with the exception of certain security protocols.

The first major cost difference between Google and Microsoft is the cost structure. Google is very straightforward with two pricing options for DOD usage, the main

productivity suite and the main productivity suite with additional storage. In contrast, Microsoft offers nine different cost structures for its productivity suite. The DOD is a dynamic entity, and only having two cost structures versus nine cost structures seems like an obvious choice for cost savings. As represented in Figure 10, Google offers the same benefits for both plans and the price change represents additional storage, while Microsoft changes with storage and program configuration difference.

	Office 365 E1	Office 365 E3	Google Apps for Work	Google Apps for Work (w/ Vault)
Max Users on Plan	Unlimited	Unlimited	Unlimited	Unlimited
Cost / User/ Month (1yr agreement)	$8.00	$20.00	$4.17	$10.00
Email Storage	50GB	50GB	30GB (shared w/ Drive + Photos)	Unlimited (5+ users needed)
Email Encryption	Add-on for $2.00/ user/mo	Included	Third Party add-on for $2.92/user/mo	Third Party add-on for $2.92/user/mo
Email Archiving & Legal Hold	Add-on for $3/user/ mo	Included	N/A	Included
Outlook Support	Native; full sync	Native; full sync	Google add-on limited sync	Google add-on limited sync
Personal Cloud File Storage	OneDrive for Business w/ 1TB per user	OneDrive for Business w/ 1TB per user	Google Drive w/ 30 GB per user (shared w/ Gmail + Photos)	Google Drive w/ 30 GB per user (shared w/ Gmail + Photos)
Enterprise Cloud File Storage	SharePoint Online (10GB + 500MB/ user)	SharePoint Online (10GB + 500MB/ user)	N/A	N/A
Company Intranet	SharePoint Online	SharePoint Online	Google Sites	Google Sites
PC & Mac Office Suite	N/A	MS Office for PC/ Mac on (5) Systems per user	N/A	N/A
Phone/Tablet Office Suite	N/A	MS Office on (5) phones & (5) tablets per user	Google Docs (Andriod/iOS only)	Google Docs (Andriod/iOS only)
Online Meetings	Office Online	Office Online	Google Docs	Google Docs
Social Networking	Skype for Business (250 user max)	Skype for Business (250 user max)	Hangouts (15 users max)	Hangouts (15 users max)
HIPAA Compliance	Yammer	Yammer	Google+ for Work	Google+ for Work
Support	Yes; All Services	Yes; All Services	Yes; Limited	Yes; Limited
	24/7 phone + email	24/7 phone + email	24/7 phone + email	24/7 phone + email

Figure 10. A Comparison of Google Apps and Microsoft Office Pricing. Adapted from Wlodaz (2015).

From Figure 10, it would appear that Microsoft wins for the cost-benefit comparisons for storage; however, when you look more closely at cloud storage plus email storage capacity, and take into account that most DOD Google contracts would service more than five employees, Google ends up on top (Wlodarz, 2015). Google's storage cap does not include documents created using Google's set of apps or files shared with a user by other Google Drive users (Singleton, 2016).

The cost-benefit analysis of Google versus Microsoft in terms of email application is a toss-up. Microsoft Outlook is very robust and has the organizational functionality one needs in a collaborative environment, such as the environment the DOD operates in on a day-to-day basis. While Google's Gmail has unlimited storage, it is fast and boasts a power search engine that Outlook does not come close to achieving. Additionally, Google's popularity gives the user a "huge range of third-party apps available for it which adds all manner of useful functionality to" Gmail (Singleton, 2016).

On average, the DOD spends approximately $617 million on Microsoft licensing for over two million users (Greene, 2013). If you serviced the same amount of customers with a cloud computing productivity suite, as displayed in Figure 10, Google would clearly be the winner purely based on dollar per user. However, while Google does succeed in the promising entry-level price point, the additional add-on features and the ability to pick, choose, and customize your office give Microsoft the upper hand.

3. RELIABILITY

For the DOD, Microsoft or Google's ability to be available and work when it is needed is what makes it truly reliable. DOD agencies operate year-round; therefore, the data and applications used are required to work at all times. Have you ever tried to Google something and Google wasn't available? "Google guarantees 99.9% uptime and build-in a robust disaster recovery, so there is never a concern about natural disasters" (Google, 2016a). Google has a Site Reliability Engineering team who "is responsible for availability, latency, performance, efficiency, change management, monitoring, emergency response, and capacity planning" (Google, 2016c).

According to Microsoft's Chief Reliability Strategist, David Bill, reliability is "trustworthy computing which focuses on creating and delivering secure, private, and reliable computing experiences based on sound business practices" (Microsoft, 2016b). Users question the reliability of Microsoft's cloud due to the recent Skype outage which runs on Microsoft Azure. Without the assurance that the system will work when needed, and if the software is considered too risky, people will avoid the new features and will chose to use Microsoft Office less (Saran, 2016).

F. HOW FINDINGS RELATE TO RESEARCH QUESTIONS

1. In What Instances Is It Appropriate to Use Freeware as the Primary Productivity/Mobile Office Software (i.e., Microsoft Office Versus Google Apps)?

Google Apps, which is a type of freeware, is appropriate to use as the primary productivity/mobile office software in almost all areas of the DOD. Google Apps has proven to be reliable with its 99.9% uptime guarantee; therefore, it can be used in most areas that Microsoft Office is currently being used by average daily users. Google's two-step security verification and secure infrastructure makes it very reliable for users within the DOD. In areas where a more advanced application is needed by users who need technical functions to complete specific tasks, it would be appropriate to use Microsoft Office.

2. What Are the Relevant DOD Cost Savings for Freeware Integration and Cloud Computing?

Some of the relevant cost savings the DOD could experience with freeware integration and cloud computing include four major points: decrease in physical file storage requirements, adaptability to dynamic working environments, security, and robust collaboration tools. Google Apps meets those needs and provides them at a streamlined cost. With additional access to government and public third-party applications in conjunction with Google Apps, the possibilities for Google Apps as a leading productive suite are endless.

3. To What Level Is Freeware Supported?

The use of freeware can be supported within the DOD. There are currently over 30 government agencies that use Google Apps as their office productivity suite, and this number is continuing to increase. Google Apps "meets the most demanding government data security requirements, including FedRAMP certification and compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)" (Google, 2016a).

4. Are There Any Significant Security Threats While Using Freeware?

No software is 100% free from security risks; therefore, there are always going to be some threats to freeware. The DOD realizes that there are always some risks involved when using any kind of software. Google has identified some areas of concern, such as "cross-site scripting, cross-site request forgery, mixed-content scripts, authentication or authorization flaws, and server-side code execution bugs," and is actively pursuing resolution (Google, 2016e). Currently, there are no significant security threats found while using freeware.

G. SUMMARY

Chapter IV illuminates the pros and cons of choosing Microsoft Office or Google Apps as a primary productivity suite for the DOD. Through SWOT analysis and an evaluation of the costs, Google looks like a clear choice for the DOD's choice of productivity suite because it would save up to $12 billion a year. However, when you dig deeper into comparing the vulnerabilities for mitigation strategies and cost and reliability controls employed by both tools, Google and Microsoft are fairly well matched. This makes sense as Google and Microsoft have been each other's competition for multiple years. Google Apps has been using and promoting cloud-based programming to a larger audience for more years than Microsoft, and the "emerging employee demographic" will force the DOD to make uncomfortable changes in order to stay current with emerging technologies and user preference (Boulton, 2016).

Chapter V highlights our recommendations to the DOD for productivity suites as well as suggestions for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

The primary objective of this research project was to determine when or if it would be appropriate for the DOD to use freeware as their primary productivity office suite. While researchers originally tried to stay within the scope of a singular command, the paper's concepts shifted to a more fundamental examination of SWOT for all of the DOD. The research provided the relevant DOD cost savings and the level at which freeware is supported, and researchers searched for but found no significant security threats while using freeware. Although Google Apps has become the primary productivity suite at multiple commands throughout the Navy, Army, and Air Force, the researchers also completed a broad comparison of Google Apps and Microsoft Office as a primary productivity suite.

The previous chapters provided background and a literature review. Chapter III discussed how the data was collected and the overall methodological thought process. Chapter IV highlighted key strengths, weaknesses, opportunities, and threats for the use of Microsoft Office and Google Apps within the DOD. Additionally, researchers categorized three important criteria for choosing a productivity suite in the DOD: vulnerabilities, cost, and reliability. Chapter V provides a summary of the research, conclusion, and recommendations for future research.

A. RESEARCH SUMMARY

This research provided an analysis of the appropriate use of freeware software, like Google Apps, within the DOD. Furthermore, the research sought to identify freeware, regulations and certifications requirements, and any significant security threats.

The researchers posed the following four questions.

1. In What Instances Is It Appropriate to Use Freeware as the Primary Productivity/Mobile Office Software (i.e., Microsoft Office Versus Google Apps)?

Researchers deemed Google Apps is appropriate to use in almost all areas of the DOD based on evidential proof of Google's availability and reliability. Users who need the technical specifications of office productivity software may have to rely on Microsoft Office

to suit their needs or have the option of enhancing their Google Apps experience with third party add-ons that provide some of the more advanced features of Microsoft Office.

2. What Are the Relevant DOD Cost Savings for Freeware Integration?

Google Apps would provide the DOD with major cost savings after a short migration and transition from the Microsoft Office Suite. Version control would significantly decrease security issues and reliability issues, while Google's cutting edge collaboration tools would bolster interagency and multinational partnerships.

3. To What Level Is Freeware Supported?

The research indicated that there are certifications and regulations currently in place for the use of freeware within the DOD; therefore, freeware is supported. FedRAMP was the primary example for this research paper on Google Apps as it covers the security and certification requirements for all cloud-based computers programs. Google Apps filed its authorization request in 2014 and became an authorized program in 2016 (FedRAMP, n.d.-a).

Research also indicated that should the DOD choose to expand into the use of freeware for other systems that are not cloud based, there would need to be a revision of the instructions that regulate software usage, implementation, and authorization within the DOD.

4. Are There Any Significant Security Threats While Using Freeware?

Ultimately, the research concluded that there are no significant threats to freeware. However, there are always minor threats present at all times. It is virtually impossible to be 100% free from risks of cyber threats.

B. CONCLUSION

Google Apps could revolutionize the DOD's productivity and cut down on annual licensing and security costs, creating a drastic ripple effect on the focus of dollars and personnel management. While multiple commands within the DOD have already begun the transition to Google Apps, Microsoft Office is still the primary productivity suite of choice. As Microsoft begins to hone its collaboration tools, Google Apps provides the DOD with a collaboration capability, formally created and managed in house, born and cultivated from

the beginning of Google's creation. This mindset and additional years of experimentation, development, and refining puts Google steps above Microsoft's attempt to catch up to complete cloud management. While these new tools provide a freedom to DOD operations, acceptance of Microsoft to Google could be an issue. While making major changes in the primary and commonly utilized IT system, there is an expectation for three groups of people to emerge. These three groups include people who welcome change, people who hate change and dislike anything that is different, and finally, people who are in the middle and just want to get their job done (High, 2016). As long as the DOD and Google highlight the new features and time-saving methods, as well as ensure compatibility with other programs that rely on Microsoft, then a majority of the personnel may not be as opposed to the migration. The cost efficiency found with switching to Google Apps also assumes that the DOD would not renew its licensing contracts with Microsoft; therefore, until integration was achieved, there would be a double cost incurred.

C. RECOMMENDATION FOR FURTHER ACTION/RESEARCH

Recommendations for further research include readdressing this thesis with DOD commands that have completely migrated to Google Apps. Additionally, another recommendation for further research includes an in-depth look at the capabilities of Microsoft 365, primary vulnerabilities of cloud computing, and increased international collaboration through cloud-based tools.

The DOD would benefit from further research on the actual cost savings experienced from the commands that have migrated, as well as the lessons learned by the workforce during the change. An interesting topic to research that might provide more clarity to the topic would include researching the DOD's initial migration to Microsoft as the primary productivity suite. The idea of creating an organization-wide common tool is something that the entire DOD still struggles with today; however, it is clear that Microsoft has become the brand of choice for basic office management.

Additionally, the benefits of researching further into the ramifications or implications of cloud computing and mobile technology, from the aspects of security and mobility for DOD units, would be a beneficial topic. This topic could specifically address Special Warfare, or simply look at the bandwidth requirements that are expected when using cloud

computing for Naval afloat units. If the Navy transitioned to Google Apps as its primary productivity suite, how reliable would this new software be in an "unplugged" environment?

Another form of research that would take more of a human interest piece would be on IT culture within the DOD. The IT culture within the DOD would largely determine the acceptance of new emerging technologies within the DOD and possibly determine the success or failure of integration into a cloud-based solution for the primary productivity suite or collaborative future tool for the DOD.

The future of the DOD is cloud computing, and it is our job as stewards of the future to ensure we are utilizing and integrating this tool to the best of our ability.

LIST OF REFERENCES

Boulton, C. (2016, April 15). Millennials force CIOs to rethink tech, training processes. *CIO.* Retrieved from http://www.cio.com/article/3056785/cio-role/millennialsforce-cios-to-rethink-tech-training-processes.html

Cabot Technology Solutions Inc. (2016). Open source solutions. Retrieved from https://www.cabotsolutions.com/services/open-source-solutions/

Chief Information Officer, Department of Defense (DOD). (2009). DOD open source software (OSS) FAQ. Retrieved from http://dodcio.defense.gov/Open-Source-Software-FAQ/#Q:_Are_.22non-commercial_software.22.2C_.22freeware.22.2C_or_.22shareware.22_the_same_thing_as_open_source_software.3F

Cooksey, G., Miller, B., & Moore, F. (2006). An empirical study of the robustness of MacOS applications using random testing. Retrieved from http://ftp.cs.wisc.edu/pub/paradyn/technical_papers/Fuzz-MacOS.pdf

Corbin, K. (2013, September 4). Microsoft in "2-horse race" for government cloud contracts. *CIO.* Retrieved from http://www.cio.com/article/2382806/government/google--microsoft-in--2-horse-race--for-government-cloud-contracts.html

Daly, J. (2013, November 11). Defense Department is the latest agency to move to Google Apps. *FedTech*. Retrieved from http://www.fedtechmagazine.com/article/2013/11/defense-department-latest-agency-move-google-apps

Delio, M. (2004, December 14). Linux: Fewer bugs than rivals. *Wired.* Retrieved from http://archive.wired.com/software/coolapps/news/2004/12/66022

Department of Defense. (2014, March 12). *Risk management framework (RMF) for DOD information technology (IT)* (DOD Instruction 8510.01). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

Department of Defense Enterprise Software Initiative. (2009, December 22). What is cloud computing and how does it impact software licensing practices? Retrieved from http://www.esi.mil/contentview.aspx?id=215

Department of Defense Enterprise Software Initiative. (2015, November 30). Renewal of DON Microsoft enterprise licensing agreement signed. Retrieved from http://www.esi.mil/contentview.aspx?id=659

Department of Defense ESI Navy Software Program Managers. (2016, November 15). Enterprise software agreements: Discounted savings for DOD components, intel community. *CHIPS.* Retrieved from http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=2392

Espadanal, M., & Oliveria, T. (2012). *Cloud Computing Adoption by firms*. Paper presented at Mediterranean Conference on Information Systems (MCIS). Retrieved from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1029&context=mcis2012

FedRAMP. (n.d.-a). The Federal Risk and Management Program Dashboard. Retrieved from https://marketplace.fedramp.gov/index.html#/product/google-services?sort=productName&productNameSearch=goog

FedRAMP. (n.d.-b). FedRAMP. Retrieved from https://www.fedramp.gov/about-us/about

Foley, M. J. (2013, October 13). Microsoft Office 365 and Google Apps face off in DOD contract. *ZDNet.* Retrieved from http://www.zdnet.com/article/microsoft-office-365-and-google-apps-face-off-in-dod-contract/

Forrester, J. E., & Miller, B. P. (2002, June 19). An empirical study of the robustness of Windows NT applications using random testing. Retrieved http://pages.cs.wisc.edu/~bart/fuzz/fuzz-nt.html

Free Software Foundation. (2016a). Categories of free and nonfree software. Retrieved from https://www.gnu.org/philosophy/categories.html

Free Software Foundation. (2016b). Free software is more reliable. Retrieved from https://www.gnu.org/software/reliability.en.html

Free Software Foundation. (2016c). Free software movement. Retrieved from https://www.gnu.org/philosophy/free-software-intro.html

Free Software Foundation. (2016d). What is free software? Retrieved from https://www.gnu.org/philosophy/free-sw.html

Free Software Foundation. (2016e). Why open source misses the point of free software. Retrieved from https://www.gnu.org/philosophy/open-source-misses-the-point.html

Gil, P. (2016, January 23). "SaaS": What is "software as a service"? Retrieved from http://netforbeginners.about.com/od/s/f/what_is_SaaS_software_as_a_service.htm

Gillette, S. (2012). *Cloud Computing and Virtual Desktop Infrastructures in Afloat Environments* (Master's thesis). Retrieved from http://calhoun.nps.edu/bitstream/handle/10945/7349/12Jun_Gillette.pdf?sequence=1

Goldstien, P. (2016a, September 14). DOD, Service Branches Say Cloud Migrations Will Depend on Missions, Interoperability, *FedTech Magazine*. Retrieved from http://www.fedtechmagazine.com/article/2016/09/dod-service-branches-say-cloud-migrations-will-depend-missions-interoperability

Goldstien, P. (2016b, October 10). FedRAMP Scores a Cloud Victory, as Microsoft Gets a Speedy Approval | FedTech Magazine. Retrieved from http://www.fedtechmagazine.com/article/2016/10/fedramp-scores-cloud-victory-microsoft-gets-speedy-approval

Google. (2016a). Benefits—Google Apps for Government. Retrieved from https://gsuite.google.com/industries/government/

Google. (2016b). Chrome Rewards – Application Security – Google. Retrieved from https://www.google.com/about/appsecurity/chrome-rewards/

Google. (2016c). Google - Site reliability engineering. Retrieved from https://landing.google.com/sre/interview/ben-treynor.html

Google. (2016d). Google 2-step verification. Retrieved from https://www.google.com/landing/2step/

Google. (2016e). Program Rules – Application Security – Google. Retrieved from https://www.google.com/about/appsecurity/reward-program/

Google. (2016f). Use less data with Chrome's Data Saver - Chrome Help. Retrieved from https://support.google.com/chrome/answer/2392284?co=GENIE.Platform%3DAndroid&hl=en

Google. (2016g). Vulnerability Research Grant Program Rules – Application Security – Google. Retrieved from https://www.google.com/about/appsecurity/research-grants/

Google. (2016h). Why Google's cloud infrastructure is right for your business. Google Cloud Platform. Retrieved from https://cloud.google.com/why-google/

Government Accountability Office . (2004). *Information technology: DOD's acquisitions policies and guidance need to incorporate additional best practices and control* (GAO-04-722). Retrieved from http://www.gao.gov/assets/240/233336.pdf

Government Accountability Office. (2016). *Cloud computing: Agencies need to incorporate key practices to ensure effective performance* (GAO-16-325). Retrieved from http://www.gao.gov/assets/680/676395.pdf

Grance, T., & Mell, P. (2011). *The NIST definition of cloud computing* (Special Publication 800–145). http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Guseva, I. (2009, March 26). Bad economy is good for open source. *CMS Wire*. Retrieved from http://www.cmswire.com/cms/web-cms/bad-economy-is-good-for-open-source-004187.php

High, P. (2016, May 31). Motorola Solutions' CIO Pushes IT To Drive Innovation. Retrieved from http://www.forbes.com/sites/peterhigh/2016/05/31/motorola-solutions-cio-pushes-it-to-drive-innovation/#17a9a4f1286b

Huger, J. (2016). What is open source software? Retrieved from https://opensource.com/resources/what-open-source

Jackson, J. (2011, November 3). Open source vs. proprietary software. Retrieved from http://www.pcworld.com/article/243136/open_source_vs_proprietary_software.html

Jurevicius, O. (2013, February 16). Microsoft SWOT analysis 2013 - Strategic Management Insight. Retrieved from https://www.strategicmanagementinsight.com/swot-analyses/microsoft-swot-analysis.html

Kelley, G. (2015, February 18). Microsoft Is The New Google, Google Is The Old Microsoft. Retrieved from http://www.forbes.com/sites/gordonkelly/2015/02/18/microsoft-google-swap/2/#6e1969561e4f

Krishnan, K. (2010, July 26). Introducing Google Apps for Government. Retrieved from https://googleblog.blogspot.com/2010/07/introducing-google-apps-for-government.html

Kundra, V. (2011, February 8). *Federal cloud computing strategy*. Washington, DC: U.S. Chief Information Officer. Retrieved from http://acmait.com/pdf/Federal-Cloud-Computing-Strategy.pdf

Levine, Y. (2014, March 4). The revolving door between Google and the Department of Defense. *Pando*. Retrieved from https://pando.com/2014/04/23/the-revolving-door-between-google-and-the-department-of-defense/

Levy, A. (2014, August 19). Five problems Google faces in the next 10 years. Retrieved from http://www.cnbc.com/2014/08/17/five-problems-google-faces-in-the-next-10-years.html

Linux Information Project. (2006). Freeware definition. Retrieved from http://www.linfo.org/freeware.html

Marzigliano, L. (2011, November 17). Goodbye DIACAP, hello DIARMF. Retrieved from http://resources.infosecinstitute.com/goodbye-diacap-hello-diarmf

McGarvey, R. (2014). Google Docs vs Microsoft Office: The Faceoff. *MainStreet.* Retrieved from https://www.mainstreet.com/article/google-docs-vs-microsoft-office-faceoff/page/2

Metcalfe, R. (2004, February 1). Top tips for selecting open source software. Retrieved from http://oss-watch.ac.uk/resources/tips

Microsoft. (2016a). Security tools & downloads for IT pros. TechNet Security. Retrieved from https://technet.microsoft.com/en-us/security/cc297183

Microsoft. (2016b). Trustworthy computing—Reliability. Retrieved from https://www.microsoft.com/en-us/twc/reliability.aspx

Microsoft. (2016c). Veteran Tech Training Programs | Microsoft Jobs After The Military. Retrieved from http://military.microsoft.com/paths/

Microsoft Azure Government. (2016). Azure government cloud computing. Microsoft Azure. Retrieved from https://azure.microsoft.com/en-us/overview/clouds/government/

Microsoft in Government. (2015, December 18). Try cloud solutions for government today. Retrieved from https://enterprise.microsoft.com/en-us/industries/government/start-your-microsoft-cloud-for-government-trial-today/

The MITRE Corporation. (2003, January 2). Use of free and open-source software (FOSS) in the U.S. Department of Defense. http://dodcio.defense.gov/Portals/0/Documents/OSSFAQ/dodfoss_pdf.pdf

Potter, T. (2012). *An evaluation methodology for the usability and security of cloud-based file sharing technologies* (Doctoral dissertation). Monterey, CA: Naval Postgraduate School.

Redman, C. (2016a, January 5). DIACAP vs. RMF: What's the difference? Retrieved from http://www.certifiedcyberassurance.com/diacap-vs-rmf-what-the-differance

Redman, C. (2016b, February 2). DOD Risk Management Framework (RMF): The tug-of-war begins. Retrieved from http://www.certifiedcyberassurance.com/dod-risk-management-framework-rmf-the-tug-of-war-begins/

Rosen, D. (2010, May 16). Open-source software is not always freeware. [Blog post]. Retrieved from http://blog.wolfire.com/2010/05/Open-source-software-is-not-always-freeware

Saran, C. (2016, September 22). Is Microsoft Office 2016 reliable enough for business? Retrieved from http://www.computerweekly.com/news/4500253928/Is-Microsoft-Office-2016-reliable-enough-for-business

Sdubois Contributions. (2010, August 9). Department of Defense. Retrieved from https://www.fsf.org/working-together/profiles/department-of-defense

Thompson, A. (2015, August 21). Google's SWOT Analysis & Recommendations - Panmore Institute. Retrieved from http://panmore.com/google-swot-analysis-recommendations

Vaughan-Nichols, S. (2009, October 29). Obama invites open source into the White House. *PCWorld*. Retrieved from http://www.pcworld.com/article/174746/obama_invites_open_source_into_the_white_house.html

Wheeler, D. (2011, August 5). How to evaluate open source software/free software (OSS/FS) programs. Retrieved from http://www.dwheeler.com/oss_fs_eval.html

Wheeler, D. (2015, July 18). Why open source software/free software (OSS/FS, FOSS, or FLOSS)? Look at the numbers! Retrieved from http://www.dwheeler.com/oss_fs_why.html#security

Wyld, D. (2010, January). The cloudy future of government IT: Cloud computing and the public sector around the world. *International Journal of Web & Semantic Technology* 1(1), 1–20. Retrieved from https://www.researchgate.net/profile/David_2/publication/45825704_The_Cloudy_Future_Of_Government_IT_Cloud_Computing_and_The_Public_Sector_Around_The_World/links/00b4953a31c25bf95f000000.pdf

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CA 93943

www.acquisitionresearch.net