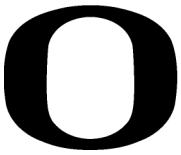
Presented to the Interdisciplinary Studies Program:



UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Security Strengths and Weaknesses of Virtualization as a Green Computing Solution

CAPSTONE REPORT

Joseph Esensten
Senior Information Security Engineer
Raytheon, Inc

University of Oregon
Applied Information
Management
Program

February 2011

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger
Senior Academic Director, AIM Program

Security Strengths and Weaknesses of Virtualization as a Green Computing Solution

Joseph Esensten

Senior Information Security Engineer

Raytheon, Inc

Abstract

Server virtualization technologies enable the data center to consolidate resources in order to improve efficiencies and save energy. This study explores security strengths and weaknesses of this technology within the context of green IT. Selected literature published from 2005 through 2010 is examined. Common attacks, security strengths, and security weaknesses are presented. Green benefits of virtualization and eight recommended security controls are identified to maximize nine positive security features, for use by IT security professionals.

Keywords: virtualization, virtualize, security, infosec, green IT, green computing, information security, energy savings, green technology, data center, security strengths, security weaknesses.

Table of Contents

List of Tables and Figures

Introduction to the Literature Review

Purpose

The purpose of this study is to identify ways in which virtualization can be used to enhance information security while simultaneously supporting green benefits, including energy efficiency and related cost reduction in the data center (Haletky, 2009; Lamb, 2009; Liao, Hu, & Jin, 2010; Webber & Wallace, 2009). Virtualization is defined as software which "enables enterprises to partition a single server into multiple virtual machines" (Virtualization Products, 2007, p. 23). Information Security is the protection of information systems and data from unauthorized use, tampering, destruction and disruption (Public Printing and Documents, 2010). Energy efficiency refers to the "delivery of the same or better service output with less energy input" and is examined within the context of the data center (Lamb, 2009, p. 30). A data center is defined by the US Environmental Protection Agency as a facility which is primarily used for data processing, storage and communications networking (2007).

The focus of the study is on two areas: (a) identification of security strengths and weaknesses of virtualization technologies including identification of mitigating factors and controls, and (b) identification of what are termed *green benefits* of virtualization (Energy Star, 2007). The intent is to provide the audience for this study with information which enables virtualization to be implemented in a manner which maximizes positive security features while ensuring energy savings, as part of a green IT strategy. In this study, the notion of a positive security feature in any particular system technology refers to a security threat that can be mitigated without the need of adding on additional security controls (Mattord & Whitman, 2008). The concept of green IT strategy refers to a corporate undertaking to focus resources upon reducing energy consumption and waste of information technology assets in order to meet

regulations, reduce costs, and satisfy stakeholder demand for social responsibility (Esty & Winston, 2009).

Understanding the security strengths and weaknesses of a specific technology requires a formal risk assessment process (Harris, 2010). Regardless of the specific business or industry, the risk assessment accounts for the identification of assets, the identification of threats, the identification of vulnerabilities, the impact upon the business, and the placement of controls (Harris, 2010; Mattord & Whitman, 2007). Even without assigning value to assets or evaluating a realized threat's impact on the company, risk analysis can still provide valuable threat and vulnerability data about information systems. The National Institute of Standards and Technology (NIST) provides a risk assessment methodology to evaluate IT risk called Special Publication 800-30, which is available for public use (2002). This nine step methodology is utilized in this study to help frame the presentation of the results of the data analysis process, but modified to use only four steps in order to meet the intent of this study, without compromising the validity of the assessment. Steps one through four of NIST SP 800-30 are used to provide (a) system characterization, (b) threat identification, (c) vulnerability identification, and (d) control analysis (NIST, 2002). Step one of the risk assessment process defines the boundaries of the IT system in question (NIST, 2002). Step two identifies possible threats to the system and step three matches those threats to weaknesses of the IT system (NIST, 2002). Step four proposes a set of controls which, if implemented, could prevent the identified threats from causing harm to the system (Harris, 2010; NIST, 2002). The output of this process is a risk matrix which can be used by IT Managers to improve decision making regarding IT assets (Harris, 2010; Mattord & Whitman, 2007).

Problem

Green IT. "The reality of rising energy costs coupled with the increased concern over the global warming climate crisis and other environmental issues –have shifted the social and economic consciousness of the business community" (Lamb, 2009, p. 15). This shift in consciousness has made many business leaders select information technology hardware and software which is cleaner for the environment and in turn more economically and socially conscious, also known as *green IT*. Business leaders are selecting technologies such as virtualization in order to lower their environmental impact (Manning, 2010). This move is twofold as it both reduces costs for the company, but also satisfies stakeholder demand for cleaner, more efficient operations.

Green IT in the data center. Technologies such as virtualization are being implemented on a large scale by businesses and education to meet increasing demands to minimize their power footprint (Stuenkel, 2009; The top 12 green-IT vendors, 2008). Virtualization, though effective in meeting the goals of green IT is not a silver bullet and poses its own unique security related challenges (The top 12 green-IT vendors, 2008). Security professional Michael Hoesing (2009) alludes to one of these security challenges: "the complexity of virtual environments, as well as the ease and speed in which a new virtual machine can be created, have increased the impact and likelihood of unfavorable events" (p. 2). Analysis of the security strengths and weaknesses of virtualization is necessary to ensure a business' information security posture is not compromised by either a malicious attack, such as a hacker, or by other phenomenon, such as a blackout (Harris, 2010).

Risk assessment. Virtualization technology within the realm of green IT is analyzed in this study for risk in order to present a picture of potential strengths and weaknesses. The process of risk assessment is used to identify vulnerabilities and threats and is used to assess the possible

impacts upon the system (Harris, 2010). The entire risk assessment process is outlined in Figure 1. It is an iterative process which builds each step upon the foundation of the previous to form a complete picture of the risk facing an IT asset (Harris, 2010; Mattord & Whitman, 2007; NIST 2002). The risk assessment methodology follows a generally accepted framework provided by NIST SP800-30 (NIST, 2002). NIST (2002) defines a set of nine steps which are followed to determine risk. Steps are listed briefly below, followed by a visual representation of the process (see Figure 1).

- System characterization: defines the boundaries of the IT system, inputs and outputs and the system resources (NIST, 2002).
- Threat identification: identifies potential sources of threats, their attack vector, and their possible impact upon the system (NIST, 2002).
- Vulnerability identification: identifies system security weaknesses based upon the system environment which could be exploited by identified threats (NIST, 2002).
- Control analysis: identifies current or planned controls to eliminate the likelihood of a threat exploiting a vulnerability (NIST, 2002).
- Likelihood Determination: the chance that a potential vulnerability will be exploited by a threat given in high, medium, or low (NIST, 2002).
- Impact Analysis: the determination of the adverse affects that a realized threat will have after exploiting a vulnerability (NIST, 2002).
- Risk Determination: assesses the overall level of risk to an IT system given the previous steps (NIST, 2002). Expressed in a matrix of impact versus likelihood (NIST, 2002).

- Control Recommendations: identifies security controls which could mitigate the identified risks (NIST, 2002).
- Results Documentation: the presentation of the risk analysis results in official report or briefing (NIST, 2002).

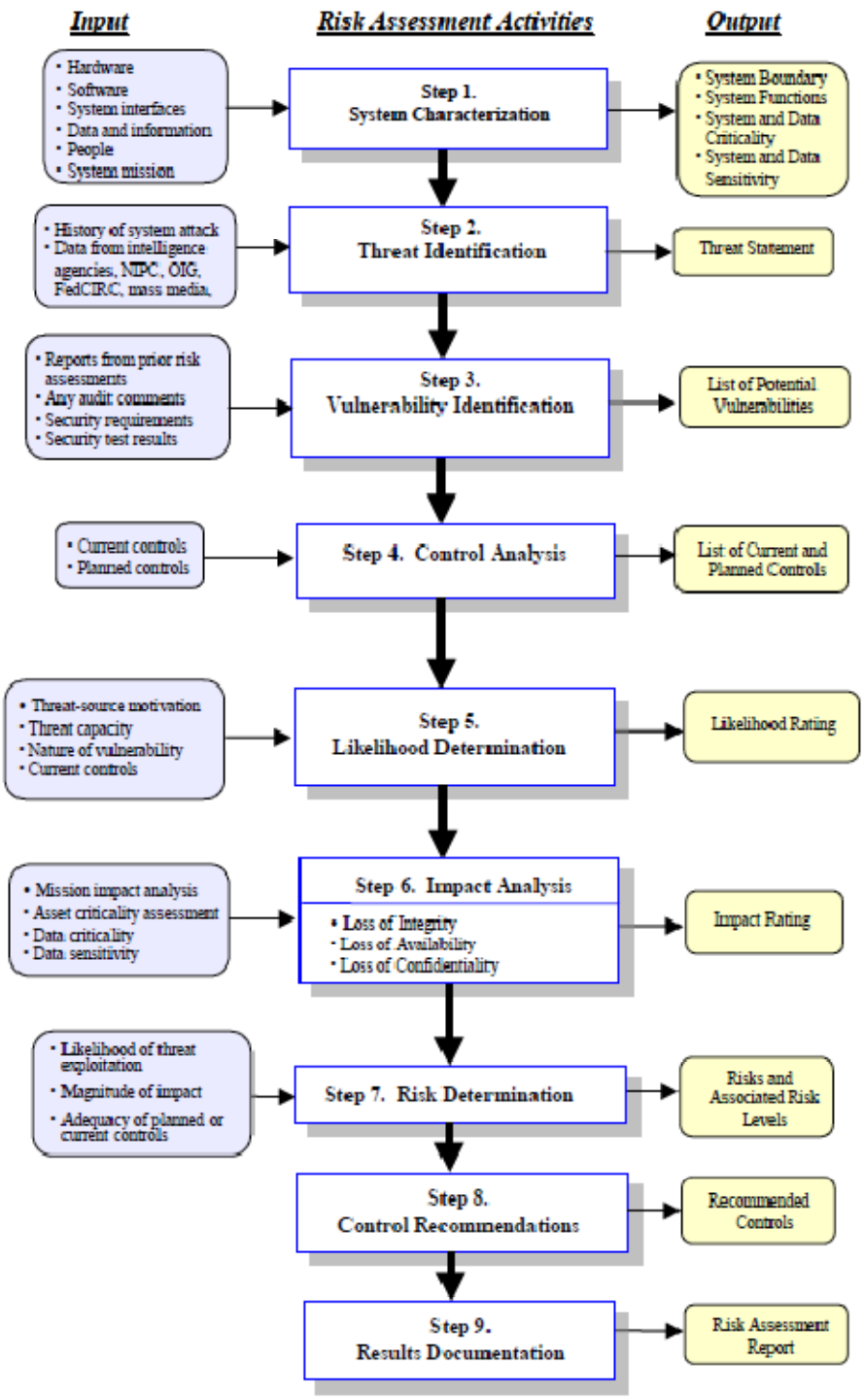


Figure 1. NIST 800-30 Risk Assessment Process

A framework for positive security features. Security strengths are determined after the identification of security threats during a risk assessment. Security threats which can be

mitigated without the need of additional security controls become positive security features of virtualization. An example of a positive security feature of virtualization is given in *The Virtualization Solution* (Cohen, 2010). Cohen states that a breakdown in one virtual environment does not affect the security in another virtual environment (2010). The author concludes that this inherent ability of virtualization to isolate one environment from another is a security strength (Cohen, 2010). The core structure of virtualization provides mitigation of the security threat, in this case an attack against a neighboring guest OS, rather than an emplaced security control (Cohen, 2010; Harris, 2010).

Significance

"Worldwide, servers require about 14 power plants and, combined with cooling, contribute about 200 million metric tons of CO2" to the atmosphere, according to Green IT columnist Kirk Cameron (2009, p. 101). CO2 emissions are the main cause of global warming and are continuing to rise according to the Intergovernmental Panel on Climate Change (2007). Additionally, electrical costs are rising due to worldwide shortages of coal, oil, and other fossil fuels (Tomlinson, 2010). In a 2007 Environmental Protection Agency study of data centers, "more than one-third (38 percent) of electricity use is attributable to the nation's largest and most rapidly growing data centers" (p. 10). Figure 2 shows rapidly rising energy usage in data centers if left unmitigated by controlling factors (Energy Star Program, 2007).

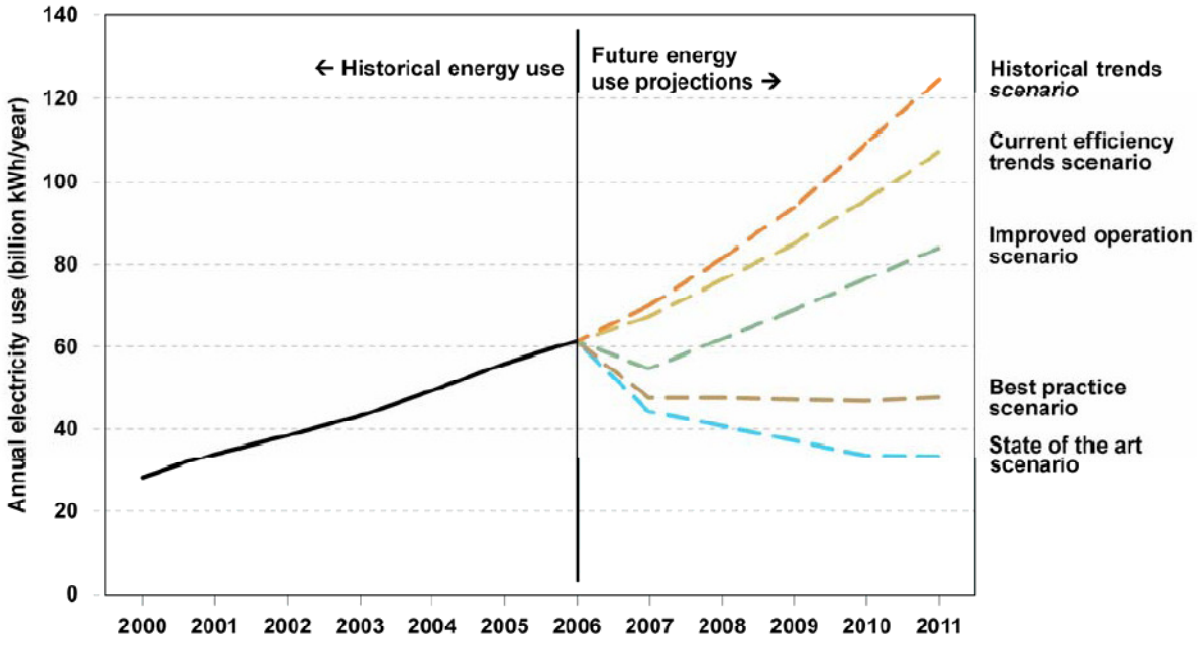


Figure 2. Comparison of projected electricity use in data centers (Energy Star Program, 2007).

Businesses are looking for new ways to reduce their energy usage to lower costs (Sinnett, 2010). The solution in recent years has been to virtualize servers to reduce the impact of global warming and rising energy costs (Webber & Wallace, 2009).

Virtualization is the first and most important step in consolidating servers and reducing energy usage in the data center (Lamb, 2009). In recent research, virtualization was found to provide an energy savings, when deployed in clusters, of up to 78 percent (Liao, X., Hu, L., Jin, H., 2010). Virtualization not only provides cost savings, but also provides additional benefits such as improved utilization, manageability, and reliability of systems (Uhlig et al., 2005). Along with these benefits is also added security features due to an abstraction layer between the virtual servers and the physical host server, offering isolation (Carpenter, Liston & Skoudis, 2007).

However, virtualization also "introduces its own security problems into the mix that composes the data center" (Haletky, 2010, p. xvii). "Enterprise requirements, for example, in

terms of application availability, performance and security, are not addressed by virtualization solutions" (Peles, 2008, p 22). Virtualization expert Edward Haletky (2010) states that "the introduction of virtualization will dramatically change the security stance of even the most secure environments" (2010, p. xvii).

A 2009 report published by the Internet Crime Complaint Center, reports $559.7 million nationwide of loss due to cyber crime. Additionally, the Computer Security Institute reported businesses in 2006 lost over $52,494,290 to security related losses (Harris, 2010). This data shows a clear need for robust security features of IT assets in order to prevent loss. It is therefore critical that virtualization technologies are understood by the business in terms of their security strengths and weaknesses (Haletky, 2010).

Audience

The study is written primarily for the business environment in which data centers are deployed to provide services to internal and external users (Energy Star Program, 2007). The primary reader is designated as an IT executive or his or her advisor in the process of making a decision to implement or expand the use of virtualization in the data center in an effort to improve energy efficiency (Cameron, 2009). It is also intended to be used by IT decision makers such as project managers, CIOs, CISOs and security managers specifically for the enhancement of knowledge regarding virtualization security for the purpose of procurement, integration, upgrade, or maintenance of virtualization technologies (Hewlett Packard, 2007). This study provides those selecting and implementing virtualization a set of security strengths and weaknesses with which to compare to their organizational security posture (Mattord & Whitman, 2008). This allows virtualization to be implemented in a way which leverages the strengths of

virtualization and allows security controls to be implemented to mitigate the security weaknesses.

Outcome of Study

This study is designed as a guide that briefly describes (a) the general factors affecting the green IT movement, (b) virtualization as a green IT solution in the data center, and (c) the security strengths and weaknesses of virtualization. The outcome of the study includes tables which present the reader with actionable options for virtualization architecture implementation that ensures the green benefits that are realized are also secure (Energy Star Program, 2007). Tables are built from the data derived from the *data analysis* which includes security strengths, security weaknesses, and green advantages of virtualization technology. The data set, which includes security weaknesses, is matched against recommended security controls from NIST, DISA, and VMWare and provides a suggested control to mitigate each identified weakness (DISA, 2008; Haletky, 2010; NIST, 2009). The tables provide the reader with a set of virtualization: (a) green advantages, (b) security strengths, (c) security weaknesses and suggested controls. These tables are supported by text which follows the form of a risk assessment based upon the data (NIST, 2002).

The intent is that the four steps of the risk assessment completed in this study can be used by enterprises to begin or update their own risk analysis processes (NIST, 2002). This feature of this study can save businesses time and effort in virtualization implementation efforts. Risk analysis steps one through four, as presented in NIST 800-30, are driven by the data analysis. Results are presented using the framework of NIST SP800-30 steps one through four as a way to ensure that resultant data is as focused as possible at providing the intended information for the audience. NIST methodologies are in use by both public and private sectors and among a wide

breadth of industries, lending further credibility to the process (NIST, 2002; NIST, 2009). Utilization of the four NIST risk analysis steps allows for a common language between disparate audiences and provides structure to the results (NIST, 2002).

The goal is to support analysis to determine if the costs of the security feature sets of virtualization outweigh the benefit of the green savings for a particular virtualization implementation. This study is meant to lay the framework for further studies which may pursue analysis and determination of the cost and benefit analysis mentioned previously. This study does not seek to answer this question directly.

Research Delimitations

Time frame. The references chosen for this study, with one exception, are all chosen with a date from January, 2005 and later. This range gives the study a full five year window of information to pull from. The one exception to this rule is *NIST SP800-30* dated 2002. This exception is allowed because this government regulation is still current and enforced at the time this study is written. Given the rapid pace of technology change and the expansion of virtualization as an enterprise solution, the five year time gap is the maximum allowable tolerance (Haletky, 2010). The intent of this decision is to ensure that only timely and accurate information is used to prepare the study as well as to ensure the study would be relevant for current applications.

Selection and evaluation criteria. Given the wide range of materials available in green IT, security and data center technologies fields, a methodic strategy is needed to define what sources should be chosen for this study (Bell & Smith, 2007). As noted by Lester and Lester (2007), “only carefully selected material that is pertinent to the argument” is selected and used in this study (p 111). Creswell (2009) presents a method for prioritizing and selecting literature

with the following precedence, in order: journal articles, books, recent conference papers, dissertations and finally, the Internet. Authors who are considered industry experts, have published in peer-reviewed journals, white papers, books, and industry publications are considered credible literature for this work. Publications by businesses are considered only if they are relevant to the topic and present data which is not specific to the product they represent. Regulatory and governmental documents are considered valid as long as they are still current under the law. Literature that does not meet the defined criteria is not included in the study. Literature not available to the general public without a fee is also not included in the study.

Focus. Literature for this study is selected that addresses one of three critical content areas, with overlap as much as possible: (a) green IT (b) virtualization (c) information security. Haletky (2010) writes "virtualization is redefining the charter of security and causes us to think within the context of solving enterprise architecture and business problems" (p. xvi). This study does not explore, except as a reference, specific virtualization brandings**,** virtualization of non-server technologies such as storage virtualization, attacks that do not directly affect virtualization-specific architecture such as network attacks, hardening procedures for virtualization technologies. It also does not explore facets of virtualization technology that are outside the realm of green IT such as high availability (HA) (Peles, 2008).

The first goal of the study is to provide executive IT leadership with knowledge of the security strengths and weaknesses of virtualization technology within the context of green IT. The second goal is to identify possible attacks against virtualization technologies (Haletky, 2010). The third goal of the study is to provide possible security controls and mitigation strategies for identified security weaknesses. The fourth goal is to present data that supports

virtualization as a viable, secure solution for business leaders to implement in order to solve green IT challenges (The top 12 green-IT vendors, 2008).

Selection of the NIST risk assessment methodology. The risk assessment methodology selected for use in this study is chosen from among many viable candidates presented in the literature. The list of candidate methods includes NIST 800-30, NIST 800-66, FRAP (Facilitated Risk Analysis Process), OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), and AS/NZS 4360 (Harris, 2010). NIST 800-30 is chosen because it is widely implemented for both government and private sectors, giving the widest and most relevant evaluation of risk for a variety of enterprise data centers users (Harris, 2010). The methodology follows a generally accepted framework provided by NIST SP800-30 (NIST, 2002). NIST (2002) defines a set of nine steps to determine risk. Only four steps of the total nine are used for this study. Further risk analysis procedures determine asset value, likelihood of impact, recommend controls and present a total risk analysis (NIST, 2002). These additional steps are not addressed as they do not provide any additional value to the outcome of this study. This methodology supports this study by providing a guide with which to correctly identify security strengths and vulnerabilities in a manner which is acceptable by the IT security community. Following NIST guidelines ensures credibility in resultant findings and gives the reader a common knowledge base with which to understand the results.

Data Analysis Plan Preview

The literature is analyzed according to guidelines recommended by Creswell (2009) and takes on the form of a conceptual analysis. Creswell (2009) defines the data analysis as the process of, “preparing the data for analysis, conducting different analyses, moving deeper and deeper into understanding the data, representing the data, and making an interpretation of the

larger meaning of the data" (p. 183). Creswell (2009) defines coding as the process of organizing the literature into segments based upon categories before brining meaning to the information. This process is accomplished through detailed analysis of selected texts with careful attention paid to grouping ideas into categories.

The particular coding process used to support the data analysis is defined by the Colorado State University Writing Lab. Within this coding process, the researcher defines a concept, chosen for analysis, which is then analyzed within the literature sources for occurrence and meaning (Busch et al., 2005). The first step in the analysis is to identify keywords or phrases to quantify (Busch et al., 2005). For the purposes of this study, initial key phrases are selected which provide the greatest focus for the study and combine one or more of the following areas: (a) virtualization, (b) security, (c) virtualization as a green IT technology.

Writing Plan Preview

The writing plan for the study provides structure for the presentation of the results derived from the data analysis (UNC, 2007). An implicit strategy is taken which assumes the knowledge of previous works and therefore only references works as necessary (Obenzinger, 2005). The writing plan takes the form of a state of the art review which considers the most current research in the given area (Busch et al., 2005). "The review may offer new perspectives on an issue or point out an area in need of further research" (Busch et al., 2005). The objective is the identification of common themes between the literature in order to identify trends, gaps in research, and fallacies in the data (Obenzinger, 2005).

Selected areas of study include current research in the fields of virtualization, security, and green IT. These results are presented in categories based upon pre-selected themes. The selected themes for this study are (a) security strengths of virtualization, (b) security weaknesses

of virtualization, and (c) virtualization as a green technology. The NIST 800-30 risk assessment steps are mapped to the presentation of the data. Architectural and functional foundations of virtualization are discussed which map to 800-30 step one, *system characteristics*. This step also addresses virtualization as a green technology in framing the following three steps. Step two, *threat identification,* matches the data about security weaknesses collected in the *data analysis* to known threat vectors. *Vulnerability identification*, or step three of NIST 800-30, presents the findings of the data analysis regarding security weaknesses. Security strengths found from the coding process are presented in relation to step four of NIST 800-30, *control analysis*.

Definitions

Unique terms to the fields of information security, green IT, and virtualization are defined. Many terms within the study can be difficult to understand and therefore are explained in this section in terms that an average reader should be able to understand. Acronyms within the study are fully expanded the first time they appear, but can be referenced in this section as well.

Attack Vector: A method of digital assault employed by a hacker to disrupt or destroy a system (Harris, 2010).

Availability: Facet of information security, which "ensures reliability and timely access to data and resources to authorized individuals" (Harris, 2010, p. 51).

CIA Model: The three main principles in information security of confidentiality, integrity and availability which provides the framework for assessing security controls as well as security risks against (Harris, 2010).

Confidentiality: Facet of information security, which "ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure" (Harris, 2010, p. 53).

Control: A technique or procedure put into place to prevent a threat from exploiting vulnerability (Harris, 2010).

Denial of Service: An attack which attempts to prevent services from being accessed on a host by means of blocking or disrupting functionality (Haletky, 2009).

DoS: see *Denial of Service*.

Dual Control: The need of two separate individuals to perform an administrative task to ensure it is performed correctly and securely (Harris, 2010).

Guest: See *Virtual Machine.*

Hacker: (criminal hacker) A person who breaks into computers for malicious intent (Gregg, 2007).

Host: Physical server which runs the virtualization application, contains the hypervisor, and has the physical resources which are allocated to the guests (Haletky, 2010).

Hypervisor: A software entity required in virtualization which multiplexes and abstracts low-level hardware resources to share with multiple virtual machines (Carbone, Lee, & Zamboni, 2007).

Information Security: The protection of information systems and data from unauthorized use, tampering, destruction and disruption (Public Printing and Documents, 2010).

Information System: Any combination of hardware, software and network communications which stores, retrieves and processes information (Information System, n.d.). This study uses this term to refer specifically to computerized information systems found in data centers.

Integrity: "Upheld when the assurance of the accuracy and reliability of the information and systems is provided, and any authorized modification is prevented" (Harris, 2010, p. 52).

Kernel: The core of an operating system which manages the machine's hardware resources and provides controls (Harris, 2010).

Malware: Malicious code which includes computer viruses, Trojan horses, logic bombs, and worms intended upon disrupting or destroying computing systems (Harris, 2010).

Mitigation: Employing a security control to alleviate a security vulnerability (Harris, 2010).

Remnance: Latent information left over from a previous process which was not wiped or destroyed (Haletky, 2010).

Risk Analysis: See *Risk Assessment*.

Risk Assessment: A process used to determine the extent of the potential threat and the risk associated with an IT system throughout its lifecycle (NIST, 2002).

Risk Management: The formal or informal process of "balancing the operational and economic cost of protective measures, and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions" (NIST, 2002, p. 4).

Rootkit: Specialized malware which hides it's presence from detection by disguising itself as a legitimate operating system **(**Carbone, Lee & Zamboni, 2008).

Stakeholder: A person who can be affected by an organization's actions.

Sustainability: "Meeting the needs of the present without compromising the ability of future generations to meet their own needs" (Lamb, 2010, p 298).

Threat: A theoretical, damaging, happening that may not occur but should be considered as a potential (Haletky, 2010).

Threat Vector: See A*ttack Vector*

VC: See Virtual Center

VIC: See Virtual Infrastructure Client

Virtual Center: Software interface for VMware which enables management of virtual machines (Haletky, 2010)

Virtual Infrastructure Client: Desktop software which enables connection between virtual hosts' management interface and a user (Haletky, 2010)

Virtualization: "Technology that lets a single PC or server simultaneously run multiple operating systems or multiple sessions of a single OS. This lets users put numerous applications and functions on a PC or server, instead of having to run them on separate machines as in the past" (Vaughan-Nichols, 2008, p. 13).

Virtual Machine: A completely or partially virtualized operating system and configuration. This operating system differs from a non-virtualized one in that it does not directly interact with the hardware of the system and instead uses the assistance of the hypervisor. One or multiple virtual machines may be run on a single host (Haletky, 2010).

Virtual Switch: A virtual OSI layer 2 networking device which provides networking for virtual machines (Haletky, 2010).

VM: See *Virtual Machine*.

VMWare: A private company who develops a mainstream virtualization software solution which is widely used (Lamb, 2010).

vSwitch: See *Virtual Switch.*

Research Parameters

The research parameters section of the paper focuses on the methods which are used to design the literature review. This section of the study provides the framework for the entire study and outlines all the methods and guidelines used to lend credibility, control, and consistency to the study (UNC, 2010).

The various methods used to find, select, code, analyze and present the literature review are discussed. Search parameters and keywords used to find and collect literature are detailed along with the criteria used to validate the credibility of sources and works. Literature which meets requirements for validity, credibility and usability are documented according to formats specified and are placed into the *Annotated Bibliography* and/or *References* depending on their use (Lester & Lester, 2007). The literature is used to provide answers to the research questions, which are also defined in this section (Creswell, 2009). The methods used to answer the research questions through coding and analysis are discussed in the *data analysis plan* (Busch et al., 2005). The presentation of this data through the use of themes of related concepts is also discussed (Creswell, 2009).

Search Report

Search terms. Search term identification is derived from Lester and Lester (2007) who recommend clustering keywords around a central subject in order to identify interconnections between terms. The base term used is *virtualization*. The search method is finding these related terms in books, journal articles, conference proceedings, white papers and other professional and scholarly sources (Creswell, 2009; Lester & Lester 2007). The following search terms are not used all-inclusively meaning they are combined with one another or had minor terms appended to them, however they are used as the basis for the majority of searches.

The initial search terms used are:

- Green IT
- Virtualization
- Information security
- Data center
- Risk analysis
- Green technologies

Additionally, search terms are identified from professional texts on security and virtualization which are not electronic sources. *CISSP All-in-One Exam Guide*, *Greening Through IT,* and *VMware vSphere and Virtual Infrastructure Security* are used to identify key words and terms associated with answering the research questions. These texts also serve as a base for the background information for this study and are heavily cited.

Literature resources. This study is designed as a literature review, with the goal of "filling in the gaps of previous research and extending prior studies" (Creswell, 2009, p. 25). The initial sources used for the literature review are: books, peer-reviewed journal articles, whitepapers, research papers, and business publications. Emphasis is placed upon identifying the most credible and relevant references available.

Search engines. Initial searches are performed online using University of Oregon Libraries search engine, Google Scholar, Summit Libraries, WorldCat, SANS Reading Room, ISSA Journal and Information Security Journal: A global perspective. As the search plan is revised after the initial searches, the following search engines are included: IEEE Xplore, Google. As the search matured, less emphasis is placed upon the initial keywords for the search

and more upon keywords found within the literature. These keywords are used with the existing set of search engines to produce additional results.

Research questions and subquestions. In order to provide a linear and focused methodology in the framing and focusing of this literature review, research questions are created. "Raising questions about the subject can provide clear boundaries for the paper" (Lester & Lester, 2007, p. 17). Performing this step gives the paper a clear theme and clears obscurity regarding the topic, keywords and purpose (Lester & Lester, 2007). The research questions developed for this study examine one of four areas (a) virtualization technology, (b) virtualization security, (c) virtualization green benefits in the data center, and (d) performing risk assessment. These questions provide a foundation to address the overall purpose of the study.

1) What security decisions are most important to implementers of virtualization as a green IT technology in the data center?
    a. Who is implementing virtualization as a green technology?
    b. Why are they implementing virtualization as a green technology?
    c. How are they implementing virtualization as a green technology?
2) What features of virtualization affect security in regards to the CIA model?
    a. What are the main threats?
    b. How would these attacks be undertaken?
    c. Which virtualization features require mitigating factors?
    d. Which virtualization features provide inherent protections from threats?
3) How should a system be analyzed for risk and mitigating controls selected?
    a. What risk analysis standards can be used?
    b. How should controls be selected?

c. What are the existing control sets for virtualization?

Documentation approach. References for this study have been collected as noted in the search report section of this study. Collected references are saved in the full-text format from their original sources. These texts are kept in a digital folder and named with the convention of "Author - Title - Year". This naming convention allows for quick identification of the file. As references are collected, they are added to a spreadsheet which tracks the date found, author, year, keyword(s) used, the database searched as well as the persistent uniform resource locator (PURL). This spreadsheet enables quick retrieval of additional information regarding the document as well as a historical ledger of documents found. Hard copy literature such as books is noted in the spreadsheet but do not include a PURL.

References are filtered and evaluated for content and applicability. Lester and Lester (2007) provide an evaluation checklist, which is used to filter sources in this study. Each reference is also analyzed for additional references and sources, which may be contained within. Abstracts, if provided, are written into a copy of the annotated bibliography. If an abstract is not provided a comment section is made and a summary of the literature is given along with author comments. Author comments are provided for all works cited in the annotated bibliography to inform the reader of intent of use of each reference.

References, which answer one or more of the research questions asked for this study and meet the guidelines posed by Lester and Lester (2010) are integrated into the references and annotated bibliography sections of this paper accordingly. References are cited in the references and annotated bibliography sections of this paper in American Psychological Association (APA) format. Digital object identifiers (doi) and PURLs are included with each reference in order to allow for easy retrieval of the reference as needed.

Data Analysis Plan

Conceptual analysis of the literature selected to address this topic involves examining and analyzing the literature and identifying and tallying thematic occurrences (Busch et al., 2005). The coding process involves a series of steps which, when defined, provide the plan with which this researcher performs analysis. Concepts are identified which this author believes provide the greatest understanding of the topic at hand within the confines of the purpose of the study and the selected literature. These concepts are information security, green IT, and security strengths and weaknesses. Key terms for the data analysis are derived from a set of base texts which include: *CISSP All-in-One Exam Guide, The Greening of IT, and VMWare vSphere and Virtual Infrastructure Security*. The aforementioned concepts are coded within the selected references, using these key terms. References selected for coding are presented in the *Annotated Bibliography.*

Creswell (2009) describes the coding process as the organization of material into common themes before making conclusions about the data. Creswell (2009) defines coding as the process of organizing the literature into segments based upon categories before brining meaning to the information. This process is accomplished through detailed analysis of selected texts with careful attention paid to grouping ideas into categories. The next step is transcribing and consolidating the data in order to address themes. This step is performed using a computer and a database program to enable quick searches. The use of these tools also provides the ability to easily identify correlations between themes. The outputs of these steps are the tables found at the end of the data analysis which, along with the narratives, explain the data. Finally, collected data is analyzed further by the author to provide meaning and to design the final outcome of the study

A detailed coding procedure is provided by Busch, De Maret, Flynn, Kellum, Le, Meyers, Saunders, and White (2005) which includes eight distinct steps as presented by the Colorado State University Writing Lab. These steps are described as articulated in this study below:

1. Level of analysis: The literature is coded for keywords such as *virtualization*, *virtualization security*, *attack*, *virtualization security vulnerability*, *virtualization security strength*, and *green IT*.
2. Number of concepts to code for: Initially, two key concepts are addressed and include (a) identification of security strengths and weaknesses of virtualization technologies including identification of mitigating factors and controls, and (b) identification of what are termed 'green benefits' of virtualization. Additional concepts may be added to the set should significant new concepts be identified. Flexibility is important should any new concepts arise and need to be incorporated into the coding process (Busch et al., 2005).
3. Coding for existence or frequency of concept: Literature is coded for existence, counting each key concept as it appears in the text (Busch et al., 2005). Literature, which contains a selected concept, is noted as described later in the process.
4. Distinguishing among concepts: Concepts are coded for meaning rather than by the explicit word. "This entails more than subtle differences in tense or spelling" (Busch et al., 2005) as with *weakness* and *vulnerability*. These two words have the same meaning for this study and therefore are coded as one concept. Distinctions are made based on context within each reference and the definitions provided in this study.

5. Translation rules: Translation rules ensure that concepts are coded appropriately and consistently. For instance, the terms, *malware*, *virus*, *DoS, hacker* are coded under *attack*. The keywords *weakness*, *exposure*, *hazard* are coded under *virtualization security vulnerability*.
6. Parsing irrelevant information: Information which does not fall into one of the identified categories or is not considered significant is discarded.
7. Coding the literature: Prior to actual coding of the literature, all rules, terms, and relationships between terms are noted separately to be used as a reference. This is used as a guide during the coding process, ensuring that coding is conducted uniformly. Coding is performed on a text by text basis with coded themes found and associated comments input into a database. This database tracks each keyword by both the text it originated from as well as the category it is coded into. This database is used to analyze the results and export into word format for presentation.
8. Analysis of results: The database can be quickly and easily scanned in order to analyze the results of the coding process, and determine relationships between concepts, thus enabling development of the research themes, and making conclusions (Creswell, 2009). Results are presented as described in the *Writing Plan.*

Writing plan

Presenting the results collected from the data analysis is important in that it must follow the strategy chosen for the study (Creswell, 2009). This is to ensure the audience is not unfamiliar with the disparate methods used in the study (Creswell, 2009). The strategy chosen for this study is a state of the art review. A state of the art review only considers the most current information on a topic or given area (Busch et al., 2005). Literature, as mentioned in *Research*

Delimitations is only considered if it is within five years of the publication of this study. Using the most current literature regarding the security of virtualization technologies provides this study with up to date literature from which to draw conclusions and recommend further study.

Conceptual analysis of the literature is conducted based a set of three preliminary themes, which are used to form the basis of this literature review and provide organization to the results of the coding process (Obenzinger, 2005). Themes are identified regarding the information security facets of virtualization as a green IT solution. Themes are divergent enough from one another so that they support discrete analysis.

The first theme investigates the background of the importance of virtualization technologies in the data center. This theme provides the audience general information regarding the environment in which virtualization is deployed as a green technology. Literature selected to address this examines virtualization as a significant step in green IT and virtualization deployed in green data centers (Lamb, 2010; Stansberry, 2005; Stuenkel, 2009; The top 12 green-IT vendors, 2008). Significant detail is spent addressing the functional and architectural facets of virtualization. Illuminating virtualization architecture allows the audience to understand the virtual environment for the following sections (Fong & Steinder, 2007; Haletky, 2010).

The second theme explores the threats to virtualization and the vulnerabilities exploited by the threats (Mattord & Whitman, 2008; NIST, 2009). Literature selected to address this theme provides actionable information regarding the most current threats against servers in the data center, including discussion of specific attack vectors (Gregg, 2007). Presentation of this theme is explicated by framing with the risk assessment process which determines the security vulnerabilities based on the threat analysis (NIST, 2002).

The third theme draws upon the previous theme's threat analysis in order to provide an understanding of the positive security features of virtualization. Inherent security strengths collected from the *data analysis* are highlighted. Literature selected to address this theme also provides a set of security controls, which mitigate the earlier identified security vulnerabilities (Cohen, 2010; Harris, 2010; Jilg, 2007). This provides the positive security feature sets as well as recommended security controls to realize a secure system.

When combined, themes are framed into a guide designed to provide IT Stakeholders with information that can be used to make decisions regarding the implementation and management of virtualization as a green IT solution in a data center. Understanding of the security threats and weaknesses of virtualization technology is necessary to protect the entire organization in which it is deployed (Harris, 2010). Furthermore, understanding the importance of security in green endeavors is critical for IT leadership (Green IT raises security fears, 2007). The three themes used to structure the writing plan in this study are outlined below:

Topic: Security Strengths and Weaknesses of Virtualization as a Green Computing Solution in the Data Center

1. Theme one: Virtualization system characteristics in the data center
    a. Virtualization architecture and foundations
    b. Green benefits of virtualization
2. Theme two: Security weaknesses of virtualization technologies, framed within the scope of green IT
    a. Determination of threats to virtualization as derived from the *data analysis*
    b. Vulnerability identification as derived from the *data analysis*

3. Theme three: Security strengths and controls of virtualization technologies, framed within the scope of green IT
    a. Determination of inherent security strengths as derived from the *data analysis*
    b. Recommendation of mitigating controls for identified security weaknesses

Annotated Bibliography

The annotated bibliography highlights selected sources from the *References* that provide information which is key to some aspect of this study (Ettinger, 2010). Each reference s below which is used in the sub-set of references selected for coding during *data analysis* is prefaced with the symbol "!". Each reference which does not contain an author provided abstract is prefaced with the symbol "*". In these cases, brief abstracts are written by this researcher. This author's comments are appended after each abstract. Author comments include, at a minimum: (a) how the reference supports the study, and (b) how evaluation criteria is applied to establish credibility for the reference.

Cameron, K. W. (2009). Green introspection. *IEEE computer, 42*(1), 101-103.

> **Abstract.** Energy consumption and e-waste have inundated computing technologies, and now we must focus on reducing environmental waste in all phases of the computing life cycle. Green IT is a moving target, and continual introspection and reevaluation are necessary.
>
> **Comment.** Cameron has a regular column about green technologies in IEEE Computer, which can be referenced for further information. IEEE Computer is a professional journal well known in the computer industry. Cameron is also a professor at Virginia Tech and is considered an expert in the field of green IT. This article speaks of e-waste, recycling, and effective energy use. It does not address virtualization. It is used in this study, mainly in the *Introduction,* to show why companies are choosing technologies like virtualization and to frame the environment in which this study is written.

!Carbone, M., Lee, W., & Zamboni, D. (2008). Taming virtualization. *Security & Privacy, IEEE*, *6*(1), 65-67. doi: 10.1109/MSP.2008.24.

Abstract. Although the term virtualization has been around for decades, only recently has it become a buzzword in the computer systems community with the revival of virtual machines (VMs), driven by efforts in industry and academia. VMs are software entities that emulate a real machine's functionality; they execute under the control of a hypervisor that virtualizes and multiplexes low-level hardware resources. Hypervisors come in two flavors: non-hosted, which run directly on top of the hardware, and hosted, which are integrated with a host operating system (OS). The presence of a hypervisor makes VMs subject to a level of visibility and control that's hard to achieve with real machines. The small size, isolation, and mediation power of an ideal hypervisor over VMs make it an interesting candidate for a trusted computing base, with applications in security research fields such as intrusion detection, integrity protection, and malware analysis, among others.

Comment. This article appears in the *Security & Privacy* journal of the IEEE. IEEE journals are highly respected in the computer field for their accuracy and relevancy and are peer-reviewed. The authors have published multiple articles on virtualization and computer security including *Secure and Flexible Monitoring of Virtual Machines* (2007), and *An Architecture for Secure Active Monitoring Using Virtualization* (2008). This article is directed towards marketing a product called GuardHype, which protects hypervisor and hardware from a malicious host. Besides the obvious sales pitch, the article contains many references to attacks against the hypervisor, which can be used to assess the weaknesses of virtualization and possibly allude to effective controls. The

article refers to one of these attacks as a “hyperjack”, an attack which places a light hypervisor which can control all virtualization operations. This article is used to build a reference of possible attacks against virtualization for the risk analysis.

!Carpenter, M., Liston, T., & Skoudis, E. (2007) Hiding virtualization from attackers and malware. *Security & Privacy, IEEE. 5*(3) 62-65. doi: 10.1109/MSP.2007.63.

Abstract. With security researchers relying on virtual machine environments (VMEs) in their analysis work, attackers and their malicious code have a significant stake in detecting the presence of a virtual machine. Virtualization, by its very nature, creates systems that have different characteristics from real machines. From a theoretical perspective, any difference between the virtual and the real could lead to a fingerprinting opportunity for attackers. This article focuses on detection techniques and mitigation options for the most widely deployed VME product today, VMware.

Comment. Carpenter et al. wrote this study for the Department of Homeland Security and the US Air Force Research Laboratory. It was then published in *IEEE Security & Privacy*. IEEE journals are highly respected in the computer field for their accuracy and relevancy and are peer-reviewed. All three authors are security professionals who have published and regularly speak at computer security conferences. Carpenter et al., discuss how attackers are using malware to detect the presence of VMs in order to attack them. They discuss various techniques to detect the difference between real and virtual machines. This article is used to provide information presented in the risk analysis to identify threats to virtualization.

!Chaudhuri, A., von Solms, SH., Chaudhuri, D. (2011, January). Auditing security risks in virtual IT systems. *ISACA Journal.* 16-25.

Abstract. Virtualization provides significant cost savings by sharing storage space and central processing unit (CPU) capacity. As with any technology, though, virtual IT systems are not risk-proof. A proper risk mitigation strategy needs to be developed and followed if organizations are to harness the benefits of virtualization technology. Information security auditors have an important role to play in auditing the risks of virtual IT systems. This article discusses virtual IT systems and the inherent risks that need to be audited for proper risk mitigation and provides guidelines for security audits of virtual IT systems that can be referenced during information security audits and the application of security to virtual IT systems.

Comment. The authors explain virtualization technology and list several weaknesses including architecture, software and configuration of virtual IT systems. The purpose of the paper is to present a list of evaluation features with which to audit virtual systems. These features are presented in a list at the end of the article. These audit features and identified security weaknesses are used to build the list of security weaknesses for virtualization as a green IT technology. Abhik Chaudhuri is a project manager with IBM. SH von Solms, PhD, is a research professor at the University of Johannesburg and chairman of the Academy for Information Technology. ISACA is the Information Systems Audit and Control Association which publishes a well respected journal and hosts several industry standard certifications for IT auditors and security professionals. ISACA also developed methodologies for standardizing IT audit and control.

!Cohen, F. (2010). The virtualization solution. *Security & Privacy, IEEE. 8*(3), 60-63.

Abstract. Is virtualization the solution to computing security? A brief look at the history of computer security salvation might provide some insight. A basic concept underlying OS protection is separation. The OS provides separation of files, directories, processes, users, and devices from each other, even though the hardware lets them interact arbitrarily. In the OS's role as mediator, it prevents user processes from subverting the OS and each other by limiting where they can read from and write to; dominating input, output, storage, and processing resources; and intermediating for the hardware mechanism so that only the OS has direct access.

Comment. Fred Cohen holds a PhD and is the president of California Sciences Institute. He has published many articles on computer security including computer security "how to" books. IEEE journals are highly respected in the computer field for their accuracy and relevancy and are peer-reviewed. This article is a commentary on security features and how the "next big thing" would always be the savior. The author argues that virtualization is another "big thing" that is destined to become main stream and is not a cure-all. The author continues to say that security professionals should very interested in virtualization and understand it well. He cites ten things to know about virtualization which includes security features. These security features are used in this study for the risk analysis portion.

!*Corporate Executive Board. (2007). Green IT initiatives. *The Corporate Executive Board: What the best companies do.* Retrieved from: http://hosteddocs.ittoolbox.com/greenit.pdf

Abstract. This paper presents several case examples of businesses, which have ventured into green IT. It presents the practices they used as well as the results, which were found. The CEB does not address security issues of the technology, but simply mentions the top green technologies used by successful companies.

Comment. The Corporate Executive Board is a research firm, which compiles industry best-practices data and releases its findings to the business community. The various companies analyzed and the references used in this study are found to be credible, professional sources. VistaPrint, Kaiser Permanente, Boehringer Ingelheim, and Tru Vue are cited as frontrunners in green IT implementations and specific technologies and methodologies are mentioned, including server consolidation, virtualization, data center cooling and alternative energies. The research presents the needs of data centers in terms of power expenditure and greenhouse gas emissions. This data is used to corroborate the assertions made in this study regarding energy usage and virtualization as a remediation.

!*Defense Information Systems Agency. (2008). *ESX Server Security Technical Implementation Guide*. Washington, DC: Department of Defense. Retrieved from: http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf

Abstract. A core mission for the Defense Information Systems Agency (DISA) Field Security Operations (FSO) is to secure Department of Defense (DoD) Computing systems. The processes and procedures outlined in this Security Technical Information Guide (STIG), when applied, decrease the risk of unauthorized disclosure of sensitive information. Security is clearly still one of the biggest concerns for our DoD customers, for example, the war fighter. This STIG is developed to enhance the confidentiality,

integrity, and availability of sensitive DoD Automated Information Systems (AIS). ESX Server infrastructures must provide secure, available, and reliable data for all customers. This document assists sites in meeting the minimum requirements, standards, controls, and options that must be in place for ESX Server infrastructures.

Comment. The Defense Information Systems Agency provides security technical implementation guides (STIGs) for use in federal agencies. They are also widely used by civilian agencies. This STIG provides a set of guidelines and controls which can be used to secure VMWare ESX server. The Department of Defense endorses VMWare as its primary virtualization platform and therefore created this STIG. Though it focuses on VMWare, the concepts in this STIG are used to formulate controls for virtualization in general. The STIG is also used to collect a list of known vulnerabilities in VMWare.

*Energy Star Program. (2007). *Report to Congress on Server and Data Center Energy Efficiency: Public Law 109-431*. Washington, DC: Environmental Protection Agency.

Abstract. This study by the Energy Star program of the United States Environmental Protection Agency was conceived in 2006 to examine energy savings for enterprise servers and data centers. Collaboration was made between utility, financial services, healthcare, Internet, and manufacturing sectors to complete this study. The Lawrence Berkeley National Laboratory led the study for the EPA. The end result is a study which presents the current energy consumption of data centers nationwide. The study also provides several scenarios of future energy consumption. In addition, the study provides ways in which the EPA can promote green efficiencies across the nation as well as provides the framework for future green leadership. The study analyzed detailed metrics

which identified the types of inefficiencies found in data centers. It also makes recommendations as to how to reduce those inefficiencies.

Comment. This is a US government report to congress regarding the efficiencies of data centers across the United States and is a public law. The references the report pulls from are professional sources including staple government sources on energy standards such as the Department of Energy. This study is a detailed report from the EPA's Energy Star Program regarding data center efficiency. It mentions virtualization as a way to reduce energy expenditure as well as defines several key topics related to my research. The references used in this study proved valuable in identifying additional references for this inquiry. This study is used to help explain the rationale behind going green.

!Garfinkel, T., & Warfield, A. (2007). What virtualization can do for security. *;login:, 32*(6), 28-34. Retrieved from http://www.usenix.org/publications

Abstract. Virtual machine technology is rapidly gaining acceptance as a fundamental building block in enterprise data centers. It is most known for improving efficiency and ease of management. However, it also provides a compelling approach to enhancing system security, offering new ways to re-architect today's systems, and opening the door for a wide range of future security technologies. Our objective is to provide readers with a better sense of what virtualization can contribute in this area. We begin by looking at the basic security benefits VMs can provide today, e.g.~its power as a mechanism for isolation. We then survey the some of the emerging security technologies supported by virtualization that we may see in the years ahead.

Comment. Tal Garfinkel is a PhD and is part of the advanced development group at VMware. Andrew Warfield is a PhD, professor at the University of British Columbia, and contributor to XenSource. ;login: is the publication of USENIX is the Advanced Computing Systems Association which hosts conferences and publishes the ;login: journal highlighting technical excellence and innovation. Garfinkel and Warfield discuss the security of virtual machine technology and the increasing use of it in data centers. Emerging security technologies are surveyed after an in depth description of what security features virtualization provides. This reference provides overviews of various security features of virtualization which help to improve the security posture of the data center. This information is used in the data analysis to derive security strengths of virtualization.

!Garfinkel, T., & Rosenblum, M. (2005). Proceedings from the 10th workshop on hot topics in operating systems: *When virtual is harder than real: Security challenges in virtual machine based computing environments. Santa Fe, NM: USENIX.*

Abstract. As virtual machines become pervasive users will be able to create, modify and distribute new ``machines'' with unprecedented ease. This flexibility provides tremendous benefits for users. Unfortunately, it can also undermine many assumptions that today's relatively static security architectures rely on about the number of hosts in a system, their mobility, connectivity, patch cycle, etc. We examine a variety of security problems virtual computing environments give rise to. We then discuss potential directions for changing security architectures to adapt to these demands.

Comment. Tal Garfinkel is a PhD and is part of the advanced development group at VMware. Mendel Rosenblum is a PhD and member of the National Academy of Engineering. The Workshop on Hot Topics in Operating Systems is held by the IEEE Technical Committee on Operating Systems and invites the brightest computer scientists and engineers from around the world. These conference proceedings are published in *;login:*, the USENIX journal. This article focuses on security problems in virtual environments including scaling, transience, software lifecycle, mobility and other topics. The article then recommends measures with which to secure virtual environments and the benefits gained by doing so. This information is used to derive security strengths as well as security weaknesses for the data analysis portion of the paper.

!Goth, G. (2007). Virtualization: Old technology offers huge new potential. *IEEE Distributed Systems Online, 6*(2), 3. doi: 10.1109/MDSO.2007.10.

Abstract. Essentially, virtualization uses a virtual machine monitor or host called a hypervisor to enable multiple operating system instances to run on a single physical server. The hypervisor can run directly on a given server's hardware platform, with the guest operating system running on a layer above the hypervisor. It can also run within an operating system, with the guest OS running on the third layer above the hardware.

Comment. Greg Goth has published 136 articles in IEEE journals over the last ten years. IEEE journals are highly respected in the computer field for their accuracy and relevancy and are peer-reviewed. This article discusses virtualization and its rapid adoption across corporate environs. It defines what virtualization is and what its components do as well as where it can go in the future. Also discusses virtual computing (cloud computing) as a

future space for virtualization. This article is used for definitions, to show virtualization's adoption in the business space, and to prove the necessity of future research in the field.

!Gregg, M. (2007). *Certified ethical hacker*. Indianapolis, IN: Que Publishing.

Abstract. The CEH certification shows knowledge of network penetration testing skills. The CEH exam takes three hours and 125 questions, requiring a broad and deep knowledge of network security issues. The CEH Exam Prep is the perfect solution for this challenge, giving you the solid, in-depth coverage you'll need to score higher on the exam. Along with the most current CEH content, the book also contains the elements that make Exam Preps such strong study aides: comprehensive coverage of exam topics, end-of-chapter review, practice questions, Exam Alerts, Fast Facts, plus an entire practice exam to test your understanding of the material. The book also features MeasureUp's innovative testing software, to help you drill and practice your way to higher scores.

Comment. Michael Gregg is a CISSP and author of multiple computer security books. He has presented at many of the security industry conferences such as *defcon* and *black hat*. Certified Ethical Hacker study material shows candidates the many methods to ethically hack and find security holes in systems. The book does not address virtualization, but does provide hacker methodologies. These methodologies are used to build attack cases in order to identify vulnerabilities in virtualization.

!*Haletky, E. L., (2010). *VmWare vSphere and virtual infrastructure security: Securing the virtual environment.* Upper Saddle River, NJ: Prentice Hall.

Abstract. Complete Hands-On Help for Securing VMware vSphere and Virtual Infrastructure by Edward Haletky, Author of the Best Selling Book on VMware, VMware ESX Server in the Enterprise. As VMware has become increasingly ubiquitous in the enterprise, IT professionals have become increasingly concerned about securing it. Now, for the first time, leading VMware expert Edward Haletky brings together comprehensive guidance for identifying and mitigating virtualization-related security threats on all VMware platforms, including the new cloud computing platform, vSphere. This book reflects the same hands-on approach that made Haletky's VMware ESX Server in the Enterprise so popular with working professionals. Haletky doesn't just reveal where you might be vulnerable; he tells you exactly what to do and how to reconfigure your infrastructure to address the problem. VMware vSphere and Virtual Infrastructure Security begins by reviewing basic server vulnerabilities and explaining how security differs on VMware virtual servers and related products. Next, Haletky drills deep into the key components of a VMware installation, identifying both real and theoretical exploits, and introducing effective countermeasures.

Comment. Edward Haletky has worked for Hewlett-Packard and now owns his own company providing computer security solutions. He hosts a blog on virtualization which is referenced by many professional sites. This book is endorsed by the largest commercial virtualization provider, VMWare. This book provides much of the data needed to describe the security strengths and weakness of virtualization. Haletky speaks of the virtualization environment and the possible ways to exploit that environment. Haletky's introduction provides material for framing the study. Haletky provides examples of

attacks as well as details of how virtualization technologies work. One limitation to note is that it is focused upon VMWare and does not address other offerings.

!*Harris, S. (2010). *All-in-one CISSP exam guide* (4th ed.). Emeryville, CA: McGraw-Hill.

Abstract: Written by Shon Harris, the number-one name in IT security certification and training, this exam guide offers complete coverage of all the material on the latest release of the Certified Information Systems Security Professional (CISSP) exam. With full treatment of all the 10 exam domains, as developed by the International Information Systems Security Certification Consortium (ISC2), this definitive tool contains learning objectives at the beginning of each chapter, sidebars with in-depth technical explanations, practice questions, and real-world scenarios. CISSP All-in-One Exam Guide, Fifth Edition serves as both a comprehensive certification study guide and an essential on-the-job reference.

Comment. Shon Harris is a CISSP who has published all five editions of this guide as well as written or contributed to various books on hacking. She has worked with various agencies such as the National Security Agency, Department of Defense, Defense Information Security Agency, and the Department of Energy. The CISSP exam is the gold standard for information security professional certifications and the Shon Harris book is the most well know and most widely used guide to prepare for the exam. The book covers managerial and technical facets to include specific technologies. This book covers the security strengths and weaknesses of a wide range of security technologies to include many of the green technologies to which other authors refer. It is also a helpful reference for the risk analysis methodologies. This book is highly referenced in this paper

as it provides the security framework, attack vectors, and analytical techniques used in this study.

*Hignite, K. (2009). Low-carbon computing. *Educause Review, 44*(6), 34 -36. Retrieved from: http://uolibraries.worldcat.org/oclc/496120088

Abstract. Green information technology (IT) is grabbing more mainstream headlines--and for good reason. Computing, data processing, and electronic file storage collectively account for a significant and growing share of energy consumption in the business world and on higher education campuses. With greater scrutiny of all activities that contribute to an institution's carbon footprint, information technology operations represent a largely untapped reservoir for energy reduction. In addition to specific efforts to reduce carbon emissions, green IT must be seen as more than an effort to reduce overall waste or limit consumption. Rather, a strategic vision for green IT must incorporate forward-reaching efforts that seek to curtail technology's environmental impact. The good news is that upfront costs for a number of opportunities have a short payback time in terms of the energy and financial savings they can produce. The college and university examples highlighted in this article point to the breadth of possibilities for shrinking ITs carbon load and the importance of working in concert to put green IT at the top of an institution's strategic agenda. Going forward, every institution should factor in the exponential impact IT can and already does have--positively or negatively--on campus sustainability success. Six Strategies for Cutting Virtual Carbon and their Assessment of Campus Sustainability are presented.

Comment. Karla Hignite has written articles for multiple higher education organizations regarding sustainability and green technology. She has been referenced in and written for business magazines and university journals. EDUCAUSE review is a professional journal serving over 2200 higher education organizations and is peer-reviewed. This article discusses energy reduction techniques to reduce the carbon footprint of computing technologies. It highlights six initiatives higher education has used to reduce costs and energy consumption. These initiatives are used as a framework to prove the plausibility of virtualization as a green technology. It lends credibility to the green movement by discussing various effective techniques which have been successful in organizations.

!Hoesing, M. T. (2009). Virtualization security assessment. *Information security journal: A global perspective, 18*(3), 124-130. doi: 10.1080/19393550902791440

Abstract. Enterprises have been increasingly adopting server virtualization technologies in recent years. Security risk identification and related controls have also been receiving increased discussion lately. Also, guidance is available on virtualization security configurations from independent groups, such as benchmarks from the Center for Internet Security and the virtualization vendors. This writing revisits the risks and controls, which is a basis for discussion of assessment techniques. As security assessors, auditors and compliance validators see more of the physical environment disappearing and being replaced by the virtual foundation, gathering the necessary metrics from virtual environment is a key part of assurance activities. This discussion is limited to the VMware ESX virtualization product but some principles may have applicability to other vendors' products. Also, any assessment techniques or tools mentioned are intended to be

a starting point and not a comprehensive list of possible assessment approaches, nor a "best of" list of tools. In adherence to solid change management practices, any items discussed herein should be thoroughly tested in an organization's lab, compared to organization policy, and aligned with business objectives before consideration for adoption in a production environment.

Comment. Michael Hoesing is a CISSP with an extensive background in IT audit and security. He teaches IT audit and security classes and has spoken at conferences on virtualization security. *Information Security Journal: A global perspective* is the official journal of ISC^2 and publishes peer-reviewed CISSP articles. In his article, Hoesing illuminates the security vulnerabilities of virtualization. He begins by presenting the two categories of vulnerabilities from virtualization: physical server risks which carry over into the virtual world, and risks which are exacerbated by the virtual environment. He presents the risks and also presents control techniques to mitigate the risks. This reference is used in identifying virtualization risks and attack vectors.

!*Lamb, J. (2009). *The greening of IT: How companies can make a difference for the environment*. Upper Saddle River, NJ: IBM Press.

Abstract. John Lamb helps you realistically assess the business case for green IT, set priorities, and overcome the internal and external challenges to making it work. He offers proven solutions for issues ranging from organizational obstacles to executive motivation and discusses crucial issues ranging from utility rate incentives to metrics. Along the way, you'll discover energy-saving opportunities—from virtualization and consolidation to cloud and grid computing—and solutions that improve business flexibility as they

reduce environmental impact. Lamb presents case studies, checklists, and more—all the practical guidance you need to drive maximum bottom-line value from your green IT initiative.

Comment. John Lamb is a certified IT architect with IBM and author of several books on technology. He has also published on popular technology websites promoting the greening of IT. Lamb's book is a resource for green IT as it cites cases of successful green implementations. Included in these cases is virtualization as a green IT technology. Lamb believes that virtualization is the first, best step in going green. This book clearly draws the critical link between virtualization and green IT. Devoting an entire chapter to virtualization technologies provides plenty of references for the ways in which virtualization is implemented. This information provides insight into the threat environment.

!*Mattord, H. J., & Whitman, M.E. (2006). *Readings and cases in the management of information security.* Boston, MA: Thomson Course Technology.

Abstract. Running case study which incorporates the CISSP common body of knowledge. Source on management of information security, but not detailed on technical details. Used as a class text for Managing IT/IS Security, this text orients students to the managerial aspects of information security from a holistic perspective. Little detail is spent discussing specific technologies or methodologies relating to the security field. Instead focus is upon understanding risk management, security planning and security management of IT programs.

Comment. Whitman and Mattord, both CISSPs, have written a guide to the management portion of information security. Whitman is a PhD and has written multiple books with Mattord for the security field covering incident response, and disaster recovery. They wrote this book following the CISSP common body of knowledge. This book does not make a good technical reference, but instead is used as a conceptual reference for information security strategy. The case studies at the end of the book are also effective resources for examples and industry trends. This book is used to corroborate risk analysis procedures, identify threats and present possible controls.

!*National Institute of Standards and Technology. (2002). *Risk Management Guide for Information Technology Systems.* (NIST SP800-30). Washington, DC: U.S. Department of Commerce.

Abstract. NIST governs federal information system security and sets various standards for government agencies to follow and for civilian entities to use as a guideline. NIST 800-30 specifically focuses on the risk management process and how it fits into the systems life cycle. The document gives step by step guidance to identifying and assessing risk in organizations.

Comment. NIST 800-30 is a US government document and is the standard for federal government computer systems. NIST has been the basis for many newer accreditation standards for the Department of Defense. NIST 800-30 is also used by many civilian agencies to assess risk. This reference is very important to this study as it both acts as a reference for the risk framework but is also widely known and recognized in the industry.

The risk assessment steps are used as a model to frame the presentation of the assessment of risk for virtualization technology in the data center.

!*National Institute of Standards and Technology. (2009). *Recommended security controls for federal information systems and organizations.* (NIST SP800-53). Washington, DC: U.S. Department of Commerce.

Abstract. The selection and implementation of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organization as well as the welfare of individuals and the Nation. Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information.

Comment. NIST 800-53 is a follow on document for 800-30 which provides the control sets for computer security. This document is published by the US government and is enforced for all federal agencies. Many civilian agencies choose to use this document as well because of its adoption by the federal government. This reference is very important to this study as it both acts as a reference for selecting controls but is also widely known and recognized in the industry. It is used as a reference for security control selection. This document makes the identification and presentation of selected security controls in this study more valid because they are modeled by NIST and the US government.

!Peles, A. (2008). Virtualization affects applications. *Communications News, 45*(5), 22-23. Retrieved from: http://uolibraries.worldcat.org/oclc/23191261

Abstract. The article focuses on the impact of virtualization in the business applications. Virtualization is considered as an important tool at the server level that functions in multiple operating systems. According to the IDC research firm, virtualization software spending and services will possibly exceed to $15 billion. The availability of the business application is ensured by addressing the failures at all levels should be monitored and users should be provided with an alternate resource. The virtualized server environments which operated and applied in a closed area is considered as secure.

Comment. Amir Peles is the Chief Technology Officer as Radware, a company who integrates virtualization technologies for businesses. This article is published in communications news which is a telecommunications industry magazine. It is not peer reviewed and therefore information contained within is corroborated with another reference. This article discusses some of the disadvantages of virtualization, especially as it relates to application performance. The information is used to highlight some of the security weaknesses of virtualization as a host for applications.

!Perez, R., van Doorn, L., & Sailer, R. (2008). Virtualization and hardware-based security. *Security & Privacy, IEE, 6*(5), 24-31.

Abstract. Hypervisors allow virtualization at the hardware level. These technologies have security-related strengths as well as weaknesses. The authors examine emerging hardware and software virtualization technologies in the context of modern computing environments and requirements.

Comment. Ronald Perez and Reiner Sailer, PhD are researchers at the IBM Watson Research Center. Leendert van Doorn, PhD is a senior fellow at Advanced Micro

Devices. All three authors have published multiple works in credible journals such as *Operating Systems Review*. This study is published in the *Security and* Privacy journal of the IEEE. IEEE journals are highly respected in the computer field for their accuracy and relevancy and are peer-reviewed. This reference addresses the security features of a hypervisor and its relation to the hardware of the system. Though very technically detailed, this article directly points to some security strengths and weaknesses for virtualization. It also offers insight into possible attack vectors and mitigation techniques.

!*SANS (2010). Overview. *The top cyber security risks.* Retrieved from: http://www.sans.org/top-cyber-security-risks/

Abstract. SANS is a de facto standard for computer security and publishes daily reports on threats and remediation techniques. They provide a reading room with white papers on various security topics. This article summarizes in plain English the top security risks facing the world today and discusses techniques to remediate each threat. SANS provides up to the date vulnerability assessments collected from industry professionals around the world.

Comment. SANS is a computer security organization which seeks to improve the odds against cyber threats. This is done by integrating themselves with professionals around the world to collect and disseminate information on vulnerability and threats. SANS as an organization also teaches classes for computer security professionals as well as hosts security white papers on their website. SANS is referenced by many computer security professionals as a standard database for the security field. This reference provides data on the most current threats. Though it does not directly address virtualization as a

technology, the attacks are relevant and would be of concern to virtualized environments. Any direct software vulnerability to a virtualization product would also be published by SANS and can be searched online.

!Susanta, N., & Chiueh, T. (2005). *A survey of virtualization technologies* (Report No. 179). Stony Brook, NY: SUNY at Stony Brook. Retrieved from http://www.ecsl.cs.sunysb.edu/tr/TR179.pdf

Abstract. Virtualization is a technology that combines or divides computing resources to present one or many operating environments using methodologies like hardware and software partitioning or aggregation, partial or complete machine simulation, emulation, time-sharing, and others. Virtualization technologies find important applications over a wide range of areas such as server consolidation, secure computing platforms, supporting multiple operating systems, kernel debugging and development, system migration, etc, resulting in widespread usage. Most of them present similar operating environments to the end user; however, they tend to vary widely in their levels of abstraction they operate at and the underlying architecture. This paper surveys a wide range of virtualization technologies, analyzes their architecture and implementation, and proposes a taxonomy to categorize them on the basis of their abstraction levels. The paper identifies the following abstraction levels: instruction set level, hardware abstraction layer (HAL) level, operating system level, library level and application level virtual machines. It studies examples from each of the categories and provides relative comparisons. It also gives a broader perspective of the virtualization technologies and gives an insight that can be extended to accommodate future virtualization technologies under this taxonomy. The paper proposes

the concept of an extremely lightweight technology, which we call as Featherweight Virtual Machine (FVM), that can be used to ”try out” untrusted programs in a realistic environment without causing any permanent damage to the system. Finally, it demonstrates FVM’s effectiveness by applying it to two applications: secure mobile code execution and automatic clean uninstall of Windows programs.

Comment. Nanda Susanta, Ph.D., is a researcher for Symantec and has published papers with Chiueh on networking and security vulnerabilities. Tzi-cker Chiueh, Ph.D., is a professor and researcher at the State University of New York: Stony Brook. The authors discuss the wide range of virtualization technologies ranging from semi-virtualized to fully-virtualized and the various vendors of the software. It is used for describing virtualization technologies and providing a base to the reader regarding how the strengths of virtualization are inherent to its architecture.

!Vaughan-Nichols, S. J. (2008). Virtualization sparks security concerns. *IEEE computer*, 41(8), 13-15. doi: 10.1109/MC.2008.276

Abstract. Virtualization is rapidly becoming a standard technology for businesses. The technology lets a single PC or server simultaneously run multiple operating systems or multiple sessions of a single OS. The approach is thus becoming a common way for users to optimize their hardware utilization by maximizing the number and kinds of jobs a single CPU can handle. Organizations now face the challenge of securing virtualized systems, which are vulnerable to the same threats as physical systems, including intrusions and malware. Virtualized systems cannot always be secured the same way as physical systems. Many virtualized systems can run on the same machine, but each one

might need a different security level. Thus, security cannot simply be applied across the entire machine, as is the case with typical physical systems.

Comment. Vaughan-Nichols is an author and blogger of technology subjects. He has published in numerous professional and peer-reviewed journals as well as magazines. This article is published in the *IEEE Computer* journal. IEEE journals are highly respected in the computer field for their accuracy and relevancy and are peer-reviewed. The author presents several situations which threaten the security of virtualized environments. He also proposes a proprietary solution for managing the security of virtualization. This reference shows virtualization's weaknesses and illuminates possible threats for the risk assessment.

!Webber, L., & Wallace, M. (2009). *Green tech: How to plan and implement sustainable IT solutions*. New York, NY: AMACOM.

Abstract. With today's electronic systems consuming massive amounts of energy, and improper disposal of old equipment threatening to release dangerous toxicity into the atmosphere, any company whose IT department isn't actively working to shrink its carbon footprint isn't just hurting the environment...it is also probably wasting money. Green Tech provides readers with practical, easily implemented strategies for sustainable computing, showing them how to: build a business case to influence their organization's green strategy, reduce costs and improve equipment utilization while maintaining current customer service levels, identify old equipment at all levels, as well as suitable green replacements, virtualize servers, find alternative methods for data center cooling, conduct an energy audit and establish an energy baseline, determine the best options for recycling

or donating old equipment. Filled with realistic, cost-efficient ideas, this book shows that going green isn't just the right thing to do, but also a good business strategy.

Comment. Webber and Wallace present a practical study on green technologies including virtualization. Webber has over thirty years of IT experience. Wallace has over 25 years of management and IT experience. AMACOM publishing is known for management and business books geared towards professionals. This book is coded for key terms such as virtualization and not for any security features. This book is used in order to present a case for the necessity of the green movement as well as ensuring there is a clear link between green, the data center, and the way IT is moving.

Review of the Literature

This review of the literature discusses the security strengths and weaknesses of virtualization technologies within the context of green IT. \References are selected which address the following core concepts: (a) security strengths of virtualization, (b) security weaknesses of virtualization, (c) energy saving factors of virtualization. The literature is documented in the Annotated Bibliography, which describes the use and provides a brief overview for each reference. References are coded for these concepts, and presented thematically in this section. Themes are presented in the context of a risk assessment in order to provide the reader with an actionable and relevant basis from which to understand the topic. The pre-selected risk assessment framework used in this study is NIST 800-30 (2002).

Virtualization technology is implemented widely across enterprises for various reasons (Haletky, 2010). One major goal for implementing virtualization is energy savings (Lamb, 2009). Lamb and others referenced in this study point to the benefits virtualization provides as a green technology. However, these studies do not address the security requirement when implementing these technologies. Without understanding the security strengths and weaknesses of virtualization, many of the monetary benefits it may bring in energy savings can be lost to a breach in security. Security studies performed by organizations such as the Defense Information Systems Agency (2008), VMWare (2008), and the Center for Internet Security (2010) have yielded results which present data on the security of virtualization technologies. Information is presented with a focus on the green benefits of virtualization in order to assist decision makers and implementers of virtualization in making better decisions.

This section includes a number of tables and figures designed to provide the security professional or IT decision maker with the information needed to make decisions regarding the

selection and implementation of virtualization technology in the data center. Following the NIST (2002) risk assessment framework or alternative, organizations should perform their own risk assessments based upon their operating environment (Harris, 2010). Analysis should be performed upon all known and possible threats to the environment, the security weaknesses, and the selected controls and not just those identified in this study (Harris, 2010; NIST, 2002; Whitman & Mattord, 2008). Analysis should also be performed upon any change in environment and at selected intervals to mitigate any unforeseen differences (Harris, 2010; NIST, 2002).

Virtualization in the Data Center

This section briefly explains how virtualization technologies can be used in the data center, and includes a list of potential green benefits. The goal is to provide a base of knowledge to better understand the discussion of security strengths and weaknesses. It is necessary to understand the architecture of virtualization in order to attack or secure it in production environments (Haletky, 2010). Also, while there are many product offerings of virtualization technologies, this section does not attempt to make reference to specific products, but rather provides focus on the particular security management research goals at hand.

Virtualization architecture and foundations. Virtualization technologies rely upon a hypervisor to provide the abstraction between the physical and virtual machines (Carbone, Lee & Zamboni, 2007; Haletky, 2010; Susanta & Chiueh, 2005). The hypervisor interacts with the hardware and software in the physical world and manages the distribution of resources to virtual machines (Goth, 2007; Haletky, 2010; Lamb, 2009; Sustanta & Chiueh, 2005). The hypervisor provides everything the virtual machine requires, including virtual networks, memory, CPU, and virtual hardware (DISA, 2008; Haletky, 2010, Susanta & Chiueh). Figure 3 shows an example of

how resources are shared under VMware architectures.

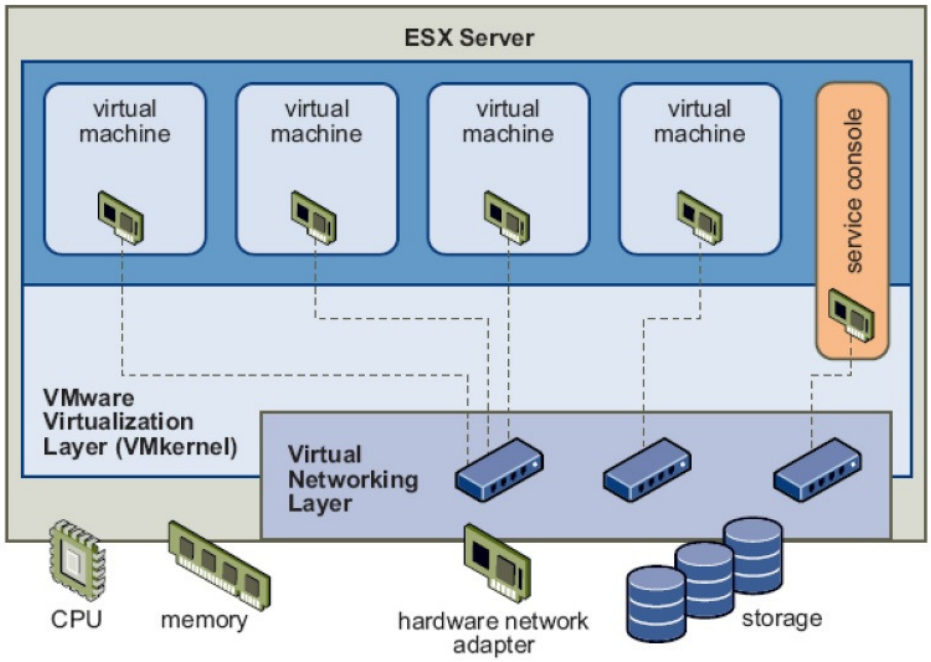
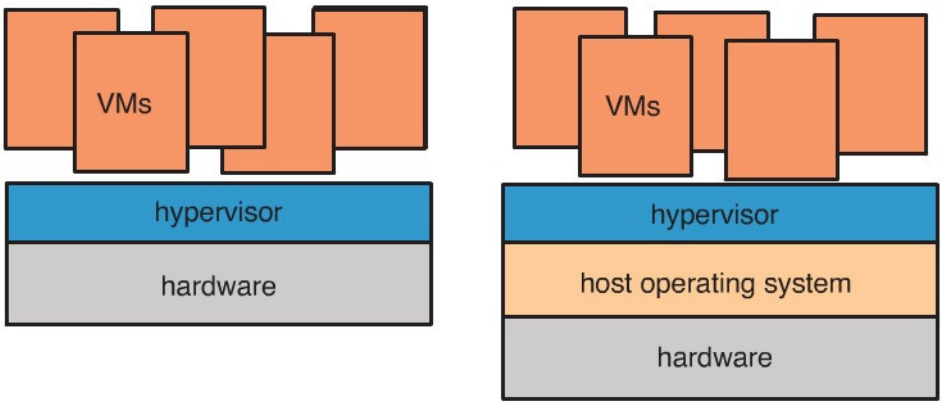


Figure 3. VMware ESX Server Resource Sharing (DISA, 2008).

According to Susanta and Chiueh (2005), hypervisors can either be standalone or hosted. Standalone (type I or fully virtualized) hypervisors directly interact with a machine's hardware, while hosted (type II or paravirtualized) hypervisors run on top of an operating system which then interacts with the hardware (see Figure 4, Haletky, 2010). To the virtual machine or guest operating system, all of these components are seen as real, tangible assets (Haletky, 2010).

All virtual machines are isolated, meaning they are not aware they are running as virtual machines nor are they aware of other virtual machines running under the purview of the hypervisor (Haletky, 2010; Susanta & Chiueh, 2005). Many virtual machines may be managed by a single hypervisor, allowing for improved host resource utilization (Goth, 2007; Lamb, 2009). This aspect is why virtualization is often chosen to consolidate data center resources, but also as a way to save energy in the data center (Lamb, 2009).



Standalone (Type I or Fully Virtualized)

Hosted (Type II or Paravirtualized)

Figure 4. Virtualization Architectures (Haletky, 2010).

Green benefits of virtualization. Table 1 describes green benefits associated with virtualization technologies. Efficiency though virtualization is gained through consolidation in the data center (Lamb, 2009). Consolidation can happen at one of many levels including, operating system, storage, network, memory, processor and power supply. Table 1 lists, from left to right, identified green benefits from the literature, a short description of the benefit, and the reference or references from which the benefit was derived. The benefits listed are only those found in the literature and further benefits may exist. Information in Table 1 can be used to understand why to select virtualization technologies for the enterprise as a way to reduce costs or as a way to begin the process of quantifying energy savings from virtualization.

Table 1

Green benefits of virtualization technologies.

Benefit	Description	Reference
Hardware utilization increase by five to twenty times.	Virtualization can increase hardware utilization by five to 20 times and allows organizations to reduce the number of power-consuming servers.	Lamb, 2009
Reduction in power consumption	Virtualization can increase hardware utilization by five to 20 times and allows organizations to	Lamb, 2009, Hignite, 2009

	reduce the number of power-consuming servers.	
Equipment cost decrease	Costs go way down because one large physical box is much less expensive to buy than ten smaller physical boxes.	Lamb, 2009 Chaudhuri, 2011
Reduced maintenance	It's significantly less expensive to maintain and operate one big server than ten smaller servers.	Lamb, 2009 Chaudhuri, 2011
Reduced heat load	It's important to note that a decrease in overall power consumption is not the only factor. Hand-in-hand with the power reduction goes the same amount of heat load reduction and another add-on for the infrastructure. This double reduction is the reason why consolidation is an enormous lever to moving to a green data center.	Lamb, 2009 Hignite, 2009
Reduced infrastructure and infrastructure power usage	The virtualized systems can communicate using the virtualization system's capabilities, often transferring in-memory data at enormous speed. Performance and energy efficiency increase because the network components are dropped.	Lamb, 2009
Reduced storage needs and storage energy savings	Each of the separate systems has its own storage system, namely disks. The virtualized systems can now share the disks available to the virtualization system. By virtualizing its storage, the virtualization system can provide optimal disk capacity - in terms of energy efficiency - to the virtualized systems.	Lamb, 2009
Reduced (TCO) total cost of ownership	In general, virtualization, including client virtualization, will significantly reduce total cost of ownership (TCO) and energy consumption.	Lamb, 2009
Increased CPU efficiency	In newer virtual server technologies - for example, Unix Logical Partitions (LPARS) with micropartitioning - each virtual server can dynamically increase the number of CPUs available by utilizing the CPUs currently not in use by other virtual servers on the large physical machine. This idea is that each virtual server gets the resources required based on the virtual server's immediate need.	Lamb, 2009 Chaudhuri, 2011
No longer need larger data centers to accommodate expansion	By using virtualization (companies) have avoided the cost of having to build a big, new data center.	Lamb, 2009 Hignite, 2009
Simplified management of servers and resources	In simple terms, server virtualization offers a way to help consolidate a large number of individual small machines on one larger server, easing manageability and more efficiently using system resources by allowing them to be prioritized and allocated to the workloads needing them most at any given point in time.	Lamb, 2009

The sharing of resources allows for increased utilization and decreased need for more physical assets. As stated by Lamb (2009), "the virtual servers still look to users as if they are separate physical servers, but through virtualization, we can dramatically reduce the amount of IT equipment needed in a data center" (p. 89). Underutilized servers can be consolidated through virtualization to reap benefits in both power savings and in increased utilization (see Figure 5). Efficiencies are also gained through reduced maintenance of physical assets as well as automation of patching, updating and reporting of virtual machines (Lamb, 2009). Additionally, less waste is generated over time and less demand for cooling and power are needed in the data center (Chaudhuri, 2011).

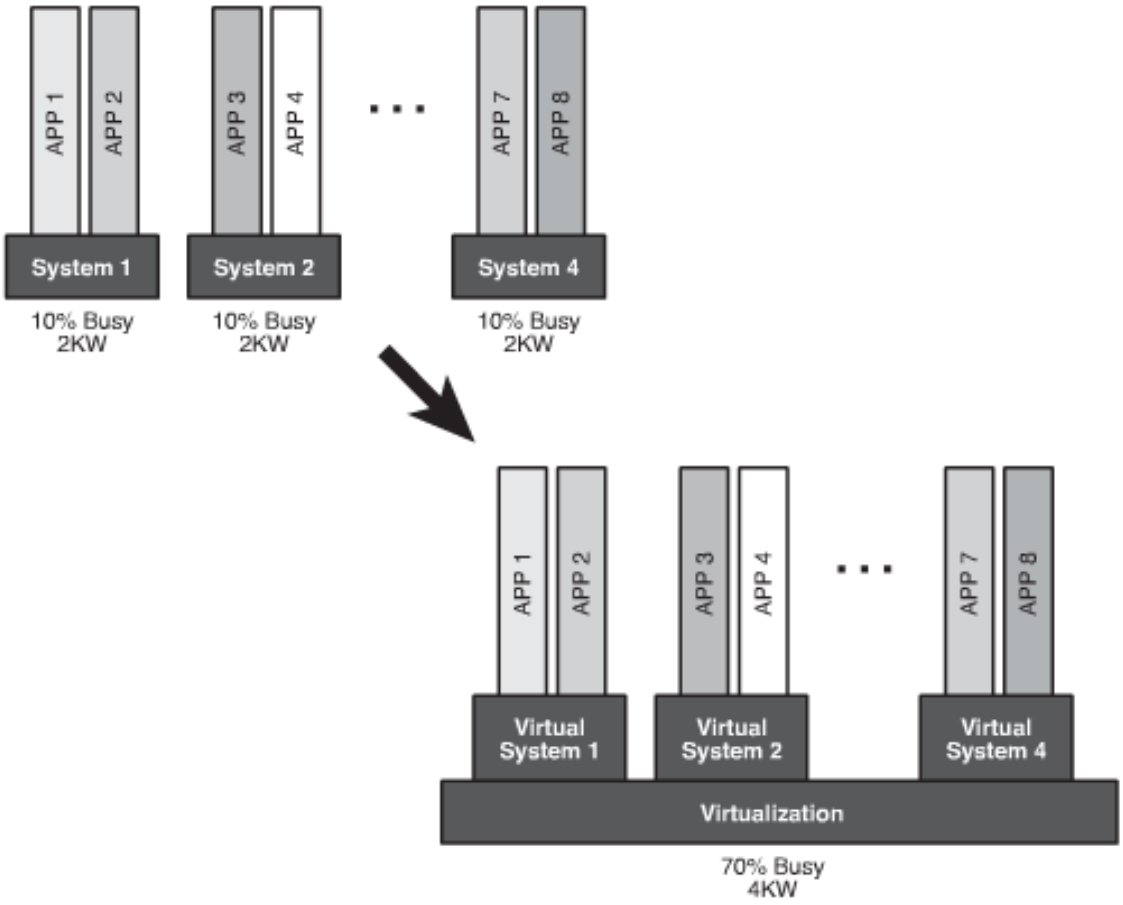


Figure 5. Utilization increase from virtualizing physical servers (Lamb, 2009).

Assessing Threats and Vulnerabilities to Virtualization

Hackers, software flaws, malware, administrator misconfigurations, and disgruntled employees all pose threats to virtualization technologies (Gregg, 2009; Harris, 2010). The VM OS, the host OS, the data center infrastructure, and data center personnel are all susceptible to common computer-aided attacks (Gregg, 2009; Haletky, 2010; Harris, 2010). Given the sheer depth and breadth of attacks against operating systems, networks and other related data center technologies, the focus is on attacks which specifically target server virtualization in the data center. (For a list of common attacks to non-virtualized environments refer to Harris (2010) and Gregg (2009)).

Attacks to virtualization technologies occur for a variety of reasons:

- What's known as the "coolness factor", or being able to access systems or data not normally available for access
- Bragging rights, or being able to brag about hacking a system and gaining access to some data not normally available
- Sabotage or destruction, ranging from the subtle changing of data, to destroying individual or company-wide reputation, to the wholesale destruction of assets
- Personal gain from the theft or changing of data, as well as the theft of funds or systems
- Attacking for hire
- Infiltration for later use
- Espionage or blackmail of the threat of attack
- What's known as White Hat or ethical hacking performed by a PenTester to find weaknesses (Haletky, 2010, p. 16).

Because attacks against virtualization can be for any of the above reasons, securing virtualization in the data center requires understanding why and how these attacks happen (Haletky, 2010). Possible attacks are chosen based upon identified weaknesses which are specific to virtualization technologies (NIST, 2002). Attacks become successful by exploiting some weakness in a system in the data center (Gregg, 2007; Haletky, 2010; Harris, 2010).

Vulnerability identification. Information security weaknesses may be software flaws, unpatched software, system misconfigurations, or any myriad of other possibilities (Harris, 2010). Weaknesses, described here as vulnerabilities, are continually being discovered by security professionals and attackers alike. "A security vulnerability is either an implementation, design or architecture failure by which a hacker may cause a system crash or hang, gain access to private data, or use as a way to gain further access into the virtual network" (Hoesing, 2009). Weaknesses are exploited via attacks which enable a threat agent to compromise the confidentiality, integrity, or availability of a system (Harris, 2010; Mattord & Whitman, 2006). Table 2 lists 15 threats to virtualization in the data center and the vulnerability each threat exploits. This table is used to understand weaknesses of virtualization technologies as well as understand how vulnerabilities might be exploited. Table 2 matches weaknesses (presented in column three) to threats (presented in column one). Matching of vulnerabilities to threats is completed by matching key concepts in a security weakness to a key concept in an attack. Matching concepts for Table 2 is not a one-to-one relationship and therefore multiple attacks may appear matched to a single weakness. A phrase, in bold, is used to summarize each category of weakness for quick reference. Each coded reference appears next to the column of vulnerability or attack vector it represents. If multiple references elicited the same information, both references are listed.

This information represents a generic set of virtualization threats and should only be a starting point for an in depth, holistic, security risk assessment. DISA (2002) states: "the threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment" (p. 15). Security professionals can use this table to either identify weaknesses based upon a threat assessment or identify threats based upon identified weaknesses. For instance, if a company was most concerned about providing availability then they should ensure they understand that virtualization can be attacked through improper virtualization CPU settings and choose controls which mitigate this threat. New threats emerge regularly and this table only lists threats as identified in the literature. It is important to stay current with threat assessments and the threat environment in order to maintain an effective information security program (Harris, 2010).

Table 2

Threats mapped to security weaknesses of virtualization technology.

Threat	Reference	Security Weakness	Reference
A Man in The Middle attack can happen if the product does not adequately verify the identity of the parties at both ends of a communications channel, or does not adequately ensure the integrity of the channel, in a way that allows the channel to be accessed or influenced by an attacker that is not an endpoint.	Haletky, 2010	**Communications** Virtual systems do not inherently protect communications.	Cohen, 2010 Haletky, 2010
Double encapsulation attacks encapsulate traffic with multiple 802.1q envelopes. An outer envelope is deleted to be backward compatible; native VLANs strip the outer envelope from the frame, leaving the inner packet. A switch then redirects to another VLAN than the one initially intended after the outer envelope is deleted.	Haletky, 2010 Harris, 2010	**vSwitch Protections** There are no vSwitch protections from encapsulation attacks that have end points outside the virtual environment.	Haletky, 2010
The virtualization server	Haletky,	**Administrative Roles**	Haletky,

administrator can access the virtual memory swap file for the VM and access its data. Not only that, but a snapshot can also make a copy of the VM's memory for later restoration, as does any sleep mode used for the VM.	2010	Virtualization server administrator roles have unrestricted access to virtual memory swap files by default.	2010
Assigning more memory than required by a VM, the absence of virtualization client software (VMware tools) or a misunderstanding of how virtual machine and host memory is shared. Rolling back virtual machines can also reintroduce malicious code, and protocols reusing TCP sequence numbers that had been previously removed, which could allow TCP hijacking attacks. A subtler issue with rolling back virtual machines is an attackers memory of what has been seen cannot be erased.	DISA, 2008 Haletky, 2010	**Memory Management** Memory management problems associated that can lead to memory remnance and memory leaks between VMs.	Haletky, 2010
Setting the CPU mask to off or allowing certain functionality according to the capabilities of the CPU.	Haletky, 2010	**CPU Mask** The fact that VMs could crash if the CPU masks are modified is a possible security issue and could result in data loss.	Haletky, 2010
It is possible, in effect, to produce a DoS style attack by pinning all VMs to the same CPU, leaving most of the system idle, but forcing the scheduler to use only one CPU for all VMs.	Haletky, 2010	**CPU Affinity** A security concern exists with setting CPU affinity which could lead to data corruption and availability issues.	Haletky, 2010
Weak management interface passwords exploited, passwords stolen through social engineering attack, or poor cryptographic protection on management interface.	DISA, 2008 Haletky, 2010	**Management Interface** If the management appliance operating system is insecure, the entire environment could be insecure.	Haletky, 2010
If a file server has been compromised, any virtual machine that was on the server may have been compromised by an attacker.	DISA, 2008	**Hardware** If the hardware below the hypervisor has insecurities, so does the vmkernel and hence the virtual machines.	Haletky, 2010
Virtual machines can connect or	DISA, 2008	**Mismanagement**	Chaudhuri,

disconnect hardware devices. Attackers may use this capability via non-privileged users or processes to breach virtual machines in several ways. Virtual machine users and processes may be configured to abuse the logging function, either intentionally or inadvertently so that large amounts of data flood the log file. Over time, the log file can consume so much of the virtual server's file system space that it fills the hard disk, causing an effective denial of service.		Like their physical counterparts, most security vulnerabilities will be introduced through misconfiguration and mismanagement.	2011
The act of hijacking an OS and turning it into a VM by inserting a hypervisor underneath it—also called hyperjacking—has a distinct behavior. Such behavior is based on the interaction between the VMBR and the hardware's virtualization extensions. VM-based rootkits (VMBRs) work by inserting a malicious hypervisor underneath the OS and leveraging virtualization to make themselves undetectable by traditional integrity monitors. This technique's feasibility is illustrated in proof-of-concept prototypes such as SubVirt, Vitriol, and Blue Pill. Communications between hypervisor and VM can be detected by malware and used to escape from a VM or run different attacks than in a physical environment.	Carbone, 2008 Carpenter, 2007	**Hypervisor** The layer of abstraction between the physical hardware and the virtualized systems running the IT services is a potential target of attack.	Chaudhuri, 2011 Haletky, 2010
Physical machine being converted to virtual crosses security zones and contaminates a secure zone with an attack vector or insecurity.	Harris, 2010	**Security Zones** One of the largest insecurities is the physical to virtual (P2V) conversion and deployment. In many cases, a P2V will cross security zones-that is, from a production to a virtualization administration network.	Haletky, 2010

Leveraging Strengths and Implementing Controls

Security weaknesses can be countered by implementing features which lower the overall risk level to the system (NIST, 2002; NIST, 2008). These features should be implemented based upon a detailed threat analysis and risk assessment of the system (Harris, 2010; Whitman & Mattord, 2008; NIST, 2002). Table 2 provides data which can be used to begin this process. Security professionals should use this data to either create or update any risk assessment information regarding virtualization assets in the data center. This section examines how to build upon the identified weaknesses and provide security strengths (see Table 3) and a set of security controls (see Table 4). These analyses aid the security professional and the IT decision maker in selection and implementation of virtualization technologies which maintain or improve the security posture of the data center (Haletky, 2010).

Inherent security strengths. Security strengths are features of a system which provide protection from attacks and improve the security posture of the organization (Haletky, 2010; Harris, 2010). Identified security strengths are inherent to virtualization technologies, meaning that they provide benefits by means of their original design or function and not by means of any mitigating factors. Nine identified virtualization security strengths are presented in Table 3. These security strengths include: isolation; improved forensic capabilities; availability; ease of security administration; granularity; trusted base; recovery; separation of security domains; and physical security. All selected strengths are capabilities of virtualization technologies, although not all are currently implemented by all vendors. Strengths are only selected if they are unique to virtualization and are provided by virtualization architecture or design. An example of this is isolation, which is a feature set of virtualization which does not rely upon other features nor does

it require any additional controls to provide system protection. Isolation is provided because the hypervisor segments each virtual machine. Table 3 presents data by the keyword of the strength, bolded, and a quote from a reference which best represents the identified strength. The references from which the data are extracted are listed in the column to the right of each identified strength. Table 3 is designed to be used as a quick reference guide for security professionals and IT decision makers to quickly understand virtualization's positive security feature sets.

Table 3

Security strengths of virtualization technology.

Security Strength	Reference
Isolation VMs are completely isolated from the host machine and other VMs. If a VM crashes, all others are unaffected. Data do not leak across VMs, and applications can communicate over configured network connections only. The narrow interface that a virtual machine presents offers a comparatively harder target for attackers, thus potentially providing higher assurance isolation.	Chauduri, 2011 Cohen, 2010 Garfinkel, 2005 Garfinkel, 2007 Haletky, 2010 Harris, 2010
Improved forensic capabilities This detailed logging has the potential to solve the very challenging task of separating good from bad in an exploited system.	Chauduri, 2011 Garfinkel, 2007
Availability VMware High Availability detects when a host or individual VM fails. Failed individual VMs are restarted on the same host. Yet if a host fails, VMware HA will by default boot the failed host's VMs on another running host.	Haletky, 2010
Ease of security administration Virtualization can make tasks such as system migration, backup, and recovery easier and more manageable. VMs can enhance monitoring and enforcement capabilities in AV and HIPS by allowing efficient interposition on hardware events in the guest OS.	Chaudhuri, 2011 Garfinkel, 2007 Harris, 2010

Safer and more effective patching.	
Granularity Many of the security mechanisms that we have today are best applied at a host granularity. The encapsulation afforded by more single-purpose VM-based environments allows much stricter security policies to be applied at a (virtual) host. Virtualization also provides the ability to strictly limit the actual hardware to which applications contained in VMs have access. For example, the discreet use of a USB memory stick to transfer applications or data off of a machine may be disallowed, a VM's access to the network may be very tightly controlled, and VM data stored on disk can be automatically encrypted.	Garfinkel, 2007
Trusted Base Uniform virtual hardware means only a single "base" operating system image is required, which can then be specialized on a per-application basis.	Garfinkel, 2007 Harris, 2010
Recovery Virtualization can make tasks such as system migration, backup, and recovery easier and more manageable. Virtualization has the potential, but not yet the promise, of distributing decisions across the infrastructure to reduce the impact of successful attacks on select elements of the infrastructure. Faster recovery after an attack.	Chaudhuri, 2011 Cohen, 2010 Garfinkel, 2007
Separation of security domains As backup, logging and monitoring, remote display, and other functionality migrate out of the application VM and into separate protection domains on the virtualization layer, a natural separation occurs between the management plane and the application plane.	Garfinkel, 2007 Harris, 2010
Physical Security Physical Virtualization also provides the ability to strictly limit the actual hardware to which applications contained in VMs have access. For example, the discreet use of a USB memory stick to transfer applications or data off of a machine may be disallowed, a VM's access to the network may be very tightly controlled, and VM data stored on disk can be automatically encrypted.	Garfinkel, 2007

Recommended security controls. Security controls are recommended as a way to reduce the level of risk to the IT system and its data to an acceptable level (Harris, 2010; NIST, 2008). It is important to note that although risk can be mitigated to an acceptable level, it cannot be completely eliminated (Harris, 2010; NIST, 2002). Before implementing a control solution to minimize or eliminate an identified risk, NIST (2002) recommends that the following factors should be considered:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability (p. 26)

The eight potential mitigating security controls presented in Table 4 are merely recommendations and should not be used without a detailed risk analysis performed of the systems involved (NIST, 2002; NIST 2008). Selecting security controls is a balance between cost and protection (Harris, 2010). When selecting controls it is important to note that the cost of protecting the system should not exceed the value of the data on the system (Harris, 2010). Specific costs relating to security controls are not provided as these vary per environment. Table 4 should only be used to understand how to mitigate identified weaknesses. Weaknesses identified in Table 2 are reused and are matched to controls identified in the literature. Identified weaknesses of a specific virtualized system can then be matched against recommended controls. This allows for quick control selection by the security professional. For instance, if the risk assessment concluded that virtualization root kits were the greatest threat to the virtualized

information system then the security professional could consult Table 4, identify the security weakness as *hypervisor*, and choose to implement a control which verifies the integrity of the hypervisor before startup. References are provided to allow for a more detailed understanding of the controls, as necessary. Matching is performed based upon common themes between the identified weakness and the control sets. The security controls in Table 4 can be used as a guide for IT security professionals in securing virtualized systems and as a tool for IT decision makers for understanding what controls to implement and what additional features to purchase or pursue to secure the data center. Hardening guides referenced in the table can be found in *References*. It is important to note that this table is not all-inclusive and is only a reflection of the selected literature used in this study.

Table 4

Security weaknesses mapped to selected mitigating controls.

Weakness	Control	Reference
Communications Virtual systems do not inherently protect communications.	Firewalls, intrusion detection systems and process separation required in greater numbers than physical systems due to the increase in virtual networks. Protection is needed regardless of whether the network is physical or virtual.	Cohen, 2010 Haletky, 2010
vSwitch Protections There are no vSwitch protections from encapsulation attacks that have end points outside the virtual environment.	The vSwitch drops all multiply encapsulated packets that the vSwitch encounters coming into it or trying to leave it.	Haletky, 2010 VMware, 2008
Administrative Roles Virtualization server administrator roles have unrestricted access to virtual memory swap files by default.	Admin role assignment to users should be documented and reviewed monthly. Flags should be set on critical files and warnings raised when they are accessed by a user. All group and role changes should be logged.	DISA, 2008
Memory Management	Install VMware tools or Xen tools, which manage the VMs memory. Ensure	Haletky, 2010

Memory management problems associated that can lead to memory remnance and memory leaks between VMs.	administrators are trained to understand memory allocation and configuration.	
CPU Mask The fact that VMs could crash if the CPU masks are modified is a possible security issue and could result in data loss.	Use guest OSs with HAL (hardware abstraction layers). Extra care should be paid to Unix and Linux OSs as they are vulnerable.	Haletky, 2010
CPU affinity A security concern exists with setting CPU affinity, which could lead to data corruption and availability issues.	Ensure administrators are trained to understand CPU affinity, especially with hyper-threaded CPUs .	Haletky, 2010 VMware, 2008
Management Interface If the management appliance operating system is insecure, the entire environment could be insecure.	Harden OS with recommended guides (DISA, VMware, CIS). Ensure all patches and software are up to date, run antivirus and intrusion detection systems.	CIS, 2009 DISA, 2008 VMware, 2008
Hardware If the hardware below the hypervisor has insecurities, so does the vmkernel and hence the virtual machines.	Ensure all firmware is up to date. Verify firmware checksums against manufacturer checksums. Disable unused hardware. Do not allow guests to control hardware devices outside of the virtual infrastructure. Ensure hardware meets hardware compatibility guidelines for the virtualization solution. Just as the guest OS is subjected to the same security risks as a physical system, security measures (e.g., antivirus agents, spyware filters, IDs) should be installed on all VMs.	Chaudhuri, 2010 CIS, 2009 DISA, 2008 Haletky, 2010
Mismanagement Like their physical counterparts, most security vulnerabilities will be introduced through misconfiguration and mismanagement.	Implement a configuration management program. Log and review all configuration changes. Ensure administrators are trained.	Chaudhuri, 2010 CIS, 2009 DISA, 2008 VMware, 2008

	Implement dual control over administrator actions. A periodic configuration assessment should be performed to achieve a known and trusted state of the virtual environment.	
Hypervisor The layer of abstraction between the physical hardware and the virtualized systems running the IT services is a potential target of attack.	Use digital signatures to certify the integrity of third party hypervisors. The virtualization layer resides on the host OS, so the utmost care should be taken to ensure that the host OS is not compromised by virus attacks. It is possible to detect root kits by using esoteric methods. Keith Adams of VMM, VMware Virtual Machine Monitor, discovered a way to detect some of these root kits by looking at resource consumption of the translation look aside buffer (TLB).	Carbone, 2008 Chaudhuri, 2010 Haletky, 2010
Security Zones One of the largest insecurities is the physical to virtual (P2V) conversion and deployment. In many cases, a P2V will cross security zones-that is, from a production to a virtualization administration network.	Network best practices should be applied to harden the network interfaces of the virtual machines. Network segmenting of VMs can be performed to mitigate the risks of various types of network attacks. The trust zones can be separated by using physical security devices. Policies and procedures as well as proper training are necessary to prevent contamination across security zones. A laptop could be used for the P2V conversion, which could then be vetted across security zones after it is brought to the security level of the zone.	Chaudhuri, 2011 Haletky, 2010

Conclusions

Virtualization technology in the data center provides new ways of reducing costs through green efficiencies (Lamb, 2010; Stansberry, 2005). Green benefits are realized through the consolidation of IT assets that virtualization provides (Lamb, 2010). The ability to provide the data center with increased server utilization while decreasing heat, maintenance, and footprint are some of the many reasons described in Table 1 that companies are choosing to implement virtualization (Hignite 2009; Lamb, 2010). The value of green IT pays off for companies not just in statistical increases in efficiencies but also in perceived social responsibility to stakeholders (Lamb, 2010).

Integration of virtualization technology into the data center relies upon the understanding of security strengths and weaknesses (Haletky, 2010). Security strengths as illuminated in Table 3 should be used by security professionals to leverage virtualization technologies in ways which enhance the confidentiality, integrity and availability of the data center. The data in Table 3 can also be used by IT managers and executives to select virtualization features and products which meet the security standards of their organizations and which also complement and mitigate security weaknesses in their infrastructures. Security weaknesses are highlighted in Table 2 and Table 4. The information in these tables should be used to evaluate virtualization products for implementation in the data center. This data can also be used to understand the security weaknesses of existing virtualization products which may already be in place in the data center.

An in depth risk assessment should be performed before taking action on any security controls or recommendations made in this study (NIST, 2002). The risk assessment framework used in this study is NIST SP800-30. This framework can be used in the data center to evaluate current and future virtualization implementations. IT security professionals can use the

information in Table 4 to begin the risk assessment process. The selection of controls should commence after the risk assessment has identified security weaknesses of virtualization implementations in the data center (NIST, 2002; NIST 2008). Controls identified in Table 4 can be used to select controls which mitigate vulnerabilities in real world enterprise data centers. IT decision makers and security professionals can use this data to select and implement controls which enhance the CIA of virtualization assets and the data center.

Effective policy, procedure, and technical controls are necessary for maintaining secure virtual environments (Haletky, 2010; NIST, 2002; NIST, 2008). This combination, along with the assurance that confidentiality, availability and integrity of systems are met, should ensure defense in depth of the data center (Harris, 2010). Ensuring that our IT systems are not creating an undue strain on power, economics and administration is key in creating a sustainable IT future (Tomlinson, 2010; Webber & Wallace, 2009). Understanding the features which make virtualization green, as discussed in Table 1, is necessary for making the right decisions for IT sustainability (Lamb, 2009). Understanding the combination of IT sustainability and IT security gives the IT professional the confidence to make decisions which benefit the data center for the new millennium.

References

Bell, C. & Smith, T. (2007). *Critical evaluation of information sources.* Retrieved from: http://libweb.uoregon.edu/guides/findarticles/credibility.html

Busch, C. De Maret, P., Flynn, T., Kellum, R. Le, S., Meyers, B., Saunders, M., & White, R., (2005). *Content Analysis*. Retrieved from: http://writing.colostate.edu/guides/research/content/

Cameron, K. W. (2009). Green introspection. *IEEE computer, 42*(1), 101-103. doi: 10.1109/MC.2009.18 .

Carbone, M., Lee, W., & Zamboni, D. (2008). Taming virtualization. *Security & Privacy, IEEE*, *6*(1), 65-67. doi: 10.1109/MSP.2008.24.

Carpenter, M., Liston, T., & Skoudis, E. (2007) Hiding virtualization from attackers and malware. *Security & Privacy, IEEE, 5*(3) 62-65. doi: 10.1109/MSP.2007.63.

Chaudhuri, A., von Solms, S.H., & Chaudhuri, D. (2011, January). Auditing security risks in virtual IT systems. *ISACA Journal,* 16-25.

Clemens, B. (2006). Economic incentives and small firms: Does it pay to be green? *Journal of Business Research, 59*(4), 492.

Cohen, F. (2010). The virtualization solution. *Security & Privacy, IEEE. 8*(3), 60-63. doi: 10.1109/MSP.2010.108.

Common Criteria. (2009). Part 1: Introduction and general model. *Common Criteria for Information Technology Security Evaluation*. Common Criteria Recognition Arrangement. Retrieved from: http://www.commoncriteriaportal.org/cc/

Corporate Executive Board. (2007). Green IT initiatives. *The Corporate Executive*

Board: What the best companies do. Retrieved from: http://hosteddocs.ittoolbox.com/greenit.pdf

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: SAGE.

Cybercrime: Public and private entities face challenges in addressing cyber threats (GAO-07-705), (2007). Washington, DC: Government Accountability Office.

Defense Information Systems Agency. (2008). *ESX server security technical implementation guide*. Washington, DC: Department of Defense. Retrieved from: http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf

Energy Star Program. (2007). *Report to congress on server and data center energy efficiency: Public Law 109-431*. Washington, DC: Environmental Protection Agency.

Esty, D., & Winston, A. (2009). *How smart companies use environmental strategy to innovate, create value, and build competitive advantage*. Hoboken, NJ: John Wiley & Sons, Inc.

Ettinger, L. (2010). Developing the annotated bibliography. *AIM 609, Terminal Project*. Retrieved from: http://blackboard.uoregon.edu

Fong, L., & Steinder, M. (2007). Duality of virtualization: Simplification and complexity. *ACM SIGOPS Operating Systems Review, 42*(1). doi: 10.1145/1341312.1341330.

Garfinkel, T., & Rosenblum, M. (2005). Proceedings from the 10th workshop on hot topics in operating systems: *When virtual is harder than real: Security challenges in virtual machine based computing environments. Santa Fe, NM: USENIX.*

Garfinkel, T., & Warfield, A. (2007). What virtualization can do for security. *;login:, 32*(6), 28-34. Retrieved from http://www.usenix.org/publications

Goth, G. (2007). Virtualization: Old technology offers huge new potential. *IEEE Distributed Systems Online, 6*(2), 3. doi: 10.1109/MDSO.2007.10.

Green IT raises security fears. (2007). *Computer Weekly*, *12*(1), 30-32. Retrieved from Business Source Premier database.

Gregg, M. (2007). *Certified ethical hacker*. Indianapolis, IN: Que Publishing.

Haletky, E. L. (2010). *VmWare vSphere and virtual infrastructure security: Securing the virtual environment.* Upper Saddle River, NJ: Prentice Hall.

Harris, S. (2010). *All-in-one CISSP exam guide* (4th ed.). Emeryville, CA: McGraw-Hill.

Hewlett Packard. (2007). *Performance evaluation of virtualization technologies for server consolidation.* Palo Alto, CA: Padala, P., Zhu, X., Wang, Z., Singhal, S., Shin, K., G. doi: 10.1.1.70.4605.

Hignite, K. (2009). Low-carbon computing. *Educause Review, 44*(6), 34 -36. Retrieved from: http://uolibraries.worldcat.org/oclc/496120088

Hoesing, M. T. (2009). Virtualization security assessment. *Information security journal: A global perspective, 18*(3), 124-130. doi: 10.1080/19393550902791440

Information System. (n.d.). In Answers.com. Retrieved from http://www.answers.com/topic/information-system

Intergovernmental Panel on Climate Change. (2007). *Climate change 2007: Synthesis Report*. Valencia, Spain: IPCC. Retrieved from: http://www.ipcc.ch/publications_and_data/publications_and_data_reports.shtml

Jilg, J. (2007). Virtualization takes hold. *Communications news, (44)*5, 13-14. Retrieved from: http://uolibraries.worldcat.org/oclc/208622926

Kant, K. (2009). Toward a science of power management. *IEEE Computer, 42*(9), 99-101. doi: 10.1109/MC.2009.303

Lamb, J. (2009). *The greening of IT: How companies can make a difference for the environment*. Upper Saddle River, NJ: IBM Press.

Landoll, D. J. (2006). *The security risk assessment handbook: A complete guide for performing security risk assessments.* Boca Raton, FL: Auerbach Publications.

Lawrence Berkeley National Laboratory. (2010). Best practices checklist: *Data center energy management.* Retrieved from: http://hightech.lbl.gov/DCTraining/best-practices.html

Lester, J. D., Lester, J. D. (2007). *Writing research papers: A complete guide, Twelfth edition*. New York, NY: Pearson.

Liao, X., Hu, L., & Jin, H. (2010). Energy optimization schemes in cluster with virtual machines. *Cluster Computing, 13*(2), 113-126. doi: 10.1007/s10586-009-0110-2

Manning, W. (2010). *CompTIA strata green IT.* Online: Emereo Pty Limited.

Mattord, H. J., & Whitman, M.E. (2006). *Readings and cases in the management of information security.* Boston, MA: Thomson Course Technology.

National Institute of Standards and Technology. (2002). *Risk management guide for information technology systems.* (NIST SP800-30). Washington, DC: U.S. Department of Commerce.

National Institute of Standards and Technology. (2008). *Managing risk from information systems: An organizational perspective.* (NIST SP800-39). Washington, DC: U.S. Department of Commerce.

National Institute of Standards and Technology. (2009). *Recommended security controls for federal information systems and organizations.* (NIST SP800-53). Washington, DC: U.S. Department of Commerce.

Obenzinger, H. (2005). *What can a literature review do for me?* Retrieved from http://ual.stanford.edu/pdf/uar_literaturereviewhandout.pdf

Peles, A. (2008). Virtualization affects applications. *Communications News, 45*(5), 22-23. Retrieved from: http://uolibraries.worldcat.org/oclc/23191261

Perez, R., van Doorn, L., & Sailer, R. (2008). Virtualization and hardware-based security. *Security & Privacy, IEE, 6*(5), 24-31. doi: 10.1109/MSP.2008.135.

Public Printing and Documents, 44 U.S.C. §3542 (2010).

SANS (2010). Overview. *The top cyber security risks.* Retrieved from: http://www.sans.org/top-cyber-security-risks/

Sharif, M. I., Lee, W., Weidong, C., & Lanzi, A. (2009). *Proceeding of the 16th ACM conference on computer and communications security:* Secure in-VM monitoring using hardware virtualization. Chicago, IL: ACM. doi: 10.1145/1653662.1653720

Sinnett, W. M. (2010). Green IT is more than a 'feel good' issue - Technology is making it possible for businesses to reap enormous benefits without sacrificing quality, efficiency or environmental goals. *Financial Executive*, *26*(2), 60.

Stansberry, M. (2005). *Data center news:* Power-saving technologies in the data center. Retrieved from: http://searchdatacenter.techtarget.com/news/1144396/Power-saving-technologies-in-the-data-center

Stuenkel, M. (2009). Green IT best practices at the University of Michigan. *EDUCAUSE Quarterly, 32*(3).

Susanta, N., & Chiueh, T. (2005). *A survey of virtualization technologies* (Technical Report No. 179). Stony Brook, NY: SUNY at Stony Brook. Retrieved from http://www.ecsl.cs.sunysb.edu/tr/TR179.pdf

The top 12 green-IT vendors. (2008). *Computer World,* 42(8), 36-37. Retrieved from Academic Search Premier database.

The Center for Internet Security. (2008). *Center for internet security benchmark for xen 3.2.* Retrieved from http://cisecurity.org/en-us/?route=downloads.benchmarks.

The Center for Internet Security. (2009). *Security configuration benchmark for vmware esx 3.5*. Retrieved from http://cisecurity.org/en-us/?route=downloads.benchmarks.

Tomlinson, B. (2010). *Greening through IT: Information technology for environmental sustainability*. Cambridge, MA: MIT Press.

Uhlig, R. et al. (2005). Intel virtualization technology. *IEEE computer*, *38*(5), 48-56. doi: 10.1109/MC.2005.163.

University of North Carolina at Chapel Hill. (2007). *Literature reviews*. In the writing center. Retrieved from: http://www.unc.edu/depts/wcweb/handouts/literature_review.html

Vaughan-Nichols, S. J. (2008). Virtualization sparks security concerns. *IEEE computer*, *41*(8), 13-15. doi: 10.1109/MC.2008.276

Virtualization Products. (2007). *Communications News, 44*(5), 23. Retrieved from http://search.ebscohost.com.libproxy.uoregon.edu/login.aspx?direct=true&db=ufh&AN=25069265&site=ehost-live&scope=site

VMWare. (2008). *Security hardening: Vmware infrastructure 3.* Retrieved from http://www.vmware.com/files/pdf/vi35_security_hardening_wp.pdf

Webber, L., & Wallace, M. (2009). *Green tech: How to plan and implement sustainable IT solutions*. New York, NY: AMACOM.

Whitman, M. E., & Mattord, H. J. (2008). *Management of information security* (2nd ed.). Boston, MA: Course Technology Cengage Learning.