

Regis University

## ePublications at Regis University

---

Regis University Student Publications  
(comprehensive collection)

Regis University Student Publications

---

Summer 2013

### The Use of Vulnerability Assessments: a Survey

Charles D. Lybrand  
*Regis University*

Follow this and additional works at: <https://epublications.regis.edu/theses>



Part of the [Computer Sciences Commons](#)

---

#### Recommended Citation

Lybrand, Charles D., "The Use of Vulnerability Assessments: a Survey" (2013). *Regis University Student Publications (comprehensive collection)*. 223.  
<https://epublications.regis.edu/theses/223>

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact [epublications@regis.edu](mailto:epublications@regis.edu).

**Regis University**  
College for Professional Studies Graduate Programs  
**Final Project/Thesis**

# **Disclaimer**

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

**THE USE OF VULNERABILITY ASSESSMENTS: A SURVEY**

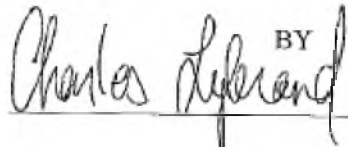
A THESIS

SUBMITTED ON 31 OF JULY, 2013


TO THE DEPARTMENT OF INFORMATION TECHNOLOGY  
OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES


OF REGIS UNIVERSITY

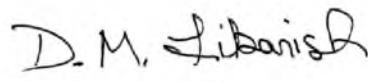
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN  
INFORMATION TECHNOLOGY MANAGEMENT

BY  
  
\_\_\_\_\_  
Charles D. Lybrand

APPROVALS

  
\_\_\_\_\_  
Robert Mason, Thesis Advisor

  
\_\_\_\_\_  
Shari Plantz-Masters

  
\_\_\_\_\_  
Daniel Likarish

### **Abstract**

One of the most significant challenges faced by senior business and technology managers is securing organizational data in light of rising threats and compliance requirements. The use of vulnerability assessments has stood out as one strategy to help protect against malicious computer attacks. Vulnerability assessments are conducted to identify security holes within information systems including: networks, servers, and applications. These assessments can be performed by an organization's internal staff or outsourced to a third-party vendor. Outsourcing is especially important for small organizations who typically do not have the resources or expertise to conduct their own vulnerability assessment. This thesis will investigate vulnerability assessments and the security of data in small organizations. Although the literature on information systems security is immense, little seems to exist on the security weaknesses of small organizations and the safeguards that vulnerability assessments can provide. This thesis will examine the literature, develop a methodology, and present the results of survey responses from at least five third-party vulnerability assessment organizations. The study intends to show the common weaknesses faced by small organizations and make recommendations on common countermeasures.

*Keywords:* external vulnerability assessment, internal vulnerability assessment, penetration test, ethical hacking, IT audit, IT risk, IT security, SMB

### **Acknowledgements**

I would like to express my sincere gratitude to my fellow colleagues in the IT security community and their passion for sharing their wealth of knowledge.

I am especially grateful to Robert Mason, Ph.D for his honest and helpful feedback in the creation of this thesis proposal to the completion of this thesis. I would also like to thank Shari Plantz-Masters, for copy editing the final drafts of this study.

I am ever so grateful to several people who helped me during the initial stages of research. They are Ernie Eugster, Tyler Tobin, Chris White, and Rey Hernandez.

I continue my thanks to Regis University and professors of the College of Professional Studies department for their support and encouragement throughout my quest to obtain a Masters in Information Technology Management.

Finally, I want to express gratitude to my parents and brothers for always setting the bar high and helping me to achieve my dreams.

THIS PAGE INTENTIONALLY LEFT BLANK

### **List of Figures**

Figure 4.1- Industry Preferred Vulnerability Assessment Software

Figure 4.2 - Vulnerability Assessment Software Overall Satisfaction

Figure 4.3 - Amount of External Vulnerability Assessment in a Year

Figure 4.4 - Amount of Internal Vulnerability Assessment in a Year

Figure 4.5 - Typical Size of Organization VA is Performed Upon

Figure 4.6 - Amount of IP Addresses Scanned During an External VA

Figure 4.7 - How Many Vulnerabilities are Found on Average Per Device

**List of Abbreviations**

CPA: Certified Public Accountant

DMZ: De-Militarized Zone

DOS: Disk Operating System

FDIC: Federal Deposit Insurance Corporation

FTP: File Transfer Protocol

GLBA: Graham Leach Bliley Act

HIPAA: Health Insurance Portability and Accountability Act

IT: Information Technology

PCI: Payment Card Industry

SMB: Small Business

SOX: Sarbanes Oxley

SQL: Structured Query Language

SSL: Secured Socket Layer

UPS: Uninterruptible Power Supply

URL: Uniform Resource Language

VA: Vulnerability Assessment

VNC: Virtual Network Computing

## Table of Contents

<b>List of Figures</b>	v
<b>List of Abbreviations</b>	vi
<b>Chapter 1 – Introduction</b>	page 1
<i>IT Security Regulation &amp; Compliance</i>	page 2
<i>Vulnerability Management Need</i>	page 4
<i>Vulnerability Assessment Software</i>	page 6
<i>Vulnerability Assessment Problems</i>	page 8
<b>Chapter 2 – Literature Review</b>	page 14
<i>Vulnerability Assessment Requirements</i>	page 15
<i>Barriers and Challenges</i>	page 17
<b>Chapter 3 – Methodology</b>	page 18
<b>Chapter 4 – Project Analysis and Results</b>	page 20
<i>Survey Questions and Results</i>	page 20
<b>Chapter 5 – Conclusions</b>	page 29
<i>Limitations and Challenges</i>	page 29
<i>Future Work</i>	page 30
<b>References</b>	page 31
<b>Appendix A – IRB Approval Letter</b>	page 38
<b>Appendix B - Survey Instrument</b>	page 39
<b>Appendix C – Sample Email to IT Professionals</b>	page 47
<b>Appendix D - Survey Email with Link</b>	page 48

## **Chapter 1 - Introduction**

An organization must always be one step ahead of a hacker or employee with malicious intent. A company should have a vulnerability assessment (VA) performed and promptly remediate the findings before a security breach occurs. Vulnerability assessments are conducted to identify security holes within information systems including: networks, servers, and applications. These assessments can be performed by an organization's internal staff or outsourced to a third-party vendor. According to a 2011 Cost of Data Breach Study in the United States, "data breaches cost companies an average of \$194 per compromised record" (Ponemon 2012, p.4). Although a VA can be expensive, a company is better off having a VA and reducing the chance of data breach. VA's are often introduced to companies as an enforcement of compliance to a privacy law, but are more than a cost expenditure. Although a VA can have its own constraints, conducted by an individual with adequate IT security knowledge, a VA can depict the risk level of an organizations network.

Rising security threats and compliance requirements have created challenges for securing the confidentiality, integrity, and availability of data. In 2008 a website was hacked every fourteen seconds and this rate was three times faster than the previous year (Sophos 2008, p. 1). With continual growth of hacking and computer related crimes, security breaches cost the global economy billions of dollars every year (McAfee 2011, p. 5). A popular attack vector amongst hackers are SQL injection attacks which exploits a security vulnerability via website or directly to a SQL database. SQL, an abbreviation for Structured Query Language, is a programming language that requests information from databases. SQL injection attacks account for 17% of attack methods and are a large majority of security breaches (Barnett 2009, p.4). Such SQL vulnerabilities have allowed hackers to obtain sensitive information from organizations'

publicly facing and internal network addresses. In March 2011, for example, a web security company discovered a "mass-injection campaign that compromised over 28,000 URLs, including several iTunes URLs" (James 2011, p.22). Most sites targeted by this vulnerability were owned by smaller companies. Along with the continually increasing number of incidents and the rising number of discovered vulnerabilities, the speed at which systems are attacked is also drastically accelerating. Identifying vulnerabilities and addressing them in a timely manner is vital for keeping data secure.

### **IT Security Regulation & Compliance**

Moreover, government regulations and industry compliance are requiring organizations to maintain an in-depth IT security program. Small businesses to large global organizations are being forced to comply with industry regulations or face financial penalties and possible jailtime. Although "the federal government does not regulate the security of non-government computer systems" (Moteff 2004, p.2), the federal government requires sensitive customer information to be kept confidential and undisclosed. Specifically, the Gramm-Leach-Bliley Act (GLBA) "requires financial institutions to protect the security and confidentiality of their customers' nonpublic personal information" (Moteff 2004, p.10). Another federal data security regulation is the Health Insurance Portability and Accountability Act (HIPAA). It requires organizations with health records "to take reasonable and appropriate administrative, technical and physical safeguards to ensure the integrity and confidentiality of individually identifiable health information held or transferred by them; to protect against any reasonable anticipated threats, unauthorized use or disclosure; and to ensure compliance with these safeguards by officers and employees" (Moteff 2004, p.10). Any company that houses medical data, especially a hospital,

can be placed under heavy scrutiny if an IT security breach has taken place that impacts medical records.

The chief regulatory law in the United States that controls financial systems is Sarbanes-Oxley. Also known as SOX, the Act of 2002 is a federal law named after its sponsors: U.S. Senator Paul Sarbanes (D-MD) and U.S. Representative Michael G. Oxley (R-OH). The law was intended to increase financial governance and accountability upon companies. Compliance with SOX created a need for review of IT controls since they are often utilized within financial systems and the financial reporting process.

An increasing number of states are also prompting public organizations to protect data. Forty-six states, Washington D.C., Puerto Rico and the Virgin Islands have legislation requiring that companies and/or state agencies disclose to consumers security breaches involving personal information. The states have different verifications on what type of data to be protected, but one state with more than average laws to protect its people, California defines personal information as including name and social security number, drivers license, financial account numbers, medical information, or health insurance data. The laws are meant to protect citizens of the state from theft of data and to disclose information regarding the breach of data. In addition to federal and state regulations, organizations have to meet industry compliance.

The payment card industry (PCI), for example is subject to the PCI Data Security Standard (PCI DSS) which establishes requirements for the detection, prevention, and appropriate reactions to handle computer security incidents. State legislatures are enacting laws around data security and breach notification based on PCI/DSS. The PCI DSS requirement 11.2 states: "Run internal and external network vulnerability scans at least quarterly and after any

significant change in the network. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, pass four consecutive quarterly scans as a requirement for compliance. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV)" (PCI 2010, p.18). This requirement enforces companies that process a certain amount of credit card transactions to conduct quarterly vulnerability scans by a qualified IT security professional. "Merchants belong to one of four levels that is determined by annual transaction volumes" (PCI-DSS 2011, p.1), level 1 being the highest with at least six million credit card transactions a year, and level 4 being less than 20,000 transactions. Level 1 to level 3 merchants require quarterly network scans, and level 4 merchants require annual network scans.

### **Vulnerability Management Need**

The increase in regulations and the greater need for security has sparked increased investment in vulnerability management and outsourcing of security functions. Vulnerability management tools and services can be used to make a system "security smart" by correcting the underlying risks and weaknesses that cyber attacks exploit, rather than attempt to block a specific attack or type of attack. This method has been tremendously successful in identifying system weaknesses, prioritizing resources, minimizing security breaches, and adhering to the data triad of confidentiality, integrity, and availability. As a result, numerous government and industry-specific regulations have been developed that directly require a vulnerability assessment.

The continual growth of vulnerability management is reflected in market analysis. According to market researchers, Frost and Sullivan, the world vulnerability assessment products market is projected to grow from an estimated \$250.8 million in 2006 to \$1 billion by 2014 (Frost & Sullivan, 2008). IT security service providers utilize a wide variety of commercial

software and open sourced software to make a customized tool set to conduct these particular assessments. These resources allow a service provider the ability to find weaknesses in the network before a security breach occurs by an intruder. A business has many reasons to have a vulnerability assessment conducted internally or by an external vendor. With a "93% increase in the volume of Web-based attacks in 2010 over the volume observed in 2009" and a "recorded 6,253 new vulnerabilities in 2010" (Symantec 2011, p.1), the security risk exposure continues to increase. More importantly, government agencies are requiring companies to have vulnerability assessments performed to protect customer information and sensitive data.

Typical users of VA in the IT profession are information security professionals, network administrators, IT managers, IT auditors, and ethical hackers. IT professionals and IT consultants perform VA and are conducted in a process of steps. The first step in performing a VA is to identify the scope of systems and IP addresses to be scanned. After the scope is defined, software is used to identify exposures, conduct risk analysis, and threat trending. Automated VA software is often capable of producing reports that can then assist with addressing exposures by fixing or mitigating the detected vulnerabilities. Finally, reports must be reviewed by the IT department of the organization and a remediation process must be tracked. The process should be tracked for auditing and general IT Security purposes.

An ethical hacker performs VA for the similar reason, except ethical hackers will take the process a step further and attempt to exploit weaknesses in identified systems or IP addresses. Ethical hackers are hired by a company to perform an internal penetration test or external penetration test, usually referred to as "PenTest". A PenTest is different from a VA in that the vulnerability is exploited to show evidence of the risk and weakness upon a system or IP address.

This can be a risk in itself, although agreement are made on testing time and how far to exploit identified weaknesses.

One of the more essential aspects to the successful use of vulnerability assessment (VA), is that the vulnerability scanning software should support a wide variety of capabilities. The software must collect data to create compliance reports for PCI, HIPAA, SOX, GLBA, or associated regulatory agency. It should also provide remediation techniques for vulnerabilities found on IT equipment and IP addresses. The remediation techniques might include links to file download, step-by-step instructions on enabling or disabling a service, or suggested removal of system. Addressing vulnerabilities could be performed by an IT manager, network administrator, computer technician, IT security professional, or consultant. The remediation and reporting process should include IP address of the vulnerability, help documentation including links or filename, and procedures taken in case a system becomes unavailable. Finally, a useful feature is to support the calculation of a risk-based score on each asset scanned. Automated VA software have different risk ranking systems, but are often based upon similar naming of risk: low, medium, and high risk. The high risks are usually referred to as "critical" and require immediate remediation or appropriate mitigation process.

### **Vulnerability Assessment Software**

The VA product market is increasing, but a few vendors produce VA software that IT professionals prefer. Nessus, GFI Languard, Qualysguard, Symantec NetRecon, Lumension Vulnerability Scanner, and Nexpose Rapid7 are among the most popular. Software is differentiated by database of vulnerabilities, ease of use, reporting capabilities, compliance requirements, and pricing.

Accordingly, the type and strategic impacts of vulnerability assessments are vast. In 2010, the state of Colorado hired a third-party vulnerability assessment vendor to conduct a security assessment. It found significant vulnerabilities throughout state government computer infrastructure that allowed the assessment team to "easily gain access to thousands of documents containing Coloradans' sensitive personal information such as Social Security numbers, birth dates and income levels" (Hoover 2010, p.1). For confidentiality purposes, specific vulnerabilities were not released by the state of Colorado.

In another example, the Institute of Electrical and Electronics Engineers (IEEE) admitted to a breach of its network including possible theft of credit card information. The IEEE, who is responsible for developing IT standards, admitted that they had no proof the PCI information disclosure had resulted in harm, but that they "discovered vulnerabilities that the professional association 'immediately corrected' to avoid future network incursions" (Infosecurity 2011, p.1).

Government agencies use vulnerability assessments on the network perimeter and to assess internal network controls. The network perimeter is the boundary between a private network and the public, such as the internet. This is often referred to as "de-militarized zone" or DMZ. The Federal Deposit Insurance Corporation (FDIC), for example, found that despite significant investments in resources to defend its network perimeter, the VA found several improvements were needed in physical access security and the protection of sensitive data. The external vendor that performed this VA, PricewaterhouseCoopers is one of the big four accounting firms and they all perform IT audits on global organizations (FDIC 2002, p.1). Small to large CPA firms are also cashing in on the increasing need for IT security and performing VA as part of an IT assessment.

Can VA produce secure networks? The IT literature seems to agree that it does. In essence, “a vulnerability is a security weakness present in a network” (Vasireddy et al. 2004, p.187) that could allow a disgruntled employee or malicious user to create harm within a network. Even a fully patched device can have vulnerabilities “because software vendors send out periodic security alerts and release patches to fix these vulnerabilities” (Wojcik 2010, p.1). The patching of a device refers to installing a software fix intended to remove security issues. Patch management is a complicated process due to vendors constantly releasing new patches and companies having so many devices to patch. Thus, vulnerabilities can exist, but often are revealed at a later time when recognized with automated vulnerability scanning software. However, since “security vulnerabilities are doubling every year” (McGee et al. 2004, p.9), preventing a security breach can be a daunting task for any organization. Security exploits are never ending and hackers become smarter every day.

Four types of security attacks can be identified: "interruption, interception, modification, and fabrication” (McGee et al. 2004, p.10). Information assurance is adversely impacted by these risks in various ways, including when a system is interrupted and the availability of the system/data is affected. Interception refers to an individual gaining access to a system that they were not authorized or allowed to access which could cause a breach in data confidentiality. Modification occurs when an individual tampers with software or hardware resulting in a data integrity issue. Such attacks cause theft of sensitive data, equipment failure, and monetary losses.

### **Vulnerability Assessment Problems**

Although a vulnerability assessment can help to mitigate these attack risks, having an assessment performed can have its own associated risk. One problem with vulnerability assessments is that they only provide a snapshot of a given point in time. Due to this fact, a VA report is only significant for a short period, as new vulnerabilities are found on a daily basis. Another issue, a vulnerability assessment could slow down a network or cause system bottlenecks and force a system to shut down. While this issue is rare, it is still a possibility and concern for the company having the VA. To address this issue, a VA might be performed outside of business operating hours. More importantly, a VA report contains confidential data that could be used against a company in various ways. VA reports can have IP addresses and reveal system information that if placed in the wrong hands could be used against a company.

While researchers have advocated regular VA, small organizations are less likely to have the skills and required resources to carry out their own VA. Small organizations comprise the majority of US businesses. Recent figures reveal that “small firms with fewer than 500 employees represent 99.9 percent of the 29.6 million businesses” (SBA 2011, p.1). Small businesses face the same security threats that large organizations might experience. The problem exists in that smaller organizations often do not have the appropriate resources to perform a VA and properly remediate the findings. Furthermore, small businesses usually don't have the expertise to manage IT and "1 in 7 small and medium sized businesses (SMB) do not have any security software installed, leaving their business open to potential attacks" (AVG 2010, p.3). Hackers are becoming increasingly aware of this issue and are targeting small businesses just as often as large enterprises. "From construction companies to local grocery stores," (Smith G. 2011 p.1) hackers are attacking small businesses in all industries. Malicious employees and

hackers understand that small businesses are often troubled by inadequate resources to fund and staff proper information security standards.

Although the vulnerability assessment process is largely automated, a VA should be performed by a qualified professional and in some cases must be for compliance and regulations. The qualified professional must have knowledge of network topology and setting a scope. IT departments are often restrained by budget and resource allocation, so staying atop of vulnerabilities can be a daunting task, even for the average IT employee. Moreover, "any manual assessment requires a security team that has current, broad and deep technical expertise in a myriad of technologies" (Beyond 2010). The IT Security industry has many certifications for professionals to obtain, but even professionals with certification might not be qualified to perform VA's. Typical IT Security certifications include: CISSP (Certified Information Systems Security Professional), CISA (Certified Information Systems Auditor), QSA (Qualified Security Assessor), CIA (Certified Internal Auditor), but the most relevant for performing VA is CEH (Certified Ethical Hacker).

Keeping an IT security professional in-house can be expensive due to the software licensing of vulnerability management software and proper computer hardware required to perform the examination. The average annual salary of an IT Security Professional is \$90,000 and trends are showing an increase of salary every year (Indeed 2012, p.1). Additionally, commercial VA software can be purchased for thousands of dollars, further driving up the cost. A few vulnerability management products offer free and trial versions, but they are restricted in functionality. These restrictions include limited scanning of IP addresses that cause scalability concerns for large organizations, reporting process that doesn't include compliance templates, and no remediation assistance. Templates are built into the VA software to provide different

reports, product a variety of file types, and omit vulnerabilities from reports. Reports that are generated for the IT department might be more complex and larger than reports generated for a steering committee.

As with any kind of product and service, there are advantages and disadvantages to outsourcing a vulnerability assessment. Qualys and Foundstone are two vulnerability management providers that offer vulnerability scans. They have a service where they manage the hardware and software that is left onsite, providing automatic scans on designated schedules. Basically, this can make it almost effortless for a company to get vulnerability scans. However, it is recommended to outsource the vulnerability management process to a qualified company. For PCI compliance it is required that an approved scan vendor (ASV) perform the VA.

Specifically, Gartner addresses many reasons why a business should outsource IT security. The reduction of risk is a key benefit, but “improved service levels and skill sets, and reduced costs” (Motorola 2010) are among a few other reasons. IT providers are recognizing the need for an assortment of security services. In Colorado, several companies provide IT security services including: vulnerability assessments, penetration tests, and IT auditing. One of the top IT Security providers in Colorado, Coalfire is a fast-growing IT Governance, Risk and Compliance (IT GRC) firm with clients in Retail, Financial Services, Healthcare, Hospitality, Higher Education, Government and Utilities. With many different reasons to choose a vulnerability assessment provider, the benefits to an organization from a VA and remediation are immense. A VA should not be overlooked as one of the vital steps to an information security program.

The thesis statement of this research is: Outsourcing vulnerability assessments to mitigate risk and be compliant with regulations creates advantages for small and medium-sized organizations who do not have the resources and skills to conduct assessments themselves. They should be performed at least on an annual basis, vulnerabilities remediated, and VA management process reviewed by a committee.

To test this thesis statement, this researcher has adopted a three-phase methodology. In the first phase, this researcher reviewed existing literature on information systems security in general and in vulnerability assessments in particular. This research will also allow the development of a survey. The survey will not be designed to ascertain the respondents' attitudes towards VA, but instead will focus on identifying common risks and weaknesses of small organizations. More specifically, the survey will address questions including:

1. What is the likelihood of smaller organizations using VA?
2. What is driving the need for VA?
3. What are key limitations that small organizations face in network security?
4. What are typical vulnerabilities that are seen across small organizations?
5. What security safeguards are recommended by service providers?
6. How do the results reflect the thesis statement?

In summary, rising threats and weaknesses of IT systems are requiring small businesses to perform VA and remediate in a timely manner. The cost of an IT security breach far outweighs the cost of outsourcing a VA or purchasing VA software and conducting in-house. Furthermore, small businesses must adhere to regulatory laws and industry related compliance

by understanding vulnerabilities and its current IT security posture. VA's are more than just a scan of devices followed by a report. Often overlooked as a cost expenditure, a VA is a critical aspect to an organizations IT security program. Having an adequate vulnerability management process can be the difference between a small business financial success or ultimate failure.

## **Chapter 2 – Literature Review**

Although the literature on information systems security is immense, little seems to exist on the security weaknesses of small organizations and the safeguards that vulnerability assessments can provide. Existing literature delves into what vulnerability assessments are, how they can benefit an organization, and best software to use. However, a list of common vulnerabilities found in small businesses to large organizations is not readily available.

The literature, which focuses on the vulnerability of networks, has rapidly developed over the past decade. The field of information technology security is interesting in that companies must constantly be reviewing all layers of data protection to mitigate risk. Two important aspects of data security layers, system patching and hardening protocols should never be overlooked. A vulnerability assessment can deliver a snapshot in time of a business posture on patching methods and system hardening processes. Most importantly, a vulnerability assessment will “test and document the effectiveness of both security policies and controls” (Qualys 2009, p.2).

A vulnerability assessment is the process of running manual and automated tools against a defined set of IP addresses or IP ranges to identify known and potential vulnerabilities in an IT environment. The IP addresses, often referred to as nodes, are active devices connected to a network that can be scanned for running services and protocols. Vulnerability assessments are important to small businesses and global organizations for many reasons. In particular, they can provide an accurate snapshot of the current threat environment for an IT department. The vulnerability assessment process and report could assist in the short and long term goals for a company's IT. Performed by a qualified individual, the VA and vulnerability management process can aid in the risk management phase of IT security.

Commercial VA software has been available since the 1990's, but didn't gain popularity until the early 21st century. Vulnerability assessment software was developed to aid in "finding and dealing with the causes of software security vulnerabilities as they are found in code, design, or system architecture" (NIST 2012, p.1). A National Vulnerability Database maintained by the Department of Homeland Security National Cyber Security Division reports at least ten new vulnerabilities a day. The increased incidents of hacking and rise of IT security compliance requirements for companies has caused the VA process to evolve. What was once a million dollar industry in the late 1990's, turned into a \$3.4 billion market in 2010 for security and vulnerability management solutions (Kolodgy, 2011).

### **Vulnerability Assessment Requirements**

Requirements and specifications for VA compliance and VA software have also dramatically increased. One of the commercially available VA software options, Rapid7 Nexpose requires a fast computer with Microsoft Windows or Linux. In addition, the minimum hardware requirements indicated by Rapid7 are:

- 2 GHz+ processor, 4 GB (32 bit\*)
- 8 GB (64 bit) RAM recommended
- 80 GB+ available disk space (10 GB for Community Edition)
- 10 GB+ available disk space for Scan engines
- 100 Mbps network interface card

Of course, the requirements listed are for a minimal VA scan, and a scan of a global organization could require more extensive hardware. Moreover, software licensing can restrict the amount of devices to be scanned.

Another commercially available VA software, Tenable Nessus Vulnerability Scanner has similar requirements and offers features such as: mobile device auditing, anti-virus auditing, and patch management integration. VA software all share the same concept of scanning for vulnerabilities, but the big difference is in the database of vulnerabilities and reporting capability. There are several other open sourced vulnerability assessment tools available for download, but reporting capabilities are often less than commercially available VA software.

Vulnerability assessment software, whether commercial or open-sourced, is capable of providing a snapshot of a point in time for an organizations vulnerabilities and potential threats to an organizations IT. However, VA software has its limitations. The software is often expensive, can require extensive time for an internal VA, and could slow down a network or potentially crash a device. A VA produces a report that is usually provided to upper management and IT department. However, this in itself is an issue in that now the VA report must then be reviewed and remediated. VA software is rarely capable of removing the vulnerability from the network, it is the IT staff whom takes the final action to remediate VA report findings.

Vulnerability assessments have been performed for several years, but related literature can be insufficient. Existing literature related to VA includes methods of attack for hackers, wireless hacking methods, evaluating IDS, securing network protocols, IT risk assessments, and the different types of VA. Subsequently, literature is usually more focused on penetration tests, which are a vulnerability test with the vulnerabilities being exploited and documented.

Research on VA exists in many different forms. The most prevalent research includes: VA for compliance and regulation requirements, the most popular commercial VA software, and reasons to conduct a VA. Moreover, most research and documentation relates to Penetration testing of networks. A Penetration Test is different from a VA in that the vulnerability is exploited to show evidence of the risk and weakness upon a system or IP address.

### **Barriers and Challenges**

A few barriers and challenges of finding adequate VA research also existed. VA exists in many industries and has different meanings. For the purpose of this research, a VA refers to one being performed on IT equipment including: network equipment, IT infrastructure, and public facing IP addresses. Upon searching for VA research and scholarly articles, several types of VA are presented. These include: climate change, water analysis, and spatial data of geology. Research websites are not always capable of reducing the search to IT VA's. Another barrier, research sites often are not able to search for "IT" and is translated as the word "it" instead, while literature can have "IT" instead of "Information Technology".

Finally, the literature presented in search engines is often expensive, or the only way to get the document is by requesting the file from the author. After requesting several documents from the authors via research website ResearchGate.net, they were rarely sent from the author. This was difficult to understand as ResearchGate.net claims to have over 2.9 million users with 10 million publications. Moreover, VA commercialized literature can be several hundred dollars for a document that might not be sufficient for this research purposes.

### **Chapter 3 – Methodology**

To test the thesis, this research will use a three-phase methodology. In the first phase, this researcher reviewed existing literature on information systems security in general and in vulnerability assessments in particular. This research will also allow the development of a survey. The survey will not be designed to ascertain the respondents' attitudes towards VA, but instead will focus on identifying common risks and weaknesses of small organizations.

In order to maintain ethical research survey standards involving human participants, the research proposal was submitted to the Institutional Review Board (IRB) for exempt status. The exempt status was approved by the Regis IRB as #13-155, per exempt study category 45CFR46.101.b(#2) indicated by Appendix A. Ethical and privacy concerns were considered and implemented during the survey research phase.

The research survey was comprised of multiple choice and several answer questions, along with a few open ended answer boxes for reasoning of answer. All seventeen questions and answer options can be viewed in Appendix B. A web-based forum was utilized to document respondents' answers and track the data into a report. The survey was pre-tested before introduced to the service providers as to ensure the survey can be completed in a timely manner. Accordingly, the service providers will be informed that the survey is voluntary and they can end the survey at any time.

During this second phase, at least five IT security professionals that conduct vulnerability assessment services will be contacted and requested to participate to the survey. The researcher will aim to interview different roles (administrator, manager, director) responsible for VA. Respondents were located from a professional online forum, LinkedIn, based upon location,

skill-set, and work experience including a consulting role. The survey respondents were contacted via e-mail, as telephone conversations caused concern with respondents. A sample e-mail can be reviewed in Appendix C. The use of several independent responses, eight responses total, will help to mitigate the effects of single-respondent bias and differentiate management and employee perceptions of VA in small organizations. More importantly, the survey responses can not be traced back to the individual submitted, in order to keep anonymity.

Finally, the third phase will analyze the data from the survey results to formulate a consensus. The overall results should assist in defining top five vulnerabilities that affect SMBs to global organizations. More importantly, the thesis is designed to fill a gap in the literature between IT security and VA management in small firms.

## **Chapter 4 – Project Analysis and Results**

As indicated in Chapter 3, a survey was created and responses were recorded for data analysis. The survey revealed significant information about vulnerability assessments. More importantly, the survey gained valuable data from industry experts that have performed a significant amount of VA at a variety of organizations. Ultimately, the data analysis can provide insight for IT professionals and enhance a company's IT security posture.

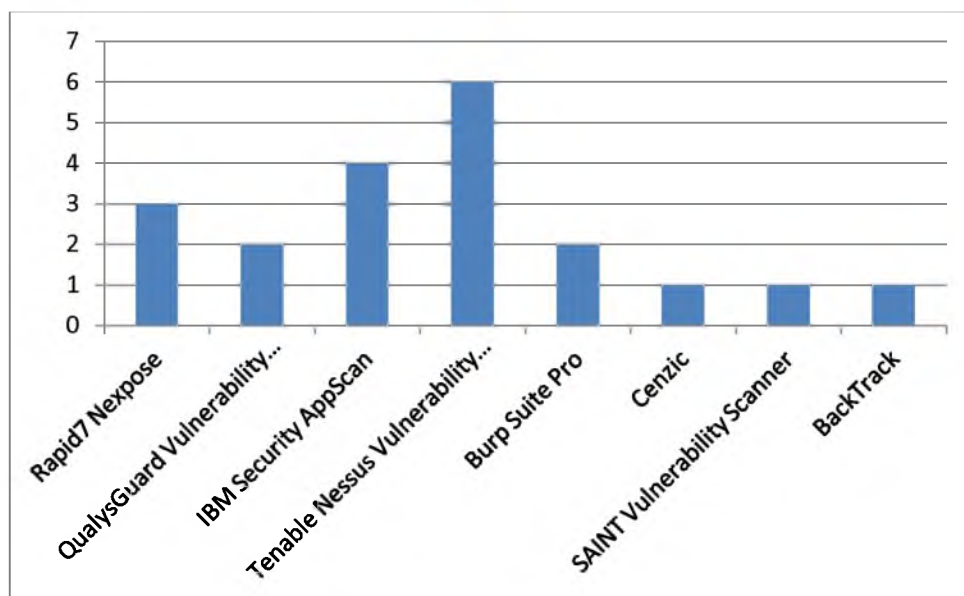
Conducted the week of June 3, 2013 the survey had eight respondents who completed the survey. The web-based survey was created and hosted via SurveyMonkey.com. A generated link was sent via the SurveyMonkey.com e-mail management system as indicated by Appendix D, to maintain anonymity of respondents. A total of seventeen questions were included. The survey was designed to take less than 15 minutes and did not ask for name of respondent, or any company name to also protect the respondents and clients. Demographics from the survey indicated the respondents lived in various parts of the United States.

### **Survey Questions and Results**

The survey instrument, Appendix B, Question 1, "What is your current role within the organization?" and Question 2, "How many years have you been in IT Security?" were asked to confirm that respondents were qualified professionals for the survey. The typical roles of respondents were: Pen Tester / IT Security, Director/Manager, and CEO. All respondents had at least five or more years of IT Security experience, with one individual indicating seventeen years of industry related experience.

Question 3, "What software do you use to perform a vulnerability assessment?" was intended to learn what commercialized and open-sourced software is used amongst industry

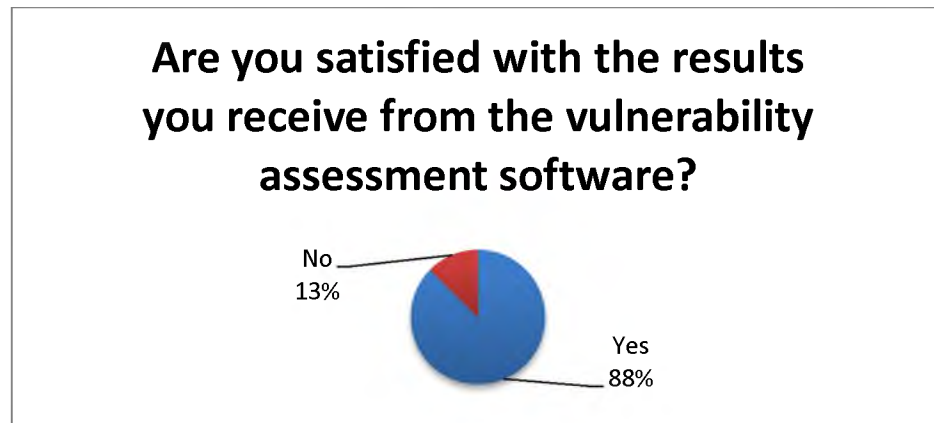
professionals to perform vulnerability assessments. Six out of seven respondents rely upon Tenable Nessus Vulnerability Scanner. Figure 4.1, displays Nessus was the preferred vulnerability assessment software.



**Figure 4.1 Industry Preferred Vulnerability Assessment Software**

The next most popular software, IBM Security AppScan is a different vulnerability scanner in that it is intended for application security testing. Rapid7 Nexpose, QualysGuard Vulnerability Scanner, Burp Suite Pro, and CenZic were Vulnerability Scanner also utilized as industry accepted commercial VA software. An Open-Sourced alternative, the BackTrack suite contains a set of tools intended for full scale penetration testing. The BackTrack suite arranges tools into twelve categories, one of which is vulnerability assessment.

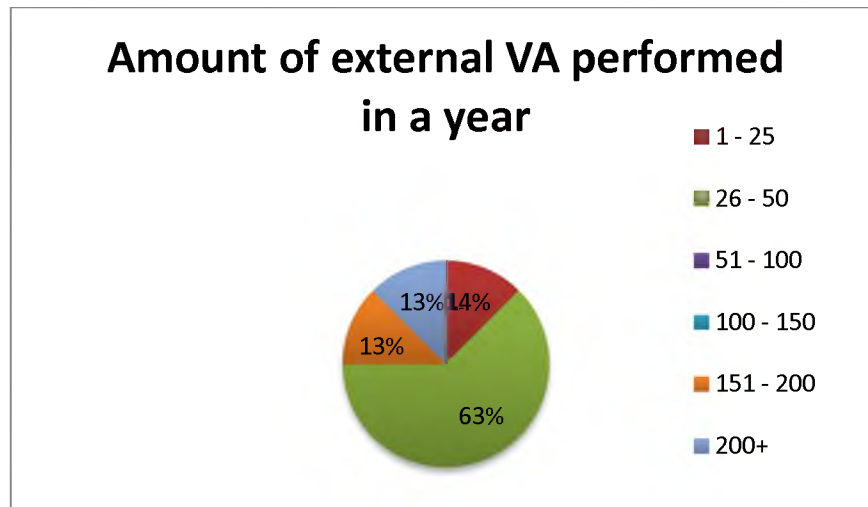
Question 4, "Are you satisfied with the results you receive from the vulnerability assessment software?" suggested that 87% of respondents were generally accepting of the VA software (See Figure 4.2), with one individual stating "Most excel at broad coverage and they are effective at identifying lots of known security issues".



***Figure 4.2 Vulnerability Assessment Software Overall Satisfaction***

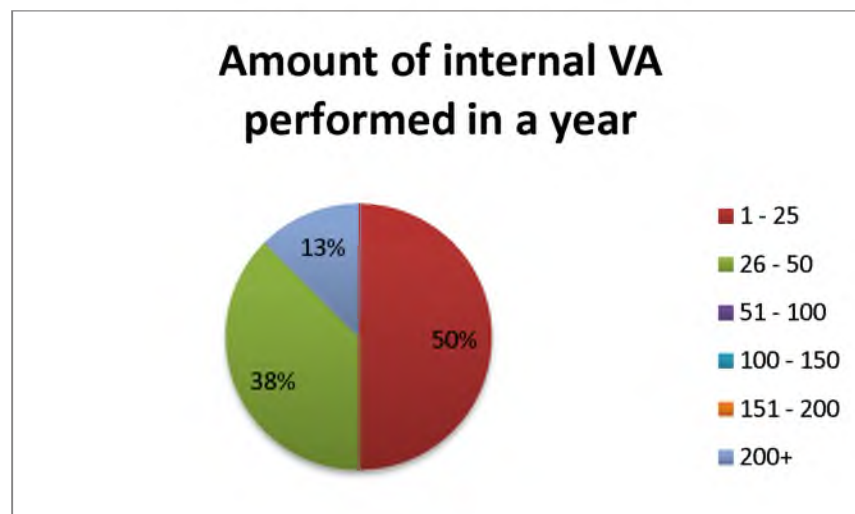
Only one person was unsatisfied with results, and two people provided feedback as to VA related issues including "false positives are annoying" and "would like a bit more robust Web App Testing Framework".

The survey also intended to understand what was generally performed more, internal vulnerability assessments or external vulnerability assessments. Question 5 and Question 6, ask how many external and internal vulnerability assessments are performed in a year. The survey revealed that 63% of respondents perform 26-50 external VA throughout the year (See Figure 4.3).



**Figure 4.3 Amount of External Vulnerability Assessment in a Year**

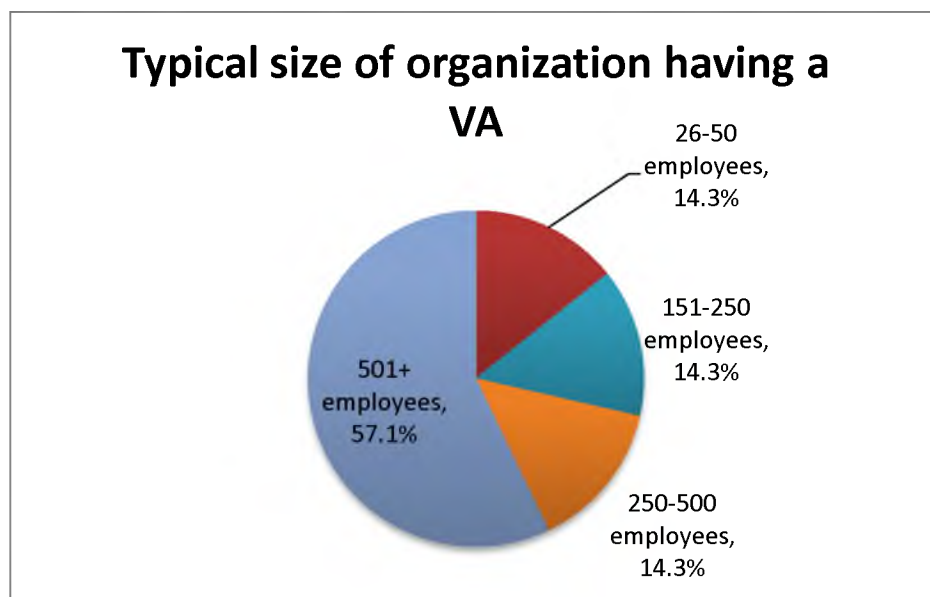
According to survey results, half of the respondents indicated that less than 25 internal VA were performed throughout the year (See Figure 4.4). The results from question 5 and question 6 also revealed that on average, more external VA are conducted than internal VA. A conclusion could be drawn that organizations are more worried about a security threat coming from outside the company network than an internally related vulnerability.



**Figure 4.4 Amount of Internal Vulnerability Assessment in a Year**

One respondent revealed "I spend a bit more time doing internals on-site" relating to the fact that an internal VA will typically have more IP addresses to scan. A global company with several offices could add time to an internal VA from network bandwidth and capability of networks. In addition, increased interaction with the organizations employees can add time to the overall VA project.

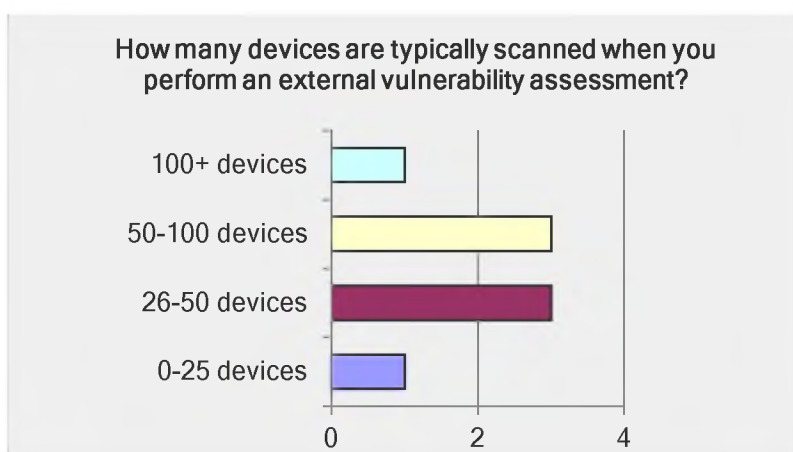
Question 7, "What is the typical size of the organization you perform a VA on?" was intended to reveal the need for VA in small organizations. As revealed from Figure 4.5, over half of survey respondents noted that when they perform VA it is usually at an organization with more than five hundred employees.



**Figure 4.5 Typical Size of Organization VA is Performed Upon**

This could indicate that large organizations and global companies are usually the ones having VA performed.

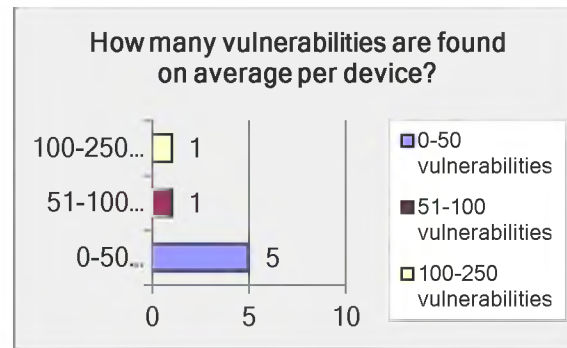
Question 8 and Question 9 ask "How many devices are typically scanned when you perform an external and internal vulnerability assessment?". Figure 4.5 reveals that an external vulnerability assessment usually consists of scanning 26-50 publicly facing IP addresses. A survey respondent revealed that "I don't often see over 100 live hosts on the external network".



**Figure 4.6 Amount of IP Addresses Scanned During an External VA**

For an internal vulnerability assessment, the survey indicated that the average organization has over one hundred IP addresses scanned within the IT environment. Some global organizations can have up to 20,000 devices that they want to have scanned for vulnerabilities. Obviously, scanning that many devices would result in a larger report. Large reports can be reduced by scanning a sample set of computers within an organization, instead of all devices.

Within the survey, questions ten through fifteen all relate to VA scan results. Question 10 asked "How many vulnerabilities are found on average per device?" and five people agreed that on average a VA scan reveals less than fifty vulnerabilities per device. (See Figure 4.6).



**Figure 4.7** How many vulnerabilities are found on average per device

Question 11, "What are common vulnerabilities that you see from vulnerability assessments?" resulted in a list of several answers. The top five vulnerabilities found were related to:

- default passwords
- Windows patches
- Java
- \*nix patches
- expired certificates

Other significant vulnerabilities were: Adobe Software, SQL injection attacks, Active Directory, DOS attack, and general configuration issues. This list of top vulnerabilities is significant to IT departments, because VA software databases of vulnerabilities can contain 20,000 or more vulnerabilities.

The next question, question 12 was trying to get a list of top services and protocols that are a concern to IT departments. Question 12, "What services and protocols are the vulnerabilities usually related to?" discovered that the vulnerabilities were usually related to services and protocols such as:

- Operating System defaults
- SQL
- Web Browsers
- SSL
- Password authentication

Question 13 was also capable of gathering a list of top devices that often have vulnerabilities. Question 13 asked "On which device do you find the most vulnerabilities?" and identified the following devices:

- firewall
- server
- workstations and laptops
- multi-function device
- tape library

Questions 14 and 15 were related to the reporting capabilities of VA software. Question 14, "What is the typical length of a VA report?" indicated that reporting documentation for internal and external vulnerability scans were usually between 26 and 50 pages. Also, question 15 asked "Do you find the length of the report to be adequate?". The individuals performing the vulnerability scans indicated that they found the length of the vulnerability assessment reports to be adequate with one person stating "The length of the report depends on documentation requirements and if they are driven by compliance". The individuals that did not find the length of the report adequate indicated that reports were too long.

The last two questions, question 16 and question 17 were related to satisfaction of VA software. Question 16, "For what reason do you choose the VA software you currently use?"

revealed the deciding factors for choosing VA software was cost, scanning capabilities, and database of vulnerabilities, functionality, and reputation. The final question, question 17 "are you satisfied with the VA software that you use, or would you prefer that it had additional features?" displayed that 75% of respondents were generally happy with VA software, but they "would always like to see additional features" and "wish it was more stable".

## **Chapter 5 – Conclusions**

Throughout this research, the correlation was drawn between the need for vulnerability assessments in small business environments and the top five vulnerabilities found within that network. Outsourcing vulnerability assessments to mitigate risk and be compliant with regulations creates advantages for small and medium-sized organizations that do not have the resources and skills to conduct assessments themselves. IT security assessment company's are a valuable resource for conducting internal and external vulnerability assessments at a business that does not have employees with an IT Security skill set.

### **Limitations and Challenges**

Unknown challenges developed in attempting to get people to complete the survey. After searching through the Internet to build a list of companies that performed vulnerability assessments, this researcher created a spreadsheet with business name, location, telephone number, e-mail, and website. Initial contact began via telephone, however the conversations did not always go well. Businesses claimed to be swamped with work and that they did not have time to complete the survey. In addition, I believe that the people thought I was a hacker and my survey was not for research purposes. I gave this method of cold calling about a week until realization that it was not producing desired results.

Surprisingly, social media ended up being the most effective method to get respondents for the questionnaire. I had made several posts to LinkedIn discussion groups, with quick and adequate results. In addition, I used the search function of LinkedIn to find professionals that perform vulnerability assessments in a consulting capacity. This method of finding a variety of respondents increased the results to eight completed surveys. A limitation of the web-based survey was that a \$24/month upgrade had to be purchased for the survey to include enhanced

security and reporting features. The reports indicated that survey results might not have limited scope to only small business, as was desired to create a list of top five vulnerabilities affecting small business.

**Future Work**

Further research on performing vulnerability assessments from a consulting capacity could be further explored. Specific items of importance are differentiating factors between internal and external VA, VA software capabilities, and VA reporting. Moreover, a VA can produce a report of threats against an organization, but the measurement of value add could be further documented.

### References

- AVG (2010). SMB market landscape report 2010. Growth from knowledge. [Electronic Article]. Retrieved from [http://download.avg.com/filedir/atwork/pdf/White\\_paper2010.pdf](http://download.avg.com/filedir/atwork/pdf/White_paper2010.pdf).
- Barnett, Ryan (2009). Web-Hacking-Incident-Database. Retrieved from <http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database#TopAttackMethodsAllEntries>.
- Berghel, H. & Uecker, J. (2004). Wireless infidelity II: Airjacking. *Communications of the ACM*, 47(12), 15-20.
- Berghel, H. & Uecker, J. (2005). WiFi attack vectors. *Communications of the ACM* 48(8), 21-28.
- Canadian Institute of Chartered Accountants, the. (2003). Using an ethical hacking technique to assess information security risk, 1-15.
- Chang, E.S. & Jain, A.K. & Slade, D.M. & Tsao, S.L. (1999). Managing Cyber Security Vulnerabilities in Large Networks. *Bell Labs Technical Journal*, 252-272.
- Clutterbuck, P. & Rowlands, T. & Seamons, O. (2007). Auditing the Data Confidentiality of Wireless Local Area Networks. *The electronic Journal Information Systems Evaluation*, 10(1), 45-56.
- Durst, R. & Champion, T. & Witten, B. & Miller, E. & Spagnuolo, L. (1999). Testing and Evaluating Computer Intrusion Detection Systems. *Communications of the ACM*, 42(7), 53-61.

FDIC (2002). Office Inspector General Semiannual Report to the Congress, 4/01/2002 - 9/30/2002. Retrieved from <http://www.fdic.gov/oig/sar2002-oct/Oct02-SAR.html>.

FDIC (2002). Phase II Network Operations Vulnerability Assessment. Federal Deposit Insurance Corporation: Office of Inspector General. [Electronic Article]  
<http://www.fdicig.gov/rep-summaries/03-007.pdf>.

Foreman, Park. (2010). Vulnerability management. [Books24x7 version] Retrieved from <http://common.books24x7.com.dml.regis.edu/toc.aspx?bookid=30514>.

Frost & Sullivan (2008). World Vulnerability Assessment Products Markets. Research and Markets.

Hoover, T. (2010). Colorado's state computer systems fail "hacker" test in cyber-security audit. [Electronic Resource]. Retrieved March 26, 2011 from [http://www.denverpost.com/legislature/ci\\_16852217](http://www.denverpost.com/legislature/ci_16852217).

Indeed.com (2010). Salary Search, Information Security Consultant Salary in USA.

Infosecurity (2011). IEEE admits to breach of members' credit card information. [Electronic Article]. Retrieved April 10, 2011 from <http://www.infosecurity-us.com/view/17025/ieee-admits-to-breach-of-members-credit-card-information/>.

Insight Consulting (2010). Penetration Testing. [Electronic Version]. Retrieved April 10, 2011 from [http://www.insight.co.uk/files/whitepapers/Penetration%20Testing%20\(White%20paper\).pdf](http://www.insight.co.uk/files/whitepapers/Penetration%20Testing%20(White%20paper).pdf).

- Ion, I. & Traian, S. & Cristian, A. (2008). The IT Audit - A Major requirement for the Management Quality and Success in the European Business Context. *Annals of the University of Oradea, Economic Science Series*, 1397-1401.
- James, T. (2011). BBC: Massive cyber attack hits huge volume of websites. [Electronic Article]. Retrieved April 14, 2011 from <http://community.websense.com/blogs/securitylabs/archive/tags/Mass+Injection/default.aspx>.
- Kavanagh, K.M. and Nicolett, M. (2011). Gartner. MarketScope for Vulnerability Assessment.
- Kim, H.J. & Kim, H.K. & Lee, H.Y. (2010). Security Requirement Representation Method for Confidence of Systems and Networks. *International Journal of Software Engineering and Knowledge Engineering*, 20(1), 49-71.
- Kolodgy, Charles J. (2011). Worldwide Security and Vulnerability Management 2011-2015 Forecast and 2010 Vendor Shares. 1-16.
- Korzeniowski, P. (2004). Pros and cons of outsourcing vulnerability assessments. Federal Computer Week. [Electronic Article] Retrieved March 24, 2011 from <http://fcw.com/Articles/2004/05/10/Pros-and-cons-of-outsourcing-vulnerability-assessments.aspx>
- Lanz, J. (2003). Practical Aspects of Vulnerability Assessment and Penetration Testing. The RMA Journal. 44-49.
- Layton, T. P. (2002). Penetration Studies - A Technical Overview. SANS Institute: Information Security Reading Room.

- Matisziw, T.C. & Murray, A.T. & Grubescic, T.H. (2009). Exploring the Vulnerability of Network Infrastructure to Disruption. Springer Sciences & Business Media B.V.
- McAfee (2011). Unsecured Economies: Protecting Vital Information. Retrieved from <http://www.mcafee.com/us/resources/reports/rp-unsecured-economies-report.pdf>.
- McGee, A.R. & Vasireddy, S.R. & Xie, C. & Picklesimer, D.D. & Chandrashekhar, U. & Richman, S.H. (2004). A Framework for Ensuring Network Security. *Bell Labs Technical Journal*, 8(4), 7-27.
- Moteff, J. (2004). Computer Security: A summary of selected federal laws, executive orders, and presidential directives. CRS Report for Congress.
- Motorola (2010). Understanding the value of outsourcing network security services. Motorola: white paper.
- NIST (2008). Technical guide to information security testing and assessment. Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>.
- NIST (2012). National Vulnerability Database. Retrieved from <http://nvd.nist.gov/cwe.cfm>.
- Olson, C. & Hardikar, A. (2010). Penetration Testing in the Financial Services Industry. SANS Institute: SANS Reading Room.
- [us.pdf?om\\_ext\\_cid=biz\\_socmed\\_twitter\\_facebook\\_marketwire\\_linkedin\\_2012Mar\\_worldwide\\_\\_CODB\\_US](#).

- PCI Security Standards Council (2010). PCI DSS Quick Reference Guide, Understanding the Payment Card Industry Data Security Standard version 2.0. Retrieved from <https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>.
- PCI Security Standards Council (2011). PCI SSC data security standards overview. [Electronic Resource]. Retrieved March 28, 2011 from [https://www.pcisecuritystandards.org/security\\_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php).
- Ponemon Institute, LLC. (2012). 2011 Cost of Data Breach Study: United States. Retrieved from [http://www.ponemon.org/local/upload/file/2011\\_US\\_CODB\\_FINAL\\_5.pdf](http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf)
- Qualys (2009). The Top 10 Reports for Managing Vulnerabilities, 1-17.
- Rapid7 (2011). Architecture, Nexpose. [Electronic Version] Retrieved April 5, 2011 from <http://www.rapid7.com/products/nexpose/technology/architecture.jsp>.
- Rapid7 (2013). Tech Specs. Retrieved from <http://www.rapid7.com/products/nexpose/tech-specs.jsp>.
- Rathaus, Noam (2010). Vulnerability Assessment Whitepaper. Retrieved from [http://www.beyondsecurity.com/pdf/AVDS\\_Whitepaper.pdf](http://www.beyondsecurity.com/pdf/AVDS_Whitepaper.pdf).
- Roumboutsos, A. & Nikitakos, N. & Gritzalis, S. (2005). Information Technology Network Security Risk Assessment and Management Framework for Shipping Companies. Maritime Policy & Management, 421-432.

- SANS Institute (2001). Guidelines for Developing Penetration Rules of Behavior. SANS Reading Room.
- SANS Institute (2006). Penetration Testing: The third-party Hacker. SANS Reading Room.
- SBA (2011). SBA: Office of Advocacy. Frequently Asked Questions. Advocacy: the voice of small business in government. [Electronic Article]  
[http://www.sba.gov/sites/default/files/FAQ\\_Sept\\_2012.pdf](http://www.sba.gov/sites/default/files/FAQ_Sept_2012.pdf).
- Sectools.org (2006). Top 100 network security tools. Retrieved from <http://sectools.org/>.
- Smith, Gerry (2011). Small Businesses A Growing Target For Hackers. Retrieved from [http://www.huffingtonpost.com/2011/10/24/small-business-hackers\\_n\\_1028781.html](http://www.huffingtonpost.com/2011/10/24/small-business-hackers_n_1028781.html).
- Sophos (2008). Hackers attack businesses, blogs and Web 2.0 sites, reveals Sophos Security Threat Report. Retrieved from <http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophossecurityreport08.pdf>
- Suma, S. (2010). Evaluation of Vulnerability Assessment in System from Hackers in Cyber Security. *International Journal of Engineering Science and Technology*, 2(7), 3213-3217.
- Symantec (2011). Whitepaper: Reducing the Cost and Complexity of Web Vulnerability Management. Retrieved from <http://www.verisign.com/ssl/ssl-information-center/ssl-resources/vulnerability-management-whitepaper.pdf>.
- Vasireddy, R. & Wolter, S. & Chandrashekhar U., Thornberry, R.J., McGee, A.R. (2004). Security Posture for Civilian and Non-Civilian Networks. *Bell Labs Technical Journal*, 8(4), 187-202.

Wakefield, R. L. (2004). Network Security and Password Policies. *The CPA Journal*.

Wohlstetter, J. (2002). The Vulnerability of Networks. *EBSCO Publishing*.

Wojcik, M. (2010). Making Risk Assessments Useful. *The Institutes*.

## Appendices

### Appendix A: IRB Approval Letter



Academic Affairs  
Academic Grants

3333 Regis Boulevard, H-4  
Denver, Colorado 80221-1009

303-455-4295  
303-954-3047 FAX  
www.regis.edu

#### IRB – REGIS UNIVERSITY

June 3, 2013

Charles Lybrand  
3333 East Bayaud #717B  
Denver, CO 80209

RE: IRB #: 13-155

Dear Mr. Lybrand:

Your application to the Regis IRB for your project, "The Use of Vulnerability Assessments: A Survey," was approved as an exempt study on June 3, 2013. This study was approved per exempt study category 45CFR46.101.b(2).

The designation of "exempt," means no further IRB review of this project, as it is currently designed, is needed.

If changes are made in the research plan that significantly alter the involvement of human subjects from that which was approved in the named application, the new research plan must be resubmitted to the Regis IRB for approval.

Sincerely,

A handwritten signature in blue ink that reads "Patsy McGuire Cullen".

Patsy McGuire Cullen, PhD, CPNP  
Chair, Institutional Review Board  
Associate Professor and Director  
Department of Accelerated Nursing  
Loretto Heights School of Nursing  
Rueckert-Hartman College for Health Professions  
Regis University

cc: Dr. Bob Mason

## **Appendix B: Survey Instrument**

Your participation in this anonymous survey is deemed valuable for a university research study on vulnerability assessments and should take less than fifteen minutes to complete.

A vulnerability assessment (VA) is a process that defines, identifies, and classifies the security weaknesses (vulnerabilities) in a computer, network, or communications infrastructure. This survey is geared towards VA in small businesses (a business with less than 100 employees).

The survey results will be used in a masters degree research project in information systems security for Regis University.

At any time you can stop the survey if you wish not to participate. The survey does not ask for client names. Your name and e-mail address will not be revealed.

Instructions: This survey is seventeen questions. Select the answer that best reflects your views. Answer all questions as honestly as possible. There are no correct or best answers.

For all questions please click on the appropriate box/circle, or type in the field for other. In addition, certain questions request a reason for your selected answer.

If you have any questions, please contact me at: [mrlybrand@gmail.com](mailto:mrlybrand@gmail.com) .

Thank you for your time and participation,

Charles Lybrand

1.) What is your current role within the organization?

Pen Tester / Web Security

IT Auditor / Analyst

IT Manager / Director

CIO / CTO / CEO

I do not work in IT

Other (please specify):

2.) How many years have you been involved in IT Security?

I don't work in IT Security

0 - 6 months

6 months - 1 year

1 year - 3 years

3 - 5 years

5+ years

Other (please specify):

3.) What software do you use to perform a vulnerability assessment? (Select all that apply and please also provide your reasoning in the "Other:" box.)

Rapid7 Nexpose

QualysGuard Vulnerability Management

IBM Security AppScan

Tenable Nessus Vulnerability Scanner

AlienVault's Unified Security Management

Tripwire (Formerly nCircle)

Other (please specify) and/or reasoning:

4.) Are you satisfied with the results you receive from the vulnerability assessment software? (Please also provide your reasoning in the text box.)

Yes

No

Please specify your reasoning:

5.) How many external vulnerability assessments do you perform in a year? (Please also provide your reasoning in the text box.)

None

1 - 25

26 - 50

51 - 100

100 - 150

151 - 200

200+

Please specify your reasoning:

6.) How many internal vulnerability assessments do you perform in a year? (Please also provide your reasoning in the text box.)

None

1 - 25

26 - 50

51 - 100

100 - 150

151 - 200

200+

Please specify your reasoning:

7.) What is the typical size of the organization you perform a VA on? (Please also provide your reasoning in the text box.)

0-25 employees

26-50 employees

51-100 employees

101-150 employees

151-250 employees

250-500 employees

501+ employees

Please specify your reasoning:

8.) How many devices are typically scanned when you perform an external vulnerability assessment? (Please also provide your reasoning in the text box.)

0-25 devices at a small business

25-50 devices at a small business

50-100 devices at a small business

100+ devices at a small business

I do not perform external vulnerability assessments

Please specify your reasoning:

9.) How many devices are typically scanned when you perform an internal vulnerability assessment? (Please also provide your reasoning in the text box.)

0-5 devices at a small business

6-10 devices at a small business

11-20 devices at a small business

20+ devices at a small business

I do not perform internal vulnerability assessments

Please specify your reasoning:

10.) How many vulnerabilities are found on average per device? (Please also provide your reasoning in the text box.)

0-50 vulnerabilities

51-100 vulnerabilities

100-250 vulnerabilities

250-500 vulnerabilities

500+ vulnerabilities

Please specify your reasoning:

11.) What are common vulnerabilities that you see from vulnerability assessments? (Select all that apply and please also provide your reasoning in the "Other:" box.)

Vulnerabilities related to Adobe software (Flash, Acrobat, Shockwave, Reader)

Vulnerabilities related to Java

Vulnerabilities related to Windows patches

Vulnerabilities related to \*nix updates

Vulnerabilities related to Cisco patches

Vulnerabilities related to expired certificates

Vulnerabilities related to Internet Explorer

Vulnerabilities related to Mozilla Firefox

Vulnerabilities related to E-mail server (Exchange/Domino)

Vulnerabilities related to Google Chrome

Vulnerabilities related to SQL injection attacks

Vulnerabilities related to generic passwords

Vulnerabilities related to Oracle databases

Vulnerabilities related to an Active Directory issue

Vulnerabilities related to a DOS / Flood attack

Other (please specify) and/or reasoning:

12.) What services and protocols are the vulnerabilities usually related to? (Select all that apply and please also provide your reasoning in the "Other:" box.)

The vulnerabilities are associated with FTP

The vulnerabilities are associated with Telnet

The vulnerabilities are associated with SSH

The vulnerabilities are associated with SSL

The vulnerabilities are associated with VNC / Remote Desktop

The vulnerabilities are associated with SQL

The vulnerabilities are associated with Web Browser

The vulnerabilities are associated with Operating System

Other (please specify) and/or reasoning:

13.) On which device do you find the most vulnerabilities? (Choose the top 3 and please also provide your reasoning in the "Other:" box.)

The vulnerabilities are usually on a firewall

The vulnerabilities are usually on a honeypot

The vulnerabilities are usually on an IDS/IPS

The vulnerabilities are usually on a switch

The vulnerabilities are usually on a router/access point

The vulnerabilities are usually on a server

The vulnerabilities are usually on a workstation/laptop

The vulnerabilities are usually on a printer

The vulnerabilities are usually on a multi-function device(copy/fax/printer)

The vulnerabilities are usually on a UPS

The vulnerabilities are usually on a VoIP phone

Other (please specify) and/or reasoning:

14.) What is the typical length of a VA report? (Please also provide your reasoning in the text box.)

0-25 pages

26-50 pages

51-75 pages

76-100 pages

100+ pages

Please specify your reasoning:

15.) Do you find the length of the report to be adequate? (Please also provide your reasoning in the text box.)

Yes

No: too short

No: too long

Please specify your reasoning:

16.) For what reason do you choose the VA software you currently use? (Choose the top 3 and please also provide your reasoning in the "Other:" box.)

Cost

Reporting features

Scanning capabilities

Database of vulnerabilities

Ease of use

Functionality

Reputation

Support

Other (please specify) and/or reasoning:

17.) Are you satisfied with the VA software that you use, or would you prefer that it had additional features? (Please also provide your reasoning in the text box.)

Yes

No

Please specify your reasoning:

END OF SURVEY

---

**Appendix C: Sample Email to IT Professionals**

ContactName,

I am conducting research for my thesis at Regis University. My research is on vulnerability assessments (VA).

I was wondering if you perform VA at several organizations throughout the year. If so, do you have 10-15 minutes to complete my survey.

I am sending emails now to get a group of people confirmed, and then will later be sending the generated survey link via SurveyMonkey.com

Thanks,

Charles Lybrand

**Appendix D: Survey Email**

To: [Email]

From: "mrlybrand@gmail.com via surveymonkey.com" <member@surveymonkey.com>

Subject: Vulnerability Assessment Survey

Body: I am conducting a survey, and your response would be appreciated.

Here is a link to the survey:

<https://www.surveymonkey.com/s.aspx>

Thanks for your participation!

Please note: If you do not wish to receive further emails from us, please click the link below, and you will be automatically removed from our mailing list.

<https://www.surveymonkey.com/optout.aspx>