



SCHOOL OF COMPUTING AND INFORMATICS

University of Nairobi

An Experiment to Determine the Effect of Ethical Hacking on IT Administrator's Patch and Vulnerability Management Attitudes, a case of a leading telecommunications company

Alex Jairo Kibe

P56/60038/2010

Supervisor

Dr. Evans Miriti

A research project report submitted in partial fulfillment for the Requirements for the award of
Degree of Masters of Science in Information Systems of the
School of Computing and Informatics, University of Nairobi

November, 2018

DECLARATION

Researcher's Declaration

I declare that this project report is my original work except where due references are cited. To the best of my knowledge, this it has not been submitted for any other award in any University. Data from other sources has been acknowledged.

Signed: _____ Date: _____

Kibe, Alex

Registration Number: P56/60038/2010

APPROVAL

This project report has been submitted in partial fulfillment of the requirements for the Degree of Master of Science in Information Systems of the University of Nairobi with my approval as the University Supervisor.

Signed: _____ Date: _____

Dr. Evans Miriti

School of Computing and Informatics

University of Nairobi

Dedication

To my family, my supervisor, my lecturers and colleagues, I wish to appreciate your valuable support and contribution you accorded me throughout the whole process, from the project initiation till completion.

Thank you and May God the almighty bless you all.

Acknowledgement

I wish to thank God for having given me strength and guidance in this project. Special thanks to my supervisor Dr Miriti and University of Nairobi staff especially those at school of computing and informatics for their great support and good relation throughout the time I was a student of this university. Contribution from friends and colleagues towards this project is highly appreciated.

Thank you all.

Abstract

As the adoption of information processing and the integration of various information systems via the internet increases, so does the risk to information systems. Electronic attacks are likely via the exploitation of vulnerabilities in operating systems, web application services and applications. Consequently, vulnerability management ought to be an important and mandatory task for IT administrators. However, studies show the persistence unpatched systems. This demonstrates that vulnerability management is far from the behavioral mindset of IT administrators. While various measures like automated updates are able to contribute towards a solution, vulnerability management is a human concern. Tackling the matter thus requires a willingness to deal with it. Scientific studies have also shown that changing user attitudes and actions concerning computer security methods to be the most difficult facet of computer security management. (AUSCERT, 2006).

The aim of this study was to determine the effect of simulated hacking on IT administrators' attitudes towards patch and vulnerability management. Ethical hacking has successfully been used as a proactive information security strategy that unearths system vulnerabilities (Saleem, 2006). This research employs an experimental approach to evaluate the effectiveness of a simulated database attack to influence the attitudes of IT administrators towards patch and vulnerability management.

The study found that IT administrators of the telecommunications organization had an unfavorable attitudes towards patch and vulnerability management with administrators overseeing outdated and insecure systems. The study also confirmed the ease with which unpatched systems can be exploited by hackers. However exposure to hacking had no significant effect on the IT administrators' attitude towards patch and vulnerability management. The main reasons for this were that the IT administrators felt that patch and vulnerability management was not a strategic priority as it had not been articulated as such. Secondly, they felt that IT security was not their KPI, rather it was the responsibility of the cybersecurity team. Thirdly, they revealed that patching is not a priority as their domains have not suffered any notable attacks.

DECLARATION	i
Researcher’s Declaration.....	i
Dedication	ii
Acknowledgement.....	iii
Abstract	iv
LIST OF TABLES	viii
LIST OF FIGURES	ix
CHAPTER 1: INTRODUCTION.....	1
1.1 Statement of the Problem	2
1.2 Main Objective.....	4
1.3 Specific Objectives.....	4
1.4 Significance of Study	4
1.5 Definition of Terms.....	4
1.6 Chapter Summary.....	5
CHAPTER 2: LITERATURE REVIEW	6
2.1 Risk Management.....	6
2.2 Vulnerabilities	7
2.2.1 Vulnerability Exploits.....	7
2.2.1.1 Social Engineering Breaches	7
2.2.1.2 Mass Defacements of Websites	9
2.3 Patch and Vulnerability Management	9
2.3.1 Attitudes towards Patching	10
2.3.2 Unpatched Systems Exploits.....	12
2.4 Hacking	13
2.4.1 Types of Hacking Attacks	14
2.4.1.1 Large Scale Stealthy Scans	15
2.4.1.2 Worm Outbreaks	15
2.4.1.3 Distributed Denial-of-Service Attacks.....	15
2.4.2 Ethical Hacking	15
2.4.2.1 Ethical Hacking Methodology.....	17
2.5 Database Security.....	18
2.5.1 Excessive Privilege Abuse.....	18

2.5.2 Legitimate Privilege Abuse	18
2.5.3 Privilege Elevation	19
2.5.4 Platform Vulnerabilities	19
2.5.5 SQL Injection	19
2.5.6 Weak Audit Trail	20
2.5.7 Denial of Service	20
2.5.8 Database Communications Protocol Vulnerabilities	20
2.5.9 Weak Authentication	21
2.5.10 Backup Data Exposure	21
2.6 Technology Use to Change User Attitudes	21
2.7 Summary of gaps.....	23
2.8 Conceptual Framework and Hypothesis Development.....	23
CHAPTER 3: Methodology.....	25
3.1 Research Design.....	25
3.2 Architecture of the simulated attack.....	26
3.3 Pre and Post Experiment Survey Design.....	27
3.3.1 Introduction	27
3.3.2 Hacking Experiment	27
3.3.3 Sampling.....	31
3.3.4 Instrument Design`	31
3.3.5 Data Collection	34
3.3.6 Data Analysis.....	34
3.4 Post Analysis Interview.....	34
CHAPTER 4: Data Analysis Results and Discussions	35
4.1 Introduction	35
4.2 Response Rate	35
4.3 Sample Characteristics	35
4.4 Demographics.....	35
4.5 Administrator Attitudes Pre and Post Exposure to Ethical Hacking.....	37
4.6 Post Survey Interview Findings	39
Chapter 5: Conclusions and Recommendations	41
5.1 Summary and Conclusions of the study	41

5.2 Limitations of the study.....	43
5.3 Recommendations	43
5.4 Suggested Areas for Further Research	44
REFERENCES	45
APPENDICES	50
APPENDIX 1: Questionnaire	50
Section A: Demographic data	50
Section B: Patch management attitudes	51
APPENDIX 2: Video Access Records	52

LIST OF TABLES

Table 1: Persuasive Technologies [Source: (Cheo, et al., 2008)].....	22
Table 2: Reliability Statistics before testing questionnaire.....	32
Table 3: Reliability statistics after testing questionnaire	33
Table 4: Item statistics showing item correlation before removal of items to enhance reliability	33
Table 5: Item statistics showing improved reliability after scale item cleanup	33
Table 6: Designation of the respondents.....	36
Table 7: Distribution of the respondents based on work experience	36
Table 8: A comparison of pre hack and post hack attitudes based on work experience.....	37
Table 9: Pre and post ethical hacking exposure paired samples statistics	38
Table 10: Comparison of Pre and post exposure to ethical hacking Item Means and Standard Deviation.....	38
Table 11: Pre and post ethical hacking exposure mean scores normality test	39
Table 12: Test of significance of the difference of means pre and post exposure to ethical hacking.....	39

LIST OF FIGURES

Figure 1: PayPal Warns User of Email Scam [Source: Walker, A.J., (2016)]	8
Figure 2: PayPal Warns User of Email Scam [Source: Walker, A.J., (2016)]	8
Figure 3: Indonesian Hackers Hacked President of Kenya Website [Source: LHN., (2015)].....	9
Figure 4: Conceptual Framework	24
Figure 5: Simulated attack architecture [Source Koret (2008)].....	27
Figure 6: Scanning for database vulnerability to TNP poison vulnerability	28
Figure 7: Target database connectivity test	29
Figure 8: Target database user query	29
Figure 9: Running the proxy to intercept connections to the database server	29
Figure 10: Continuous remote registration of the local attack database on the database server ..	30
Figure 11: Client connection failure due to DOS attack.....	30

LIST OF ABBREVIATIONS

ARP	Address Resolution Protocol
BFID	Banking Fraud Investigations Department
BYOD	Bring your own Device
CAMNEP	Cooperative Adaptive Mechanism for Network Protection
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technologies
CSIS	Center for Strategic and International Studies
CVE	Common Vulnerabilities and Exposures
DBMS	Database Management System
DDoS	Distributed Denial-of-Service
DLL	Dynamic Library Link
ERM	Enterprise Risk Management
FBI	Federal Bureau of Investigations
FTP	File Transfer Protocol
GAO	Government of Accountability Office
IDS	Intrusion Detection System
IP	Internet Protocol
IS	Information Systems
IT	Information Technology

CHAPTER 1: INTRODUCTION

Corporations are today confronting many IT security challenges as they've to rely increasingly more upon computer systems. The blend of the useful data in systems and challenges protecting it make computer systems susceptible to a number of attacks and threats (Arbaugh et al., 2000). Statistics indicate the typical downtime created by a cyber security encounter is between 4 to 8 hours at one time with a lot of businesses oftentimes experiencing as many as 3 days of downtime. The duration and amount of such severe incidents is rising (Hulme, 2006). It is estimated that ninety five percent of security incidents could be avoided by keeping systems up to date with necessary patches (Cavusoglu et al., 2008).

According to Ioannidis et al. (2012) there could be a link between the level of applied patches and the level of data security in an organization. This statement is corroborated by evidence of situations where unpatched software led to a security breach as shown by the Code Red and Slammer worm examples below. Code Red infected hundreds of thousands of computers although a patch had been released months prior to the attack. According to Moore and Shannon (2002), the worm spread through the internet by using Hypertext Transfer Protocol (HTTP) requests and exploited the buffer overflow vulnerability. In this case, there was more than enough time to test and deploy the curative patch, yet 115000 websites were attacked by Code Red (Moore & Shannon, 2002). Patching is often done months or even years after vulnerabilities are discovered (Cavusoglu et al., 2008). The Slammer worm struck in 2003 and highlighted the importance of patching vulnerabilities as soon as patch release as the curative patch was released six months prior to the worm attack (Zhou et al., 2010).

Despite general awareness of the dangers of attacks on vulnerable computer systems, many organizations realize the seriousness of the problem after becoming victims of damaging attacks. Staff and decision makers in organizations have indifferent attitudes and perspectives toward threats to their computer systems, often viewing them as a disruption to the core work processes (Beattie, 2002). Additionally, proactive threat management is frequently ignored because companies completely focus on the main business activities of theirs and consider cyber-attacks of secondary importance (Bentley, 2006). Based on a survey by Security Company Kaspersky Lab and B2B International, forty eight percent of financial businesses took steps to cope with online

fraud instead of preventing incidents. About twenty nine percent think it is cheaper to deal with the implications of fraud rather than to try to avoid them, the IT Security Risks Survey 2015 found.' Relying entirely on mitigating the bad result of fraud is akin to trying to deal with the symptoms of an illness instead of its root cause. The symptoms are going to recur, and also the illness will progress', Ross Hogan, Kaspersky Lab. The survey, performed with more than 5000 business representatives, such as 131 banks and payment services from thirty eight countries, found that even if online fraud including a customer occurred, measures to keep the incident from occurring again were taken by only forty one percent of companies. One reaction to this particular state of matters is vulnerability identification through ethical hacking which in turn increases security protection by determining and patching security vulnerabilities on systems. (Hughes, 2016).

Ethical hacking can be identified as the practice of hacking without destructive or malicious intent. "Ethical online hackers deploy the same methods and tools as attackers, but without ruining or perhaps stealing information. They assess the target systems' report to system owners with all the vulnerabilities they discovered as well as directions for how to remediate. (Palmer, 2004). There are many studies on ethical hacking, however they mostly dwell on describing ethical hacking and its role as an information security counter measure. Palmer (2004) explores ethical hacking and its challenges through the lens of its experiences in information security consultancy. Juneja (2013), Smith et al., (2002) and Prasad et al., (2014) examined ethical hacking as a security countermeasure. There is an apparent dearth of studies investigating the effect of ethical hacking on IT administrator attitudes. This indicates a gap that needs to be filled.

1.1 Statement of the Problem

Information technology and communication systems development give rise to design, implementation, and management errors or bugs. A lot of those bugs are exploitable by malicious agents. Studies at Carnegie Mellon Faculty revealed that there are 5 to 15 security bugs per one 1000 lines of code in launched software applications (Schneier, 2000). A comparable analysis estimates the number of bugs or perhaps defects in virtually any developer's code range from 5 to 15 per one 1000 lines of code to just one in every 10 lines of code (Lynn 2002). These errors may lead to vulnerabilities flaws in an information technology products that could cause violations of security policy. An example is the Nimda worm that exploited the Microsoft IIS vulnerability

'Extended Unicode Directory Traversal Vulnerability' where an anonymous user is able to substitute a '/' or perhaps a '\' with executable code. While Microsoft posted a patch to remediate this vulnerability 6 months before it had been exploited, thousands of organizations worldwide had been afflicted causing significant disruptions. The CMU analysis estimated that ninety five percent of all attacks can be avoided by having the computer systems updated with patches (Schneier, 2000). Despite this, organizations often find themselves running IT systems that may either be unstable or prone to intrusion because of challenges and complexities involved in patch management at an enterprise level (Hughes, 2016). A major part of these challenges are the attitudes of system custodians and users towards patch and vulnerability management as a security measure. According to Zhao, Furnell and Al-Ayed (2009), not all IT users and administrators realize and understand the importance of software patch management.

Easttom (2006) singled out 3 attitudes towards computer security: The very first group assumes there's no actual threat, that there's little genuine threat to computer systems and they just take enough security measures to make certain the safety of systems, they've a reactive outlook of security. The second attitude tends to overestimate the risks, folks in this particular team think that there are many skilled hackers and all pose imminent risks to information systems. The third and much more balanced view, and a better method to evaluate the threat level, will weigh the attractiveness of the system to potential attackers against the protection measures in place. Ethical hackers assess the identified systems' security and report uncovered vulnerabilities and directions on how to remedy them (Palmer, 2004). Studies have shown ethical hacking is an effective information security countermeasure which reduces IT security exposure by exposing vulnerabilities inherent in systems (Palmer, 2004) and (Berger and Jones, 2016). Nevertheless, there has not been sufficient investigation of the use of ethical hacking to influence the information security behavior of IT administrators.

1.2 Main Objective

The main objective of this study is to determine the effects of simulated hacking attacks on IT administrators' attitudes towards information security practices focusing on patch management.

1.3 Specific Objectives

- i. Carry out a pre-study to determine attitudes towards patch management among IT administrators in the organization.
- ii. Execute a simulated ethical hacking attack on a targeted database system in the organization.
- iii. Carry out a post-study to determine attitudes towards patch management among IT administrators after exposure to the simulated ethical hacking attack.

1.4 Significance of Study

The findings have practical value for IT managers, information security experts and academia. IT administrator attitudes have an impact on effective patch management and security compliance. The results of this research will contribute input to decision making in integrating ethical hacking activities into information systems security policy and practices. The study also came up ways of improving IT administrator attitudes towards patch and vulnerability management.

1.5 Definition of Terms

Hacking refers to the use of the computer to have unauthorized access to data in a system.

Ethical hacking indicates the action of finding vulnerabilities and weaknesses of info systems by duplicating the activities of malicious hackers.

The term zero day has been used in this paper to note that the CVE 2012-1675 was discovered as a zero-day vulnerability rather than show that is it currently a zero-day vulnerability.

Session Hijacking is the taking over of an active communication session of a legitimate user (i.e. victim) once it has authenticated to a server.

The term **ARP poisoning** refers to an attack where the ARP cache table of a system is poisoned by introducing new ARP entries.

Penetration testing means testing a computer system to find security vulnerabilities that could be exploited by attackers.

1.6 Chapter Summary

The chapter introduced the topic of ethical hacking and its implication on attitudes towards patch and vulnerability management. The chapter also gave the rationale, objectives and significance of the study.

CHAPTER 2: LITERATURE REVIEW

Literature review describes patch and vulnerability management in relation to risk management, hacking, the use of hacking to exploit unpatched vulnerabilities, the use of technology to alter user perceptions as well as the theoretical framework to determine user attitudes.

2.1 Risk Management

Current regulation requires that Telecommunications Service Providers (TSPs) manage the risks posed to the security of networks and services by taking appropriate organizational and technical actions including adoption of Information Security Risk Management processes (KICA, 2015).

Risk management includes all tasks associated with the control of risk, that is, risk assessment, risk acceptance, protective measures, risk reduction, and chance assignment. Businesses depend on information technology to effectively carry out the business functions. Information technology encompasses but isn't restricted to business networks, monetary and personnel systems to special systems. IT systems are subject to threats that can have damaging effects on organizational assets and operations, individuals, other organizations, and the Nation through exploitation of each acknowledged and unfamiliar vulnerabilities to compromise the confidentiality, integrity, and availability of the information getting processed, stored, or perhaps transmitted by those IT systems. Environmental disruptions, human errors, structural failures and purposeful attacks are included in these threats and could lead to harm.

Risk assessment is one facet of the organizational threat management procedure and is utilized to identify, estimate, and prioritize threats to organizational activities, property, other organizations and individuals resulting from using information systems (NIST, 2012). Risk assessments inform decision makers as well as help risk responses by identifying vulnerabilities and threats to organizations, their impacts and the likelihood to happen. Risk assessments can be done at all 3 tiers in the threat management hierarchy. Tier one at the group level, Tier two in the business activity level, as well as Tier three at the IT systems level (NIST, 2012). At Tiers one and two, risk assessments are utilized to evaluate information security related risks connected with organizational governance. At Tier 3, risk evaluations are used to effectively support implementation of the Risk Management Framework that involves security selection, categorization, implementation and control. Identification of vulnerabilities falls within the

purview of risk assessment. This involves assessment of systems on a regular basis with vulnerability scanning tools like nessus, nmap and Internet Scanner, in combination with a penetration testing. Pen-testing is very useful in identifying application and environmental vulnerabilities. Impact analysis on the vulnerability threat in terms of likelihood and cost will follow. Depending on the impact, various options are chosen to managing the risk - risk avoidance, risk transfer, risk reduction and risk acceptance. Patching known vulnerabilities is one way of avoiding information security related risks (Medzich, 2004).

2.2 Vulnerabilities

Security vulnerabilities are defects that allow an attacker to avoid security procedures (Schultz and Brown, 1990). Malicious attackers seek to determine and exploit program vulnerabilities to occasion security breaches. Eliminating or reducing the amount as well as severity of vulnerabilities in a system is essential. Exploiting a vulnerability implies that a process is in an insecure state and an attacker accesses and or perhaps compromises the system to grant or perhaps deny service without authorization (Goseva-Popstojanova et al., 2001).

2.2.1 Vulnerability Exploits

2.2.1.1 Social Engineering Breaches

Scammers employ a range of tactics to carry out social engineering exploits. Examples are phishing, a typical type of social engineering, instilling a feeling of fear or urgency in somebody to hand over private information. The LinkedIn email scams in 2015 are an illustration of phishing (Forbes, 2015). Baiting, another instance provides a reward in return for someone signing up to a service or perhaps providing some information. Pretexting plays on individuals trust by crafting a believable story to be able to get personal data for instance email messages from another person purporting to work at your bank requesting for your password. The "Business email Compromise" Scams in 2015 and PayPal Phishing Breach in 2016 (Figure 1 and 2) are good examples (SM, 2015). In Quid pro quo social engineering, money or some other form of bribery is offered in exchange for personal data such as passwords.

Here is an example of the form:

The screenshot shows the PayPal website interface. At the top, there are links for "Log Out", "Help", and "Security Centre", along with a search bar. Below this is the PayPal logo and a navigation menu with options like "My Account", "Send Money", "Request Money", "Merchant Services", "Auction Tools", and "Products & Services". The main heading is "Profile Update" with a "Secure Transaction" icon. A message states: "Please complete the form below to update your Profile information and remove limitations in your account." The section is titled "Personal Information Profile" and includes instructions: "Make sure you enter the information accurately, and according to the formats required. Fill in all the required fields." The form fields are: "Card Holder Name:" (text input), "Date of Birth:" (dropdowns for month, day, year), "Mother's Maiden Name:" (text input), "Social Security Number:" (text input), and "Home Phone Number:" (text input). A note below the phone number field says: "We may contact this phone number if there are any invalid data specified." The next section is "Home Address Profile" with the instruction: "Enter your information as accurately as possible." The fields are: "Address Line 1:" (text input), "Address Line 2:" (text input, optional), "City:" (text input), "State:" (text input), and "Zip Code:" (text input).

Figure 1: PayPal Warns User of Email Scam [Source: Walker, A.J., (2016)]

Below is an example of the email from scammers:

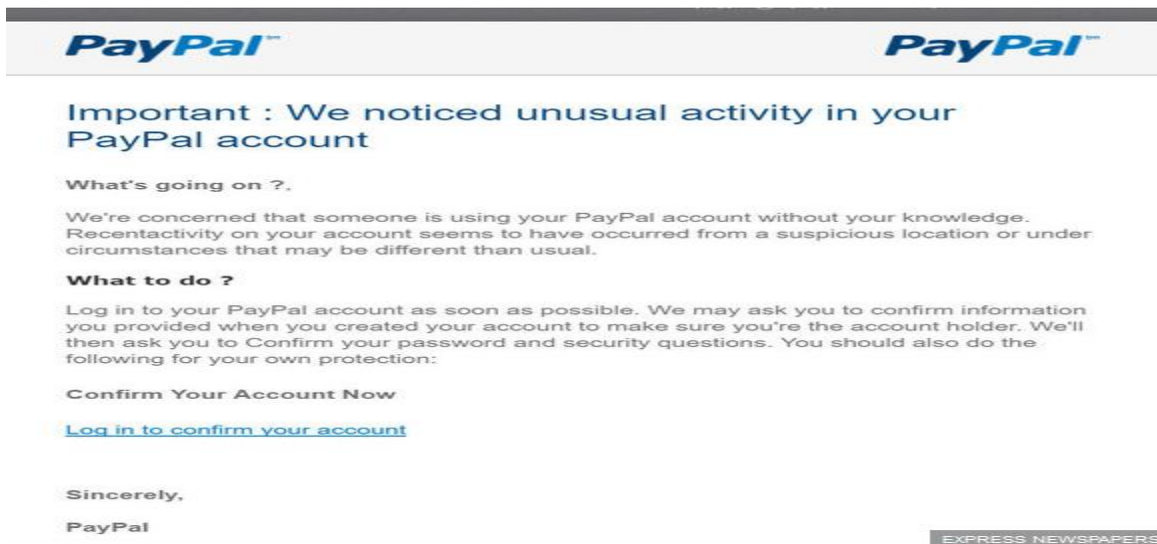


Figure 2: PayPal Warns User of Email Scam [Source: Walker, A.J., (2016)]

2.2.1.2 Mass Defacements of Websites

Fayo (2012) cited by Bongo (2012) reported that in 2012, a Forum Code Security "hacker known as direxer, exploited a Web vulnerability and took down 103 government of Kenya websites overnight sitting unfixed programming errors in code" in a major security breach.

(LTN, 2015) found that in May 2015, the popular Indonesian hackers from Gantenger's Crew hacked and defaced the President of Kenya's site. Along with a defaced webpage hackers left their internet handles on the hacked Kenyan President site. They replaced the page with one of their own. The reason behind targeting President's site was showing the authorities exactly how effective the hackers are, as reported by Hack Read reports.



Figure 3: Indonesian Hackers Hacked President of Kenya Website [Source: LHN., (2015)]

As noted by Cavusoglu et al., (2008), such exploits cause security breaches that can be easily avoided by promptly applying patches that remediate inherent vulnerabilities.

2.3 Patch and Vulnerability Management

Patch and vulnerability management is a security management practice developed to proactively stop exploitation of IT vulnerabilities which are present within the IT infrastructure of a company. The likely outcome is reduced financial resources and time used working on security incidents. Proactively managing systems vulnerabilities reduces or even eliminates the possibility of being

attacked as well as substantially reduces the effort and time spent on security incidences (NIST, 2005).

Patches are a program appendages designed to deal with bugs in software. Additional functionality is introduced by patches or perhaps address security flaws within a software program (NIST, 2005). Vulnerabilities are security flaws which may be exploited by attackers to gain unauthorized access or perhaps privileges on a system. Nevertheless, not all vulnerabilities have patch fixes. System administrators have to be aware of vulnerabilities, available fixes and other methods of remediation including device or network configuration modifications and patching of identified security problems to be able to maintaining integrity, confidentiality, and operational availability of IT systems. Nevertheless, failing to patch operating systems and application programs is among the most frequent problems identified by security and IT professionals. New patches are released every day, and it's often arduous for even experienced system administrators to keep abreast of all of the released patches and ensure appropriate deployment in a prompt fashion. Known vulnerabilities for which patches existed before the outbreaks have been targeted by a majority of major attacks in the past couple of years. Certainly, within moments of a patch release, assailants quickly reverse engineer the patch, determine the vulnerability, create and discharge exploit code. Appropriately, the time right after the introduction of a patch is ironically an especially risky moment for many organizations as a result of time lag in acquiring, testing, as well as deploying a patch (NIST, 2005).

2.3.1 Attitudes towards Patching

Patching is a major challenge for IT managers. As the WannaCry ransomware and its variants demonstrated, keeping up with patches is a challenge. Research indicates that 70% of systems administrators did not resolve a major software defect after its announcement and 30% of them still failed to patch the problem even after the vulnerability had been exploited to spread a damaging worm (Bloor, 2003). This happens even when patches are available to fix the vulnerabilities.

So if patches are the cure, why doesn't everyone apply them as soon as they're available? There are assorted operational attitudes for not patching promptly. To begin with, there are a lot of vulnerabilities to patch. On a weekly basis, about one hundred and fifty vulnerabilities along with

their fixes are released (McGhie, 2003). Evaluating these vulnerabilities to look for relevant ones is labor-intensive and tedious. Secondly, patches have to be tested before they are deployed (Donner, 2003). Before deploying in production environments, patches should be tested to make sure system function is not lost and doesn't clash with other pre-existing functionality in the system. In some instances, systems may have to be reconfigured or recoded after patching to prevent problems. Thirdly, patch distribution is not standardized. Patches may or may not be available on the vendor web site. In instances where they're there, firms are way too busy to constantly monitor the vendor web site. Fourth, patch installation calls for having the system shut down and restarting it. Patch application for critical production systems may result in expensive downtime. Consequently, patching systems can be costly. Conversely, the impact of failure to promptly patch systems can be severe too.

A 2015 study on security practices elicited attitudes such as “Automatic software updates are not safe in my opinion, since it can be abused to update malicious content.”, “there are often bugs in these updates initially, that must be worked out by the software vendor.”, “sometimes the patches [...] are glitchy [...]. I prefer to have control and know what’s being installed by applications.” and “cumbersome.” (Bloor, 2003).

Another study shows that users have a passive attitude towards patching stating that although 68.9 % of the computer users enable the auto update features when using software, just 45.6 % think it's beneficial, with 34.4 % of the other users remaining neutral and 17.8 % of the users responding unfavorably to these features (Prichard and Zhang, 2009). (Vania et al., 2014) discovered users won't apply security updates because previous updates modified critical user interface elements. This, according to the 2017 Duo trusted access report has led to only 31% of organizations running Windows having the latest operating system (OS) version, with 60% running Windows versions for which there is no vendor support. Further, 13% of users are browsing using unsupported versions of IE that no longer receive security updates. 53% of flash users are not protected from the latest known vulnerabilities with 21% of them running a flash version with 11 listed critical vulnerabilities listed in February 2017. In the health care field, 3% of enterprises continue to use Windows XP for which security support ended in 2014. Consequently, DUO 2017 predicts that criminal data breaches are going to cost enterprises a total of eight trillion dollars over another five years, because of increased Internet connectivity along with inadequate enterprise wide security.

Additionally, the amount of individual data records taken by cyber criminals will get to 2.8 billion in 2017, nearly doubling to five billion in 2020, despite innovative and new cybersecurity solutions emerging. The report singles out SMEs as especially at risk from cyber-attacks as they are inclined to operate out of date software, which recent cyber-attacks have happily exploited. Organizations therefore have to find the time and finances to update and secure systems. (DUO, 2017). Running an out of date OS triples the risk of an attack (BITSIGHT, 2017).

2.3.2 Unpatched Systems Exploits

Below are a few example exploits on vulnerabilities for which remediation patches were available. Below are a few example exploits on vulnerabilities for which remediation patches were available. While Equifax blamed a vulnerability in web software for its September 2017 security breach in which 143 million users' records were placed at risk that was interesting was that a patch to fix the flaw was released in March 2017. The particular vulnerability labeled as CVE-2017-5638 was discovered in Apache Struts, a Java web application development framework. The flaw allowed remote code execution. As noted by several security firms, it had been exploited severally in March 2017 (Brewster, 2017).

Exploits to the CVE-2013-2423 vulnerability in Java impacted 14,180,927 owners in 2016. Despite a fix being provided in April 2013, exploit developers still create malware exploiting the flaw. This mainly because lots of PCs linked to the Internet have not been updated despite the availability of patch fixes.

A May 2017 nationwide ransomware attack in the UK, may have been launched from the UKs NHS which ran systems with a vulnerability for which Microsoft released a patch for in March 2017 (Right, 2017).

Symantec reported that the Petya ransomware exploited the SMBv1 EternalBlue vulnerability, taking advantage of unpatched Windows machines in Rosneft, a Russian state owned oil company, Ukrainian state owned electricity suppliers and several banks.

As noted in the Equifax case where a known vulnerability for which a patch had been published was exploited to breach 143 Million Americans information (Brewster, 2017), hackers are always on hand to exploit unpatched systems.

2.4 Hacking

Hackers have in the past been viewed as an individuals with exceptional technical talent (Falk, 2005). In the recent past though, the phrase has acquired a bad reputation and it is used to refer to an individual who accesses computers and information stored on computers without permission. Examples abound in this particular literature review. Clarkson and Logan (2005) concur with that perspective in describing hacking as accessing a system with no authorization and accessing a system with a level beyond their authorization. "It involves the use of computer capabilities to access a system without authorization and also to eliminate evidence of access to a system" (Clarkson and Logan, 2005). In the USA, over 1093 data breaches have been recorded in 2016 by businesses, other organizations and government agencies that had customer or perhaps worker information exposed through hacking or perhaps inadvertent leaks, as stated by the Identity Theft Resource Center. This is 40% over the 780 incidents reported in 2015. (ITRC, 2017). In April 2017, there was a much publicized unsuccessful attempt to hack into the company's systems. However, intrusion detection saved the day, with the company assuring its customers of their data's safety.

There are 3 types of hackers, black hats, white hats in addition to grey hats. White Hats are hackers who use their skills in an ethical manner. Examples include hackers who are sanctioned to assess a company's system to unearth weaknesses as well as law enforcement agents who use their skills to investigate and resolve crimes (Falk, 2005). This study employs (white) ethical hacking in an attempt to reshape IT administrator's attitudes towards information security. "Black Hats" are talented individuals who use their mastery in criminal endeavors. These include organized crime units who employ the skills of talented individuals for extortion and fraud as well as illegal access of information stored on computer systems with criminal intent (Falk, 2005). Gray Hat hackers include vigilantes (self-appointed law enforcement using computer systems) and "hacktivists" who use computer technology for activism, among others (Hartley, 2006; Falk, 2005).

(Norfolk, 2001) explores a number of ways in which people conduct hacking activities. Passive info gathering, active info gathering, vulnerability mapping, and the actual exploit. A lot of business information is within the public domain and may be seen through documents and sites, a method referred to as passive information gathering. These public press provides a hacker completely legitimate ways of collecting information to use in bad ways. For instance, a review of

the source code of an institutions site may reveal email addresses, names, and naming conventions of staff, as well as IP addresses of host devices located behind the institution's firewall. This information can then be used as a basis for active information gathering through social engineering, dumpster diving and port scanning (Norfolk, 2001).

Exploitation of vulnerabilities by hackers is caused by poor programming and inadequate security practices within a company. For instance, buffer overflow is a well-known security exploit done by injecting data meant to result in a buffer overflow as well as coding into regions recognized to keep executable code replacing the legitimate code. Buffers are prevalent in operating system code which makes it easy to perform attacks that perform privilege escalation as well as gain administrative entry to a computer's compute resources. The famed Morris worm utilized this as part of its assault methods.

2.4.1 Types of Hacking Attacks

The motivation driving hackers on the Internet now has shifted from the goal of recognition to the pursuit of gain. Instead of increasing their prestige by defacing sites, hackers now use phishing and spam for monetary gain (Chiueh, 2007).

- The attacker uses large scale stealthy scans in order to hunt for software application vulnerabilities or perhaps to document insecure addresses that could be utilized for spreading a worm (Zhou et al., 2010).
- With a known vulnerability or perhaps a vulnerable targets checklist acquired during stealthy scans or perhaps purchased from the vulnerability market (Miller, 2007), worms are written by attackers to compromise hosts at the same time by exploiting this particular vulnerability. The compromised host systems, also referred to as zombies may then be used as conduits to launch DDoS attacks or perhaps can be offered on the market (Zhou et al., 2010).
- After recruiting tens of thousands of zombies, the attacker can then employ large-scale DDoS attacks to blackmail victims for financial benefit (Zhou et al., 2010).

To know how patching can secure IT systems, we describe each attack strategy in regards to the attack's objective, the vulnerabilities exploited, the strike frequency as well as the strike topology, comprehending and determining the typical attributes of these attacks upon which a preventive patch strategy may be built (Zhou et al., 2010).

2.4.1.1 Large Scale Stealthy Scans

Scans are used to browse for a particular port of interest on all the IP addresses in a certain range to find a vulnerability in a specific service which may be exploited. For example, an intruder could scan TCP port 139 in sequential IP addresses to exploit a NetBIOS vulnerability (Zhou et al., 2010).

2.4.1.2 Worm Outbreaks

A worm is a self-replicating computer program which could propagate duplicates of itself to other computers in the system with no user involvement (Zhou et al., 2010). For example, the Storm worm set about infecting a huge number of computers installed with the Microsoft Windows operating system in Europe and also the United States on 19th January 2007, using a mail with a subject line about a recently available environmental catastrophe (Symantec, 2007). Of interest is the infection stage that is utilized to check for exposed hosts then exploits the vulnerability to make for the next phase.

2.4.1.3 Distributed Denial-of-Service Attacks

DDoS attacks are effective tools used by assailants to interrupt victim's web services. A DDoS attack may be split into 2 stages, attacking and recruiting. In the recruiting phase, an assailant hunts for exposed hosts on the Internet and also installs strike tools on them. Next, the assailant transmits attack commands to these compromised programs to start an attack. (Zhou et al., 2010). A typical attribute of these assault strategies is 'scanning for vulnerabilities' that would exist primarily due to not patching and use of obsolete systems. Hackers are classified into a variety of groups, some that are clearly ethical, others deceitful, and other in between whose ethics could be debated.

2.4.2 Ethical Hacking

In the hunt for a way to address the issue of hacking, businesses discovered that 1 of the best methods to assess the intruder threat will be to get independent computer security experts try to attack their systems (Farsole, A.A. et al., 2010). Ethics in computing is a relatively more complicated issue than in some other places. Based on (Johnson,2004), if an action: "promotes the normal well being of society, maintains or perhaps increases individual freedoms and rights, protects people from harm, treats humans as valuable beings as well as accords those beings respect, as well as upholds religious, social, cultural, and federal laws and morals", then it could be seen as ethical. Actions which don't harm an individual or perhaps society are usually regarded

as ethical. Computer ethics aren't that cut and dry. The burden of stopping and defending against unethical use of computers are borne by computer professionals. Ethical hacking is an effective way of doing so.

Ethical hacking is the practice of hacking without destructive or malicious intent. "Ethical online hackers deploy the same methods and tools as black hats, but without damaging or perhaps stealing information. They assess the target systems security and report to system owners with all the vulnerabilities they discovered as well as directions for exactly how to remediate (Palmer, 2004). This technique of system security analysis is used from the beginning of computer use. In the beginning of ethical hacking, a security assessment of the Multics operating system was conducted by the United States Air Force. Their findings were that while Multics was considerably better than some other standard operating systems, it had vulnerabilities in hardware, software, and procedural security which could be exploited with essentially minimal degree of endeavor. With the aim of increasing the level of protection online and intranets, they released their strategies and tools on the web (Palmer, 2004). Penetration testing is a common activity in ethical hacking. It's purposefully attempting to get unlawful access to a system in order to figure out the level of a network's security (Hartley, 2006). Trabelsi, Z. et al. (2013), Curbelo and Cruz (2013) and Pike (2013) explored the ethics of teaching ethical hacking in the development of information security talent. Advocates of teaching honest hacking argue that integrity teaching permeates similar curriculum providing pupils with adequate planning to recognize the risks and select good information security behaviors (Pike, 2013). In a study to evaluate attitudes towards teaching ethical hacking to university students, Curbelo, A. et al. (2013) noted that faculty members agreed that to meet the need for upskilled security experts with hacking and defense skills, colleges and universities have to impart hacking and penetration capabilities as part of their Information Assurance programs. Overall, ethical hacking is about information security and assurance. Farsole, A.A. et al. (2010) note Network infrastructure attacks, specifically exploiting vulnerabilities in network transport layer components such as NetBIOS and TCP/IP as one of the possible attacks against information systems. In this study the hijacking of a user's TCP/IP connection to a vulnerable database was simulated employing the ethical hacking methodology.

2.4.2.1 Ethical Hacking Methodology

This concerns utilizing publicly accessible information like Google searches and community networks to get info concerning a target. Information gathered in this way can be IP address ranges, worker information, facility information and telephone numbers (Greenblat and DeFino, 2013).

The next stage is scanning. This requires use of the information acquired from foot printing to find the services and active hosts administered on every host. An ethical hacker is able to choose attacks which will be most profitable such as ping sweeps and port scans. Some common tools used are Nessus and Nmap (Engebretson, 2013).

The third phase is enumeration that applies the information gathered throughout the scanning stage and also consists of initiating connections to the target system. It's regarded as a high risk procedure. Analysis of data from Nessus or Nmap determines which info will be used for a cyber-attack (Collier and Endler, 2014).

The fourth stage is system Hacking. Armed with target information and location, the access to the target system is gained (Engebretson, 2013).

The 5th stage is privilege escalation. Dependent upon the usefulness of the prior stage, this allows hackers to use higher privileged accounts than all those accessed during the hacking stages, e.g. extending the guest account to have full permission to access all network resources (McKay 2012).

Next is covering tracks. This calls for eradicating proof of the attack on the target, e.g. removing logs produced in the system hacking stage to eliminate details of the attack, minimizing detecting of an intrusion within the system (Manjula and Prasad, 2014).

The seventh stage involves backdoor planting. Backdoors automate hacking through special accounts or Trojans enabling hackers repeat attacks without performing earlier steps e.g. the NetCa backdoor (Oriyano, 2014).

Hackers thrive on unresolved vulnerabilities which they exploit to breach information systems security. To demonstrate how unpatched database systems may be breached, this study employs the ethical hacking methodology the carry out a simulated database system vulnerability exploit.

2.5 Database Security

Database security is a combination of database technology and computer security and therefore affects confidentiality, integrity, availability and non-repudiation of information systems. With the automation of operational functions through information systems comes the requirement to store information or data in databases. This data may be sensitive and crucial to the organization. Database security then becomes a serious concern. Database security deals with securing database systems from any form of illegal access or perhaps risk. This involves permitting or prohibiting user actions on the database and the objects inside it. Organizations ensure confidentiality of their databases through access control to their data or information (Basharat et al., 2012).

The tenets of database security are integrity, availability and confidentiality (Ahmad et al., 2012). Confidentiality imposes data access limits to prevent unauthorized access. Integrity ensures data consistency. Availability ensures data is available to all interested parties as and when required (Baraani et al., 1996). An overview of database security threats and their mitigation is espoused in this section.

2.5.1 Excessive Privilege Abuse

Granted of excessive database access privileges to applications or user accounts may lead to abuse of these privileges for malicious purpose (Shulman, 2006). For instance, an accountant whose job is to only modify general ledger information may use excessive database update privileges to modify sub ledgers. Granular access privilege control should be defined for each user to prevent Database users from ending up with excessive privileges (Shulman, 2006).

Implementation of query-level access control prevents excessive privilege abuse. This describes a mechanism which restricts database privileges to the bare minimum needed Data and sql operations.

Sufficient data access granularity certain roles to perform their functions and issue alerts when illegal operations are performed (Shulman, 2006).

2.5.2 Legitimate Privilege Abuse

Users may misuse legitimate database privileges for unsanctioned purposes. A user with view only privileges but unauthorized to make copies of those records may circumvent these restrictions by connecting to the database using an alternative client such as MS-Excel. The user then extracts

and saves all records on the local client. Making personal copies of company records does not fulfil an organization's data protection policies for two reasons. Users may trade company information for money. Secondly, negligence where data stored on insecure client machines for legitimate work purposes is vulnerable to all sorts of risks (Shulman, 2006).

The solution is database access control applicable to both specific queries and context around database access. Through enforcement of client applications policy, identifying legitimate database access privileges abuse is possible (Shulman, 2006).

2.5.3 Privilege Elevation

Attackers may exploit database software vulnerabilities to promote normal access privileges to those of an administrator. For instance, a software developer may use a vulnerable package to gain database administrative privileges and proceed to perform administrative functions with malicious intentions (Shulman, 2006).

Privilege escalation exploits could be avoided through combining intrusion prevention systems (Query-Level access and IPS) control. IPS monitor database website traffic to recognize patterns matching acknowledged attacks. For instance, if a given package is vulnerable, then an IPS may block all access to it.

2.5.4 Platform Vulnerabilities

Vulnerabilities in operating systems and other services installed on a database server may lead to successful attacks. An example is the Blaster Worm that took advantage of a Windows 2000 vulnerability to create a DOS attack in August 2003 (Shulman, 2006).

To abate platform attacks, regular software updates and IPS is required. Software updates are provided to get rid of vulnerabilities found in database platforms. Because software updates are furnished and implemented by enterprises in periodic cycles, databases stay susceptible between the cycles. Compatibility issues between applications often stop software updates entirely. In order to abate these risks, IPS are needed to be deployed (Shulman, 2006).

2.5.5 SQL Injection

In attacks where SQL injection is used, a hacker injects unsanctioned database statements into an exposed SQL information path. These may be code in stores procedures as well as Web program

input variables. These statements are then directed to the database for execution. Attackers may use SQL injection to gain privileged access to a database (Shulman, 2006).

IPS, event correlation and query level access management would be the 3 methods that may be combined to properly mitigate against SQL injection. An IPS is able to identify SQL injection strings and vulnerable packages. Correlating SQL injection signatures along with other violations like query-level access control violations may identify attacks with accuracy (Shulman, 2006).

2.5.6 Weak Audit Trail

Automatic cataloguing of specific identified database transactions ought to be deployed in any database. A weak database audit policy represents organizational risks such as regulatory, detection and recovery of security violations and lack of a preventive mechanism (Shulman, 2006).

Weaknesses inherent in native audit tools are dealt with by Network based audit devices. Since these devices work separately from database administrators, it's feasible to distinguish audit duties from management tasks. They're also unsusceptible to privilege elevation attacks performed by non-administrators (Shulman, 2006).

2.5.7 Denial of Service

A DOS attack happens when intended users are denied access to IT services. DOS situations may be achieved using various techniques. Examples include compute resource overload, data corruption and network flooding (Shulman, 2006).

To abate DOS attacks, database, application and network level defenses should be implemented. At the database level, implementation of response timing control, query access control, IPS and connection rate control is required (Shulman, 2006).

2.5.8 Database Communications Protocol Vulnerabilities

Security vulnerabilities have been discovered virtually in all the database communication protocols. For instance, 57% of security patches in the two latest IBM DB2 FixPacks concern protocol vulnerabilities while about 48% of database vulnerabilities fixed in the latest Oracle quarterly patch concern protocols. Attacks targeting these exposures include DOS, data corruption and unauthorized data access. An example is the SQL Slammer2 worm which compromised a weakness in the Microsoft SQL Server protocol to cause a DOS. Worse still, tracing these fraud vectors is not possible since protocol functions are not included in native database audit techniques

(Shulman, 2006). Another example is the Oracle database TNS poison attack vulnerability, an assault on the TNS listener which this study exploits in a simulated database attack.

Protocol validation can be a mitigation against database communication protocol attack risks. Protocol validation technology essentially parses database traffic and compares it to a preconfigured baseline taking alert or blocking actions in case of exceptions (Shulman, 2006).

2.5.9 Weak Authentication

A lack of strong authentication schemes allows attackers to steal login credentials through brute force and social engineering enabling them to take over the identity of authorized database users (Shulman, 2006). To abate these risks, two-factor authentication and a strong password policy should be enforced (Shulman, 2006).

2.5.10 Backup Data Exposure

Backup storage media is most of the time unguarded leading to theft of hard disks and tapes (Shulman, 2006).

To abate backup media exposure risks, database backups should be encrypted. Secondly, encryption of online production data is ideal though cryptographic key management challenges and performance issues make this impractical (Shulman, 2006).

2.6 Technology Use to Change User Attitudes

Technology has for some time been used as a user attitudes and behavior change agent. Fogg (2003) defines Captology as “design, research, and analysis of interactive computing products” made for use in influencing people’s attitude or behaviors. Persuasion is a major technique for influencing people. Pervasive computing technology enables persuasion messages using technology to be interactive by altering the structure of interaction depending on the actions or attributes of the persuaded individual, user input, needs and context (IJsselsteijn et al., 2006). Persuasive technology is the application of persuasion strategy by utilizing computing technology.

Fogg (2003) developed a working triamvirate for captology which describes the three different functions computers play in persuasion. One, the computer as a utility persuades people by making target behavior easier to perform, or directing people stepwise through a procedure or doing mensuration that encourages. Two, the computer as a means of persuading people by allowing them to investigate cause-and-effect associations, or present people with derivative experiences

that drive people practice a behavior. Three, the computer as a civic player that can convince people by gifting them with useful feedback. Table 1 summarizes the persuasive technology strategies. Empirical studies have demonstrated that persuasive technology can shift people's behaviors and attitude. (Fogg and Nass, 1997) conducted an experiment that produced empirical evidence that utilizing the rule of reciprocity in human computer associations can encourage users to shift their behavior. (Lapolla and Salvucci, 2000) employed a drunk driving simulator to change attitudes of students towards drunk driving. (Lenert et al., 1991) used the internet to promote change in unhealthy behavior, smoking. Although a range of studies have been outlined in the literature on ethical hacking as a risk management technique, there have been few studies that assess its effectiveness as a persuasive technology in reshaping IT administrators attitudes towards security practices. This study employs persuasive technology to reshape attitudes towards patch and vulnerability management.

Table 1: Persuasive Technologies [Source: (Cheo, et al., 2008)]

TABLE I
PERSUASIVE TECHNOLOGY STRATEGIES

	Strategies
Computer as Persuasive Technology Tools	<ul style="list-style-type: none"> a) Reduction: Persuading through Simplifying b) Tunneling: Guided Persuasion c) Tailoring: Persuasion through customization d) Suggestion: Intervening at the Right Time e) Self-monitoring: Taking the Tedium Out of Tracking f) Surveillance: Persuasion through observation h) Conditioning: Reinforcing Target Behaviours
Computers as Persuasive Media (Simulation)	<ul style="list-style-type: none"> a) Simulated cause-and-effect scenarios: Offering Exploration and Insight b) Simulated environments: Creating Spaces for Persuasive Experiences c) Simulated Objects: Providing Experiences in Everyday Contexts
Computers as Persuasive Social Actors	<ul style="list-style-type: none"> a) Physical Attractiveness b) Similarity c) Influencing through language: Praise d) Reciprocity e) Authority

Cheo, et al. (2008) and Qudaih, et al. (2014) studied the application of persuasive technology towards enhancing information security awareness in an organization. As organizations grapple with situations in which they need to persuade their stake holders (customers, employees,

regulators, etc.) to increase their awareness of information security, persuasive technology is poised to assist them to address this situation. For a successful and effective awareness program, organizations need to target the user behaviors and attitude towards change (Qudaih, et al., 2014). Cheo, et al. (2008) went further and evaluated the efficacy of the use of persuasive technology in improving end user information security awareness through a survey, pre and post the awareness program. This research employs ethical hacking as a persuasive technology to influence information security behavior.

2.7 Summary of gaps

As espoused in the literature review, ethical hacking as a security countermeasure has value in exposing vulnerabilities in information systems and related infrastructure (Palmer, 2004), (Farsole, et al., 2010) and (Hartley, 2006). However “some companies still find it difficult to embrace unknown researchers finding flaws in their networks” and “.....some companies may be wary of ethical hackers given these people work as freelancers under no contract, potentially causing issues around confidentiality and whether the company's security flaws will remain a secret” (Kharpal, 2015). Accordingly, ethical hacking as a security counter measure is yet to gain significant credence as an information systems security countermeasure. A 2017 ethical hacking report shows that more than 72% of companies surveyed are ‘somewhat’ open to vulnerability disclosure by ethical hackers (Hackerone, 2018). That they did not have a vulnerability disclosure policy points to a negative view of ethical hacking as a risk management technique. This study aims to trigger an attitude shift in information security behavior using ethical hacking as a risk management technique. According to Beattie (2002), poor patch and vulnerability management practices are a result of negative administrator attitudes towards the same. Accordingly, it is the author’s hypothesis that exposure of ethical hacking on systems one manages affects the administrators’ attitudes towards information security practices.

2.8 Conceptual Framework and Hypothesis Development

From the extensive literature review and in particular section 3.2.1, IT administrators’ revealed that patching was overwhelming, tedious, disruptive, time consuming risky and costly. These concepts formed the basis of the conceptual framework to organize and direct the research. The diagram in Figure 4 shows that the independent variable is ethical hacking and the dependent

variable is attitudes towards patch management which consist of prioritization, negative impact on applications, lethargy, and risk.

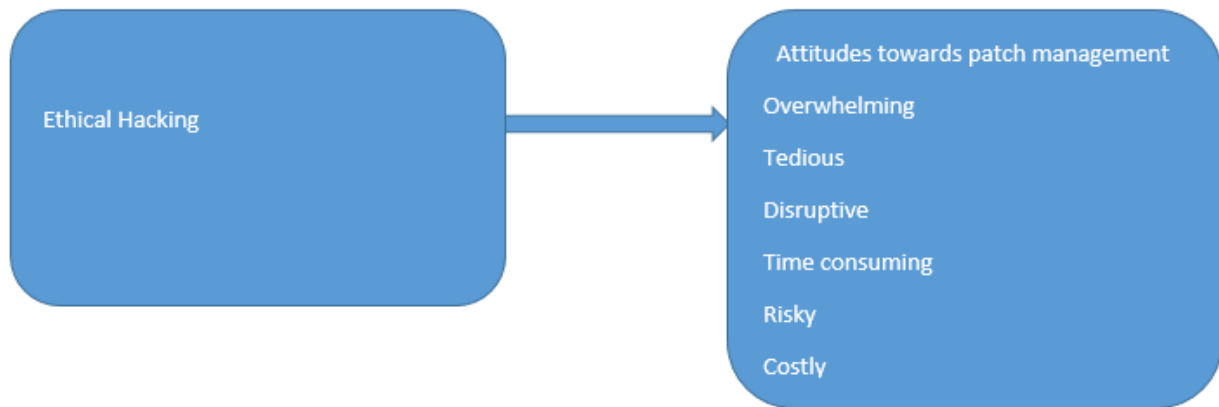


Figure 4: Conceptual Framework

Based on this conceptual framework, the study developed the research hypotheses for the study. From the above discourse, the following hypotheses were drawn:

Ho: Exposure of ethical hacking on systems one manages does not affect administrators' attitudes towards better information security practices.

Ha: Exposure of ethical hacking on systems one manages affects the administrators' attitudes towards better information security practices.

CHAPTER 3: Methodology

This chapter focuses on the methodology employed in the study. The section explains the research design, population, sampling procedure, data collection instrument, data analysis and presentation.

3.1 Research Design

"Research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy procedure therefore giving structure in which the research is conducted and, it contains the collection, measurement and analysis of data" (Kothari, 2008).

This particular study employed descriptive survey and experimental research design using a single case study approach. Descriptive survey was chosen because it helps in collection of information by administering a questionnaire to a sample of the population. The method can be utilized when collecting data about people's opinions, habits, attitudes and other social or educational issues (Orodho, 2003). It enabled the researcher to gather data on IT administrator attitudes towards patch and vulnerability management before and after exposure to a simulated ethical hacking video.

The Before-and-after without control experimental design was used to evaluate IT administrators' attitudes towards patch and vulnerability management before and after exposure to the ethical hacking simulation. In this design, a single test group, IT administrators was chosen, attitudes towards patch management, the dependent variable was measured, then the treatment was introduced - exposure to the ethical hacking video and the dependent variable was measure again after treatment was introduced (Kothari, 2008).

This research followed consisted of five stages: literature review: design of instrument; ethical hacking simulation; survey administration and analysis of results.

Stage 1 involved a literature review of information security in general, hacking, ethical hacking and persuasive technology. The literature review identified attitudes towards patch and vulnerability management and the ethical hacking methodology to be used in performing the ethical hacking simulation.

In stage 2, python hacking scripts were downloaded from the internet and developed for use in simulating a database attack. The scripts were then used to simulate a database attack. The simulation was recorded in a 3 minute video to be used as a cause-and-effect persuasive media.

The aim of the simulated database attack was to influence the attitudes of IT administrators towards information security practices, in particular patch and vulnerability management.

In stage 3, to measure the effectiveness of the ethical hacking simulation, a Likert web survey instrument was developed for use in a pre-test post-test approach.

In stage 4, case study was conducted with 30 IT administrators from the Information Systems Department of a leading telecommunications company. The IT administrators' attitudes toward patch and vulnerability management were measured before and after they had watched a simulation of the man in the middle attack.

In stage 5, paired t-tests were applied to compare the difference of the mean between pre-simulation and post-simulation attitudes. Existence of a significant difference between the means of pre-hacking attitudes and post-hacking attitudes means this hacking simulation is effective in changing IT administrators' attitudes towards patch and vulnerability management.

3.2 Architecture of the simulated attack

The Oracle TNS Listener is the database server software component that handles network traffic between the client and the database using the configured instance ID the user requests to connect to. These instances are configured at the TNS Listener. Remote registration is one of the methods used to configure database instances. Here, the database's process monitor process connects to the remote TNS Listener and configures its instance ID in the remote listener. Connection requests to the TNS listener using the specified instance ID will be forwarded to the remote database server.

An attacker is able to exploit remote registration by registering a duplicate instance name or service name similar to an already existing one. The TNS listener considers this duplicate instance name a fail over or cluster instance. The listener will now load balance between all the registered database instances. Connections will be forwarded to both instances in a round robin fashion. All connections will be distributed equally between the attack and the genuine instances.

This attack mechanism was used to forward genuine client connection requests to the attacker controlled machine and block the connections from reaching the legitimate database server instance causing a denial of service.

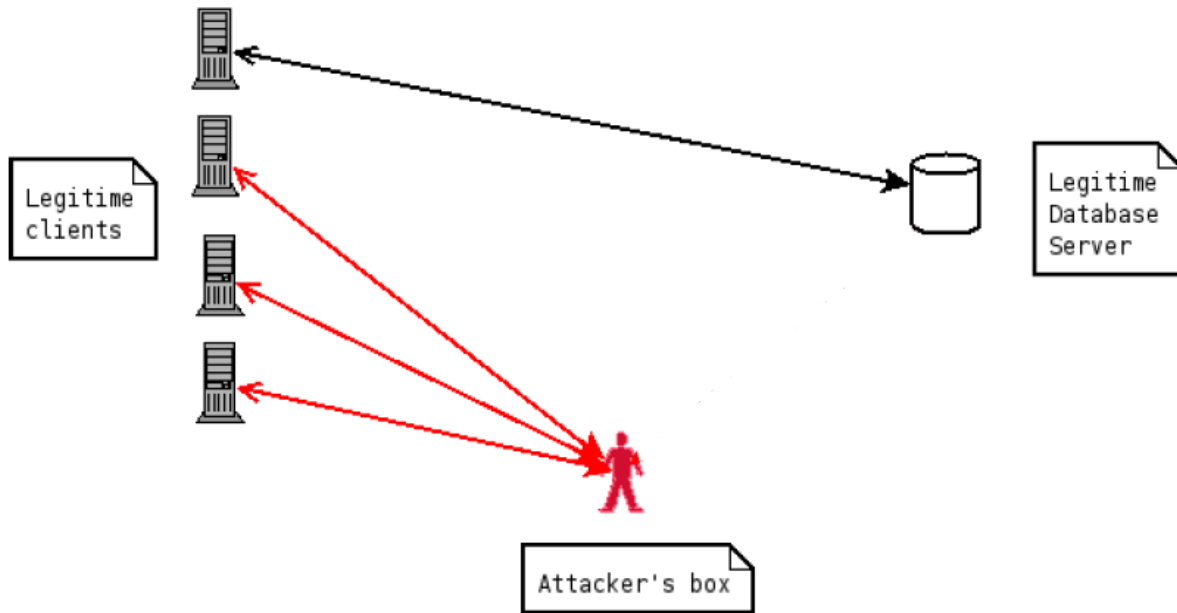


Figure 5: Simulated attack architecture [Source Koret (2008)]

At least 50% of the client requests connect to the attacker's computer which behaves as a TNS proxy and either routes or blocks connection requests to the database server, as shown in figure 5. Continuously registration of the same instance will ensure that at least fifty percent of the requests will be forwarded through the hijacker controlled machine.

3.3 Pre and Post Experiment Survey Design

3.3.1 Introduction

The pre study involved using a survey to determine the attitudes of the respondents towards patch and vulnerability management before they were exposed to hacking while the post study involved getting the attitudes of the respondents after exposure to ethical hacking.

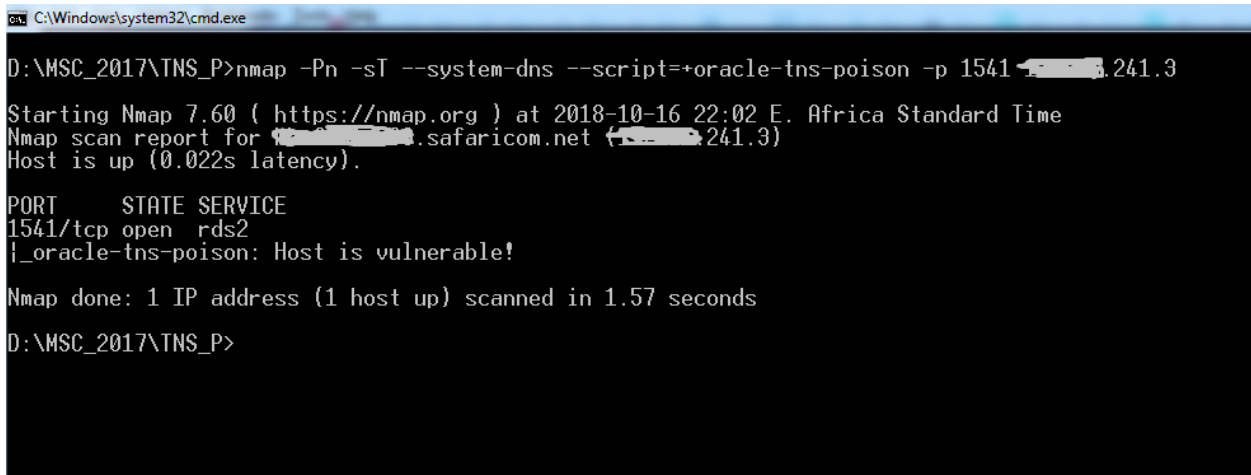
3.3.2 Hacking Experiment

To achieve the second objective, the ethical hacking methodology was used. Python scripts downloaded from the internet, modified to suit the man in the middle attack and used to scan the environment to confirm existence of the vulnerability. The scripts were also used to simulate a database attack by proxying database server connection requests from clients to the attack

machine. The simulation was recorded in a 3 minute video to be used as a cause-and-effect persuasive strategy. The video was then uploaded to an online storage location, google drive.

A simulated hacking attack was accomplished using the following steps.

1. Scanning for vulnerable databases. This is illustrated in figure 6.



```
C:\Windows\system32\cmd.exe
D:\MSC_2017\TNS_P>nmap -Pn -sT --system-dns --script=+oracle-tns-poison -p 1541 [redacted].241.3
Starting Nmap 7.60 ( https://nmap.org ) at 2018-10-16 22:02 E. Africa Standard Time
Nmap scan report for [redacted].safaricom.net ([redacted].241.3)
Host is up (0.022s latency).

PORT      STATE SERVICE
1541/tcp  open  rds2
|_oracle-tns-poison: Host is vulnerable!

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
D:\MSC_2017\TNS_P>
```

Figure 6: Scanning for database vulnerability to TNP poison vulnerability

2. Test and confirm connectivity from a client on the LAN to the target. This is illustrated in figure 7 and 8.

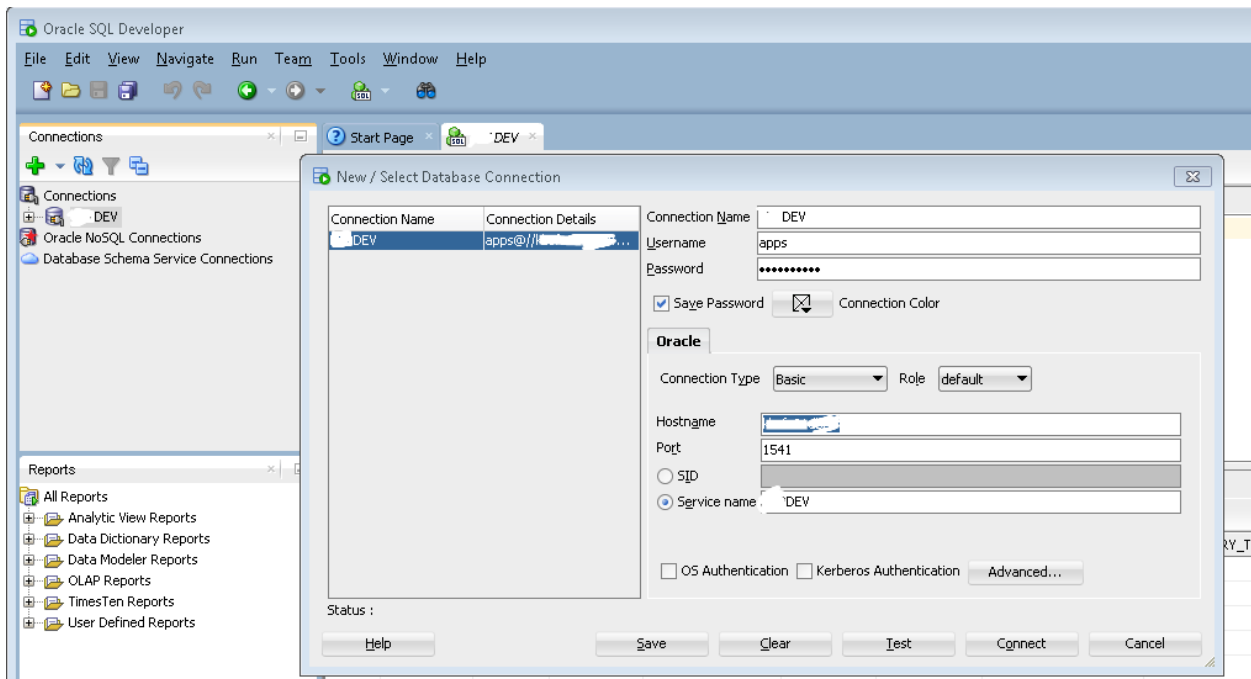


Figure 7: Target database connectivity test

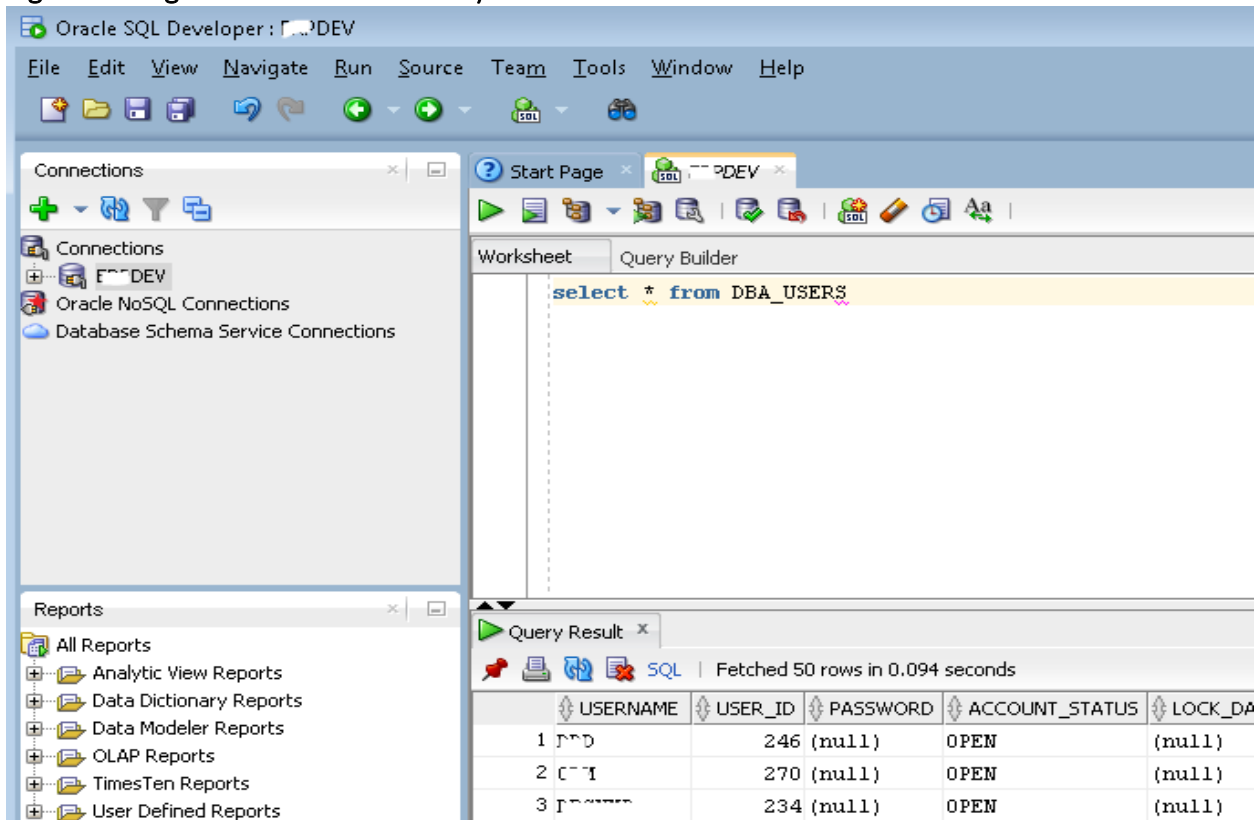


Figure 8: Target database user query

3. Run the python proxy script to proxy database connections via the attack computer. This TCP proxy script intercepted client connections to the real database's server port 1541 and forwarded them to the attack machine's port 1541. This is illustrated in figure 9.

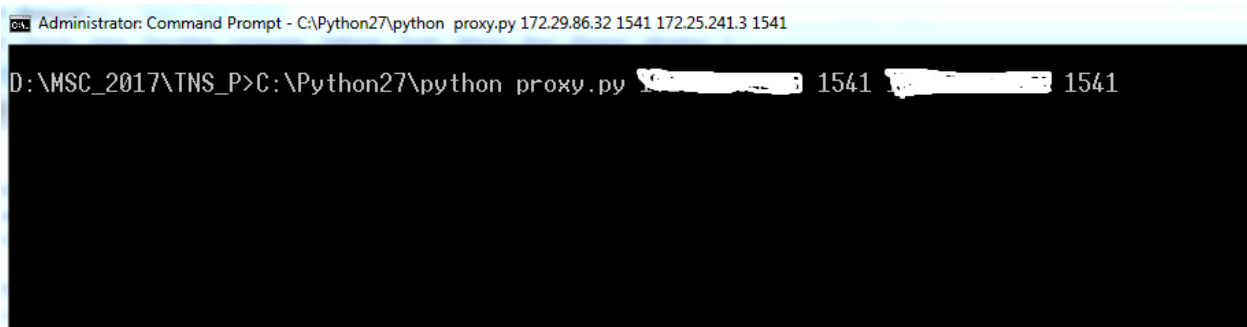


Figure 9: Running the proxy to intercept connections to the database server

4. The python database instance registration script ensured it registered the same database instance every 10 seconds to ensure continuous remote DB registration even when an

administrator tried to kill earlier established connections. This gave the attack control over the database. This is illustrated in figure 10.

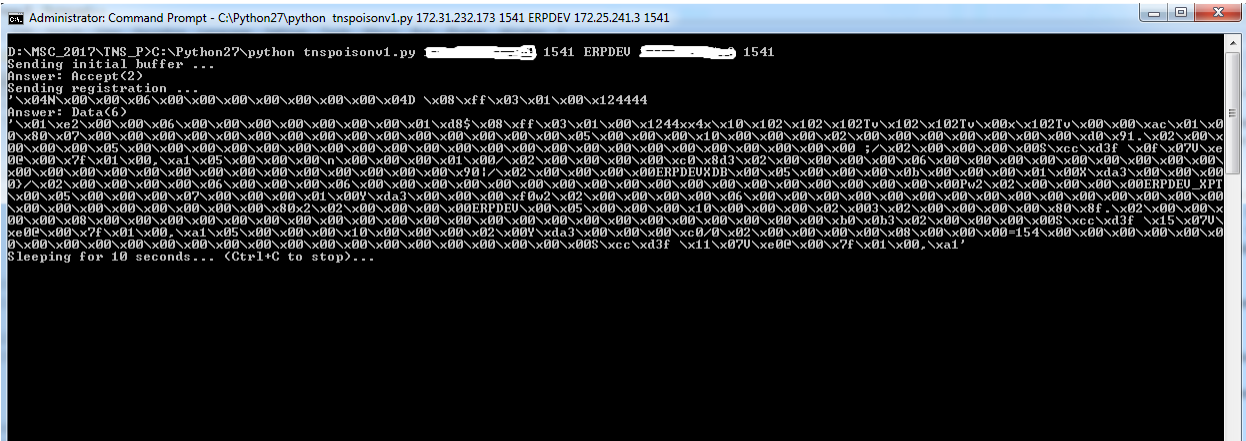


Figure 10: Continuous remote registration of the local attack database on the database server

5. As long as the proxy script is running, clients were not able to connect to the target DB, successfully achieving a DOS attack. This is illustrated in figure 11.

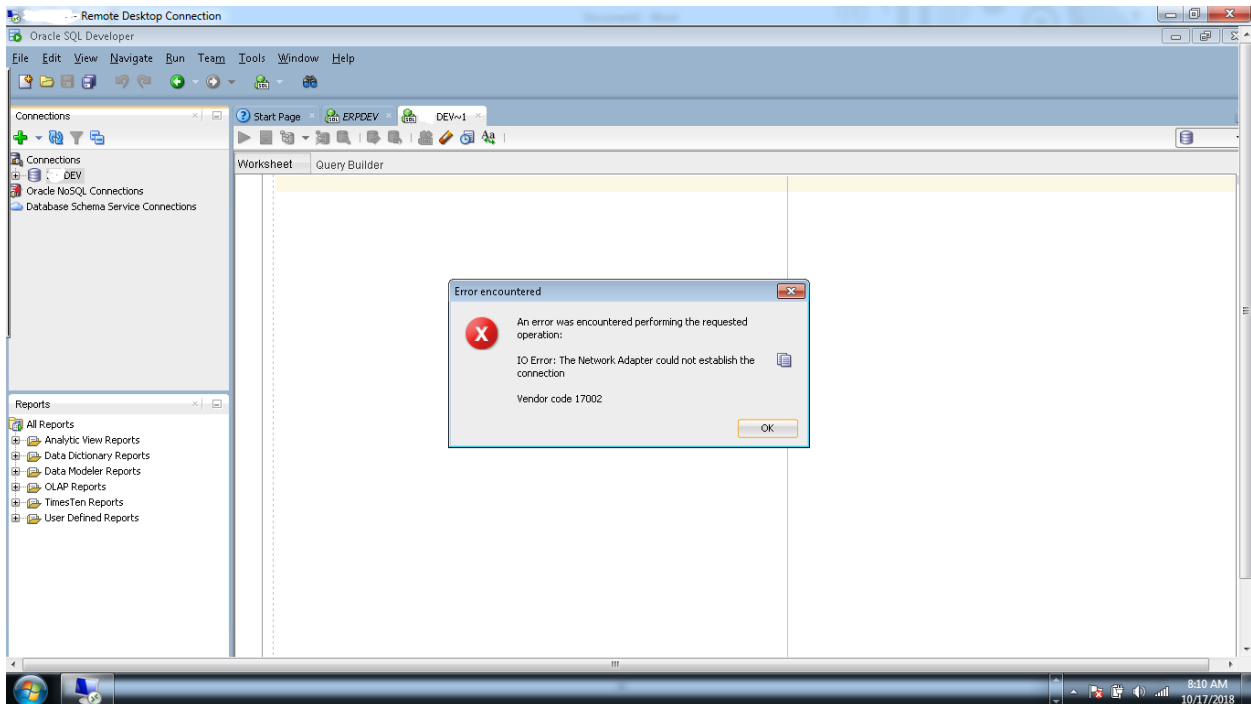


Figure 11: Client connection failure due to DOS attack

Any client attempting to login to the database is redirected to the attack box and connectivity fails as the credentials supplied are not applicable in the attack machine.

3.3.3 Sampling

The population of this research included IT administrators in the Information Systems (IS) department at a leading local communications company. The study chose IT administrators because patch management is concerned with updating software on systems (Palumbo, 2015). It is the responsibility of IT administrators to ensure the systems they administer are up to date. The communications company's IS department has a total of 100 employees based at the Headquarters in Nairobi out of which 30 are IT administrators and formed the population. These include network, database and system administrators. The research focused on this population because they own and are responsible for managing vulnerabilities in their domains. Their attitudes on information security against this backdrop is important.

This study employed simple random sampling to choose 17 respondents from the target population. Data of the population was manually populated to excel using an extract from the department's employee records. The 'insert random numbers' function of the kutools for excel was then used to generate and assign thirty unique random numbers to the population. The data was then ordered by the random numbers and the top 17 records chosen from the population of 30. An appropriate sample should be 10% to 30% of the population (Mugenda and Mugenda, 2003), this study achieved 57% of the entire population - 17 respondents, which is above the recommended threshold of 30%.

3.3.4 Instrument Design`

To evaluate the effectiveness of the simulated database attack in influencing IT administrators' attitudes on patch management, a questionnaire (appendix 1) was developed and administered to IT administrators' online through survey monkey website. Likert items used in the instrument were derived from literature review on attitudes towards patch management (2.3.1). Since the simulated database hack is aimed at changing the attitudes of IT administrators' toward patch and vulnerability management, the focus in this research is the 'attitudes toward behavior'. 'Attitudes toward the behavior' refers to the measure to which the person has an appreciative or unappreciative assessment of the behavior in question in this case patch management. The Likert scale was designed to measure attitude in a scientific manner in 1932 (Likert, 1932). In research

that employs Likert scale questionnaires, conclusions reached are dependent on the reliability and the validity of the questionnaires or scales used (Raubenheimer, 2004). The instrument consisted of nine items. To enhance reliability and validity, these were reduced to seven after testing the instrument. Because the instrument contained a uni-dimensional scale, reliability was checked using Cronbach's alpha. All items measure the same construct, attitudes towards patch and vulnerability management. Cronbach's alpha was used to check reliability of the scale. The questionnaire attained an acceptable reliability, $\alpha = 0.708$ after removal of 2 items from the 9 item scale. Table 2 shows the alpha value before the two items were dropped while table 3 shows the alpha value after. As shown in tables 4 and 5, items 8 and 9 were dropped because they had a very low correlation (-.103 and .132) with the scale overall. 0.7 is a suitable reliability coefficient (Nunnaly, 1978). Attitudes toward patch management were measured on a 5-point Likert scale from strongly agree to strongly disagree. The items were arranged to produce stems that contained both positive and negative statements. Since the items were stated in a negative way, a higher rating for items 1,2,3,4,5 and 7 reflects a negative attitude towards patch management while a lower rating for item 6 reflects a negative attitude towards patch management. A study by Lei and Rahaman (2009) found the impact of narrative ways on respondents' attitudes to be inconclusive. Levels of opinion were classified along with the Likert's five rating scales namely:

- Strongly agree = 5 points
- Agree = 4 points
- Undecided = 3 points
- Disagree = 2 points
- Strongly disagree = 1 points

Table 2: Reliability Statistics before testing questionnaire

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.627	.641	9

Table 3: Reliability statistics after testing questionnaire

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.708	.731	7

Table 4: Item statistics showing item correlation before removal of items to enhance reliability

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
I feel there are there are too many vulnerabilities to prioritize and patch. 1	28.00	18.750	.270	.532	.610
I feel that sorting through patchable vulnerabilities to find the relevant ones is a tedious and labor intensive.	27.71	16.096	.628	.783	.510
I believe that testing of patches and configuring the system is time consuming and costly	27.76	17.816	.594	.714	.541
I am too busy to continually check for security update patches.	28.00	18.750	.207	.743	.632
I believe that patching production systems requires taking the system down causing expensive downtime.	27.94	17.809	.401	.756	.574
I believe that not updating systems promptly with necessary patches can be costly.	26.82	19.279	.425	.592	.580
I believe that patches negatively impact critical user applicaton interface elements.	28.76	18.066	.377	.753	.580
I believe automatic software patch updates are not safe, since they can be abused to introduce malicious content.	27.88	22.860	-.103	.260	.687
I believe that patch updates often have bugs that must be fixed by the vendor.	28.41	20.882	.132	.199	.636

Table 5: Item statistics showing improved reliability after scale item cleanup

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
I feel there are there are too many vulnerabilities to prioritize and patch. 1	25.00	16.250	.343	.496	.601
I feel that sorting through patchable vulnerabilities to find the relevant ones is a tedious and labor intensive.	24.71	14.346	.635	.780	.513
I believe that testing of patches and configuring the system is time consuming and costly	24.76	15.941	.610	.713	.544
I am too busy to continually check for security update patches.	25.00	16.750	.219	.743	.644
I believe that patching production systems requires taking the system down causing expensive downtime.	24.94	16.309	.364	.751	.595
I believe that not updating systems promptly with necessary patches can be costly.	23.82	17.529	.409	.586	.593
I believe that patches negatively impact critical user applicaton interface elements.	25.76	16.441	.354	.753	.598
I believe automatic software patch updates are not safe, since they can be abused to introduce malicious content.	24.88	20.985	-.121	.239	.708

3.3.5 Data Collection

The data was collected by means of structured questionnaire developed according to the study's objectives. Structured questionnaires are effective in data collection particularly in quantitative analysis because respondents are subjected to the same questions. The method is offers a faster cost effective, unbiased and convenient to collect data. IT administrators were requested to fill in the questionnaires which contained closed questions to extract accurate information from the respondents. The questionnaire had two sections, Section A which covered the respondent's designation and years of experience and Section B which covered attitudes towards patch and vulnerability management. The questionnaire was administered online via the survey monkey website. This enabled the researcher to easily reach out to geographically dispersed administrators.

3.3.6 Data Analysis

Statistical package for social sciences (SPSS) was used to process and analyze primary data. Results were presented in form of descriptive statistics, reliability testing and paired t-test analysis. The purpose of testing for reliability was to get consistency of all variables. Hypotheses testing was done using paired sample t-test. The study used paired t-test to determine the significance of the difference of the mean between pre-exposure and post-exposure attitudes (the higher the better). *t*-test is considered an appropriate test for determining the significance of difference between the means of 2 samples where samples re small (Kothari, 2009). A significant difference between the means of pre-exposure attitudes and post-exposure attitudes would mean that exposure to ethical hacking is effective in changing administrators' attitudes toward patch and vulnerability management.

3.4 Post Analysis Interview

Study findings indicated the existence of negative results by some of the respondents. Negative results are findings where the post ethical hacking exposure attitude scores were worse than pre exposure scores. To explain this scenario, the study carried out a post survey interview targeting three respondents whose survey data analysis produced negative results. Post survey data was collected using a questionnaire developed by the researcher drawn from the two research questions.

CHAPTER 4: Data Analysis Results and Discussions

4.1 Introduction

This chapter discusses data analysis and the subsequent findings. Apoyo (2011) defines data analysis as the process of interpreting data to address the initial proposition of the study. The research findings correspond to the research objectives that steered the study. The data from the finished questionnaires was evaluated and the key findings presented. 17 questionnaires were distributed targeting IT administrators as they most likely to be involved or knowledgeable in the area of study. Statistical methods which included standard deviation, mean and paired t-test analysis were used. Paired t-test is considered suitable for a before and after experiment study (Kothari, 2008).

The chapter has two sections: Section One highlights the demographic characteristics of the population, Section Two reports on patch management practices in the organization the IT administrators' attitudes towards patch and vulnerability management.

4.2 Response Rate

17 out of 17 respondents accessed and completed the questionnaire resulting in a response rate 100%. All respondents also watched the video. Video access statistics are provided in appendix 2. The response rate was achieved after the researcher sent automated reminders on the survey monkey, called and visited the respondents to prompt the respondents to fill and complete the questionnaires. "A response rate of 50% is adequate for analysis and reporting; a rate of 60% is good and a response rate of 70% and over is excellent;" thus, this response rate was ideal for analysis and reporting (Mugenda and Mugenda, 1999).

4.3 Sample Characteristics

Data from the questionnaires was administered to the IT administrators and is presented and analyzed according to the background information designation and work experience of the respondents in Section A while Section B of the questionnaire stressed on establishing attitudes towards patch management.

4.4 Demographics

To capture general information, the researcher endeavored to establish the position and experience level of the respondents. The target respondents in targeted organization were IT administrators as

they were perceived to have a deeper understanding of the research subject. This was exemplified in table 6 below which show that 100% of the respondents were IT administrators. Table 7 illustrates the distribution of the respondents based on work experience. 17.6% of the respondents have less than 3 years' experience, 23.5% have worked for between 4-6 years and 58.8% have worked for more than 6 years. The mean for respondents with over 6 years of experience at 21.30 is lower than that of respondents with 4-6 years of experience at 21.50 and that of those who have less than 3 years' experience at 23.30 showing a more favorable attitude towards patch and vulnerability management generally. This is true post exposure to ethical hacking at 19.90, 22.50 and 24.00 respectively. This is illustrated in table 8.

Table 6: Designation of the respondents

Designation	Frequency	Percent
IT Administrators	17	100

Table 7: Distribution of the respondents based on work experience

Work experience					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 to 3 years	3	17.6	17.6	17.6
	4 to 6 years	4	23.5	23.5	41.2
	above 6 years	10	58.8	58.8	100.0
	Total	17	100.0	100.0	

Table 8: A comparison of pre hack and post hack attitudes based on work experience

Work experience		Pre_Hack_total	Post_Hack_Ttotal
1 to 3 years	Mean	23.33	24.00
	N	3	3
	Std. Deviation	4.726	3.000
4 to 6 years	Mean	21.50	22.50
	N	4	4
	Std. Deviation	4.435	2.380
above 6 years	Mean	21.30	19.90
	N	10	10
	Std. Deviation	3.802	3.348
Total	Mean	21.71	21.24
	N	17	17
	Std. Deviation	3.901	3.382

4.5 Administrator Attitudes Pre and Post Exposure to Ethical Hacking

To achieve objective three and evaluate the effectiveness of the simulated ethical hacking in influencing administrators' attitude toward patch and vulnerability management, the participants were requested to complete the survey instrument on survey monkey after watching the simulated ethical hacking video. Seventeen administrators from the information systems department participated in the study. Appendix 2 shows an extract of tracking of the video link on the cisco firewall. The standard deviations and means are shown in Table 9 and 10. As illustrated in table 9, the PostHack mean is slightly lower than the PreHack mean. Being a negatively worded item scale, the results show a slight improvement in IT administrator attitude after exposure to the ethical hacking video. Table 10 shows that the means of third, fourth and sixth items are lower after administration of the hacking video depicting and improvement in attitudes. The means of the second item are equal before and after administration of the hacking video depicting no improvement in attitudes. The means for first, fifth and sixth items are higher after participants have watched the ethical hacking simulation video depicting a deterioration in attitudes.

Table 9: Pre and post ethical hacking exposure paired samples statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Pre_Hack_total	21.71	17	3.901	.946
	Post_Hack_Total	21.24	17	3.382	.820

Table 10: Comparison of Pre and post exposure to ethical hacking Item Means and Standard Deviation

	Attitudes Towards Patch Management			
	Pre-Hack		Post-Hack	
	Mean	Std. Deviation	Mean	Std. Deviation
I feel there are too many vulnerabilities to prioritize and patch.	3.41	1.176	3.76	1.091
I feel that sorting through patchable vulnerabilities to find the relevant ones is a tedious and labor intensive.	3.71	1.105	3.71	1.047
I believe that testing of patches and configuring the system is time consuming and costly.	3.65	.862	3.47	1.125
I am too busy to continually check for security update patches.	3.41	1.326	3.06	1.029
I believe that patching production systems requires taking the system down causing expensive downtime.	3.47	1.125	3.53	1.125
I believe that patches negatively impact critical user application interface elements.	2.65	1.115	2.35	.931
I believe that not updating systems promptly with necessary patches can be costly.	4.59	.795	4.65	.786

Before performing the paired sampled t-tests to determine whether the differences of the means of administrators’ attitudes responses prior and after the administration of simulated ethical hacking was significant, it is essential to establish that the attitude data follows a normal distribution. The

Shapiro-Wilk normality test was used to determine normal distribution for both pre-hacking and post-hacking administrator attitude response data. The Shapiro-Wilk values for pre and post-simulation attitude responses have a p-value greater than 0.05 as shown in table 11, hence the distribution of administrator responses can be presumed to be normally distributed.

Table 11: Pre and post ethical hacking exposure mean scores normality test

Tests of Normality						
When are you taking this survey?	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
PreHackTest	.131	17	.200 [*]	.955	17	.540
PostHackTest	.125	17	.200 [*]	.961	17	.659

To determine the significance of the difference in the overall attitude of administrators prior and after administration of the simulated ethical hacking video, a paired-sample t-test was performed. The confidence interval was 95%. The findings are shown in Table 12, the p value of .546 is higher than our significance level, 0.05 indicating the lack of a significant difference in administrator attitudes towards patch and vulnerability management showing there is no effect of the simulated ethical hacking in influencing administrators' attitudes towards patch and vulnerability management. $t(16)=.617$, $p \leq .05$. The null hypothesis holds true – exposure to ethical hacking on systems one manages has no impact on administrator attitudes towards better information security practices.

Table 12: Test of significance of the difference of means pre and post exposure to ethical hacking

Paired Samples Test									
		Paired Differences			95% Confidence Interval of the Difference		t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	Lower	Upper			
Pair 1	PreHack - PostHack	.35294	3.80692	.92331	-1.60440	2.31028	.382	16	.707

4.6 Post Survey Interview Findings

The study carried out a post survey interview on three respondents whose survey data analysis returned a negative results. A sample of three respondents was interviewed. According to a February 2018 survey on employee awareness of IT security threats, more than 28% of employees are unaware of their company's cybersecurity policy. Similarly, 46% of entry-level employees are

unaware of such a policy. 63% of employees are uncertain of the threat landscape in their company over the next year (Kemper, 2018). Despite more than 85% of business leaders citing cyber security as a top priority for their company, only 11% said they'd adopted and articulated a cyber risk strategy. Of those who had a strategy in place, 28% said they had effectively communicated the cyber risk strategy with stated objectives and goals to employees. Just 8%, meanwhile, reported to have embedded cyber risk management within their company culture (EDC, 2018). The IT administrators were asked their view on keeping IT systems they manage up to date in order to secure them from cyberattacks? As in the above studies, the IT administrators felt that patch and vulnerability management was not a strategic priority as it had not been articulated as such. They also felt that IT security was not their KPI, rather it was the responsibility of the cybersecurity team. Studies reveal that Cyber-attacks like fatal diseases are treated with irreverence – they seem distant and intangible, myths relegated to the back pages, that is until they strike. The recent WannaCry and Petya attacks prove our vulnerability is being exploited and practically ridiculed. Only post attacks did the UK government increase cyber security budget allocations to the National Health Service. This funding was allocated for ethical hacking activities, systems upgrades and patching, threat intelligence, among other IT security activities (Davis, 2017). This implies real and consequential attacks are a proven trigger for attitude change more than non-consequential attacks. The respondents were therefore asked if they had experienced a major cybersecurity incident on the IT systems they manage. This attitude is replicated across as the post survey interview with IT administrators revealed that patching is not a priority as their domains have not suffered any notable attacks.

Chapter 5: Conclusions and Recommendations

This chapter provides a summary of the research conclusions and recommendations as noted in the study. It also levels out the limitations of the written report and provides hints for further inquiry as well as implications of the study of policy and practice.

5.1 Summary and Conclusions of the study

As a recap the study had three objectives namely to carry out a pre-study to determine attitudes towards patch management among IT administrators in a leading telecommunications company, to execute a simulated ethical hacking attack on a targeted database system and to carry out a post-study to determine attitudes towards patch management among IT administrators after exposure to the simulated ethical hacking attack.

To find out the effect of ethical hacking on IT administrator attitudes, the first objective was to carry out a pre-study to determine attitudes towards patch management among IT administrators in a leading telecommunications company. The attitudes were identified through literature review (2.3.1) and formed the basis for the questionnaire administered to the IT administrators. The findings indicate that the IT administrators had a negative attitude towards patch and vulnerability management with a mean of 21.71. The respondents felt that there are too many vulnerabilities to prioritize and patch at a mean of 3.41, that sorting through patchable vulnerabilities to prioritize is labor intensive and tedious at a mean of 3.71, that testing of patches and configuring the system is time consuming and costly at a mean of 3.65, that they were too busy to continually check for security update patches at a mean 3.41 and that patching production systems requires taking the system down causing expensive downtime at a mean of 3.47 all above the mean score 3. This means the attack surface continues to increase even as remediation to vulnerabilities are provided by system vendors in form of application patches. It also explain why IT administrators continue to be caught off guard by hackers time and time again. Even where remediation is a matter of system configuration, negative attitudes towards vulnerability management ensure the configuration changes required are not carried out. Brewster (2017), Right (2017), and Brewster (2017) highlight costly major vulnerability exploits on unpatched systems despite availability of patches that remediate these vulnerabilities.

The mean for respondents with over 6 years of experience at 21.30 is slightly lower than that of respondents with 4-6 years of experience at 21.50 and that of those who have less than 3 years'

experience at 23.30 showing a more favorable attitude towards patch and vulnerability management generally. The less the years of experience, the less favorable the attitude towards patch management.

The second objective was to execute a simulated ethical hacking attack on a targeted database system. This was achieved by researching on known and published database vulnerabilities, scanning for the same in the organization's LAN, researching and downloading exploit kits and proceeding to cause a DOS attack on an identified database. The aim was to influence the IT administrators' attitudes by exposing them to ethical hacking. The study demonstrated that it is relatively easy to hack into systems with easily available instructions, tools and utilities that are available over the internet. This as long as vulnerabilities are not remediated. A scan of the database servers revealed that many of them were vulnerable to the TNS poison attack. For privacy reasons the statistics are not published in this study.

The third objective was to carry out a post-study to determine attitudes towards patch management among IT administrators after exposure to the simulated ethical hacking attack. There was a slight improvement on attitudes towards patch and vulnerability management with a sum mean of 21.24 post exposure to ethical hacking against a sum mean of 21.71 pre exposure to ethical hacking. However overall, attitudes towards patch management remain negative among the IT administrators.

The findings indicate the absence of a significant difference in IT administrators' attitudes towards patch and vulnerability management meaning exposure to ethical hacking has no effect on IT administrators' attitudes towards information security aware behavior with some of the respondent's mean scores showing a negative effect after exposure to ethical hacking.

The post survey interview to seek clarity on negative survey results revealed that the IT administrators felt that patch and vulnerability management was not a strategic priority as it had not been articulated as such. They also felt that IT security was not their KPI, rather it was the responsibility of the cybersecurity team. They also revealed that patching is not a priority as their domains have not suffered any notable attacks.

This finding is useful to IT professionals and researchers in coming up with effective strategies and policies for enhancing patch management attitudes for IT administrators since it provides a basis for making decisions when formulating information security strategies or policy.

5.2 Limitations of the study

These findings should to be treated with caution as the respondents of this research were limited to IT administrators of a single organization in the case study. Hence, this research could be extended to other IT end users within the organization and by extension IT administrators of other organizations. Gender differences in attitudes toward patch and vulnerability management practices could also be investigated. Only one aspect of information security management was explored in the study. Future research could include other security aspects.

Finally, the evaluation of the effectiveness of the information security breach simulation was performed soon after exposure of the ethical hacking video. The long term effectiveness of ethical hacking on administrator attitudes towards patch and vulnerability management is still not known. These will need to be explored in related future studies.

5.3 Recommendations

The following are recommendations of the study.

Since IT administrators felt that patch and vulnerability management was not a strategic priority as it had not been articulated as such, this study recommends that cybersecurity should be a top priority in corporate strategy and should be clearly communicated as such. To clarify IT security domain responsibilities, corporate IT security policy should also be clear on application patching responsibilities. This study recommends that IT administrators be given ownership of application patching. This will ensure they are given priority in training and sensitization which in turn will improve their attitudes towards patch management.

To effectively utilize ethical hacking as a risk management technique, this study recommends that the company enhances its bug bounty program by offering better reward for high impact bugs. Proactive patch management will remediate up to 95% of exploitable vulnerabilities greatly minimizing losses to organizations.

The above measures will contribute towards improving IT administrator attitudes towards patch and vulnerability management.

5.4 Suggested Areas for Further Research

The study suggest that a similar study be extended to IT administrators in other organizations in the telecommunications sector as well as other sectors of the economy including financial services, retail and others as this study was a case study. The study chose Computers as Persuasive Media (Simulation) as a persuasive technology to influence administrator attitudes towards patch management. The study recommends exploration of other persuasive technology strategies to influence administrator attitudes towards patch management.

The study chose a production replica database as its attack target which the respondents did not take seriously. The study recommends extension of the hacking scope to production systems. This may achieve the desired results of impacting IT administrator attitudes towards patch and vulnerability management considering the impact and attention a real attack gets.

REFERENCES

- Ahmad, K., JayantShekhar, Kumar, N., Yadav, K.P. 2011. Policy Levels Concerning Database Security; International Journal of Computer Science & Emerging Technologies (E-ISSN: 2044-6004) 368 Volume 2, Issue 3, page(s); 368-372
- Arbaugh W.A., W.L Fithen, and J.M Hugh. 2000. Windows of Vulnerability: A case Study Analysis. Computer 33 (12):52-59.
- Ajzen, I., Fishbein, M. 1980. Understanding Attitudes and Predicting Social Behavior. Englewood Cliffs, N.J.: Prentice-Hall.
- Ajzen, I. 1991. The Theory of Planned Behavior [Online] Available from https://s3.amazonaws.com/academia.edu.documents/32876859/Ajzen_1991_The_theory_of_planned_behavior.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1522314736&Signature=3cgKkeXqsuMqLimVqBv1CXsf48M%3D&response-content-disposition=inline%3B%20filename%3DAjzen_1991_The_theory_of_planned_behavior.pdf [Accessed: 23rd May 2018]
- AUSCERT, “2006 Australian Computer Crime and Security Survey”, Available at: www.auscert.org.au [Accessed: 23rd May 2018]
- Baraani-Dastjerdi, A., Pieprzyk, J., Pieprzyk, B. J., ReihanedSafavi-Naini. 1996. Security In Databases: A Survey Study
- Basharat, I., Azam, F., Wahab, Muzaffar, A. W. 2012. Database Security and Encryption: A Survey Study, International Journal of Computer Applications (0975 –888) Volume 47–No.12
- Beattie, S., S. Arnold, C Cowan, P Wagle, and C Wright. 2002. Timing the Application of Security Patches for Optimal Uptime. LISA XVI (November 3-8, 2002):101-110.
- Bentley, A. 2006. Developing a patch and vulnerability management strategy 2005 [cited January, 25 2006]. Available from <http://www.scmagazine.com/uk/news/article/523151/developing-patch-vulnerability-management-strategy/>. [Accessed: 24rd June 2018]
- BITSIGHT. 2017. A growing risk ignored: Critical updates [Online] Available from <https://info.bitsighttech.com/bitsight-insights-a-growing-risk-ignored-critical-updates> [Accessed: 16th June 2018]
- Bloor, Baroudi. 2003. THE PATCH PROBLEM It’s Costing your Business Real Dollars [Online] Available from https://www.netsense.info/downloads/PatchProblemReport_BaroudiBloor.pdf [Accessed: 26th January 2018]
- Brewster, T.F 2017. How Hackers Broke Equifax: Exploiting A Patchable Vulnerability [Online] Available from <https://www.forbes.com/sites/thomasbrewster/2017/09/14/equifax-hack-the-result-of-patched-vulnerability/#7fdb0cde5cda> [Accessed: 18th January 2018]
- Bulgurcu B., Cavusoglu H., Benbasat I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly

[Online] Available from https://s3.amazonaws.com/academia.edu.documents/30986994/bulgurcucavusoglubenasat.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1522667434&Signature=ETPUBwXyyAyOAP3zRNleb%2BkFwrk%3D&response-content-disposition=inline%3B%20filename%3DInformation_Security_Policy_Compliance_A.pdf

[Accessed: 14th January 2018]

Cavusoglu, H., Cavusoglu, H. & Zhang, J. 2008. Security patch management: share the burden or share the damage? *Management Science*, 54(4):657-70.

Collier, M., Endler, D. 2014. *Hacking Exposed: Unified Communications & VoIP Security Secrets & Solutions*. McGraw Hill, New York

Davis, J., 2017. After WannaCry knocked it offline, UK's National Health Service banks on new security center to improve cybersecurity. [Online] Available from <https://www.healthcareitnews.com/news/after-wannacry-knocked-it-offline-uks-national-health-service-banks-new-security-center-improve> [Accessed: 2nd November 2018]

DeFino, S., Greenblatt, L.(2013). *Official Certified Ethical Hacker Review Guide: For Version 7.1*. Cengage Learning, USA

Donner, M. (2003). Patch management - bits, bad guys, and bucks! *Secure Business Quarterly*, 3(2), 1-4. Available from: <https://nygeek.wordpress.com/2012/08/31/patch-management-bits-bad-guys-and-bucks/>. [Accessed: 23rd January 2018]

DUO. 2017. *Trusted Access report: The current state of enterprise endpoint security*. [Online] Available from <https://duo.com/assets/ebooks/duo-trusted-access-report-2017.pdf> [Accessed: 24th March 2018]

EDC., 2018. *Cyber Risk Management Has Become Essential to Protecting Business Operations* [Online] Available from <https://edc.trade/cyber-risk-component-of-enterprise-risk-management/> [Accessed: 2nd November 2018]

Engelbreton, P.(2013). *The Basics of Hacking and Penetration Testing*.Elsevier, USA

Falk, C. (2005) *Ethics and hacking: the general and the specific*, *Norwich University Journal of Information Assurance*,1(1).

Fogg, B.J. and Nass, C. 1997 'How users reciprocate to computers: an experiment that demonstrates behaviour change', in *Extended Abstracts of the CHI97 Conference of the ACM/SIGCHI* (New York: ACM Press, 1997).

Fogg B.J. 2003. *Persuasive Technology: using computers to change what we think and do*, Morgan Kaufmann Publishers, CA

Hackerone. 2018. *THE 2018 HACKER REPORT* [Online] Available from https://www.hackerone.com/sites/default/files/2018-01/2018_Hacker_Report.pdf [Accessed: 11th January 2018]

- Hirsh J.B., Kang S.K., Bodenhausen G.V. 2012. Personalized persuasion: tailoring persuasive appeals to recipients' personality traits. [Online] Available from <https://www.scholars.northwestern.edu/en/publications/personalized-persuasion-tailoring-persuasive-appeals-to-recipient> [Accessed: 15th March 2018]
- Hughes, G.D. 2016. A FRAMEWORK FOR SOFTWARE PATCH MANAGEMENT IN A MULTI-VENDOR ENVIRONMENT [Online] Available from <http://etd.cput.ac.za/bitstream/handle/20.500.11838/2478/208049517-Hughes-Grant-Douglas-Mtech-Information-Technology-FID-2017.pdf?sequence=1&isAllowed=y>. [Accessed: 4th January 2018]
- Hulme, G.V. 2006. Under Attack 2004 [cited February 12 2006]. Available from <http://www.informationweek.com/industries/showArticle.jhtml?articleID=22103493&pgno=1>. [Accessed: 4th January 2018]
- IJsselsteijn, W.A., de Kort, Y.A.W., Midden, C., Eggen, B., and van den Hoven, E. 2006. 'Persuasive technology for human well-being: setting the scene', Persuasive 06 Eindhoven: Springer.
- Ioannidis, C., Pym, D. & Williams, J. 2012. Information security trade-offs and optimal patching policies. European Journal of Operational Research, 216(2):434-44.
- Kemper, G., 2018. Employee Awareness of IT Security Threats. [Online] Available from <https://clutch.co/it-services/resources/employee-awareness-it-security-threats#Companies> [Accessed: 2nd November 2018]
- Kharpal, A. 2015. Ethical hacking: Are companies ready? [Online] Available from <https://www.cnbc.com/2015/06/17/are-companies-still-scared-of-white-hat-hackers.html> [Accessed: 4th January 2018]
- Koret, J. 2008. Oracle Database TNS Listener Poison Attack
- Lapolla, N.A. and Salvucci, A. 2000. 'Evaluation of a Youth Driving Simulator Program', available at: http://apha.confex.com/apha/128am/techprogram/paper_13286.htm. [Accessed: 4th January 2018]
- Lei, W., Rahaman, M. A. 2009. Two Experiments with Likert Scale [Online] Available from http://users.du.se/~lrn/C_upps09/EssayE_C-level.pdf [Accessed: 23rd January 2018]
- Lenert, L., Muñoz, R.F., Stoddard, J., Delucchi, K., Bansod, A., Skoczen, S., Pérez-Stable, E.J. 2003 'Design and Pilot Evaluation of an Internet smoking cessation program', J AM Med Inform Assoc.
- Likert, R. 1932. A TECHNIQUE FOR THE MEASUREMENT OF ATTITTUDES Online] Available from https://legacy.voteview.com/pdf/Likert_1932.pdf [Accessed: 8th January 2018]
- Lynn, Tracy. 2006. Vulnerability Risk mitigation--Patching the Microsoft Windows Environment 2002 [cited February 3 2006]. Available from <http://www.sans.org/rr/whitepapers/windows/291.php>. [Accessed: 15th March 2018]

- Masadeh, M.A. 2012. Focus Group: Reviews and Practices. [Online] Available from https://s3.amazonaws.com/academia.edu.documents/32876859/Ajzen_1991_The_theory_of_planned_behavior.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1522314736&Signature=3cgKkeXqsuMqLimVqBv1CXsf48M%3D&response-content-disposition=inline%3B%20filename%3DAjzen_1991_The_theory_of_planned_behavior.pdf [Accessed: 15th March 2018]
- McGhie, L. (2003). Software patch management - the new frontier. *Secure Business Quarterly*, 3(2), 1-4.
- McKay, M.(2012). Best Practices in Automation Security. In 53rd IEEE-IAS/PCA Industry Technical Conference, 1-15
- Medzich, M. 2004. Global Information Assurance Certification Paper. Patch Management. [Online] Available from <https://www.giac.org/paper/gsec/3876/deploying-process-patch-management-relation-risk-management/106152> [Accessed: 18th March 2018]
- Moore, D. & Shannon, C. 2002. Code-Red: a case study on the spread and victims of an Internet worm. *Proceedings. The 2nd ACM SIGCOMM Workshop on Internet measurement*. ACM: 273-284.
- NIST. 2005. Creating a Patch and Vulnerability Management Program [Online] Available from <http://tim.kehres.com/docs/nist/SP800-40v2.pdf> [Accessed: 14th March 2018]
- Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory*. Sydney: McGraw-Hill.
- Oriyano, S. (2014). *Ceh: Certified Ethical Hacker Study Guide*. John Wiley, Indianapolis
- Palumbo, T. Patch Management: The Importance of Implementing Central Patch Management and Our Experiences Doing So. [Online] Available from <https://dl.acm.org/results.cfm?query=patch+management&Go.x=0&Go.y=0> [Accessed: 2nd November 2018]
- Pham, Hiep Cong et al. Information Security and People: A Conundrum for Compliance. *Australasian Journal of Information Systems*, [S.l.], v. 21, jan. 2017. ISSN 1449-8618. Available at: <<http://journal.acs.org.au/index.php/ajis/article/view/1321>>. [Accessed: 6th March 2018]
- Prasad, M., Manjula, B. (2014). Ethical Hacking Tools: A Situational Awareness. *Int J. Emerging Tec. Comp. Sc. & Elec.*11, 33-38
- Raubenheimer, J. E. (2004). An item selection procedure to maximize scale reliability and validity. *South African Journal of Industrial Psychology* , 30(4), 59-64.
- Right, Tom. 2017. Did unpatched Microsoft exploit lead to massive NHS ransomware attack? [Online] Available from <https://www.channelweb.co.uk/crn-uk/news/3010030/did-unpatched-microsoft-exploit-lead-to-massive-nhs-ransomware-attack> [Accessed: 20th January 2018]

- Roisin, B.C. 2017 Persuasive Technology [Online] Available from <https://engineering.dartmouth.edu/~d30345d/courses/engs44/PersuasiveTechnology.pdf> [Accessed: 28th January 2018]
- Saldana, J. 2009. The Coding Manual for Qualitative Researchers. London ECIY ISP: SAGE.
- Schrader, P. and K. A. Lawless (2004). The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments.
- Sekaran U. 2004. Organizational behavior: text and cases. Southern Illinois: Tata Mcgraw Hill Publishing Company Limited.
- Shulman, A. 2006. Top Ten Database Security Threats, How to Mitigate the Most Significant Database Vulnerabilities, White Paper
- Spencer, L. Ritchie, J. (2002) Quality in Qualitative Evaluation; A framework for assessing research evidence, The British academy Journal, 6:99-105
- Symantec Threat Advisory Center. 2007. Outbreak alert: storm trojan [Online] Available from http://www.symantec.com/outbreak/storm_trojan.html. [Accessed: 28th March 2018]
- Valois, P., Turgeon, H., Godin, G., Blondeau, D., and Cote, F. 2001. 'Influence of a persuasive strategy on nursing students' beliefs and attitudes toward provision of care to people living with HIV/AIDS', Journal of Nursing Education.
- Vania, K., Rader, E., and Wash, R. 2014. Betrayed by updates: How negative experiences affect future security. In Proceedings of the ACM Conference on Human Factors in Computing (CHI), Toronto, Canada.
- Zhang, C., Prichard, Janet, J. 2009. AN EMPIRICAL STUDY OF CYBER SECURITY PERCEPTIONS, AWARENESS AND PRACTICE [Online] Available from <https://pdfs.semanticscholar.org/cb71/db1034059bf2464f63f09cd217fd2a5e97d4.pdf> [Accessed: 26th January 2018]
- Zhao, D., Furnell, M. & Al-Ayed, A. 2009. The research on a patch management system for enterprise vulnerability update. Paper presented at the 2009 International Conference on Information Engineering –ICIE 2009, Taiyuan, 10-11 July
- Zhou, C.V., Leckie, C. & Karunasekera, S. 2010. A survey of coordinated attacks and collaborative intrusion detection. Computers and Security 29(1):124-40.

APPENDICES

APPENDIX 1: Questionnaire

I am carrying a research on ethical hacking in relation to patch management practices. I would appreciate your views on this. I am hopeful that you will respond to all of the questions. The information you provide will be used for research intentions only and will be kept private and confidential. None of the information will be disclosed to any party nor will the identity of the respondent revealed. Feel free to engage for any clarifications.

Thank you.

Section A: Demographic data

Your Thoughts On Patch Management

Section A: Demographic data

* 1. Designation

* 2. Work experience

1 to 3 years above 6 years

4 to 6 years

Section B: Patch management attitudes

Your Thoughts On Patch Management

Patch management attitudes

- * 1. I feel there are too many vulnerabilities to prioritize and patch.

Strongly Disagree Disagree Undecided Agree Strongly Agree

- * 2. I feel that sorting through patchable vulnerabilities to find the relevant ones is a tedious and labor intensive.

Strongly Disagree Disagree Undecided Agree Strongly Agree

- * 3. I believe that testing of patches and configuring the system is time consuming and costly.

Strongly Disagree Disagree Undecided Agree Strongly Agree

- * 4. I am too busy to continually check for security update patches.

Strongly Disagree Disagree Undecided Agree Strongly Agree

- * 5. I believe that patching production systems requires taking the system down causing expensive downtime.

Strongly Disagree Disagree Undecided Agree Strongly Agree

- * 6. I believe that not updating systems promptly with necessary patches can be costly.

Strongly Disagree Disagree Undecided Agree Strongly Agree

- * 7. I believe that patches negatively impact critical user application interface elements.

Strongly Disagree Disagree Undecided Agree Strongly Agree

[DOS - Please copy hyperlink and watch a short 3 minute video on unpatched systems vulnerability](#)

APPENDIX 2: Video Access Records



CONTENT SECURITY MANAGEMENT APPLIANCE

Web Tracking

Search Criteria: Website: r2---sn-hc57en7d.c.drive.google.com, Web Appliance:

Results				
				Items Displayed: 31
Time (GMT +03:00)	Website	Disposition	Bandwidth	User / Client IP
29 Jun 2018 13:08:50	tunnel://r2---sn-hc57en7d.c.drive.google.com:443/	Allow	6.4MB	sochieng1 172.
29 Jun 2018 13:01:43	tunnel://r2---sn-hc57en7d.c.drive.google.com:443/	Allow	3.9MB	sochieng1 172.
19 Jun 2018 10:25:22	tunnel://r2---sn-hc57en7d.c.drive.google.com:443/	Allow	4.0MB	jitumbo 172.
14 Jun 2018 18:07:00	tunnel://r2---sn-hc57en7d.c.drive.google.com:443/	Allow	2.0MB	jkmutua 172.
14 Jun 2018 15:46:02	tunnel://r2---sn-hc57en7d.c.drive.google.com:443/	Allow	5.0MB	hdaudi 172.
14 Jun 2018 15:44:28	tunnel://r2---sn-hc57en7d.c.drive.google.com:443/	Allow	5.5MB	hdaudi 172.
14 Jun 2018 15:42:33	tunnel://r2---sn-hc57en7d.c.drive.google.com:443/	Allow	979.4KB	hdaudi 172.
14 Jun 2018 14:31:03	tunnel://r2---sn-hc57en7d.c.drive.google.com:443/	Allow	10.9MB	jkmutua 172.