A Multiple Case Study Approach to Identify Vulnerabilities of Advanced Persistent Threats

Mathew Nicho, Shafaq Khan
College of Information Technology, University of Dubai, UAE

ABSTRACT

One of the most serious and persistent threat that had emerged in recent years combining technical as well as non-technical skills is the Advanced Persistent Threat, known commonly as APT where the hackers circumvent the organizational defenses and instead target the naivety of the employees in making an unintentional mistake. While this threat has gained prominence in recent years, research on its cause and mitigation is a scant area of research. Analysis of high profile cases during the last three years where it (APT) had gained prominence revealed that unintentional mistakes of employees and the persistence of the attackers in using social engineering methods have largely contributed to this threat. To further analyze the detailed causes of APT attacks, we conducted interviews of senior IT managers in three large organizations in Dubai. The analysis of the findings suggested that the APT threat environment is affected by multiple factors spanning the technical as well as non technical domain.

Keywords: Advanced Persistent Threats, APT, information security, data breach, spear-phishing

INTRODUCTION

The major threat faced by organizations concerning APT is the hacker's ability and persistence to exploit the vulnerability of the employees in gaining entry to the organizational network rather than directly targeting the organizational defenses. In this aspect, prevention of this threat depends to a large extent on the information security awareness level of employees in detection and prevention. The purpose of this paper is to find out vulnerable areas of information security from an APT perspective, to provide guidance to IS security managers in taking the necessary steps to close the gaps in security.

APT is one of the least studied and researched topic in the academic domain. Research on linking IS security awareness to APT is scant in the academic domain. A title search using the words, 'Advanced Persistent Threats', 'APT' and 'security awareness' was conducted in the Association of Information Systems (AIS) journals database (www.ais.com) and Google Scholar spanning the years 2008 to 2013. While a search in AIS eLibrary (provided with ten AIS journals and two conferences) yielded only four papers, a similar search on Google Scholars returned six papers focussing on APT. Three out of the four AIS published articles looked at the linkage between online social networking and APT. Molok, Chang, & Ahmad (2010) identified online social networking as the most challenging channel of information leakage and an attack vector of APT and, recommended security education, training and awareness for organisations to combat this threat. Molok, Ahmed & Chang (2011), further investigated the way online social networking leads to information leakage and the strategies utilized by organizations to control such a threat. The cultural change of employees' online social network behaviour in APT attacks was also researched by Molok (2011). While the above papers covered the social networking

aspect of APT threat, Ooi, Kim, Wang, & Hui (2012) investigated the behaviours of hackers using a longitudinal dataset of defacement attacks

Six papers related to APT and security were generated from Google scholar search. Daly (2009) explained APT attack methods and suggested techniques to combat this threat, while Binde, McRee, & O'Connor (2011) provide signature based methodology, manual analytical practices, statistical tactics, correlation concepts, as well as automatic leak prevention as countermeasure approaches to APT. Some of the other issues addressed include the role of APT in political espionage {Li, 2011 #570} predicting the organizations and individuals that might be the target of APT attacks (Lee & Lewis, 2011a), and an analysis of APT attacks to develop a roadmap of detecting and managing these threats (de Vries, van den Berg, Warnier, & Hoogstraaten, 2012).

While past studies shed light on APT vulnerabilities like social networking, and technical combat measures, an in depth study into the different dimensions of vulnerabilities existing in an organization along with technical as well as non-technical preventive measures have not been researched. Hence, there is a need to understand the awareness of computer users regarding APT threats and the corresponding security measures which will certainly aid in understanding and formulating measures to manage APT threats.

Advanced Persistent Threat (APT) is a term used for a new breed of insidious threats that use multiple attack techniques and vectors and that are conducted by stealth to avoid detection so that hackers can retain control over target systems unnoticed for long periods of time (Tankard, 2011). APT gained prominence during the first half of 2011 through a number of high profile and persistent IS security breaches in organizations namely Sony, the data-security firm RSA, Lockheed Martin, the email wholesaler Epsilon, the Fox broadcast network, NASA, PBS, the European Space Agency, the FBI, the British and French treasuries, the banking and insurance giant Citigroup, along with dozens of other companies and government agencies (Liebowitz, 2011). Cybercrime is big business, and according to the written testimony to the US Senate by the Chief Security Officer, Mr. Edward Amoroso of AT & T, cybercrime revenues are worth US $ 1 trillion (Unknown, 2009). While it is difficult to verify this figure and critics have given much lower estimates on this, recent statistics on IT security breaches point out the fact that networks are witnessing more frequent and sophisticated targeted attacks.

The central objective of any security system is the ability to prevent undesired access, while still allowing authorized access to information (Post & Kievit, 1991) but with cyber incidents growing in intensity and severity (Kjaerland, 2006) the risks related to information security have become a major challenge and a top management priority for many organizations (Bulgurcu, Cavusoglu, & Benbasat, 2010). Thus, despite the critical role and relevance of information and information security in an organization, unauthorized breaches into organizational internal and the extended networks occur with greater frequency and severity (Kjaerland, 2006; Straub & Welke, 1998 ; Whitman, 2004; Yadav, 2010).

The paper is structured as follows. The following section defines APT along with its process and the role of employees. Section two analyzes a few of the high profile cases to highlight the role of end users in APT, the attack methodology and the potential targets of such

attacks. The third section analyses the role of people and security culture in mitigating the attacks while the fourth section provides a summary of the research method and description of the data analysis. The final section analyzes the survey results to extract the factors that eventually lead to APT vulnerability along with the recommendations.

1. PHISHING, SPEAR PHISHING AND APT

In an APT attack, the victim/s is/are lured to either download a harmless file attachment or to click a link to a malware or an exploit-laden site through an email. When the user downloads the file, which is a vulnerability exploit, it installs a malware in a compromised computer which then opens a backdoor and access the hackers control server. It has been stated that the term "Advanced Persistent Threat" was first coined by the US Air Force, in 2006, to describe complex cyber-attacks against specific targets over long periods of time (Websense, 2011). APT has been described as a well-funded and well-organized espionage that are financially motivated, employs social engineering techniques and stealthier zero-day exploits to breach networks that are rarely detected by preventive security systems with aims to establish long-term occupying force inside an organization's perimeter (Molok, Chang, & Ahmad, 2010). It can also be spread through SQL injection and the attack process (see figure – 1) can consists of four stages namely incursion, discovery capture and exfiltration (Symantec, 2011) or five stages namely system exploitation, downloading malware, malware call back, data exfiltration and lateral spreading of malware {FireEye, 2013 #6@@author-year}(see figure – 2). According to NIST, APT is defined as an "adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors of APT (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives(ISACA, 2013).

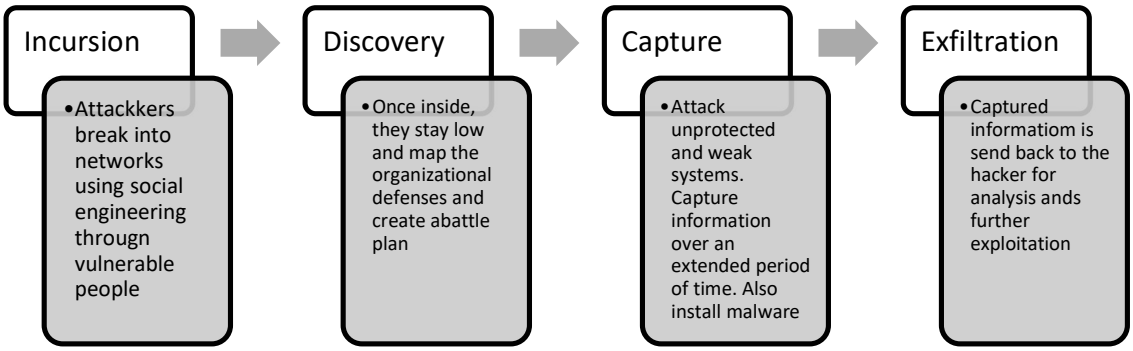

Figure – 1 APT Attack Process (Symantec, 2011)

The APT is one of the most difficult challenges faced by the anti-virus community (Lee & Lewis, 2011b). Since, the concept of APT originated from 'phishing' these and similar type of attacks comes under the umbrella of 'phishing.' Phishing has been described as an attempt to gain personal or financial information from an individual by posing as a legitimate entity

propagated through spam, whereas 'spear phishing' applies to a highly targeted phishing attack targeting a small group or even one specific person (Whitman & Mattord, 2012). In a typical phishing attack, a user receives an email with an embedded URL. On clicking the URL, the phony website will be used to harvest secret information to perform fraudulent transactions in that user's name{Wang, 2009 #604} . Because these phishing emails look so official, up to 20% of unsuspecting recipient's respond to them {Alex Kosachev, 2009 #605}.

Figure – 2 APT Attack Process (FireEye, 2013)

Targeted phishing attack leads to customers' personal information being sold to criminals, used for identity theft which leads to lawsuits, damages, loss of customers, and negative publicity (Moore, 2010). APT is a form of spear phishing attack, where the attacks are targeted at individual employees rather than the organizational security defenses, where one simple flaw or overlook of the employee is all needed for an entry inside these defenses. When it comes to APTs it is not about how safe, secure and good the company is, but a totally new approach for entering the organization is selected where the attacker don't bother to hack the organization and its infrastructure, rather focus on hacking the employees (Nicho, 2012).

Role of End Users in APT{Wang, 2009 #604}

Although firms are expending substantial resources to develop technology and processes for the protection of IS resources, currently firms are focusing their attention on the role people play in maintaining a safe computing environment (Anderson & Agarwal, 2010). Information security has not only become a critical issue for IS executives (Culnan, Foxman, & Ray, 2008) but also crucial to the continuous wellbeing of modern organizations (Kruger & Kearney, 2008). Subsequently, security and privacy of information systems has remained as one of the top ten key issues for IS executives since 2003 (Luftman & Ben-Zvi, 2011). Hence, organizations need to protect information assets against cyber-crime, denial-of-service attacks, web hackers, data breaches, identity and credit card theft, and fraud (Smith, Winchester, & Bunker, 2010). It is an accepted fact that a firm's information related assets are now among its most valuable assets (Gordon, Loeb, & Sohail, 2010) and being a fundamental asset within any organization, the protection of this asset, through the process of information security, is of equal importance (Thomson & Solms, 2005). Even though the application of existing technical IS security frameworks and IS controls have been effective in preventing attacks from external entities into the organizational networks, novel type of attacks using APT have diverted the attention of organizations from perimeter defenses to their own staff who happen to be "the weakest link" in information systems (IS) security management in the workplace (Guo, Yuan, Archer, & Connelly, 2011; Paans & Herschberg, 1987). Thus the involvement of humans in information security is equally important and many examples exist where human activity can be linked to

security issues (Kruger & Kearney, 2008). As noted by (Schultz, 2005), information security is primarily a people problem and technology is designed and managed by people, leaving opportunities for human error. Thus, this section highlights the vital role played by users in view of the APT attacks.

2. APT – TRENDS AND ANALYSIS OF CASES

Trends in APT Attacks

According to statistics revealed by Symantec overall in 2011, 1 in 238.8 emails were identified as malicious, but approximately one in 8,300 of those were highly targeted. Likewise, 28.3% of all targeted attacks are targeted at small to medium-sized companies, and 48.9 % of targeted attacks are targeted at large companies where the basis of target is not the size but factors influencing the attack include organizations with high intellectual property or customer data and the "footprint" of the company on the internet. And despite the commonly held belief of small businesses that they would never be the victims of a targeted attack, 17.8% of all targeted attacks are directed at small businesses with up to 250 employees (Symantec, 2011). Also, while government and defensive industries are more likely to see APT attacks, industries like oil and energy, healthcare, agriculture, construction, mainly see attacks that are highly targeted at a small number of companies and individuals within them (Encode, 2012; FireEye, 2013).

According to a report by FireEye (2013), comparing the first six months of 2011 to the first six months of 2012, there has been a dramatic increase of 392% infections per company. This increase is not only in terms of volume but also in its effectiveness in bypassing traditional security infrastructure and infecting targeting systems, which is a feature of APT attacks. On average, organizations are experiencing a staggering 643 web-based malicious events each week. Email is the primary channel through which the attacks are initiated. During 2012, there was a 56% increase in the amount of email based attacks that successfully penetrated organizations' traditional security mechanisms where malicious malware is delivered through the emails either as attachments or as links.

ISACA conducted a global survey of 1551 respondents (mostly among its ISACA members who are working in the information technology governance, audit and security domain) in more than 20 sectors on APT threat awareness, where even if only 21.6 % of respondents reported to have been victimized by an APT and 63.0 % believe that it is only a matter of time before their enterprise is targeted. Regarding defensive mechanisms, nearly 60 percent of respondents believe that they are ready to respond to APT attacks (ISACA, 2013).

Traditionally targeting only defense establishment, APTs are now targeting enterprises in a wide range of industries, where attackers are moving beyond custodial data like credit cards to pursuing high-value digital assets such as intellectual property, access to mission-critical operations, and other proprietary data and systems (RSA, 2011). According to Trend Micro (2012) report on APT, the most top spear-phishing email attachment file types are .rtf followed by .xls and .zip (see figure – 3).

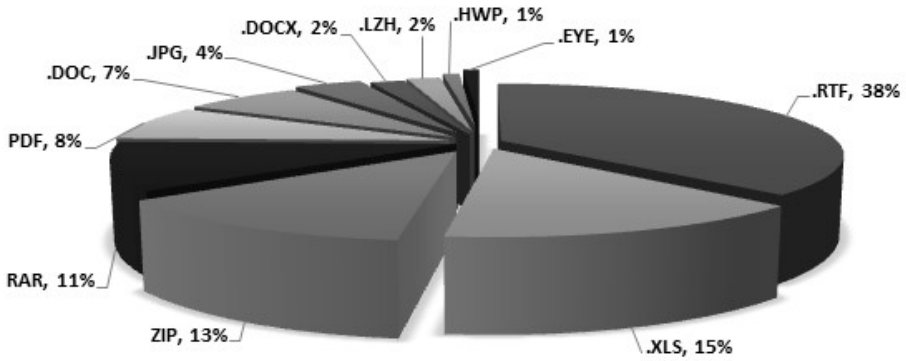

Figure – 3 Files types that are carriers of APT exploits (TrendMicro, 2012)

Cases of APT Attacks

One of the sensational APT attack happened at RSA, a division of EMC Corp that provides security, risk, and compliance solutions for more than 90% of Fortune 500 companies for managing their security. On March 17th 2011 the company disclosed to the Securities and Exchange Commission that a data breach has occurred. The attackers used a common form of phishing called spear phishing. In this type of attack, the attacker sent two different phishing emails over a two-day period. The two emails were sent to two small groups of lower level employees with the email subject "2011 Recruitment Plan." The email went to the junk folder but one employee retrieved it from their Junk mail folder, and opened the attached excel file. It was a spreadsheet titled "2011 Recruitment plan.xls". The spreadsheet contained a zero-day exploit that installs a backdoor through an Adobe Flash vulnerability (CVE-2011-0609). The attacker then proceeded to install a remote administration tool that allows the attacker to control the machine. The tool used for this was a variant of Poison Ivy set in reverse-connect mode that makes it more difficult to detect where the victim machine reaches out and connect to the command and control rather than the other way around where the attacker machine connect to the victim machine. Then, the attacker started digital shoulder surfing to establish the employee's role and their level of access, escalated the user privilege where they could discover valuable data sources and extract them to external rouge servers. In this case sensitive information from more than 40 million employees may have been compromised. The estimated cost to the company by various sources is $ 66 million in direct and attributable costs (Rivner, 2011).

In 2011, Sony announced that the company's PlayStation network servers had been hacked, exposing the records of more than 70 million customers, along with 25 million customer records of its Online Entertainment network. Security experts are describing the assault has the characteristic of APT carried out over several months that exploited multiple vulnerabilities to ultimately gain access to the most sensitive areas of Sony's networks (Headlines, 2011). Likewise the breach of Epsilon, the world's largest email service provider, involve the details of customers of at least 50 major companies where the attackers used fake personalized emails to

trick people into disclosing personal information, including passwords and financial details (Schwartz, 2011).

The trends in APT reveal that the security awareness of employees especially in knowing the APT vulnerabilities is a major factor in preventing these types of threats as APT vulnerability lies in the unintentional mistake of employees in an organization. Thus it is widely believed that organizational efforts to manage IT security risks traditionally focus on vulnerabilities in technical assets at the expense of people, processes, and culture (Spears & Barki, 2010).

3. IS SECURITY CULTURE

User participation in IS security risk management is valuable for two reasons namely user awareness of the risks to IS security is widely believed to be fundamental to effective IS security and secondly security controls need to be aligned with business objectives to be effective (Spears & Barki, 2010). In this respect, it is believed that an information security-awareness culture will minimize risks to information assets and specifically reduce the risk of employee misbehavior and harmful interaction with information assets (Veiga & Eloff, 2010). Information security awareness and training fosters awareness which in turn create a IS security culture within the organization. *Culture*; from a corporate perspective have been defined as a blend of the corporate values, beliefs, symbols, and rituals that companies develop over time. In this context, an information security culture is therefore based on the interaction of employees with information assets and the security behavior they exhibit within the context of the organizational culture in the organization (Veiga & Eloff, 2010). To evaluate the need for a IS security culture it is imperative to answer the question "Why do organizations need a IS security culture?" A culture is a unifying mechanism that makes all concerned to act in a unified manner. A uniform IS security culture not only enforces uniform behavior in terms of enforcing IS security procedures and polices but also creates IS security awareness among IS and non IS employees alike. According to (OECD, 2002) there are nine principles for an IS security culture namely awareness, responsibility, response, participants, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment. It has been stated that an appropriate security culture can be maintained by a good awareness-program (Schlienger & Teufel, 2003). Thus, achievement of a secure environment of IT assets is largely dependent on the organization's security awareness, protection, monitoring, investigative, assurance and survivability plans afforded to its valued assets (Onwubiko & Lenaghan, 2009).

In the light of the analysis from section one, two and three we look at APT causes and mitigation from a people, technology, and IT control perspective. This directs us to the research question – ***What are the vulnerabilities of APT attacks in the organizations?*** The research questions further focus on the nature of APT attacks, the vulnerabilities, awareness and training of users, and preventive measures.

4. RESEARCH METHODOLOGY

The nature of the research question leads us to an exploratory study using qualitative methods. Qualitative method of data collection was planned due to the depth and nature of qualitative data that is to be collected from the respondents. Moreover, qualitative research is more concerned

with understanding the social phenomenon from the actors' perspectives through participation in the life of those actors, while quantitative research seeks to explain the causes of changes in social facts, primarily through objective measurement and quantitative analysis (Firestone, 1987). The case study research approach is chosen since it "is a common way to do qualitative enquiry" (Stake, 2003, p. 443) and "investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin, 1994 p. 13). For this effect, it was decided to interview IT managers who have experienced different forms of phishing attacks (successful or unsuccessful) in their organisation and elicit the responses. The responses were digitally recorded, verbatim transcribed, imported into NVIVO, and coded into defined and emergent themes. The questions for the interview were based, on the definition of APT (section one), the methodology of APT attack (section one and two), the vulnerability of the employees and the role of technical as well as non-technical controls (section one, two and three).

5. DATA ANALYSIS AND DISCUSSION

Data Collection

Three respondents from three organizations, who directly manage the information securty have been selected for the interview. Out of the three organization, one is a media company, one company is in the oil and natural gas sector and the third company is in the aviation sector. The five criteria which were used to select the respondents were the organizational size, the number of years of experience of the respondents in the industry, working in the IT department with a role in security, relevant certifications certifications in information security governance domain, and have experienced any attempts of the known methods of APT (phishing).

Position	Industry	No. of computers	Professional profile	Turnover
IT Manager (23 years in IT)	Media	70 servers (systems not specified)	CGEIT Certified, ISO 27000, ISO 20000 & ISO22301 Certified Lead Auditor, ITIL Expert, IT Governance Certified, COBIT 4.1, Cloud Computing Associate, TOGAF 9.1 Professional, Dubai Government Excellency Program Certified Auditor, Certified Ethical Hacker, Microsoft Certified Technology Specialist, ITIL Service Manager V2 Certified, CCNA, MCSE, MCDST	Not available
Manager - IS Audit and Security (15 years in IT)	Aviation	Not specified	CISM, CISA, CISSP, CEH, CGEIT, CRISC, ISA	>US $ 1 billion
IT Manager - Planning and Performance (29 years in IT)	Oil and gas	5 Mainframes. 220 servers, 650 Network Devices	CISM, CGEIT, CRISC, PMP	>US $ 1 billion

The interviews were transcribed and imported to NVIVO 10, a qualitative analysis software where the analysis was conducted based on the guideline of Whittaker (2006) where (1) the data (especially the interview data) was coded, (2) the transcribed text was systematically examined to identify key concepts, (3) grouped into similar categories, and (4) searched for relationships between a category and all its concepts and between different categories. We also use the quantitative method of weighing the frequency of a repeated theme, as according to Leech and Onwuegbuzie (2007), qualitative researchers can use quantitative method of counting the number of words, which not only improve the rigor of an analysis but also also prevents the researcher from overweighting or underweighting the emergent themes. Counting words also prevents the researcher from overweighting or underweighting the emergent themes. Regarding the fourth type of analysis, we limit the relationship to only a few overlapping sub-themes and wherever a relationship is evident. Regarding vulnerabilities, one introductory and two major themes that had emerged are the different perspectives of APT, the technical and non-technical vulnerabilities. The three major themes and the subsequent sub themes are illustrated in figure 3. Since the objective of the paper was to indentify the vulnerabilities, we have not gone into the preventive mechanisms. Even though it was not asked, the respondents inadvertently gave tips on APT mitigation.

Perspectives of APT

Respondents have defined APT as 'advanced' which means that the vendors are not able to catch up with the technical advancement of the perpetrators; 'persistent' which has been explained as the different and continuous attempt of a mix of social engineering and technical skills to bypass the organizational defenses; and 'threat' which was explained as the magnitude of threat facing organizations and individuals alike from APT. One respondent have outlined APT as the fifth stage in the IS threat scenario (virus → worm → polymorphic → blended → APT). This threat perspective of APT has been characterized as one with no solution but only mitigation. Since the magnitude of threat stems from the concept of 'Zero day virus', respondents describe it as an efficiently run business with quality assurance and where highly skilled people work to create 'zero days'.

APT has been likened to cloud computing by one respondent when he stated that like cloud computing which existed for a long time, APT is not new, but an old concept which gained momentum and importance due to the spate of high profile attacks that happenned in the last three to four years where "the only difference is that the knowledge about APT has started growing". This was contradicted by another respondent who stated that "APT is still a jargon" and not defined clearly.

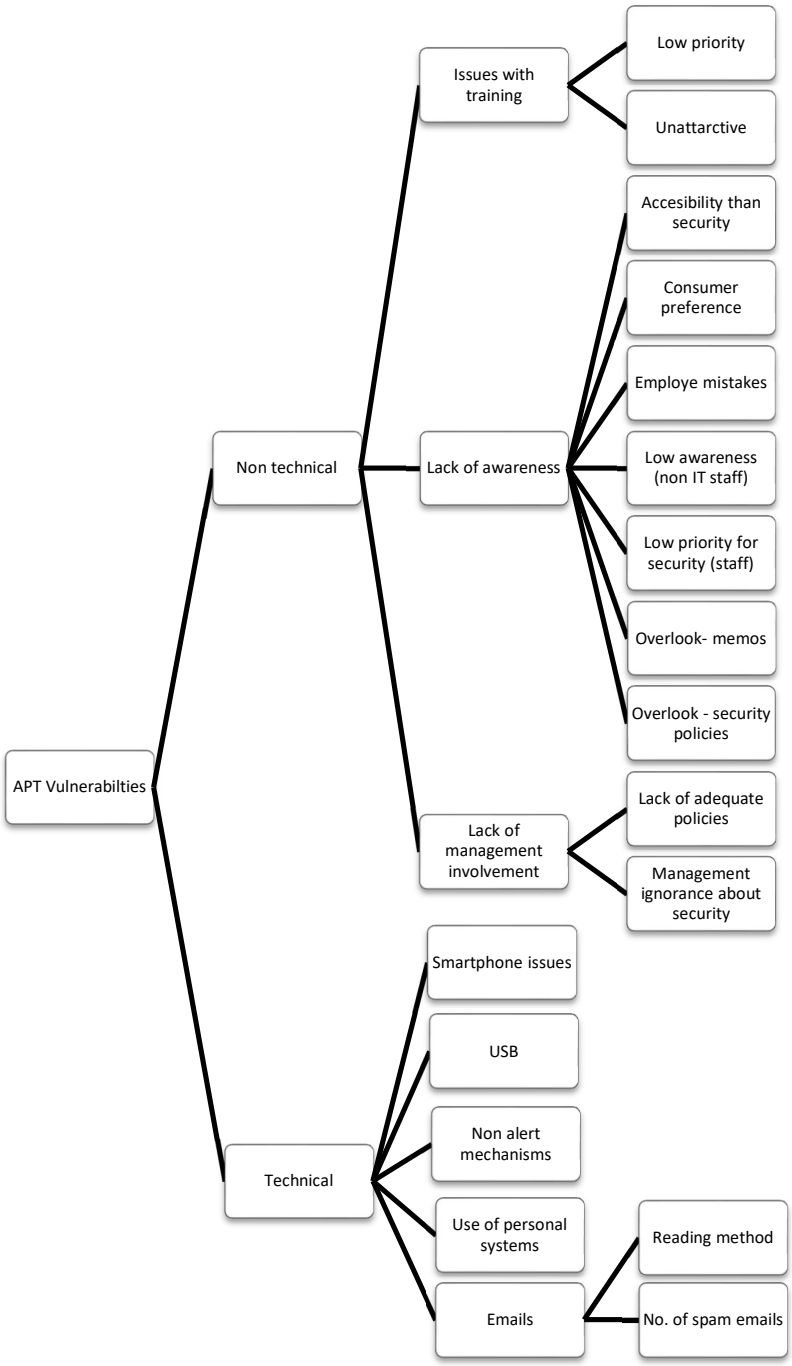

Figure – 3 APT Vulnerabilities

Non Technical Vulnerabilities

This was described to be the most critical to the organisation in terms of vulnerability where numerous factors were cited. Three major themes that characterize non technical persepctive are the issues with training, the lack of awarness among technical as well as non technical employees and the lack of management involvement:

Issues with training

Two issues that have been cited by the respondents are the low priority given to training by the management and staff; and the nature of training that makes it unattractive to the system users in an organization. According to one respondent some employees don't care about the training given to them as they don't find it attractive. In this case the respondents agreed that the normal methods of training (class room training) are not efffective. In one organisation, traning is done by external consultants and done in batches so as not to disrupt the normal working environment.

Lack of awareness

This theme occupied most of the conversation with the three respondents and as such is regarded as the most critical concern in APT attacks. Regarding the sub theme 'accessibility than security' one respondent stated that when it comes to accessing a device or information with ease or going through the stages of security screening most of the staff would prefer accessibility and this jeopardize security. When asked about what he will do in this case of an urgent report to be submitted to the management, he said that he is willing to sacrifice security for accessibility and thus this sub theme is contextual in nature. Secondly, consumerism plays a vital role and it was explained as the preference of consumers to go for faster, high-end devices marketed by companies and almost disregarding the security aspect of the device. Here people go for high-end smartphones and use these to access the company emails and store company data and in most cases use common Wi-Fi, where most of these devices don't incorporate the defenses of the company security system. This was described as a smooth entry point for APT attacks. Thirdly, employees' unintentional mistake can cause APT vulnerabilities. To illustrate this he gave an incident in an organization he knows in UAE, where a fake email with a fake payload was sent to all employees which a prior communication about the email, but to the dismay of the white box testing team, most of the employees opened the fake email and downloaded the contents. This can be due to the other sub themes listed namely the low awareness level of APT threats among the non-IT staff, and low priority given for security, the overlooking of IT security communications, and the occasional overlooking of security policies. Regarding the last sub theme one respondent stated that "having the employees sign on the security policy doesn't mean that they read it" stating that employees are normally given the security policies only when they join and most of the newly hired staff sign it without reading it. Since lack of awareness is a major theme, from the analysis of the sub themes a cause and effect relationship was evident between employee mistakes and related four themes which is illustrated in figure – 4.

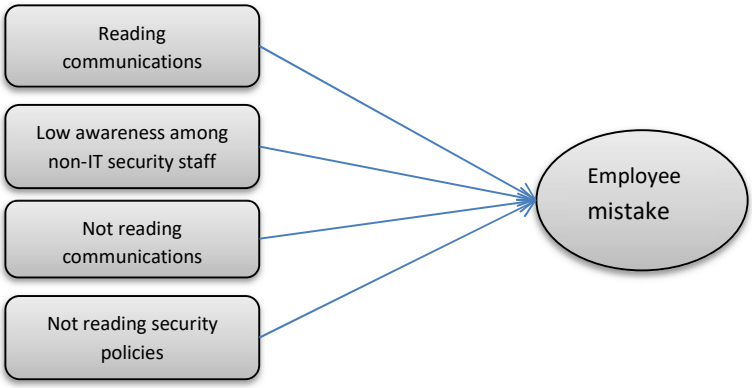

Figure – 4 Reasons for employee mistakes

Lack of management involvement

The first sub theme under 'management' that was put forward by the respondents is the lack of appropriate and adequate policies. In this regard, one respondent stated that the policies are more tuned to satisfy the certification of standards. Respondents are unanimous in the statement that the management's view of IS security is through the return on investment (ROI) concept which is not that easy to justify in terms of tangible benefits, which leads to poor security implementation in terms of technical as well as non-technical controls, processes and procedures. One respondent stated that they "do not understand or appreciate investment on security, and so there is this challenge."

Technical Vulnerabilities

While non-technical vulnerabilities occupied most of the discussion time of the three respondents (with less avenues for prevention), technical vulnerabilities have been highlighted as an area that can be mitigated through commercially available tools with less lead time. The five sub themes that have emerged are the method of using emails by the employees, lack of an alert mechanism, use of USB devices, smartphones and personal systems at work.

Emails

The method of opening, viewing and reading emails has been cited as the major concern for IT security managers trying to close the vulnerability gap. The method of reading emails in an organisation was described by one respondent as a major concern where two factors have been described namely the workload and deadlines which makes the employee overlook the spams for genuine email and the number of spams in the mailbox. Two respondents unanimously stated that in any organisation 80% to 85% of the emails being spam, the employee's attention to the finer details of the email tend to be overlooked with the results that they may download a malicious attachment and/or click a malicious link. In all of the two situations, all three respondents agreed that effective spam filtering mechanisms can mitigate this to a certain extend.

USB

The misuse of USB devices have been cited as a major concern for the spread of APT attacks by all the three respondents. One respondent gave a scenario that the probability of an employee plugging a lost and found USB inside the company premises to either identify the user based on the media properties, or to see the contents inside is far greater than an employee who will take it to the IT security manager for scrutiny. In this case he emphasized the role of awareness and training.

Non alert mechanisms

This is a vulnerability that happens at the discovery stage of the APT stage (figure – 1). In this respect two respondents stated that organisations need an alert mechanism that should alert the concerned manager if an attempt of privilege escalation occurs. One of the respondent cited two high profile APT attack cases that happened in 2011 and 2013 where this mechanism was not present, of which the latter case was in the financial sector incurring a loss of millions of dollars in a well-co-ordinated APT attack.

Use of personal systems

Regarding the use of personal systems like laptops and personal computers one respondent stated that if given the choice he would trust the company systems more than his own systems because "we know we have good consultants who are monitoring everything and they understand if there is something wrong". According to him use of portable personal computers is a high risk domain that can create a vulnerability to company systems if connected to the company network. The main concern he pointed out is the multiple users that use the personal system at the employee's home coupled with the almost non-existence of monitoring mechanism.

Smartphone issues

Even though this theme partially overlaps with the non-technical issue (lack of awareness), the perception is from a technical point of view. One respondent is of the opinion that smartphones is a "very difficult animal that does not follow the normal trend of activity" while the other respondent stated that the applications that are downloaded and installed like games can be spam vectors. When the researcher queried how any programs installed through the proper method (ex. Googleplay) could be malicious, he responded back by stating "nobody can be sure about the authenticity of the games"? With the increasing number of usage of smartphones two respondents stated that the probability of APT vulnerabilities is likely to rise in the future.

6. CONCLUSION, LIMITATIONS AND FUTURE DIRECTIONS

This paper has given an account of and the reasons for APT attacks. From the empirical research, there is no doubt that the combined technical and non-technical factors contribute to APT vulnerabilities which is a key problem faced by managers in the IS security domain. The findings from this study make several contributions to the current literature. Since, previous research in this domain is scant, this study has defined APT from different perspectives, categorized the vulnerabilities into meaningful domains and gave specific instances of the vulnerabilities in an

organisation from a practitioner's point of view. This serves a guideline for IS mangers to consider multiple factors that need to be taken into account while managing IS security in an organisation.

The study is not without its limitations as a number of caveats need to be noted regarding the present study. First of all with a small sample of three respondents, a comprehensive list of vulnerabilities may not be evident. Secondly, as stated in the literature review section, security culture plays an important part in the exposure or closing of vulnerabilities. In these two instances, extension of this study in different countries with a more sizeable sample may provide a richer repository of data. While this study has not differentiated the sectors nor the managers' positions, it would be promising to replicate this study with two or three dimension namely sectors of the industry, context (cultures, countries), and managers position as the perception of APT vulnerabilities as security mangers may look at APT from a different lens than an IT Governance or IT service manager.

7. REFERENCES

Anderson, C., & Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *Mis Quarterly, 34*(3), 613-643.

Binde, B. E., McRee, R., & O'Connor, T. J. (2011). Assessing outbound traffic to uncover advanced persistent threat *Joint Written Project*: SANS Technology Institute.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *Mis Quarterly, 34*(3), 523-548.

Culnan, M. J., Foxman, E. R., & Ray, A. W. (2008). Why IT Executives Should Help Employees Secure Their Home Computers. *MIS Quarterly Executive, 7*(1), 49056.

Daly, M. K. (2009). *Advanced Persistent Threat*. Paper presented at the 23 Large Installation System Administration Conference, Baltimore, MD.

de Vries, J., van den Berg, J., Warnier, M., & Hoogstraaten, H. (2012). An analysis framework to aid in designing advanced persistent threat detection systems.

Encode. (2012). Demystifying Advanced Persistent Threats (APTs) ENCODE Extrusion Testing Facts & Statistics. Retrieved May, 2013, from http://www.encodegroup.com/solutions.aspx?page=APT

FireEye. (2013). Less Secure Than You Think. Retrieved May, 2013, from http://www2.fireeye.com/cso-less-secure-than-you-think.html

Firestone, W. A. (1987). Meaning in Method: The Rhetoric of Quantitative and Qualitative Research. *Educational researcher, 16*(7), 16-21.

Frankie, L. (2011). *Evidence of Advanced Persistent Threat: A case study of malware for political espionage*.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly Executive, 34*(3), 567-594.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems, 28*(2), 203-236.

Headlines. (2011). Hacker Offers Insight on Sony PSN Breach. Retrieved May, 2013, from http://www.infosecisland.com/blogview/13864-Hacker-Offers-Insight-On-Sony-PSN-Breach.html

ISACA. (2013). Advanced Persistent Threat Awareness. Retrieved May, 2013, from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Advanced-Persistent-Threats-Awareness-Study-Results.aspx

Kjaerland, M. (2006). A Taxonomy and Comparison of Ccomputer Security Incidents from the Commercial and Government Sectors. *Computer & Security, 25*, 522 – 538.

Kruger, H. A., & Kearney, W. D. (2008). Consensus Ranking – An ICT Security Awareness Case Study. *Computers & Security, 27*, 254-259.

Lee, M., & Lewis, D. (2011a). *Clustering disparate attacks: mapping the activities of the advanced persistent threat.* Paper presented at the 21st Virus Bulletin International Conference, Barcelona, Spain.

Lee, M., & Lewis, D. (2011b). *Clustering Disparate Attacks: Mapping the Activities of the Advanced Persistent Threat* Paper presented at the Virus Bulletin Conference October 2011, Barcelona.

Liebowitz, M. (2011). 2011 Set to Be Worst Year Ever for Security Breaches. *SecurityNews*. http://www.securitynewsdaily.com/2011-worst-year-ever-security-breaches-0857/

Luftman, J., & Ben-Zvi, T. (2011). Key Issues for IT Executives 2011: Cautious Optimism in Uncertain Economic Times. *MIS Quarterly Executive, 10*(4), 203 - 212.

Molok, N. N. A. (2011). *Disclosure of Organizational Information by Employees on Facebook: Looking at the Potential for Information Security Risks.* Paper presented at the Australasian Conference on Information Systems (ACIS), Sydney, Australia.

Molok, N. N. A., Ahmad, A., & Chang, S. (2011). *Exploring the Use of Online Social Networking By Employees: Looking at the Potential for Information Leakage* Paper presented at the 15th Pacific Asia Conference on Information Systems (PACIS 2011) Brisbane.

Molok, N. N. A., Chang, S., & Ahmad, A. (2010). *Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats.* Paper presented at the Proceedings of the 8th Australian Information Security Management Conference.

Moore, J. W. (2010). From Phishing To Advanced Persistent Threats: The Application Of Cybercrime Risk To The Enterprise Risk Management Model. *Review of Business Information Systems, 14*(4), 27-36.

Nicho, M. (2012). An Information Governance Model for Information Security Management. In D. Mellado, L. E. Sánchez, E. Fernández-Medina & M. Piattini (Eds.), *IT Security Governance Innovations: Theory and Research*: IGI Global.

OECD. (2002). *OECD Guidelines for the Security of Information Systems and Networks* (Vol. OECD). Massachussets.

Onwubiko, C., & Lenaghan, A. P. (2009). Challenges and Complexities of Managing Information Security. *International Journal of Electronic Security and Digital Forensics, 2*(3), 306-321.

Ooi, K. W., Kim, S. H., Wang, Q.-H., & Hui, K. L. (2012). *Do Hackers Seek Variety? An Empirical Analysis Of Website Defacements.* Paper presented at the Thirty Third International Conference on Information Systems, Orlando.

Paans, I. R., & Herschberg, I. S. (1987). Computer Security: The Long Road Ahead. *Computers & Security, 6*, 403-416.

Post, G. V., & Kievit, K.-A. (1991). Accessibility vs. Security: A Look at the Demand for Computer Security. *Computers & Security*(10), 331-344.
Rivner, U. (2011). Anatomy of an Attack Retrieved September, 2011, from http://blogs.rsa.com/rivner/anatomy-of-an-attack/
RSA. (2011). When Advanced Persistent Threats Go Mainstream. Retrieved May, 2013, from http://www.rsa.com/innovation/docs/sbic_rpt_0711.pdf
Schlienger, T., & Teufel, S. (2003). Information Security Culture – From Analysis to Change. *Information Security South Africa*.
Schultz, E. (2005). The Human Factor in Security. *Computer & Security, 24*, 425-426.
Schwartz, M. J. (2011). Epsilon Fell To Spear-Phishing Attack. *InformationWeek Security*. http://www.informationweek.com/security/attacks/epsilon-fell-to-spear-phishing-attack/229401372
Smith, S., Winchester, D., & Bunker, D. (2010). Circuits of Power: A Study of Mandated Compliance to An Information Systems Security De Jure Standard inaA Government Organization. *MIS Quarterly Executive, 34*(3), 463-486.
Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *Mis Quarterly, 34*(3), 503-522.
Stake, R. E. (2003). Qualitative Case Studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage Handbook of Qualitative Research* (pp. 443). California: Sage Publications.
Straub, D., & Welke, R. (1998). Coping with Systems Risk: Security Planning Models for Management Decision-Making :Working paper version. *Mis Quarterly, 22*(4), 441-469.
Symantec. (2011). Advanced Persistent Threats: A Symantec Perspective. Retrieved May, 2013, from http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf
Tankard, C. (2011). Persistent Threats and How to Monitor and Deter Them. *Network Security*(August), 16-19.
Thomson, K.-L., & Solms, R. V. (2005). Information Security Obedience: A Definition. *Computers and Security, 24*(69-75).
TrendMicro. (2012). Spear-Phishing Email: Most Favored APT Attack Bait 2013, from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf
Unknown. (2009). Cyber-crime Revenues Exceed $1 Trillion Annually. Retrieved November, 2012, from http://www.govtech.com/security/Cyber-crime-Revenues-Exceed-1-Trillion-Annually.html
Veiga, A. D., & Eloff, J. H. P. (2010). A Framework and Assessment Instrument for Information Security Culture. *Computers & Security, 29*, 196-207.
Websense. (2011). Advanced Persistent Threats and Other Advanced Attacks. Retrieved March, 2013, from http://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf
Whitman, M. E. (2004). In Defense of the Realm: Understanding the Threats to Information Security. *International Journal of Information Management 24*, 43-57.
Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security*. United States: Cengage Technology.
Yadav, S. B. (2010). A Six-View Perspective Framework for System Ssecurity: Issues, Risks, and Requirements. *International Journal of Information Security and Privacy, 4*(1), 61-92.

Yin, R. K. (1994). *Case Study Research: Design and Methods* (2nd ed.). Thousand Oaks: Sage Publications, Inc.