

Journal of International Technology and Information Management

Volume 26 | Issue 1

Article 7


1-1-2017

Cyber Security, Threat Intelligence: Defending the Digital Platform

Emmnauel U. Opara Dr
Emmanuel Uzoma Opara, euopara@pvamu.edu

Mohammed T. Hussein Dr
Prairie View A&M University Prairie View TX

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/jitim>

 Part of the [Business Intelligence Commons](#), [Communication Technology and New Media Commons](#), [Computer and Systems Architecture Commons](#), [Data Storage Systems Commons](#), [Digital Communications and Networking Commons](#), [E-Commerce Commons](#), [Information Literacy Commons](#), [Management Information Systems Commons](#), [Management Sciences and Quantitative Methods Commons](#), [Operational Research Commons](#), [Science and Technology Studies Commons](#), [Social Media Commons](#), and the [Technology and Innovation Commons](#)

Recommended Citation

Opara, Emmnauel U. Dr and Hussein, Mohammed T. Dr (2017) "Cyber Security, Threat Intelligence: Defending the Digital Platform," *Journal of International Technology and Information Management*. Vol. 26 : Iss. 1 , Article 7.

Available at: <https://scholarworks.lib.csusb.edu/jitim/vol26/iss1/7>

This Article is brought to you for free and open access by CSUSB ScholarWorks. It has been accepted for inclusion in *Journal of International Technology and Information Management* by an authorized editor of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.

Cyber Security, Threat Intelligence: Defending the Digital Platform

Emmanuel U Opara

(Corresponding author: Emmanuel U Opara)

**College of Business,
Prairie View A&M University,
Prairie View - Texas U.S.A.¹
(Email: euopara@pvamu.edu)**

Mohammed T. Hussein

**College of Business,
Prairie View A&M University,
Prairie View - Texas U.S.A
(Email: mthussein@pvamu.edu)**

ABSTRACT

Network breaches are happening at a phenomenal scale. The unabated exponential level is forcing enterprise systems to scramble for solutions since the world is so interconnected and digitized and the internet knows no boundaries. Due to big data explosion, the platform for attackers to work continues to grow. Most breached entities are not aware that they have been compromised for weeks but finds out after an external audit or a third party notifies the organizations. Since most networks will be breached at some point, it is proper to note that legacy platforms will no longer stand a chance to defend against the signature-less attacks. This study will create threat awareness, find out capabilities of threat actors, their motivations and objectives and identify best practices.

KEYWORDS: Breaches, Exploits, Network Security, Threats, Vulnerabilities.

INTRODUCTION

Enterprise systems have high value information that are valuable and vital to its existence and survival. The battleground is defined. In today's networked inter-connectivity, more than 500,000 new malware variants surface on a regular basis. Most of these are polymorphic malware and are cryptic to bypass latest detection tools in the market [Gallagher, 2014; Weimer, 2014]

As cyber exploitations become more sophisticated, cyber espionage become the “digital gold” for hackers. Breaches exact expensive toll on victims, in terms of money and time. These costs often do not appear as line items on enterprise financial statements. The reason could be that the costs are often indirect, resulting in wasted resources and missed opportunities. The average data breach cost U.S. organizations approximately \$6.5 million [4]. This estimates cost include but not limited to costs incurred in detecting, responding and mitigating to a breach. Time lost is a concern as organizations analyze attacks coming from malicious insiders, malicious codes, and web-based attacks, denial of service, stolen devices, phishing, social engineering, malware, botnets, virus, worms and Trojans [Clover 2014; Greenburg 2014].

Breaches in 2015, witnessed a growing number of disruptive attacks from foreign actors. Some of these attacks came from Crypto Locker who hold data for ransom and threaten to release, delete, damage, add malicious code to a sources code repository [Vaughan, 2015].

Advanced Persistence Threats [APTs] are escalating to a magnitude unheard in the past. These threats have been a nuisance in the cyber world and have been very daunting. Advanced exploits are routinely used to penetrate perimeter defenses by circumventing signature based anti-virus technologies and compromising endpoints and servers. Several entities have expressed difficulties detecting and identifying these layers because of the stealthy nature of the threats. Advanced threats are normally well organized and are formidable adversary that target specific goals for exploitations. Enterprise systems, nation states and individuals exploited by advanced threats are at the receiving end of a military attack and should mitigate the risk to avoid unrecoverable damages [Schmidt et.al 2012].

Some of the most potent weapons used by cyber actors include the following, Zero-day, APT Tactic, Zeus Trojan [Zbot], Stuxnet, Malicious Computer Worm, Duqu, Flame, RATs [Remote Access Trojan], GhOst RAT, Shell Shock also known as Bashdoor. Exploitation of software vulnerabilities give access to attackers by enabling them to bypass security perimeter. These mentioned threats are examples of anomalies that are very difficult to detect by the signature detection baseline tools. The concern behind these anomalies is that there are no immediate patch mechanisms for early detection in real time that the breached organization may implement to prevent systems and network from becoming victims [Gallagher 2014; Weimer, 2014].

Stuxnet as mentioned earlier is a worm designed to target only specific Siemens SCADA (industrial control) systems. This worm utilizes an unprecedented four zero-day vulnerabilities attack tool that make use of a security vulnerability in a targeted application, before the vulnerability is exposed to security experts. This family of worm uses rootkits advanced techniques to obscure itself from users and anti-malware software that it attacks [Smith, 2014].

Signature oriented polymorphic malware is harmful, destructive to a network. Examples of these are the Virus, Worm, Regin, Watering Hole attack, Trojan or Spyware that constantly changes ("morphs") that makes it difficult to detect with anti-malware programs. These are problem areas to a network.

In 2015, the cyber environment, outlined the data breach suffered by some major global and national entities. The breach at Target Corporation that involved theft of over 45 million individuals' records, was surpassed months later when Home Depot suffered the loss of 58 million customers' information. Organizational leaders are concerned about the impact of a breach, the legal implications and consequences and the toll to organizational reputation, but are striving to have all the right information to make the best possible choices [Vaughan, 2015].

LITERATURE REVIEW

Gorman et.al, [2014], in their study, it was noted that when an advanced attacker seeks to infiltrate an exploit, it follows a sophisticated, well-coordinated and defined process that enables it to leverage its skills effectively and avoid detection. Their study concludes that organizations should understand the Cyber Kill Chain in order to get inside the minds of advanced threats while engaging in intelligence-driven network defense.

[Sweeney, 2013; Ashford, 2012], among others, cited that the "Cyber Kill Chain" process is an effective way of understanding the highly orchestrated, technically and sophisticated activities of advanced threats life cycle.

[Clayton, 2012; Zetter, 2011] in their report stated that the Flash Player zero-day vulnerability whose existence was brought to the surface by Adobe has been exploited by a relatively new advanced persistent threat (APT) group named by Kaspersky Lab "ScarCruft.". Further, that "Scar Cruft" was been observed targeting Russia, Nepal, South Korea, China, Kuwait, India and Romania. The researchers concludes stating that the group used two Flash Player and one

Microsoft Windows vulnerabilities in its attacks.

[Williams, 2011; Rapid Report, 2012], in their reports suggested that, the Flash zero-day (CVE-2016-4171), which Adobe plans on patching, has been used by the threat actors in a campaign dubbed “Operation Daybreak.” The campaign, launched in March 2016, has focused on high-profile targets.

A study by [FireEye, 2012; Goldman, 2012], among others, found that Russian and Chinese hackers have been penetrating the computer network of the United States government to access database of confidential secret service documents for potential espionage.

In another report by [Hosenball, 2012], it was found that Chinese hackers were behind U.S. ransomware attacks - using tactics and tools previously associated with Chinese government-supported computer network intrusions. Ransomware, which involves encrypting a target's computer files and then demanding payment to unlock them, has generally been considered the domain of run-of-the-mill cyber criminals.

Ponemon Institute, in its global analysis of 2016 cost of Data Breach study, found that the average total cost of a data breach for the 383 companies participating in their research increased from \$3.79 to \$4 million. It was also found that the average cost paid for each lost or stolen record containing sensitive and confidential information increased from \$154 in 2015 to \$158 in 2016. Also, that organizations in Brazil and South Africa are most likely to have a material data breach involving 10,000 or more records, in contrast to organizations in Germany and Australia that are least likely to experience a material data breach [Ponemon Institute Research Report, 2016].

METHODOLOGY

Survey questionnaires were designed and distributed to IT security professionals at a technology security conference, in Orlando Florida in 2015. The goal is to examine and understand the patterns and behavior of cyber actors on various networks.

The survey participants are IT professionals that are employed in network environment and handle cyber security concerns, involving network security, and have extensive years of experience in the field. These folks are network administrators, security consultants, or senior security executives. The companies

under study represent mid-size and large organizations. These professionals conduct research and publish white papers on cyber-security matters

The sample population comprises of 249 participants. All were randomly selected. The survey had a total of 11 questions, using Likert scales tool that ranged from 5 (“mostly concerned”) to 1 (“do not know”) on rating questions regarding security threats, and categorical yes/no questions for gender and IT position ranks. The purpose of the questionnaire was to assess the concerns of IT professionals and researchers on security related issues at their respective organizations

DATA ANALYSIS AND RESULTS

The present study analyzes the responses from participants based on their gender and rank in the organization, regarding their perceptions to security effectiveness, IDS, Hackers, employees foreign, and third party vendors. Number of all participants in each survey question is shown below table 1. SPSS software used for data analysis, a total of 7 hypotheses are analyzed. Independent samples t tests are used for data analysis, the t test was used since the F test for testing equality of variance in any given pair of samples was not significant.

Table 1. Part I: Statistics for all Participants in each Survey Question

| | Gender | Administration | Security | Effectiveness | IDS | Hackers |
|---------|--------|----------------|----------|---------------|-----|---------|
| N Valid | 245 | 243 | 244 | 244 | 244 | 245 |
| Missing | 4 | 6 | 5 | 5 | 5 | 4 |

Table 1- Part II: Statistics for all Participants in each Survey

| | Employees | Foreign | Vendors |
|---------|-----------|---------|---------|
| N Valid | 245 | 245 | 245 |
| Missing | 4 | 4 | 4 |

GENDER

Gender was examined, there is total of 249 participants in this survey, 168 are male and 77 are female as it is illustrated below in table 2.

Table 2. Gender Participants in the Survey Questionnaire

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|--------|-----------|---------|---------------|--------------------|
| Valid | Male | 168 | 67.5 | 68.6 | 68.6 |
| | Female | 77 | 30.9 | 31.4 | 100.0 |
| | Total | 245 | 98.4 | 100.0 | |
| Missing | System | 4 | 1.6 | | |
| Total | | 249 | 100.0 | | |

ADMINISTRATION

H₀: There is no difference in perspective between Executive /Senior IT Administration and lower-level IT personal regarding the network security systems and other related issues.

H_a: There is difference in perspective between Executive / Senior IT Administration and lower-level IT personal regarding the network security systems and other related issues.

There is no significant difference in perspectives between Executive / Senior IT Administration and lower-level IT personal regarding the security systems and other related issues; hence both groups view it equally as an important issue. The mean for both groups are very close, as illustrated in table 3-6.

Table 3. Case Processing Summary

| | Cases | | | | | |
|---------------------------|----------|---------|----------|---------|-------|---------|
| | Included | | Excluded | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Administration* Gender | 243 | 97.6% | 6 | 2.4% | 249 | 100.0% |

Table 4. Administration Mean

| Gender | N | Mean | Std. Deviation |
|--------|-----|--------|----------------|
| Male | 166 | 1.4277 | .49624 |
| Female | 77 | 1.5325 | .50222 |
| Total | 243 | 1.4609 | .49950 |

Table 5. T- Test Group Statistics

| Administration | Gender | N | Mean | Std. Deviation | Std. Error Mean |
|----------------|--------|--------|--------|----------------|-----------------|
| | Male | 166 | 1.4277 | .49624 | .03852 |
| Female | 77 | 1.5325 | .50222 | .05723 | |

Table 6.- Part I: Independent Samples Test

| | | t-test for Equality of Means | | |
|----------------|-----------------------------|------------------------------|-----------------|-----------------------|
| | | Sig. (2-tailed) | Mean Difference | Std. Error Difference |
| Administration | Equal variances assumed | .129 | -.10476 | .06868 |
| | Equal variances not assumed | .131 | -.10476 | .06899 |

Table 6.- Part II: Independent Samples Test

| | | t-test for Equality of Means | |
|----------------|-----------------------------|---|--------|
| | | 95% Confidence Interval of the Difference | |
| | | Lower | Upper |
| Administration | Equal variances assumed | -.24005 | .03054 |
| | Equal variances not assumed | -.24109 | .03158 |

SECURITY

The first hypothesis tests whether male and females have differences in perspective regarding the security of company network. The mean for both gender groups are very close.

H₀: There is no difference between male and female perspectives regarding the security of company network.

H_a: There is a difference between male and female perspectives regarding the security of company network, as illustrated in table 7-10.

Table 7. Security

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|-----------------|-----------|---------|---------------|--------------------|
| Valid | Somehow Secured | 33 | 13.3 | 13.5 | 13.5 |
| | Secured | 160 | 64.3 | 65.6 | 79.1 |
| | Very Secured | 51 | 20.5 | 20.9 | 100.0 |
| | Total | 244 | 98.0 | 100.0 | |
| Missing | System | 5 | 2.0 | | |
| Total | | 249 | 100.0 | | |

Table 8. Means Case Processing Summary

| | Cases | | | | | |
|-----------|----------|---------|----------|---------|-------|---------|
| | Included | | Excluded | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Security* | 244 | 98.0% | 5 | 2.0% | 249 | 100.0% |
| Gender | | | | | | |

Table 9. T-Test Group Statistics

| Gender | | N | Mean | Std. Deviation | Std. Error Mean |
|----------|--------|-----|--------|----------------|-----------------|
| Security | Male | 167 | 4.1078 | .60150 | .04655 |
| | Female | 77 | 4.0000 | .53803 | .06131 |

Table 10. Independent Samples Test

| | | t-test for Equality of Means |
|----------|-----------------------------|---|
| | | 95% Confidence Interval of the Difference |
| | | Upper |
| Security | Equal variances assumed | .26579 |
| | Equal variances not assumed | .25978 |

EFFECTIVENESS

The second hypothesis tests whether male and females have differences in perspective regarding the effectiveness of network security systems of the organization. The mean for both gender groups are very close.

HO: There is no difference between male and female perspectives regarding the effectiveness of network security systems of the organization.

Ha: There is a difference between male and female perspectives regarding the effectiveness of network security systems of the organization, as illustrated below in table 11-14.

Table 11. Effectiveness

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|----------------|-----------|---------|---------------|--------------------|
| Valid | Undecided | 36 | 14.5 | 14.8 | 14.8 |
| | Agree | 143 | 57.4 | 58.6 | 73.4 |
| | Strongly Agree | 65 | 26.1 | 26.6 | 100.0 |
| | Total | 244 | 98.0 | 100.0 | |
| Missing | System | 5 | 2.0 | | |
| Total | | 249 | 100.0 | | |

Table 12. Mean Case Processing Summary

| | Cases | | | | | |
|----------------|----------|---------|----------|---------|-------|---------|
| | Included | | Excluded | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Effectiveness* | 244 | 98.0% | 5 | 2.0% | 249 | 100.0% |
| Gender | | | | | | |

Table 13. T-Test Group Statistics

| Gender | N | Mean | Std. Deviation | Std. Error Mean |
|----------------------|-----|--------|----------------|-----------------|
| Effectiveness Male | 167 | 4.1138 | .64396 | .04983 |
| Effectiveness Female | 77 | 4.1299 | .61453 | .07003 |

Table 14. Independent Samples Test

| | | t-test for Equality of Means | |
|---------------|-----------------------------|---|--------|
| | | 95% Confidence Interval of the Difference | |
| | | Lower | Upper |
| Effectiveness | Equal variances assumed | -.18836 | .15617 |
| | Equal variances not assumed | -.18589 | .15370 |

IDS

The third hypothesis tests whether male and females have differences in perspective regarding the investment of more money in intrusion detection systems [IDS] in 2015-2016. The mean for both gender groups are very close.

H₀: There is no difference between male and female perspectives regarding the investment of more money in intrusion detection systems [IDS] in 2015-2016.

H_a: There is a difference between male and female perspectives regarding the investment of more money in intrusion detection systems [IDS] in 2015-2016, as illustrated below in table 15-18.

Table 15. IDS

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|-------------------|-----------|---------|---------------|--------------------|
| Valid | Strongly Disagree | 3 | 1.2 | 1.2 | 1.2 |
| | Disagree | 10 | 4.0 | 4.1 | 5.3 |
| | Undecided | 46 | 18.5 | 18.9 | 24.2 |
| | Agree | 136 | 54.6 | 55.7 | 79.9 |
| | Strongly Agree | 49 | 19.7 | 20.1 | 100.0 |
| | Total | 244 | 98.0 | 100.0 | |
| Missing | System | 5 | 2.0 | | |
| Total | | 249 | 100.0 | | |

Table 16. Case Processing Summary

| | Cases | | | | | |
|--------|----------|---------|----------|---------|-------|---------|
| | Included | | Excluded | | Total | |
| | N | Percent | N | Percent | N | Percent |
| IDS * | 244 | 98.0% | 5 | 2.0% | 249 | 100.0% |
| Gender | | | | | | |

Table 17. T-Test Group Statistics

| Gender | | N | Mean | Std. Deviation | Std. Error Mean |
|--------|--------|-----|--------|----------------|-----------------|
| IDS | Male | 167 | 3.9581 | .77889 | .06027 |
| | Female | 77 | 3.7532 | .86078 | .09810 |

Table 18. Independent Samples Test

| | | t-test for Equality of Means |
|-----|-----------------------------|---|
| | | 95% Confidence Interval of the Difference |
| | | Upper |
| IDS | Equal variances assumed | .42340 |
| | Equal variances not assumed | .43253 |

HACKERS

The fourth hypothesis tests whether male and females have differences in perspective regarding hacker's issue. The mean for both gender groups are very close.

H₀: There is no difference between male and female perspectives regarding hacker's issue.

H_a: There is a difference between male and female perspectives regarding hacker's issue, as illustrated below in table 18-21.

Table 18. Hackers

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|--------------------|-----------|---------|---------------|--------------------|
| Valid | Somewhat Concern | 29 | 11.6 | 11.8 | 11.8 |
| | Moderately Concern | 132 | 53.0 | 53.9 | 65.7 |
| | Extremely Concern | 84 | 33.7 | 34.3 | 100.0 |
| | Total | 245 | 98.4 | 100.0 | |
| Missing | System | 4 | 1.6 | | |
| Total | | 249 | 100.0 | | |

Table 19. Mean Case Processing Summary

| | Cases | | | | | |
|---------------------|----------|---------|----------|---------|-------|---------|
| | Included | | Excluded | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Hackers * Gender | 245 | 98.4% | 4 | 1.6% | 249 | 100.0% |

Table 20. T- Test Group Statistics

| Gender | | N | Mean | Std. Deviation | Std. Error Mean |
|---------|--------|-----|--------|----------------|-----------------|
| Hackers | Male | 168 | 4.2560 | .63808 | .04923 |
| | Female | 77 | 4.1558 | .65020 | .07410 |

Table 21. Independent Samples Test

| | | t-test for Equality of Means |
|---------|-----------------------------|---|
| | | 95% Confidence Interval of the Difference |
| | | Upper |
| Hackers | Equal variances assumed | .27411 |
| | Equal variances not assumed | .27593 |

EMPLOYEES

The fifth hypothesis tests whether male and females that pose the greatest network security concerns/threats to the organization. The mean for both gender groups are very close.

H₀: There is no difference between male and female employees that pose the greatest network security concerns/threats to the organization.

H_a: There is a difference between male and female employees that pose the greatest network security concerns/threats to the organization, as illustrated below in table 21-24.

Table 21. Employees

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|--------------------|-----------|---------|---------------|--------------------|
| Valid | Not at all Concern | 1 | .4 | .4 | .4 |
| | Seldom Concern | 9 | 3.6 | 3.7 | 4.1 |
| | Somewhat Concern | 55 | 22.1 | 22.4 | 26.5 |
| | Moderately Concern | 117 | 47.0 | 47.8 | 74.3 |
| | Extremely Concern | 63 | 25.3 | 25.7 | 100.0 |
| | Total | 245 | 98.4 | 100.0 | |
| Missing | System | 4 | 1.6 | | |
| Total | | 249 | 100.0 | | |

Table 22. Mean Case Processing Summary

| | Cases | | | | | |
|-------------|----------|---------|----------|---------|-------|---------|
| | Included | | Excluded | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Employees * | 245 | 98.4% | 4 | 1.6% | 249 | 100.0% |
| Gender | | | | | | |

Table 23. T-Test Group Statistics

| Gender | | N | Mean | Std. Deviation | Std. Error Mean |
|-----------|--------|-----|--------|----------------|-----------------|
| Employees | Male | 168 | 4.0000 | .81894 | .06318 |
| | Female | 77 | 3.8312 | .80136 | .09132 |

Table 24. Independent Samples Test

| | | t-test for Equality of Means | |
|-----------|-----------------------------|---|--------|
| | | 95% Confidence Interval of the Difference | |
| | | Lower | Upper |
| Employees | Equal variances assumed | -.05169 | .38935 |
| | Equal variances not assumed | -.05059 | .38825 |

FOREIGN

H₀: There is no difference between male and female of foreign state that pose the greatest network security concerns/threats to the organization.

H_a: There is a difference between male and female of foreign states that pose the greatest network security concerns/threats to the organization.

The sixth hypothesis tests whether male and females of foreign state that pose the greatest network security concerns/threats to the organization. The mean for both gender groups are very close, as illustrated below in table 24-27.

Table 24. Foreign

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|--------------------|-----------|---------|---------------|--------------------|
| Valid | Somewhat Concern | 26 | 10.4 | 10.6 | 10.6 |
| | Moderately Concern | 124 | 49.8 | 50.6 | 61.2 |
| | Extremely Concern | 95 | 38.2 | 38.8 | 100.0 |
| | Total | 245 | 98.4 | 100.0 | |
| Missing | System | 4 | 1.6 | | |
| Total | | 249 | 100.0 | | |

Table 25. Mean Case Processing Summary

| | Cases | | | | | |
|---------------------|----------|---------|----------|---------|-------|---------|
| | Included | | Excluded | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Foreign * Gender | 245 | 98.4% | 4 | 1.6% | 249 | 100.0% |

Table 26. T-Test Group Statistics

| Gender | N | Mean | Std. Deviation | Std. Error Mean |
|--------------|-----|--------|----------------|-----------------|
| Foreign Male | 168 | 4.2976 | .64334 | .04963 |
| Female | 77 | 4.2468 | .65204 | .07431 |

Table 27. Independent Samples Test

| | | t-test for Equality of Means |
|---------|-----------------------------|---|
| | | 95% Confidence Interval of the Difference |
| | | Upper |
| Foreign | Equal variances assumed | .22600 |
| | Equal variances not assumed | .22747 |

VENDORS

H₀: There is no difference between male and female of third party contractors-vendors that pose the greatest network security concerns/threats to the organization.

H_a: There is a difference between male and female of third party contractors-vendors that pose the greatest network security concerns/threats to the organization.

The seventh hypothesis tests whether male and females of third party contractors-vendors that pose the greatest network security concerns/threats to the organization. The mean for both gender groups are very close, as illustrated below in table 27-31.

Table 28. Vendors

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|--------------------|-----------|---------|---------------|--------------------|
| Valid | Seldom Concern | 3 | 1.2 | 1.2 | 1.2 |
| | Somewhat Concern | 50 | 20.1 | 20.4 | 21.6 |
| | Moderately Concern | 149 | 59.8 | 60.8 | 82.4 |
| | Extremely Concern | 43 | 17.3 | 17.6 | 100.0 |
| | Total | 245 | 98.4 | 100.0 | |
| Missing | System | 4 | 1.6 | | |
| Total | | 249 | 100.0 | | |

Table 29. Mean Case Processing Summary

| | Cases | | | | | |
|-----------|----------|---------|----------|---------|-------|---------|
| | Included | | Excluded | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Vendors * | 245 | 98.4% | 4 | 1.6% | 249 | 100.0% |
| Gender | | | | | | |

Table 30. T-Test Group Statistics

| Gender | | N | Mean | Std. Deviation | Std. Error Mean |
|---------|--------|-----|--------|----------------|-----------------|
| Vendors | Male | 168 | 3.9821 | .65179 | .05029 |
| | Female | 77 | 3.8701 | .65596 | .07475 |

Table 31. Independent Samples Test

| | | t-test for Equality of Means |
|---------|-----------------------------|---|
| | | 95% Confidence Interval of the Difference |
| | | Upper |
| Vendors | Equal variances assumed | .28905 |
| | Equal variances not assumed | .29006 |

SUMMARY OF THE HYPOTHESIS

A total of 7 hypotheses were analyzed using SPSS software. Independent samples t tests were also used since the F test for testing equality of variance in any given pair of samples was not significant.

All seven hypotheses were examined with respect to gender. In all of the hypotheses, namely administrator, security, effectiveness, IDS, hackers, employees, foreign nation states, and vendors, both females and males did not differ significantly in their perspectives regarding the seven hypotheses as the mean values for both genders was very close. Hence, they agree on the parameters of the survey, given the values of the means of their responses.

OVERALL CONCLUSION

Security professional should be equipped with mitigation tools and knowledge that enhances their power over adversaries since awareness of specific

circumstances that give rise to vulnerabilities allow security practitioners to address the root causes of a given breach.

As the study found, threats from sophisticated malware will continue to rise as attacks on organizations escalates. Majority of the IT staff in the study agree that security teams can no longer afford to wait for attacks to occur instead, they need to implement a dynamic adaptive defense approach that search and eliminate unseen exploits. After a breach, the most important step for security administrators is to identify the root cause of a breach. This can be achieved by utilizing forensic to analyze traffic by finding the root cause of an event. These could include data capture, storing all packets for post-incident for forensic analysis, combing through captured traffic for anomalies and signs of problems in the network and logging results of investigations and network vulnerabilities for post mortem mitigation.

Shielding against anomalies requires the use of security technologies that leverage techniques other than blacklisting. Mitigating against these types of attack requires IT security professionals to rely on a defense-in-depth strategy that utilizes real-time, signature-less detection mechanisms to proactively respond on potential threats.

Security professional seeking to build secure networks may use the Cyber Kill chain process as an added tool to understand the nature and methodologies of their adversaries.

The best method of dealing with polymorphic malware is to employ multiple and diverse blocking, filtering, detection and removal programs. These programs should be kept current and should be run as often as possible. Auto-protect features, if available, should be enabled.

REFERENCES

- Ashford, Warwick; (2013), "Why Has DLP Never Taken Off?," Computer Weekly, 22 January 2013
www.computerweekly.com/news/2240176414/Why-has-DLP-never-taken-off
- Clayton Mark, Stuxnet cyber weapon looks to be one on a production line, researchers say. Technical report, World Wide Web, <http://www.csmonitor.com/USA/2012/0106/Stuxnet-cyberweapon-looks-to-be-%one-on-a-production-line-researchers-say>, January 2012.
- Clover, Juli (29 September 2014). "Apple Releases OS X Bash Update to Fix 'Shellshock' Security Flaw in Mavericks, Mountain Lion, and Lion". MacRumors.com. Retrieved 2 October 2014.
- "FireEye advanced threat report – 2H 2012," FireEye, Apr.3, 2013, accessed Jan 3, 2014, www2.fireeye.com/re/fireeye/images/fireeye-advanced-threat-report-2h2012.pdf.
- Gallagher, Sean (26 September 2014). "Still more vulnerabilities in bash? Shellshock becomes whack-a-mole". Arstechnica. Retrieved 26 September 2014
- Gorman, Gavin, and McDonald, Geoff, "Ransomware: A growing menace," Symantec Security Response, Nov. 8, 2012, accessed Jan. 6, 2014, www.symantec.com/connect/blogs/ransomware-growing-menace.
- Goldman, David, "Hacker hits on U.S. power and nuclear target spiked in 2012," CNN Money, Jan 9, 2013, accessed Jan 27, 2014, <http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/>.
- Greenberg, Andy (25 September 2014). "Hackers Are Already Using the Shellshock Bug to Launch Botnet Attacks". Wired. Retrieved 28 September 2014.
- Hosenball Mark, Experts say Iran has "neutralized" stuxnet virus. Technical report, World Wide Web, <http://www.reuters.com/article/2012/02/14/us-iran-usa-stuxnet-idUSTRE81%D24Q20120214>, February 2012.

- Ponemon Institute Research Report 2016, “Cost of Data Breach Study: Global Analysis
- Rapid Report (2012): “Data Breaches in the Government Sector.” Rapid7. September 6, 2012. <http://www.rapid7.com>.
- Schmidt, M. & Perlroth, N. (October 23, 2012). Credit card data breach at Barnes & Noble stores, New York Times.
- Smith, A. 2014, “ Newly Discovered Sophisticated Malware Has Been Spying on Computers for Six Years, “Newsweek, November 24, <http://europe.newsweek.com/new-sophisticated-malware-has-been-spying-computers-six-years-2886640>
- Sweeney, Patrick, “Defending against exploit kits, “ Network World, Jun. 3 2013 accessed Dec. 7, 2013, www.networkworld.com/news/tech/2013/060313=exploit-kits-270404.html
- Vaughan Nichols, S 2015. “Securing the Internet: Let’s Encrypt to Release First Security Certificate September 7, “ ZDNet, August 24. <http://www.zdnet.com/article/securing-the-internet-let-encrypt/>
- Weimer, Florian (25 September 2014). "Re: CVE-2014-6271: remote code execution through bash". Openwall Project. Retrieved 2 November 2014.
- Williams Christopher. Israeli security chief celebrates stuxnet cyber-attack. Technical report, World Wide Web, <http://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chi%ef-celebrates-Stuxnet-cyber-attack.html>, February 2011.
- Zetter Kim, How digital detectives deciphered stuxnet, the most menacing malware in history. Technical report, World Wide Web, <http://www.wired.com/threatlevel/2011/07how-digital-detectives-deciphe%red-stuxnet/all/1>, 2011. Retrieved December 12, 2012, from <http://www.nytimes.com/2012/10/24/business/hackers-get-credit-data-at-barnes-noble.html>