International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(4): 246-261
The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2305-0012)

Security Breaches, Network Exploits and Vulnerabilities: A Conundrum and an Analysis

Oredola A. Soluade
Iona College
Hogan School of Business
New Rochelle - New York 10801
osoluade@iona.edu

Emmanuel U Opara
College of Business
Prairie View A&M University
Prairie View - Texas U.S.A.
euopara@pvamu.edu

ABSTRACT

Enterprise systems are continuously on cyber-attacks as struggle for solutions are sort. Today, these organizations spend over $70 billion on IT security, but are unable to protect the organization since cyber criminals routinely discover exploits and breach those defenses with zero-day attacks that bypass traditional technologies. These attacks occur during the vulnerability window that exists in the time between when a loophole is first exploited and when software developers start to develop and publish a counter to that threat. Many organizations had been breached by the zero-day attack concept. This means that at least one attacker had bypassed all layers of organization defense-in depth architecture. Using data from our survey of 202 participants, this study analyses how attacks are changing the cyber platform and why traditional and legacy defenses are functioning below par and expectations.

KEYWORDS: Security Breaches, Vulnerabilities, Threats, Malware, Adware, Exploits.

1 INTRODUCTION

Enterprise systems function in a globally-connected world, which constantly are witnessing globally-distributed cyber threats. Study has indicated, these threats are not restricted by geographical boundaries, but are targeted at all technologies, hardware/software/service providers, end-users, consumers, private and the public sector alike. The cost and frequency of these incidences are on the rise. There threats have evolved as a new dimension of interest and concerns, gaining political and societal attention. Understanding the exponential growth and magnitude of cyber threats, the future tasks and responsibilities associated with cybersecurity is critical to enterprise systems competitiveness, survival and profitability.

Cyber-attacks are now facts of organizational concerns because the rates of occurrences are growing exponentially [1]. Today's security defenses are failing because organization's legacy platforms leverage technologies have been dependent on signatures as security authentication mechanisms. These platforms may be good at blocking basic malware that

are known and documented, however legacy platform technologies do not stand a chance against today's sophisticated, dynamic cyber-attacks that occur across multiple vectors and stages of the cyber platform. Examples are biological weaponries, nukes, climate change, zero-day attacks, and transactional crimes. An example for bio-threats is the public health community's dream making the arrival and spread of communicable diseases as easy to predict and track as weather. This study found that potential exploits, and threat levels have escalated to the point that with time, motivation, and funding, a resolute criminal will likely be able to penetrate any system that is accessible directly from the Internet

In 2013, Hackers concentrated on placing malware content on enterprise systems and organization's Websites as a means to gain entrance into the network. These criminals employ "drive-by-downloads" from fake websites as well as "water hole to exploit potential vulnerabilities. Also in same year, a press report describes pages on an official U.S. Government website that contain content promoting third-parties products that were enriched with malicious payloads. As these threats evolve, they could infiltrate the interior of the network, the core, the distribution layer and the user access edge where the defense and visibility is minimal. Once inside a system, the payload quietly target specific assets and individuals in the enterprise system. Most of the objectives of such attacks are to collect and exfiltrate intellectual property of state/trade secrets for competitive advantage within industry, and use for economy and sociopolitical ends [2].

The fact remains that current antivirus solutions are not capable of eradicating targeted attacks. Study has shown that organization's Industrial Control System [ICS] platforms are targets for cyber attackers. These include automation, process control, access control devices, system accounts and asset information that are considered valuable to attackers. Cyber criminals can leverage the lack of corporate security policies, procurement languages, asset inventory that are present in many Industrial Control Systems [ICS]. A coordinated and known security exploit can be combated by a structured and adequately designed security infrastructure that includes preventive mechanisms such as intrusion prevention, antivirus, content security and internal and external firewalls. However, targeted threats designed for specific exploits could pose a tougher challenge. Further attackers could come from nation states, insiders and other trusted parties such as contractors or vendors. Hacktivists or politically motivated attackers and script kiddies are also included in this group. Based on these facts, the potential-risk and challenges are very high.

The key in this study is to identify what's at stake and the key challenges in gaining visibility to customized threats. Also to create threat awareness in areas where systems could be vulnerable. These include but not limited to the following areas: [I] Network Access: Malware can spread vertically through the network by trusted system to system connections of VPN because it is easy for it to maneuver undetected through a controlled platform. [II] System Management; when there are extensive delays by security professionals in patching and operating systems upgrades, attackers can exploit such systems. Further, criminals can leverage default usernames and

passwords or weak authentication mechanism. [III] Supply Chain; Criminals can attack third party vendors, contractors or integrator in an attempt to exploit an ICS environment asset owner or multiple enterprise systems. [IV]Interconnects; Criminals can attack ICS systems by exploiting applications that communicate through network segmentation because many ICS platforms are susceptible to network-based Man in the Middle attacks.
This study will provide actionable intelligence to ensure enterprise systems breach discover and mitigate exploits as they occur in the organization.

In our survey questions 8 – 22 [appendix 1], we asked in the survey, who the top cyber-threats, that are facing their organization? This question was raised because, most members of security teams, do not agree on what constitutes the significant threats to their organizations. We also asked survey respondents the type of proactive tools they use to counter zero-day attacks and Advanced Persistent Threat [APT]. This is a commonly use term to define remote attacks employed by sophisticated threats actors. These actors could be nation states or their intelligence services. Some of the intelligence services include these:

- Malware
- Outbound Traffic
- Rogue Device
- Geolocation of IP Traffic
- Distribution intrusion detection systems (DIDS)
- Deep Packet Inspection [DPI]
- External Footprint
- Co-operating security managers (CSM)
- Watermarking/tagging

The findings from this study, will articulate the current cyber security measures enterprise systems will have to deploy to counter vulnerabilities, potential breaches and threats.

2 LITERATURE REVIEW

In 2013, study showed that at least ten major banks were attacked by “hacktivists: These attacks were motivated by individuals whose exploit achievement is to destroy the reputation of the firm or its principals by employing techniques such as defacing websites to leaking enterprise private content. JPMorgan Chase, Bank of America, Citigroup, Wells Fargo and others have faced such attacks [3].

Baldor [4] in their study noted that a data security breach at Montana State health records compromised the social security numbers and other important information of about 1.5 people. These cyber-criminal gained access to a computer server tied to the Montana Department of Public Health and Human Services, exposing sensitive or confidential information of current and former medical patients, health agency employees and contractors.

Oyemade [5], among others, cited that information technology faces a constant flood of alerts from every system, challenging organization’s security expert’s to find the critical threats in a sea of false alerts or insignificant events. They noted that ultimate protection means the near elimination of false positive and remediation of infected endpoints.

Tester, [6]) in their report noted that more zero-day vulnerabilities were discovered in 2013 than any other year. The 26 zero-day

vulnerabilities discovered represent an 81 percent increase over 2012 and are more than the three previous years combined. Zero-day vulnerabilities are coveted because they give attackers the means to silently infect their victim without depending on social engineering.

Target Corp and Neiman Marcus as a study summarized are not the only U.S. retailers whose networks were breached over the holiday shopping season last year, however, it reported that smaller breaches on of at least three other well-known U.S. retailers took place and were conducted using similar techniques as the one on Target, [13].

A recent study found that restaurant chain "P.F. Chang's China Bistro" had a breach on its card processing systems that could have resulted in theft of customer payment card information at 33 of its 210 U.S. locations. The potentially stolen data includes card numbers, cardholder's name and/or the card's expiration date and other relevant information [7].

In another report [8], it was stated that the 9/11 Commission, in its 10th anniversary report, cautions Americans and the U.S. government to treat cyber threats more seriously than they did terrorist threats in the days and weeks leading to Sept. 11, 2001.

Steinbart [13], in their study also indicated that baby monitors, security cameras and routers, were famously hacked in 2013. Furthermore, security researchers demonstrated attacks against smart televisions, automobiles and medical equipment. This gives this study a preview of the security challenge presented by the rapid adoption of the Internet of Things (IoT).

Later studies, [9], [10], among others summarized that data shows that companies are learning from past cyber-attacks and breaches. There is evidence companies are becoming better at managing the costs incurred to resolve a data breach incident and for the first time in seven years both the organization cost of a data breach and the cost per lost or stolen record declined in 2012.

According to a study by [12], citing rising number of high profile cyber-attacks — most recently at Twitter, LinkedIn and Yahoo— it was noted that governmental agencies are stepping up its scrutiny of cyber security. This is leading to increased calls for legislation and regulation, placing the burden on companies to demonstrate that the information provided by customers and clients is properly safeguarded online.

Another studies by [10], also summarized that despite the fact that cyber risks and cyber security are widely acknowledged to be a serious threat, a majority of companies today still do not purchase cyber risk insurance, though this is changing. Their study suggests that more companies are now purchasing cyber coverage and that insurance has a key role to play as companies and individuals look to better manage and reduce their potential financial losses from cyber risks in future.

3 METHODOLOGY

In order to pilot test the cyber-security concerns, the authors constructed, distributed and collected responses from survey questionnaires at a cyber-security business professional conference in May 2013 at San Antonio Texas.

The survey population comprises of professionals who publish research findings and work in their respective fields. These are

experts with extensive history in teaching and in the business world. Survey data was distributed to senior IT professionals from midmarket (100 to 999 employees) and enterprise-class (1000 employees or more] organizations. The survey questionnaires were distributed to 320 attendees. The number completed and returned was 202. Overall, we consider these as an equitable representative random sample. Most of the survey items were Likert scale types, yes/no responses or categorical, ordinal items, gender, ranks of personnel.
The study conducted a survey of 24 questions covering a range of security issues that are of importance and of concern to IT and security administrators in small and medium size businesses [SMBs]. The questions were designed and conducted to obtain a snapshot of the state of security issues in SMBs and to confirm issues that have been raised in other security studies.

4 FINDINGS/RESULTS

A series of hypotheses were tested to determine the extent of awareness of potential threats to data at rest. and attitude of the respondents to security in their organization.

The first hypothesis is to determine the extent to which the respondent's attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other affect their feeling of security in their organization.

H_0: There is no dependence between feeling secure in an organization on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: The sense of feeling secure in an organization depends on a number of factors – including: their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging.

Conclusion: Attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Taggings, do not significantly impact the feeling of respondents about the security in their organization.

The second hypothesis is to determine the extent to which the male respondent's attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other affect their feeling of security in their organization.

H_0: For male respondents, there is no dependence between feeling secure in an organization on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: For male respondents, the sense of feeling secure in an organization depends on a number of factors – including: their attitude to hackers, current and former employees, foreign nation-

states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging.

Conclusion: When this analysis is controlled for gender, it turns out that male respondents, who have confidence in their company network, also believe that Rogue Device Scanning is the most proactive activity/technique to counter persistent threats to their organization. This dependency is found to be significant at the 1% significance level with a p-value of 0.008)

The third hypothesis is to determine the extent to which the female respondent's attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other affect their feeling of security in their organization.

H_0: For female respondents, the sense of feeling secure in an organization depends on a number of factors – including: their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging.

H_1: For female respondents, the sense of feeling secure in an organization depends on a number of factors – including: their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging.

Conclusion: When this analysis is controlled for gender, it turns out that female respondents who have confidence in their company network is independent of their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging.

In order to determine whether there is dependence between the assessments of the effectiveness of an organization's network system on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other, the following hypothesis was tested.

H_0: There is no dependence between the assessment of the effectiveness of an organization's network system on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between the assessment of the effectiveness of an organization's network system on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: Attitude of respondents to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging, does not significantly impact the assessment of the effectiveness of an organization's

network system and their feelings about the security in their organization.

The hypothesis was then tested for a subset of male respondents. The result is as follows:

H_0: There is no dependence between the assessment by male respondents, of the effectiveness of an organization's network system on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between the assessment by male respondents, of the effectiveness of an organization's network system on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: Attitude of male respondents to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Taggings, does not significantly impact the assessment of the effectiveness of an organization's network system and their feelings about the security in their organization.

When the hypothesis was tested for a subset of female respondents, the result is as follows:

H_0: There is no dependence between the assessment by female respondents, of the effectiveness of an organization's network system on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between the assessment by female respondents, of the effectiveness of an organization's network system on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: Attitude of female respondents to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Taggings, does not significantly impact the assessment of the effectiveness of an organization's network system and their feelings about the security in their organization.

Another hypothesis that was tested is to determine if there is dependence between Investment in cybersecurity as best solution for cyber-attacks on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other. The resultant test is as follows:

H_0: There is no dependence between *Investment in cybersecurity as best solution for cyber-attacks* on the one hand, and their attitude to hackers, current and former

employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between *Investment in cybersecurity as best solution for cyber-attacks* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: Attitude of respondents to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Taggings, do not significantly impact *Investment in cybersecurity as best solution for cyber-attacks*.

The hypothesis was then tested for a subset of male respondents. The result is as follows:

H_0: There is no dependence between male *Investment in cybersecurity as best solution for cyber-attacks* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between male *Investment in cybersecurity as best solution for cyber-attacks* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: At the 5% significance level, it is determined that the attitude of male respondents to foreign nation-states, do significantly impact male *Investment in cybersecurity as best solution for cyber-attacks*.

Table 1. Regression output of attitude of male respondents to Foreign Nation-States

	Coefficients				
	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
Var014: Foreign Nation-states are perceived as the groups that pose the greatest cybersecurity threat to the organizations of male respondents	-0.398	0.173	-0.23	-2.301	0.024

When the hypothesis was tested for a subset of female respondents, the result is as follows:

H_0: There is no dependence between female *Investment in cybersecurity as best solution for cyber-attacks* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External

footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between female *Investment in cybersecurity as best solution for cyber-attacks* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: At the 5% significance level, it is determined that the attitude of female respondents to organized crime do significantly impact *Investment in cybersecurity as best solution for cyber-attacks* in their organization.

Table 2. Regression output of attitude of female respondents to Organized Crime groups

Coefficients[a]						
		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig.
	(Constant)	-1.426	3.282		-.434	.665
	Var015: Organized crime groups are perceived as the groups that pose the greatest cybersecurity threat the organizations of female respondents	.384	.128	.345	3.003	.004
a. Dependent Variable: Var005: Do you agree that investment in cybersecurity in 2013-2014....will provide the best systems solutions to thwart cyber-attacks?						

Another hypothesis that was tested is to determine if there is dependence between *Rating Downtime as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other. The result of that test is as follows:

H_0: There is no dependence between *Rating Downtime as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between *Rating Downtime as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: At the 5% significance level, it is determined that the attitude of respondents to hackers (p-value 0.047) and organized crime (p-value 0.037) do significantly impact *Rating Downtime as the greatest IT concern of their organization*.

Table 3. Regression output of attitude of respondents to Hackers and Organized Crime groups

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.219	.815		5.175	.000
	Var012: Hackers are the groups that pose the greatest cybersecurity threat to your organization	.098	.049	.141	2.002	.047
	Var015: Organized crime are the groups that pose the greatest cybersecurity threat to your organization	-.076	.036	-.153	-2.097	.037
a. Dependent Variable: Var006: Rate your company's IT concerns with regard to Downtime						

The hypothesis was then tested for a subset of male respondents. The result is as follows:

H_0: There is no dependence between male *Rating Downtime as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between male *Rating Downtime as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: At the 5% significance level, it is determined that the attitude of male respondents to hackers (p-value 0.029) does significantly impact *Rating Downtime as the greatest IT concern of their organization*

Table 4. Regression output of attitude of male respondents to Hackers

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
	(Constant)	3.421	1.344		2.545	.013
	Var012: Hackers are perceived as the group that poses the greatest cybersecurity threat to the organizations of male respondents	.164	.074	.235	2.214	.029
a. Dependent Variable: Var006: Rate your company's IT concerns with regard to Downtime						

When the hypothesis was tested for a subset of female respondents, the result is as follows:

H_0: There is no dependence between female *Rating Downtime as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between female *Rating Downtime as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: At the 5% significance level, it is determined that the attitude of female respondents to organized crime (p-value 0.020) does significantly impact *Rating Downtime as the greatest IT concern of their organization.*

Table 5. Regression output of attitude of male respondents to Hackers

Coefficients[a]						
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	4.393	1.169		3.758	.000
	Var015: Organized crime is perceived as the group that poses the greatest cybersecurity threat to the organizations of female respondents.	-.108	.046	-.279	-2.378	.020
a. Dependent Variable: Var006: Rate your company's IT concerns with regard to Downtime						

Another hypothesis that was tested is to determine if there is dependence between *Rating of Compliance as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other. The result is as follows:

H_0: There is no dependence between *Rating of Compliance as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between *Rating of Compliance as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized

H_1: There is dependence between male *Rating of Compliance as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: Attitude of respondents to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Taggings, does not significantly impact male *Rating* crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: Attitude of respondents to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Taggings, do not significantly impact *Rating Compliance as the greatest IT concern of their organization*

The hypothesis was then tested for a subset of male respondents. The result is as follows:

H_0: There is no dependence between male *Rating of Compliance as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Compliance as the greatest IT concern of their organization.

When the hypothesis was tested for a subset of female respondents, the result is as follows:

H_0: There is no dependence between female *Rating of Compliance as the greatest IT concern of their organization* on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

H_1: There is dependence between female *Rating of Compliance as the greatest IT*

concern of their organization on the one hand, and their attitude to hackers, current and former employees, foreign nation-states, organized crime, malware analysis, Geolocation of IP traffic, Subscription Services, External footprints, and Document Watermarking and Tagging on the other.

Conclusion: At the 5% significance level, it is determined that the attitude of female respondents to Penetration Testing (p-value 0.021), and Examination of External Footprints (p-value 0.050) as the most proactive activity/techniques used to counter persistent threats to their organization, significantly impact *Rating Compliance as the greatest IT concern of their organization.*

Table 6. Regression output of attitude of female respondents to Penetration Testing & External Footprints

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	4.705	1.037		4.536	.000
	Var017: Penetration Testing is the most proactive activity/technique used to counter persistent threats to your organization	.219	.093	.253	2.357	.021
	Var022: Examining External Footprint is the most proactive activity/technique used to counter persistent threats to your organization	-.144	.072	-.230	-1.992	.050

a. Dependent Variable: Var007: Rate your company's IT concerns with regard to Compliance

5 OVERALL CONCLUSION

Despite the tremendous amount of money organizations pour into traditional security measures every year, attackers are able to penetrate security defenses and compromising networks at will. As this study shows, it doesn't matter what vendor or combination of security in-depth tools an organization employs, hackers will continue to hack a system when they can exploit vulnerabilities in a network. At a minimum, organizations should include reducing waste on redundancy, backward-looking technologies and redeploying those resources on defenses designed to find and stop today's zero-day and advanced attacks.

6 IMPLICATION FOR PRACTIONERS AND RESEARCHERS

As this study has indicated, today's attacks often involve malware tailored to compromise a single vector. When such attack commences, they never stop until the objective is achieved. Typical security in-depth architecture

comprising of framework of discrete layers that include anti-virus software, intrusion-prevention systems, next generation firewalls, Web gateways, are poorly equipped to combat today's advanced attacks. However, without a comprehensive and cohesive analysis across all attack vectors, the current defense mechanism can miss the signs that an attacker has breached organization defenses.

7 CHALLENGES

A bigger challenge is foundational. The reason is because the cores in the typical architecture rely on a mix of binary signatures, blacklists, and reputation to identify threats. As the study showed, signatures are ineffective because antivirus (AV) vendors are not able to keep up with the speed of new malware binaries. This is because the malware is custom-made for specific target and as result, AV vendors will never be able to detect the malware and create signature for its defense. Other concerns include many attacks that exploit zero-day vulnerabilities and application blacklist that are blind to attacks because it uses encrypted binaries or hijack legitimate apps and processes. Further, reputable defenses such as Web gateways and IPS are not poised to stop attacks from newly setup universal resource locators [URLs] or compromised websites that are used as drive-by-downloads.

8 SUMMARY AND CONCLUSIONS

The study reveals that IT professionals were generally optimistic about the levels of their policies, technical control and mitigation implementation strategies; however, our finding proved that organizations could better align its investments and resources in order to cope with the advanced exposures and attacks as they develop. Phishing attacks, compliance policy violations, unsanctioned device and applications use, unauthorized data access, comprise the top list issues of concerns. Network device intelligence and system integrity, core components of all compliance frameworks and security best practices should be beefed up. The study concludes by noting that without a security policy, the availability of a network can be compromised. An adequate policy comprises of assessment of the risk to the network, organizing a response team, implementing a security change management practice, monitoring the network for security violations, maintaining a review process that modifies the existing policy and adapt to lessons learned.

9 REFERENCES

1. Anderson, Kerry A.; "A Case for a Partnership Between Information Security and Records Information Management," *ISACA Journal*, vol. 2, 2012, www.isaca.org/archives

2. 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

3. Steinbart, Paul John; Robyn L. Raschke; Graham Gal; William N. Dilla; "Information Security Professionals' Perceptions about the Relationship between the Information Security and Internal Audit Functions," forthcoming in the *Journal of Information Systems*, 2013

4. Baldor, Lolita C. (2013), ""US Ready to Strike Back Against China Cyberattacks," Yahoo News, 19 February 2013, http://news.yahoo.com/us-ready-strike-back-against-china-cyberattacks-225730552--finance.html

5. Oyemade, Ronke; "Effective IT Governance Through the Three Lines of Defense, Risk IT and COBIT," *ISACA Journal*, volume 1, 2012, www.isaca.org/archives

6. Tester, Darlene; "Is the TJ Hooper Case Relevant for Today's Information Security Environment?" *ISACA Journal*, vol. 2, 2013

7. Constantin, Lucian; "South Carolina Reveals Massive Data Breach," *PC World*, 27 October 2012, www.pcworld.com/article/2013186/south-carolina-reveals-massive-data-breach.html

8. Forrester,(2012), "Rethinking DLP: Introducing the Forrester DLP Maturity Grid," September 2012, www.forrester.com/Rethinking+DLP+Introducing+The+Forrester+DLP+Maturity+Grid/fulltext/-/E-RES61231

9. Gelbstein, Ed; "Strengthening Information Security Governance," *ISACA Journal*, vol. 2, 2012, www.isaca.org/archives

10. Mashable, "How Much Does Identity Theft Cost?," 28 January 2011, http://mashable.com/2011/01/28/identity-theft-infographic

11. Romanosky, Sasha; David Hoffman, Alessandro Acquisti, (2014), "Empirical Analysis of Data Breach Litigation," Temple University Beasley School of Law, Legal Studies research paper no. 2012-29, 2012, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461

12. Goldman, C. FreeWave Technologies. www.elp.com/articles/powergrid_international/print/volume-17/, 2012.

13. Steinbart, Paul John; Robyn L. Raschke; Graham Gal; William N. Dilla; "The Influence of Internal Audit on Information Security Effectiveness: Perceptions of Internal Auditors," working paper, 2013

Appendix I: Cybersecurity Survey Questionnaire

	1	2	3	4	5
Var001: Gender	Male	Female			
Var002: Executive or Senior IT Administrator?	Exec	Snr. IT			
Var003: How secure is the company network?	Very Secure	Secure	Somewhat Secure	Not Very Secure	Don't Know
Var004: How effective is the network security system of your organization?	Extremely Effective	Moderately Effective	Effective	Not Effective	Don't Know
Var005: Do you agree that investment in cybersecurity in 2013-2014....will provide the best systems solutions to thwart cyberattacks?	Extremely Agree	Moderately Agree	Agree	Disagree	Don't Know
Var006: Downtime is the greatest IT concern of my organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var007: Compliance is the greatest IT concern of my organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var008: eDiscovery is the greatest IT concern of my organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var009: Security Issues is the greatest IT concern of my organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var010: Network Growth is the greatest IT concern of my organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var011: User support is the greatest IT concern of my organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var012: Hackers are the groups that pose the greatest cybersecurity threat to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var013: Current & former employees are the groups that pose the greatest cybersecurity threat to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var014: Foreign Nation-states are the groups that pose the greatest cybersecurity threat to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var015: Organized crime are the groups that pose the greatest cybersecurity threat to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var016: Malware Analysis is the most proactive activity/technique used to counter persistent threats to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var017: Penetration Testing is the most proactive activity/technique used to counter persistent threats to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var018: Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var019: Analysis & Geolocation of IP Traffic is the most proactive activity/technique used to counter persistent threats to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var020: Subscription Services is the most proactive activity/technique used to counter persistent threats to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var021: Deep Packet Inspection is the most proactive activity/technique used to counter persistent threats to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var022: Examining External Footprint is the most proactive activity/technique used to counter persistent threats to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var023: Don't Know/Not Sure of the most proactive activity/technique used to counter persistent threats to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree
Var024: Document Watermarking & Tagging is the most proactive activity/technique used to counter persistent threats to your organization	Strongly Disagree	Disagree	Not Sure	Agree	Strongly Agree