Straddling the Next Cyber Frontier: The Empirical Analysis on Network Security, Exploits, and Vulnerabilities

Emmanuel U Opara[1], Oredola A. Soluade[2]
(Corresponding author: Emmanuel U Opara)

College of Business, Prairie View A&M University, Prairie View, Texas U.S.A. [1]
P.O. Box 519, MS 2310, Prairie View A&M University, Prairie View, Texas 77446
Iona College, Hagan School of Business, New Rochelle - New York [2]
(Email: euopara@pvamu.edu)
(Received Apr. 20, 2014; revised and accepted July 5, 2014)

Abstract

Network crime is rising at an exponential level because the world is so interconnected and the internet knows no borders. The magnitude of network breaches and attacks have changed in sophistication as incidents have increased significantly over the past few years. Security defenses at this present time are failing because, security teams are implementing outdated defensive arsenal. These experts are using legacy platforms that leverage technology that are dependent on signatures. However, in today's sophisticated network-attacks that occur across multiple vectors and stages, legacy platforms will not stand a chance to defend a network. This study will create threat awareness; identify who the network threat actors are, find out their capabilities, motivations and objective and identify best practices.
Keywords: Breaches, Exploits, Network Security, Threats, Vulnerabilities

1 Introduction

As enterprise systems evolve, Information Technology [IT] security needs to evolve even faster. Today's competitive platform presents an awkward conundrum. To maintain competitiveness in global market, organizations are under scrutiny to streamline operations and safeguard assets while keeping up with new technologies and maintaining usability of assets for employees, partners, vendors, investors etc. The need to balance speed with demand for security become paramount. In order for enterprise systems to build stronger customer relationship with their clients, they opened up their networks to remote employees, business partners and third parties. This resulting porosity of the network perimeter created security vulnerabilities and exploits in various systems, resulting in breaches and threats.

Network security threats as witnessed in 2013 exploded exponentially as security experts seek for solutions to undermine the potential threats. A number of new attacks in today's increasingly sophisticated toolkits include zero day attacks, Distributed Denial of Service (DDoS), and server-based botnets and encrypted layer attacks. These are just a few of the new attacks challenging organizations. Since 2012, these attacks have been continuous against U.S. financial institutions. This problem continues to be one of the most pressing challenges facing chief information security officers in the global systems. The new network breed of hackers are a new group with a potential or social agenda as noted by a recent study in [1]. This breed as the study will identify, implore sophisticated methods that uses evolving technologies that target network infrastructures. A recent breach was the "Target Corporation" incident. These criminals' capabilities of extracting value and intellectual properties from computers or networks of unsuspecting companies and governmental agencies have become a big business. Enterprise systems can no-longer ignore these threats.

No matter the size of these organizations, network security should be a top priority concern for all organizations. Enterprise networks are more vulnerable than ever due to the inherent risk of facilitating remote access in conjunction with the volume of traffic and the speed at which that traffic is flowing. As organizations migrate from gigabytes to terabytes capacity etc., managing, updating various applications, and closing loopholes at back-end systems becomes a monumental challenge.

Most foreign entities have identified that the four highest priority risk faced by most governments are those arising from international terrorism, network-attacks, international military crises and major accidents or natural hazards. Of this group, network-attacks ranked highest among the four high-priority risks. In recent year, study did show evidence in a series of highly advanced persistent attacks (APT) posed by organized crime and state-level entities, with attacks against

enterprises like Google, Coca-Cola, NASA and Lockheed Martin as reported in [2].

The potential impact of network-risk to a governmental entity, states, individuals and organizations, are very high. Some of these risks include, financial loss from theft or fraud, loss of invaluable customer information or intellectual property, possible fines from legal and regulatory bodies, loss of reputation through 'word of mouth', adverse press coverage and survival of the enterprise systems itself.

Other new attacks in today's increasingly sophisticated toolkits include Web exploits that target Java, mobile malware that target Android devices, server-based botnets and encrypted layer attacks. These are just a few of the new attack tools challenging organizations. Most recently, these tactics were leveraged by perpetrators in the attacks against U.S. financial institutions that have been ongoing since September 2012.

Our goal is to provide actionable intelligence to ensure organizations can better detect and mitigate threats that plague their network infrastructure,

As this study will indicate, network threat anecdotes or solutions have become routine within various organization, however, the barrage of alarms has not significantly raised survey respondents' understanding of who these network adversaries are, or what they target and how they operate.

Most of corporate executives have neither adequate knowledge of who the most serious threat actors are, nor do they have a network-security strategy to defend against them.

The key in this study is to create threat awareness; identify who the network threat actors are, find out their capabilities, motivations and objective. With this information, this study will recommend and develop an adequate network security strategy by providing the contextual background against which organizations can identify key assets that will likely be of interest to network adversaries. Such awareness and our result findings will help streamline methodologies for assessment of vulnerabilities to network-attacks which will come from potential network threat actors.

As the authors survey questions 12-15 [appendix 1] revealed, participants were asked, who the top network-threat actors are, that are menacing their organization. This question was raised because, most members of security teams, do not agree on what constitutes the most significant network-threat to their systems. The result of the survey will point us to a direction.

Also in questions 16-24 [appendix 1], survey respondents were asked to respond to the types of proactive tools used to counter Advanced Persistent Threat [APT]. These are commonly use terms to define remote attacks employed by sophisticated threats actors. These actors could be nation states or their intelligence services etc. Some of the intelligence services are classified as:

- Malware
- TCP/IP based network support tools
- Rogue device
- Network subnetting as geolocation of IP Traffic
- Distribution intrusion detection systems (DIDS)
- Deep Packet Inspection [DPI]

The survey results will point us to a direction. The findings from this study, will articulate the current network security measures enterprise systems will have to deploy to counter vulnerabilities, potential breaches and threats.

2 Literature Review

Steinbart, Raschke, Graham William [4] in their study noted that millions of pieces of malware and thousands of malicious hacker-gangs roam today's online world preying on easy unsuspecting exploits. These hackers as cited are seeking for backdoors and vulnerabilities in an un-suspected network so as to steal valuable data.

Vijayan [5], Goldman [6], Javelin [7], among others, cited that companies that have become more reliant on external internet connectivity for daily business operations are susceptible to financial loss if the network is compromised. Distributed denial of service (DDoS) attacks or worm outbreaks that affect a given network infrastructure can have devastating effect on that business as reported in [8].

Lockhart [9], in their report noted that enterprises and government agencies are under virtually constant attack on a daily basis. The report further cited that significant breaches at RSA, Global Payments, Automatic Data Processing, Symantec, International Monetary Fund, and a number of other organizations have made headlines—and undoubtedly

thousands more have occurred that have not been reported.

According to report in [2], Government infrastructure has come under attack from network espionage. This report summarized that several cases involving human errors indicated that the governmental agencies need to be more proactive when it comes to protecting critical infrastructures, intellectual property, economic data, employee records and sensitive information [2].

A recent study found that hacking incidences "represent more than one-quarter of the total recorded data breaches for 2013[3]. This according to the study was followed by Subcontractor (third party involvement) at 14.3% and Data on the Move at 13%. Insider Theft was identified in 11.7% of the breaches, Employee Error/Negligence accounted for 9.3% followed by accidental exposure at 7.5%" [3].

In another report by Lockhart [9], it was stated that more that 95% of all attacks tied to state-affiliated espionage employed phishing as a means of establishing a foothold in their intended victim's systems.

Early studies as reported by [7], [10], [11], showed that yesterday's workforce was monolithic. That means that workers were working within tightly controlled corporate perimeters, using computer terminals with limited capabilities and with restricted access to data. The average employee as a result was not a significant security risk to the enterprise system. Later studies by [6], [9], [12], [13], summarized that the rise of new technology has fragmented the monolith. This means that employees now use high-powered pocket-sized gadgets to access and manipulate a wealth of data, most of which is stored in the cloud. As a result, a mobile, fragmented working population that was made possible by combinations of cloud and mobile computing technologies created more opportunities for data breaches and network crimes.

More earlier studies by Skoudis [15], [16], [17], among others noted that "Advanced Exploit Development for Penetration Testers" teaches the skills required to reverse engineering 32-bit and 64-bit applications, performing remote user application and kernel debugging, analyze patches for 1-day exploits, and writing complex exploits, such as use-after-free attacks, against modern software and operating systems. These, will help security experts pinpoint vulnerabilities and develop fixes before damages are done to enterprise data.

Later studies by Lockhart [9], also summarized that to combat the ever-escalating danger posed by network security threats by enterprise systems, forward-thinking organizations have two options. These are to invest significantly in the people, processes and technology required to maintain world-class, 24/7 network security operations, or outsource the function to the growing number of highly effective managed security services providers (MSSPs).

3 Methodology

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

```
NONPAR CORR
  /VARIABLES=Var005 Var006 Var009 Var018 Var019
with Var001 Var002
  /PRINT=KENDALL TWOTAIL NOSIG
  /MISSING=PAIRWISE.
```

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 population. Most of the survey items were Likert scale types, yes/no responses or categorical, ordinal items, gender, ranks of personnel, etc.

The study conducted a survey of 23 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 non-parametric correlation analysis was done to determine the extent of collinearity among all the variables. It was discovered that there was significant correlation between Investment in network security and the use of rogue device scanning when broken down by gender. There was also a significant correlation between the respondent's perception of Downtime as the most effective network security in their organization, or perceiving security issues as the most effective

network security tool, or whether geolocation and IP traffic pose the greatest threat to their organization, when it is broken down by the status of the respondent.

Table 1: Non-parametric Correlation

Correlations

			Var001: Gender	Var002: Executive or Senior IT Administrator?
Kendall's tau_b	Var005: Do you agree that investment in cybersecurity in 2013-2014....will provide the best systems solutions to thwart cyberattacks?	Correlation Coefficient	.153*	.017
		Sig. (2-tailed)	**.020**	.792
		N	200	200
	Var006: Downtime is the greatest IT concern of my organization	Correlation Coefficient	-.044	.136
		Sig. (2-tailed)	.536	**.050**
		N	200	200
	Var009: Security Issues is the greatest IT concern of my organization	Correlation Coefficient	.122	.160*
		Sig. (2-tailed)	.079	**.021**
		N	200	200
	Var018: Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to your organization	Correlation Coefficient	-.138	.127
		Sig. (2-tailed)	**.050**	.072
		N	200	200
	Var019: Analysis & Geolocation of IP Traffic is the most proactive activity/technique used to counter persistent threats to your organization	Correlation Coefficient	-.052	.178*
		Sig. (2-tailed)	.459	**.011**
		N	200	200

*. Correlation is significant at the 0.05 level (2-tailed).

One basic question that required further investigation is the degree to which the responses between male and female respondents differed, regarding what they considered to be the greatest network security threat to their organization. The hypothesis is as follows:

H0: There is no significant difference in perspective between male and female respondents regarding whether Investment in network security in 2013 -2014 would increase with private software companies and system integrators and provide the best systems solutions to thwart network attacks.

H1: There is a significant difference in perspective

between male and female respondents regarding whether Investment in network security in 2013 -2014 would increase with private software companies and system integrators and provide the best systems solutions to thwart network attacks.

The test statistic was found to be t n-2 = 0.073. It can therefore be concluded that at the 5% significance level, there is not sufficient evidence that there is a significant difference in perspective between male and female respondents regarding whether Investment in network security in 2013 -2014 would increase with private software companies and system integrators and provide the best systems solutions to thwart network attacks.

Table 2: T-Test on Investment in Cybersecurity

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Var005: Investment in Cybersecurity	Equal variances assumed	.001	.977	-1.802	198	.073	-.314	.174	-.658	.030
	Equal variances not assumed			-1.798	191.025	.074	-.314	.175	-.658	.030

The second hypothesis that was tested was to determine if there is any difference in perspective between male and female respondents regarding whether Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to their organization.

H0: There is no significant difference in perspective between male and female respondents regarding whether Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to their organization.

H1: There is a significant difference in perspective between male and female respondents regarding whether Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to their organization.

The test statistic was found to be t n-2 = 0.050. It can therefore be concluded that at the 5% significance level, there is sufficient evidence that there is a significant difference in perspective between male and female respondents regarding whether Rogue Device Scanning is the most proactive activity/technique used to counter persistent threats to their organization.

The SPSS syntax for these tests is shown below:

```
T-TEST GROUPS=Var001(1 2)
/MISSING=ANALYSIS
/VARIABLES=Var005 Var018
/CRITERIA=CI(.95)
```

Table 3: T-Test for Rogue Device Scanning as the most proactive

Independent Samples Test										
		Levine's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Var018:Rogue Device Scanning is the most proactive	Equal variances assumed	16.113	.000	1.964	198	.051	.125	.064	-.001	.251
	Equal variances not assumed			1.986	197.907	.048	.125	.063	.001	.250

A third hypothesis was tested to determine if there is any difference in perspective between Senior IT Executives and Administrators in terms of how they Rate their company's IT concerns with regard to Downtime.

H0: There is no significant difference in perspective between Senior IT and Admin. Respondents in terms of how they Rate their company's IT concerns with regard to Downtime.

H1: There is a significant difference in perspective between Senior IT and Admin. respondents regarding how they Rate their company's IT concerns with regard to Downtime.

At the 5% significance level, there is sufficient evidence to conclude that there is a significant difference in perspective between Senior. IT Executives and Admin. respondents in terms of how they Rate their company's IT concerns with regard to Downtime. The test statistic was t n-2 = 0.050.

A fourth hypotheses was tested to determine if there is any difference in perspective between Senior IT Executives and Administrators in terms of how they Rate their company's IT concerns with regard to Security Issues.

H0: There is no significant difference in perspective between senior IT and Admin. respondents regarding how they Rate their company's IT concerns with regard to Security Issues.

H1: There is a significant difference in perspective between senior IT and Admin. respondents regarding how they Rate their company's IT concerns with regard to Security Issues.

Table 4: T-Test on Downtime as greatest IT concern

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Var006: Downtime is the greatest IT concern	Equal variances assumed	22.862	.000	-1.926	198	.050	-.158	.082	-.319	.004
	Equal variances not assumed			-2.480	56.250	.016	-.158	.064	-.285	-.030

Table 5: T-Test on Security Issues as greatest IT concern

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Var009: Security Issues is the greatest IT concern	Equal variances assumed	20.432	.000	-2.375	198	.019	-.271	.114	-.496	-.046
	Equal variances not assumed			-3.029	55.420	.004	-.271	.090	-.451	-.092

At the 5% significance level, there is sufficient evidence to conclude that there is a significant difference in perspective between Senior. IT and Admin. respondents regarding how they Rate your company's IT concerns with regard to Security Issues.

The test statistic was t n-2=0.019 or 0.004; which justifies the conclusion that there is a significant difference between the two groups. A fifth hypotheses was tested to determine if there is any difference in perspective between Senior IT Executives and Administrators in terms of whether geolocation and IP traffic poses the greatest network security threat to their organization.

H0: There is no significant difference in perspective between Senior IT and Admin. respondents in terms of whether geolocation and IP traffic poses the greatest network security threat to their organization.

H1: There is a significant difference in perspective between Senior IT and Admin. respondents in terms of whether geolocation and IP traffic poses the greatest network security threat to their organization.

The SPSS syntax for these tests is shown below:

```
T-TEST GROUPS=Var002(1 2)
  /MISSING=ANALYSIS
  /VARIABLES=Var006 Var009 Var019
  /CRITERIA=CI(.95).
```

Table 6: T-Test on Geolocation of IP Traffic

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Var019: Analysis & Geolocation of IP Traffic	Equal variances assumed	35.230	.000	-2.483	198	.014	-.240	.097	-.431	-.049
	Equal variances not assumed			-4.607	139.546	.000	-.240	.052	-.343	-.137

Overall Conclusion

Quite a number of tests were run comparing responses of male versus female respondents, as well as between Senior IT Executives and Administrators. The results presented here are the ones that indicated a significant difference between the two groups. In addition, the correlation coefficients among all the variables are low– so the assumption of a t-test based on independent samples is validated. All these results were based only on the assumption of homogeneity of variance or homoscedasticity.

5 Implication for Practitioners and Researchers

Exposure to securities litigation following the disclosure of a network-security breach should be a concern to management. Also the impact such an announcement would have on the stock prices of compromised companies should also be a concern. However, announcements of network breaches, in 2013 by Facebook and Apple did not affect the companies' share prices. Despite the high-profile disclosures, these companies were not hit with securities lawsuits about the breaches, either. More studies will be devoted to this concern.

6 Challenges

National state agencies and enterprise systems depend on digital processes, data and a network system to function effectively. This makes them increasingly vulnerable to being manipulated. Network security is about ensuring that enterprise network is resilient to prevent fraud, breaches, theft of sensitive data or business disruption, and the severe risks to reputation that comes with it. Having an Incident Response policy and plan in place is a crucial first step to ensuring that organization has the information and processes needed to respond to a security breach. However, most organizations lack the expertise and resources to perform incident and penetration testing that could disprove a false positive breach result.

7 Summary and Conclusion

The study has shown that continuous monitoring of network infrastructure with proper penetration, detection testing and analyses of the results, will remedy security exploits and vulnerabilities. Also understanding that most modern networks rely on the TCP/IP protocol suite. Network security implications must be considered before proceeding with TCP/IP network designs. Since subnetting separates a network into multiple logically defined segments or subsets, each subnet's traffic must be separated from each other subnet's traffic to harden the network topology.

This study concludes that breach prevention strategies should include adequate risk assessment, mitigation, compliance, breach preparedness etc. Risk assessment should examine all the risk factors an organization encountered during a data breach. A penetration testing and analyses should provide a detailed assessment and remedies for mitigating an exploit. Mitigation and compliance methodology should ensure that an organization enforces the rules, regulations and laws that will help provide extensive regulatory assessments. Also organizations should strive to identify and create the right policies, an efficient incident workflow, establish a network-incident response team' (CIRT). Breach preparedness help create a customized data breach response plan that minimizes the impact of an incidence.

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] Rapid7 Report (2012): "Data Breaches in the Government Sector." Rapid7. September 6, 2012. http://www.rapid7.com.

[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] 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

[5] Vijayan, J. (2006), "Possible S&P Security Holes Reveal Risks of E-Commerce," Computerworld, 34(22), May, 29 6.

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

[7] Javelin, "2009 Identity Fraud Survey Report Consumer Version (2009)," Javelin Strategy and Research, February 2009.

[8] Rob, M., & Opara, E. (2003), "Online Credit Card Processing Models: Critical Issues to Consider by Small Merchants,'' Human Systems Management, 22(3), 133-142.

[9] Lockhart, B. and Gohn, B. Utility Network security: Seven Key Smart Grid Security Trends to Watch in 2012 and Beyond. Pike Research. 2011.

[10] Alhazmi et al., (2006). "Measuring, analyzing and predicting security vulnerabilities in software systems", Computers & Security (2006), doi:10.1016/j.cose.2006.10.002.

[11] Holz, T, Gorecki, C Rieck, K and Freiling. F. (2008), "Measuring and detecting fast-flux service networks". In Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS 08) NDSS.

[12] 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.

[13] 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.

[14] Scholtz, T. (2004), "The Benefits of an Information Security Architecture," Meta Group, December.

[15] Skoudis, E. (2005), "Five Malicious Code Myths and How to Protect Yourself in 2005,"SearchSecurity.com, Retrieved January 4, from, (http://searchsecurity.techtarget.com/tip/1,289483,sid14_gcu041736,00.html)

[16] Antonopoulos. A, (2008) "Georgia network war overblown". *Network World*, August 19, 2008 (http://www.pcworld.com/businesscenter/article/150021/georgia_networkwar_overblown.html).

[17] Endeavor, et.al [2009]. Conference for Homeland Security 2009 (CATCH '09), Network security Applications and Technology, March 3–4, 2009. The IEEE proceedings of this conference include relevant papers on detection and mitigation of botnets, as well as correlation and collaboration in cross-domain attacks, from the University of Michigan and Georgia Tech. *Network & Distributed System Security (NDSS) Symposium*, February 2008.

Dr. Emmanuel U Opara is an Associate Professor of Management Information Systems at the College of Business, Prairie View A&M University. He teaches Networking, Cyber Securities, E-Commerce Technologies, and Strategic IT Management, Information Systems, and Fundamentals of MIS.

He has interest in Integrated Network Systems Securities, Biometrics Technology, Data Communication, Strategic IT Management and Decision Making, SAP-ERP, HANA Technology.

His passion is in computer forensics, vulnerability and exploits discovery, intrusion detection/prevention analysis, incident response and penetration testing while deploying python programming.

Prior to joining the Texas A&M Systems, at Prairie View, he worked for Chevron Corporation as a Systems Analyst. He also worked in the upstream division.

Dr. Opara received commendations for his contributions in the field of Information technology and cyber security.

Dr. Oredola A. Soluade is currently an Associate Professor of Information Systems at Iona College, where he teaches, among other courses, Information Systems, Production & Operations Management, Statistics, and Quantitative Tools for Management.

Prior to joining Iona College, Dr. Soluade taught for several years in the field of mechanical engineering, specializing in Thermodynamics and Heat Transfer.

His current research interests include: Quality Assurance in an Interactive Voice Response System, as well as Statistical

Analysis of the automobile industry. Dr. Soluade is the author of an Operations Management book published by McGraw-Hill.

Dr. Soluade has served as guest editor of an International Journal of Business Continuity and Risk Management, and

has contributed chapters to a book on Risk Management. He is a Cisco Certified Network Associate, and a member of the Editorial Board of the International Information Management Association.

Dr. Soluade holds a bachelor's degree in mechanical engineering, a master's degree in mechanical engineering, a master's degree in Operations Research, and a doctorate in Operations Research.

Appendix 1: Network-Security Survey Questionnaire

1	**Select Gender Male = 1; Female = 2**								
2	**Are you an executive or a senior IT administrator? Yes = 1 No = 2**								
3	**How secured do you think your company network is?**								
4	**How strongly do you agree to the effectiveness of the Network security systems of your organization?**								
5	Do you agree that investment in networksecurity in 2013 -2014 that would increase with private software companies and system integrators will provide the best systems solutions to thwart network-attacks [Extremely agree, Moderately agree, Agree, disagree, Don't know]								
On a scale of 1 [least] to 5 [most], rate your company's daily IT concerns									
6	**Downtime**				1	2	3	4	5
7	**Compliance**				1	2	3	4	5
8	**eDiscovery**				1	2	3	4	5
9	**Security Issues**				1	2	3	4	5
10	**Network Growth**				1	2	3	4	5
11	**User support**				1	2	3	4	5
On a scale of 1 [least] to 5 [most], rate the groups that poses the greatest networksecurity threat to your organization									
12	Hackers				1	2	3	4	5
13	Current and former employees				1	2	3	4	5
14	Foreign nation-states examples China, Russia, North Korea,				1	2	3	4	5
15	Organized crime				1	2	3	4	5
On a scale of 1 [least] to 5 [most], rate the following proactive activities and techniques that your organization uses to counter advance persistent threats to your organization?									
16	Malware analysis				1	2	3	4	5
17	Inspection of outbound traffic				1	2	3	4	5
18	Rogue device scanning				1	2	3	4	5
19	Analysis and relocation of IP traffics				1	2	3	4	5
20	Subscription services				1	2	3	4	5
21	Deep packet inspection				1	2	3	4	5
22	Examining external footprint				1	2	3	4	5
23	Don't know; not sure				1	2	3	4	5
24	Document watermarking/tagging				1	2	3	4	5