EXPLORING THE STRATEGIES NETWORK SECURITY MANAGERS NEED TO PROTECT THEIR NETWORKS FROM BACKDOOR INTRUSIONS

A Dissertation Presented in Partial Fulfillment of the Requirements for the Degree of Doctor of Computer Science

By

Luis Omar Rivera-Lopez

Colorado Technical University

November, 2018

Committee

Debra Burrington, Ph.D., Chair

Kelly L. Hughes, DCS, Committee Member

Mary L. Lind, Ph.D., Committee Member

November 2, 2018
Date Approved

Abstract

The problem addressed is the strategies network security managers need to protect their networks from backdoor intrusions. Twelve participants that had experience as network managers or systems administrators were interviewed using nine open-ended questions. The research methodology chosen for this study is a qualitative exploratory approach. The findings on this research resulted in four major themes including human factor, backdoor detection techniques, defense-in-depth and network monitoring strategies. The three prominent topics found were involvement of management, effective administrative policies and ethical hacking services. The analysis based on the responses provided details related to strategies needed to protect networks from backdoor intrusions relying on the experience of twelve participants. The implications for practice in the cybersecurity and information assurance field suggests that current backdoor detection techniques are complex and challenges are still present in order to enhance strategies to deter backdoor intrusions.

Keywords: backdoor, network defense strategies, network countermeasures

Dedication

To my wife, Kari Ann Edwards.

Acknowledgements

After 14 arduous months, my dissertation is finally complete. This would not be the case however, where it not for a few very important people who kicked me into gear and kept pushing me to work.

My deepest thanks go out to Dr. Debra Burrington who never gave up on me, offering both guidance and motivation. Without your dedication, I would not be writing this.

To Dr. Rae Denise Madison, Dr. Steven H. Munkeby, and Dr. Marva Brewington, for giving me the advice and knowledge I needed to make my dream a reality. To my loving wife Kari, for all of your help and sacrifice; with your support I was able to focus all of my time on this project.

Table of Contents

Table of Contents v

List of Tables x

List of Figures xiv

Chapter One 1

Topic Overview/Background 2

Problem Statement 3

Purpose Statement 3

Research Question 4

Propositions 4

Conceptual Framework 5

Assumptions/Biases 6

Significance of the Study 8

Delimitations 9

Limitations 10

Definition of Terms 10

General Overview of the Research Design 11

Summary of Chapter One 12

Organization of Dissertation 14

Chapter Two 15

Synthesis of the Literature 17

Four Strategies to Defend and Secure IT networks from backdoor intrusions 19

A Brief History of Information Technology (IT) Network Security 19

Defense-in-Depth Strategy 21

Defense Countermeasures as a Strategy 22

Network Perimeter 23

Enclave Boundary 24

Host Computers 24

Information Assurance Core Principles 25

Defense Tools & Practices Strategy 27

Strategic Use of Many Security Technologies and Network Management Tools 28

Firewall Practice on Networks 32

Network Operations Best Practices 33

Defense Funding (Cost) & Staffing Strategy 34

Defense Funding Allocated for the Information Technology Department 34

Possible Lower Cost Solutions for Information Technology (IT) Departments 35

Cost of Staffing and Devices 36

Defense Culture & Awareness Strategy 36

Importance of Ethics 36

Shared Culture Values 37

Information Technology (IT) Best Practices 38

Sharing Intrusion Response System Techniques 38

Information Security Awareness 39

Human Behavior 40

Information Assurance and Enterprise Information Systems Awareness 41

Conceptual Framework 43

Summary of Literature Review 45

Chapter Three 47

Research Tradition 48

Research Question 49

Research Design 49

Population and Sample 50

Sampling Procedure 51

Instrumentation 52

Validity 53

Reliability 54

Data Collection 55

Data Analysis 55

Ethical Considerations 56

Summary of Chapter Three 58

Chapter Four 59
Participant Demographics 59
Presentation of the Data 62
Interview Question 1 64
Interview Question 2 71
Interview Question 3 78
Interview Question 4 85
Interview Question 5 91
Interview Question 6 98
Interview Question 7 106
Interview Question 8 113
Interview Question 9 120
Presentation and Discussion of Findings 128
Summary of Chapter Four 133
Chapter Five 134
Findings and Conclusions 135
Major Theme 1: Human Factor 143
Major Theme 2: Defense-in-Depth Strategies 143
Major Theme 3: Backdoor Detection Techniques 144
Major Theme 4: Network Monitoring Strategies 145

Prominent Topic 1: Involvement of Management 146
Prominent Topic 2: Effective Administrative Policies 146
Prominent Topic 3: Ethical Hacking Services 147
Limitations of the Study 147
Implications for Practice 148
Recommendation 1 149
Recommendation 2 149
Recommendation 3 149
Recommendation 4 150
Implications of Study and Recommendations for Future Research 150
Conclusion 151
Human Factor 153
Defense-in-Depth Strategies 153
Backdoor Detection Techniques 154
Network Monitoring Strategies 155
References 156
Appendix A 173
Appendix B 176
Appendix C 182

List of Tables

Table 1 *Participant Demographics*……...60

Table 2 *Additional Statistics from Participants*..……...61

Table 3 *Themes for Interview Question 1*……..64

Table 4 *Interview Question 1, Theme 1 Responses: Protect Data*..……..65

Table 5 *Interview Question 1, Theme 2 Responses: Risk Analysis* ……...……66

Table 6 *Interview Question 1, Theme 3 Responses: Recommend Findings*…….…….67

Table 7 *Interview Question 1, Theme 4 Responses: Monitoring Team* ……...…68

Table 8 *Interview Question 1, Theme 5 Responses: Internal Message Alerts* …….....69

Table 9 *Interview Question 1, Theme 6 Responses: Log Notifications* ……..…….70

Table 10 *Interview Question 1, Theme 7 Responses: Third Party Services* …….……..….71

Table 11 *Themes for Interview Question 2*…….....72

Table 12 *Interview Question 2, Theme 1 Responses: Backdoor Analysis*…….....72

Table 13 *Interview Question 2, Theme 2 Responses: Brute Force*……...….73

Table 14 *Interview Question 2, Theme 3 Responses: Backdoors Detection* ..…….….74

Table 15 *Interview Question 2, Theme 4 Responses: Phishing Emails* ……....75

Table 16 Interview Question 2, Theme 5 Responses: *Compartmentalized Email Gateways* ...…76

Table 17 *Interview Question 2, Theme 6 Responses: Zero Day* ……...……...77

Table 18 *Interview Question 2, Theme 7 Responses: Identifying Backdoors*…….…...78

Table 19 *Themes for Interview Question 3*…….…...79

Table 20 *Interview Question 3, Theme 1 Responses: Executive* ……..……79

Table 21 *Interview Question 3, Theme 2 Responses: Organizational* ……..…….....80

Table 22 *Interview Question 3, Theme 3 Responses: Information Technology*……..……..…81

Table 23 *Interview Question 3, Theme 4 Responses: Client* ……...…...…..…82

Table 24 Interview Question 3, Theme 5 Responses: Financial …….……..83

Table 25 *Interview Question 3, Theme 6 Responses: Staffing* …….…….....84

Table 26 *Interview Question 3, Theme 7 Responses: Leadership*…….……85

Table 27 *Themes for Interview Question 4*……....86

Table 28 *Interview Question 4, Theme 1 Responses: Notify Upper Management* …….……..86

Table 29 *Interview Question 4, Theme 2 Responses: Systems Update* ……..…….…..87

Table 30 *Interview Question 4, Theme 3 Responses: Collecting Evidence*……..…….…....88

Table 31 *Interview Question 4, Theme 4 Responses: Isolate Devices* ……..…...89

Table 32 *Interview Question 4, Theme 5 Responses: Backdoor Issue* …….90

Table 33 *Interview Question 4, Theme 6 Responses: Firmware*……..……90

Table 34 *Themes for Interview Question 5*……....91

Table 35 *Interview Question 5, Theme 1 Responses: Educate and Share* ……...…92

Table 36 *Interview Question 5, Theme 2 Responses: Investigate Network Sections*…….93

Table 37 *Interview Question 5, Theme 3 Responses: Disabling Traffic* ……...…..94

Table 38 *Interview Question 5, Theme 4 Responses: Counter Intrusion Service* …….....95

Table 39 *Interview Question 5, Theme 5 Responses: Isolate software* …….…..…..96

Table 40 *Interview Question 5, Theme 6 Responses: Identify Anomalies* …….…...……97

Table 41 *Interview Question 5, Theme 7 Responses: Stopping Traffic*……...…..98

Table 42 *Themes for Interview Question 6*……..…….99

Table 43 *Interview Question 6, Theme 1 Responses: Certifications* ……...…...100

Table 44 *Interview Question 6, Theme 2 Responses: Awareness* …….…..101

Table 45 *Interview Question 6, Theme 3 Responses: Expertise*……..…102

Table 46 *Interview Question 6, Theme 4 Responses: Culture* …….……...…...103

Table 47 *Interview Question 6, Theme 5 Responses: Teamwork* ……..….....104

Table 48 *Interview Question 6, Theme 6 Responses: Weakest Link* …….....….105

Table 49: *Interview Question 6, Theme 7 Responses: Network Protocol Analysis* …….…..106

Table 50 *Themes for Interview Question 7*…….…….107

Table 51 *Interview Question 7, Theme 1 Responses: Dynamic Awareness* ……..….107

Table 52 *Interview Question 7, Theme 2 Responses: Understanding Defense*…….....….108

Table 53 *Interview Question 7, Theme 3 Responses: Network Security*……...…….…109

Table 54 *Interview Question 7, Theme 4 Responses: Understanding Threats* …….…...…...110

Table 55 *Interview Question 7, Theme 5 Responses: Human Factor*……...…..111

Table 56 *Interview Question 7, Theme 6 Responses: Enforcing Defense*…….……...….112

Table 57 *Interview Question 7, Theme 7 Responses: Defense Tasks* …….…...113

Table 58 *Themes for Interview Question 8*…….….114

Table 59 *Interview Question 8, Theme 1 Responses: Weak Network Sections*……..….114

Table 60 *Interview Question 8, Theme 2 Responses: Network Layers*……..….115

Table 61 *Interview Question 8, Theme 3 Responses: Access Points*…….…..117

Table 62 *Interview Question 8, Theme 4 Responses: Defense-in-depth*……...….118

Table 63 *Interview Question 8, Theme 5 Responses: Network Segmentation*……..……..…...119

Table 64 *Interview Question 8, Theme 6 Responses: Internal Network Defense*……..…..119

Table 65 *Interview Question 8, Theme 7 Responses: Strategic Value*…….……...…120

Table 66 *Themes for Interview Question 9*…….….121

Table 67 *Interview Question 9, Theme 1 Responses: Internet Security*…….….121

Table 68 *Interview Question 9, Theme 2 Responses: Risk Assessment Team*……..…123

Table 69 *Interview Question 9, Theme 3 Responses: Leaders*…….……...……124

Table 70 *Interview Question 9, Theme 4 Responses: Ethical Hacking*……..…..…125

Table 71 *Interview Question 9, Theme 5 Responses: Administrative Policies*……..…..….126

Table 72 *Interview Question 9, Theme 6 Response: Cloud Security*…….…..……126

Table 73 *Interview Question 9, Theme 7 Responses: Wireless Security*……..……..….127

Table 74 *Themes and Topics Emerging from the 12 Interviews*…….……..…...128

Table 75 *Major Themes and Prominent Topics of Research Data*……..…...132

List of Figures

Figure 1 *Low Cost-Effective Information Assurance Program* ……..……..…35

Figure 2 *Conceptual Framework* ……..……45

CHAPTER ONE

Defense-in-depth is an essential principle in the field of information assurance. It is used as a strategy based on adding layers of security to information systems because no single product can detect multiple cyberattacks that happen simultaneously (Boggs, Du, & Stolfo, 2014). This important principle has been widely adopted by the United States Department of Defense and its information assurance policies. Best practices and product reviews support organizations in designing their defense-in-depth strategy (Boggs et al., 2014). One of the issues with the defense-in-depth strategy is when a business transfers large amounts of data, this can result in a weakness against the fiber route passing the data (Goztepe, Kilic, & Kayaalp, 2014), thus making the system vulnerable to backdoor intrusions. Choi and Cho (2013) stated that many policies are needed to detect backdoors. These backdoors are easy to install on network devices and are subject to exploits contributing to the weakening of the defense-in-depth strategy.

According to Almorsy, Grundy, and Ibrahim (2013), defense-in-depth is a process that takes a long time to identify threats and is based on adding layers of security to computer network systems. Information assurance professionals implement security controls as part of a strategy to ensure the network infrastructure of the organization is protected by adding security layers to the system. It is unknown if network administrators have the tools to detect stealth intrusions entering the network systems via unknown network devices. Poonia (2014) stated the development of information technology has made it possible for cybercrimes to happen. Also, he declared that information could be obtained from logs, including added backdoors.

The networks and infrastructures framework area relies on the principle of defense-in-depth, in which many security layers are added in order to protect information and computer systems. For example, malware can be installed in networks, resulting in systems creating bots

that can open backdoor intrusions to computers (Crossler & Bélanger, 2014). Weak points in networks can enable backdoor intrusions and compromise the operation of information systems which can then be exploited by attackers (Fielder & Hankin, 2016). Mansfield-Devine (2016) argued that defense-in-depth causes challenges by not knowing exactly what is going on in the networks, resulting in misunderstandings on security devices. Governments, corporations and the public depend on computer information systems whether the network is used at the workplace, at home or on mobile devices. Investigating strategies needed to protect networks from backdoor intrusions can benefit network managers and systems administrators. The disconnection between assuring and securing information affects strategies used by Information Technology (IT) departments to defend their computer network needed to support the parent organization.

Topic Overview/Background

Software developers insert backdoors into applications, leaving the application layer of the open system interconnection model (OSI model) vulnerable to backdoor attacks (Pant & Khairnar, 2014). Defense-in-depth is an information security practice used by the military for the purpose of forcing cyber attackers to overcome many obstacles (Cleghorn, 2013). The topic of interest discussed in this work is the strategies network security managers need to protect their networks from backdoor intrusions. Backdoor intrusions can be created by a malware that slows down the daily operation of systems causing damage to devices. This affects the productivity of business entities, governments and the public in general.

The area of focus for this research was the strategies network security managers need to protect their networks from backdoor intrusions. The strategies used to protect networks suggests the possibility that adding too many layers of defense technologies can trigger an increase in the amount of administrative overhead resulting from a defense-in-depth weakness in network systems (Cleghorn, 2013). The defense-in-depth architecture must balance security with

administrative overhead to adequately defend resources at different layers of the open systems interconnection (OSI) model. This is a concern for many businesses, governments and other public networks accessing the Internet.

According to Cleghorn (2013), layering multiple technologies that are installed in the system that have been acquired from different vendors increases administrative overhead and must be appropriately handled by system administrators. This research was necessary because there is a gap in knowledge related to what leads ultimately to organizations deciding to put effective strategies in place to secure their networks. There is a need for better handling of this growing strategic problem in networks to enhance strategic solutions enabling better protection against backdoor intrusions for business, government and public use of network information systems.

Problem Statement

The problem addressed in the study was the strategies network security managers need to protect their networks from backdoor intrusions. Current detection techniques are designed to search for vulnerabilities or ways to infiltrate Information Technology (IT) assets, but they still possess serious issues and challenges due to cyber scanning campaigns that render current detection techniques impractical (Bou-Harb, Debbabi, & Assi, 2014). The use of millions of botnets that can access backdoors introduces sophisticated stealth scanning strategies, representing a disastrous advancement in modern malware (Dainotti, King, Claffy, Papale, & Pescapé, 2015). This malware evolution degrades the network defense strategies used by IT departments and negatively affects the business of their parent enterprise.

Purpose Statement

The purpose of this qualitative study was to explore the strategies network security managers need to protect their networks from backdoor intrusions. According to Awan, Memon,

Khan, Noonari, Hussain, and Usman (2017), the United States uses a cybersecurity strategy called Cybersecurity Policy Review where the key area is to defend the network from malicious cyber actors such as backdoor intrusions. The study provides strategies that IT managers use in order to explore if the defense-in-depth principle reveals possible weaknesses instead of adding strength to the system. Hyden, Moskowitz, and Russell (2016) concluded that their strategy is to manage risk and security of the network through observing information about the network to estimate its threatened nodes in order to offer real-time risk management suggesting a good strategy against backdoor intrusions. Parameshwarappa, Chen and Gangopadhyay (2018) analyzed backdoor intrusion attacks that can adapt to rule-based intrusion detection systems in order to evade detection; their analysis suggests that network security managers might not have the correct tools to evade backdoor intrusions.

This study explored gaps that network security managers are not taking into consideration while protecting their networks from backdoor intrusions. Chen, Liu, Li, Lu, and Song (2017) stated that backdoor attacks can poison the strategies of adversaries because the goal of the attacker is to mislead. The research method was of a qualitative nature to provide information on how IT managers perceive backdoor attacks in their network systems and what countermeasures they apply to minimize cyber-attacks related to backdoor incidents. The results of this research can be of use to practitioners as well as future researchers.

Research Question

What are the strategies network security managers need to protect their networks from backdoor intrusions?

Propositions

The study focused on the strategies network security managers need to protect their networks from backdoor intrusions. According to Tehranipoor, Salmani, and Zhang (2014), there

is an essential issue with integrated circuits reported to bypass security that can open a backdoor available to be exploited by hackers or hacking machines. This allows cyberattacks to take place through these Trojan circuits that can connect to networks with low controllability and observability. These backdoor intrusions are also known as unseen scan-based attacks (Ren & Tavares, 2016). Backdoor intrusions affect the strategies of network managers, especially when backdoor intrusions are unseen by network administrators. Moustafa and Slay (2015) stated that numerous studies showed backdoor intrusion datasets do not reflect network traffic attacks, showing a gap in network intrusion detection systems. Wu, Ganesan, Hu, Wong, Wong, and Mitra (2016) presented an approach to detect backdoor intrusions during system operations that network managers might not be aware that is available, because, backdoors can be access in devices throughout the network especially in IT departments that many businesses depend upon to perform their daily network operations. This study explored the strategies network security managers need to protect their networks from backdoor intrusions.

Conceptual Framework

Goodyear, Barela, Jewiss, and Usinger (2014) stated that a robust conceptual framework is needed in order to guide data collection and analysis. The conceptual framework in this study holds four defense strategies necessary in the field of information assurance to secure network systems from backdoor intrusions. The first strategy is to enforce an active information assurance defense-in-depth approach which balances three critical elements: people, technology, and operations. Xingguo, Qing, Zheng, and Jiangxing (2016) stated that active defense technologies work best against backdoor intrusions versus passive defense technology because the active approach enables detection before the system gets compromised.

The second strategy is to include defense tools & practices to mitigate backdoor intrusions. Ji-Ho, Han, and Geuk (2016) suggested an intrusion prevention method using log file

and password to overcome integrity check failed in most intrusion detection system tools. Parameshwarappa et al., (2018) studied attack strategies against rule-based intrusion detection system tools to prevent cyberattacks that can be useful for network security managers.

The third strategy is having defense funding and staffing available to enforce information assurance policies and procedures that can ensure personnel know their roles and responsibilities and that they are aware of their hardware device vulnerabilities to implement protection of those devices against backdoor attacks. For example, using a technique called Correlation Policy, Li and Zhang (2015) came up with an intrusion protection system making up for a firewall, a honeypot, and an intrusion detection system.

The fourth strategy is the defense culture and awareness strategy that should ensure that an organization has members with the ability to protect the network from hardware-based attacks and use countermeasures to defend against such intrusions. Farhaoui (2016) declared that human mistakes cause internal faults to systems enabling backdoor intrusions. A defense culture concept must be enforced within all personnel in the organization spreading the idea of defending the network against backdoor intrusions. The objective of the conceptual framework was to enhance information assurance strategies for the use of information technology departments.

Assumptions/Biases

Assumptions are thoughts that rely on experience, education, common sense, intuition and beliefs that are necessary to conduct the research and are foundational givens assumed to be true (Simon & Goes, 2013; Willis, Jost, & Nilakanta, 2007). The first key assumption in the knowledge of network defense from the information assurance perspective is that the defense-in-depth strategy makes the network safer against backdoor intrusions due to various defense technologies and layers added in the network system that cause the infrastructure to become redundant. Mavroeidakos, Michalas, and Vergados (2016) proposed a defense-in-depth security

architecture dividing the network into defense zones in order to achieve better security controls. The second fundamental assumption is that information technology administrators are required to work with network issues when their procedures fail to give expected results in the situation when they cannot detect stealth backdoor attacks when these hidden backdoor intrusions have breached their networks. Akhmetov, Lakhno, Boiko and Mishchenko (2017) stated that incomplete information on designing integrated systems for information protection is a weak attribute suggesting an IT infrastructure weakness from the start.

The third key assumption is that although network infrastructure is well financed, backdoor intrusions are still damaging systems and causing monetary losses to small and medium-sized businesses and government agencies. According to Vasiu and Vasiu (2017) misappropriation of trade secrets for monetary benefits can result in loss of sales affecting the enterprise. The fourth key assumption is that information technology employees and staff are scheduled to conduct network security training. However, some employees still cause breaches (e.g., hacking, data extrusion and other similar cases). Bucak (2016) confirmed that not taking the thoughts, behavior, and feelings of employees into account results in negative behavior affecting information security. Finally, the IT infrastructure weakness is the fifth key assumption that allows backdoor intrusions to be a problem that affects not only the IT department but its parent organization. Khan and Hasan (2017) stated that firewall administrators configure the network perimeters to filter data packets as a security measure for networks.

A key feature of taking a qualitative approach in research is the subjective position of the researcher based on the topic they select as a key component of the research process guiding the research from biases that can potentially influence the analysis of data in a study (Goodyear et al., 2014; Simon & Goes, 2013). The following facts are reasons that could potentially reflect

bias in the study on the part of the researcher: first, the lack of experience working in any position in the IT department. Positions range from help desk up to Chief Information Officer. Gilbert (2000) stated that at a minimum, researchers filter what they experience in the research process through their own biases. Second, the researcher does not have any certifications related to jobs in the information security field. Certifications can range from CISSP, Security plus to network security certifications. The researcher lacks other skills such as outstanding computer programming and high-level mathematics that can affect a complete understanding of how backdoor code works and how they are built. There are many reasons that a study can yield compromised results because of the investigator being biased (Willis, Jost, & Nilakanta, 2007). Also, the lack of experience making strategic decisions on enterprise network using software tools and knowing the relationship between the mission of the network and the business objective is also a bias that can affect the study. There are concerns in locating and eliminating possible sources of bias or making the research as much like the real world as possible (Robson, 1993; cited in (Bauer & Gaskell, 2000).

Significance of the Study

There is a need for enhancing network security strategies to benefit network managers and their IT departments against backdoor intrusions. He (2017) stated that firewall technology is a strategy that protects the network from backdoor intrusions but it is difficult to provide a consistent security strategy for the user. Sabillon, Cano, Cavaller, and Serra (2016) confirmed that backdoor intrusions are capable of disabling firewalls, generating fake traffic and deleting system files. A Trojan horse allows a backdoor intrusion that can be activated by specific actions on network systems affecting the strategy network managers used to secure the network from backdoors.

The study is significant because, for decades, the defense-in-depth strategy has been a model for many different types of business and government entities, including the public sector when using cloud services. Yu, Li, Li, Zhao, and Zhao (2017) stated that cloud computing is an IT paradigm where services are provided to people using internet technologies. Smith and Green (2017) declared that surveillance backdoors could damage the reputation of standardization of committees. Network managers can have their reputation affected as a result of surveillance backdoors including damage to ethics and collateral damage.

This study argues backdoor intrusions continue to occur due to unthoughtful strategies allowing backdoor intrusions. Akhunzada, Ahmed, Gani, Khan, Imran and Guizani (2015) stated that backdoor intrusion attacks would lead to illegal access to the network. Having multiple layers of defense makes hard for network managers to figure out when and where backdoor intrusions took place for illegal access to occur. Pierson and DeHaan (2015) declared that in theory doing business on the Internet is cost effective but in practice damage caused by backdoor intrusions can be very expensive and not easy to manage. The study investigated current network defense strategies used by managers that may reveal gaps in defensive strategies needed against backdoor intrusions.

Delimitations

According to Simon and Goes (2013), delimitations are qualities or traits that arise from boundaries the researcher chooses and places around the study. The study focused on strategies IT network managers use to defend the systems against backdoor intrusions. The first delimitation was the time constraint allowing up to an hour for interviews as the period scheduled set to question each participant. The second delimitation was focusing the study in one geographical location where participants were investigated.

Limitations

Limitations are inherent characteristics of method and design (Simon & Goes, 2013). Limitations are aspects of the study that cannot be controlled by the researcher. For instance, limitation one was to investigate a large sample of network managers. Limitation two was not having explicit knowledge of how the business objective of each sample could influence the defense strategies against backdoor intrusions affecting the network systems. Limitation three was not being aware the budget of each organization under study that could potentially influenced the defense strategies used by network security managers.

Definition of Terms

The following defined terms may assist the reader to understand important terms used in the study.

Administrative overhead: Costs not involved in the development of services (Bragg, 2018). "Administrative overhead results in administrators becoming overwhelmed allowing security responsibilities to slip, opening the door to security threats" (Cleghorn 2013, p.145).

Backdoor: A backdoor is a malicious code located on hardware components inserted by an insider or third-party internet provider (IP) provider (Sethumadhavan & Waksman, 2015).

Defense-in-depth: Defense-in-depth is a multi-layered security strategy (Orojloo & Azgomi, 2017).

Identification & Authentication (I & A): Identification and authentication are forms of recognizing people (Gui, Jin, & Xu, 2014).

Intrusion Detection: Intrusion detection is defined as the process of monitoring events that occur on computers and networks (Keegan, Ji, Chaudhary, Concolato, Yu, & Jeong, 2016).

Network-on-Chips (NoCs): An electronic circuit where network traffic in the form of packets flow and where flood-based, latency inducing or denials of service (DoS) attacks take place (Boraten & Kodi, 2018).

Remote access Trojan: Remote access Trojans are programs that use backdoors to gain access to target machines or systems giving the hacker administrative privileges (Hoque, Bhuyan, Baishya, Bhattacharyya, & Kalita (2014).

Rootkit: A rootkit hides malicious code that can run on compromised machines (Song, Choi, Kim, Kim, Kim, & Kim, 2016).

Stealth attack: A stealth attack happens when a device masked itself from the network, also known as deception attack (Trouw, Rangel & Cable, 2018).

General Overview of the Research Design

The research design study selected was the qualitative research methodology approach in order to explore the experience and views of the research participants (Creswell, 2014). This methodology was appropriate for the study because it explored the strategies that network security managers need to protect networks from backdoor intrusions. The research design for the study followed a series of steps that helped to answer the research question. The first step of the research design was to select 12 network security managers in order to explore the strategies needed to protect networks from backdoor intrusions. The instrument in a research study focuses on the process and events to be studied and involves devices used to observe and record events (Miles, Huberman & Saldana 2014).

The second step of the research design was to collect the data. In this qualitative study, the researcher became the instrument and was responsible for collecting the data throughout the process of conducting interviews from 12 experienced system administrators and network managers working in IT departments who were responsible for managing and monitoring the

network infrastructure of their parent organization. The job of the researcher is to explain how their sample represents the population in the study (Bauer & Gaskell, 2000). Goodyear et al. (2014) stated that researchers must adapt to local conditions and accommodate the needs of the management population because most essential insights are generated with direct and open-ended communication with representatives of the population. The study participants provided meaningful insight to benefit IT departments and their parent organizations. Participants provided ideas for a new program component to be developed in the area of information assurance to mitigate backdoor intrusions that are stealth in nature.

The third step of the research design was to analyze the data. Goodyear et al. (2014) declared data analysis emerges during the collection process and continues to evolve after the data has been collected. The interview feedback must be recorded for later use by the researcher as part of an analytical process that refines and codes the data to facilitate the presentation of the data analysis in a coherent form. There is a potential for management to influence the data with their own bias so ensuring professional standards of practice is advised. The data was analyzed manually, and software analysis was not used.

Summary of Chapter One

Cleghorn (2013) stated that systems using third-party layered technologies cause an administrative overhead resulting in systems administrators being overwhelmed. This situation suggests that backdoor intrusion problems have been dismissed exposing a gap in the information assurance field. For example, extended payload features coming from internet traffic are difficult to manage (Hamed, Dara, & Kremer, 2018). All network systems face the problem of backdoor intrusions. Therefore, there is a need to explore the strategies needed to protect the network from backdoor intrusions. Despite the increasing sophistication of methods for securing computer networks, backdoor intrusions continue to occur. The purpose of the qualitative study

was to explore the strategies network security managers need to protect their networks from backdoor intrusions. Chapter 1 has provided an overview of the study, which has included a statement of the research problem, the rationale for the study, the guiding research question, the research design to be used, and possible limitations to the study. The research question was: What are the strategies network security managers need to protect their networks from backdoor intrusions?

Chapter 2 presents the literature review providing evidence from previous research that supports the necessity for this study. The topic of the study was significant because the defense-in-depth concept is a de facto model and backdoor intrusions are still penetrating network systems suggesting a severe information assurance gap in defense-in-depth strategies. This study argues that backdoor intrusions are still happening and is likely to continue to occur because having many layers of defense causes administrative overhead resulting in backdoor intrusions. The literature review presents a broader picture from scholarly sources that complement the problem statement, the purpose statement, and the research question addressing the fact that network systems still have a problem of being the target of backdoor intrusions. With the help of systems administrators and network managers, it was possible for the researcher to analyze the process of applying defense-in-depth strategies for network computer systems in order to clarify the gap.

The results of this study brought a different point of view leading to a better strategic defensive posture for future applications. In addition, this research presented evidence that may impact the cybersecurity and information assurance field. Many organizations can benefit from the results of this study because network information systems and IT departments are a necessity for business entities.

Organization of Dissertation

The dissertation is composed of five main chapters. Chapter 1 introduces the research problem which is the strategies network security managers need to protect their networks from backdoor intrusions. The technique of the defense-in-depth approach that has been used for many years in the government and corporate entities is still allowing backdoor intrusions to occur. Chapter 2 offers the current evidence related to the topic of defense-in-depth and potential vulnerabilities related to backdoor intrusions. Chapter 3 describes the methodology used in more detail to study the problem of the strategies network security managers need to protect their networks from backdoor intrusions. Chapter 4 presents data findings and analysis derived from nine interview questions used in the interviews. Chapter 5 contains the interpretations and conclusions of the investigator based on the analysis in chapter 4 produced through the methodology described in chapter 3.

CHAPTER TWO

The purpose of this qualitative study was to explore the strategies network security managers need to protect their networks from backdoor intrusions. Teo, Toh, and Chung (2015) recommended a security policy strategy idea installing end-user security software to secure against backdoor intrusions. There is a model that can check the network system and verify flow against network security policies in order to enforce those (Akhunzada et al., 2015). Rostami, Koushanfar, and Karri (2014) asserted that in order to provide a well-founded countermeasure against backdoor intrusions, a thought out threat model needs to be developed first. (Acquaviva, Mahon, Einfalt, & LaPorta, 2017) stated that re-installing the operating system will always return the asset to a non-compromised state, but more advanced malware allows backdoors to exist and the malware cannot be removed even after the re-install strategy approach has been utilized.

A network that lacks security strategies while accessing distributed cloud services is vulnerable to intrusions (Khaldi, Karoui, & Ghezala, 2014). Cyber analysts have the responsibility to monitor networks and prepare incident reports based on intrusions in order to quickly detect perceived emerging threats (Buchler, Rajivan, Marusich, Lightner, & Gonzalez, 2018). The defense-in-depth strategy used to protect the computer systems against unauthorized access needs to be reviewed to determine if intrusions have been met by a countermeasure. It is important to understand how backdoor intrusions are bypassing the network systems and if network managers are missing this unauthorized access type in their process of defending the network.

The argument in this study is that many defense-in-depth layers add more backdoor entry points allowing for cyber-attacks to compromise the IT department of the organization. Wolff

(2016) declared that although the intention of the defense-in-depth strategy is to strengthen security, in some cases it may backfire due to interactions between many layers of defense that can interfere with each other. The defense-in-depth strategy is a strategic principle based on adding multiple layers of defense in networks with the intent to make unauthorized access more difficult. Watkins et al. (2017) declared that a traditionally secured enterprise deals with the issue of Big Data by using the defense-in-depth strategy. Ignoring an overwhelming amount of data that Watkins et al. (2017) categorized as non-malicious could be problematic because it may actually be malicious. Backdoors are malicious code that may be embedded on Big Data, thus allowing unauthorized access.

Managing information technology departments has different purposes including improving the technology management that can be used to monitor indicators and take necessary actions to improve performance (Balaman, Wright, Scott, & Matopoulos, 2018). For instance, the IT department can follow its network performance to minimize unnecessary costs and to avoid repeating intrusions. Network management can be improved by using software-defined networking techniques (Kim & Feamster, 2013). Also, there is software networking solutions to help IT departments on network management issues.

Responsibility for information technology is shared between information technology management, business partners and service providers (Wu, Straub, & Liang, 2015). Da Veiga, and Martins (2017) declared board members should delegate responsibility for implementing the needs of the information systems and the management sections to show their commitment and buy-in to the organization. In addition, senior managers have the responsibility to promote a comprehensive defense-in-depth program into their IT departments to manage the resources and services of the network infrastructure.

Another network security strategy to protect networks from backdoor intrusions is the use of intrusion detection systems. There are numerous network intrusion detection systems (NIDSs) that can detect wireless backdoor intrusions (Santoro, Escudero-Andreu, Kyriakopoulos, Aparicio-Navarro, Parish, & Vadursi, 2017). These types of cyber-attacks can affect the wireless network of the IT department. The literature presents evidence of four defense strategies with the intent to defend the enterprise network against backdoor intrusions. The four defense strategies are: (a) defense-in-depth strategy, (b) defense tools & practices strategy, (c) defense funding & staffing strategy, and (d) defense culture & awareness strategy. These strategies are the backbone of the conceptual framework for this study described in more detail in this chapter.

Synthesis of the Literature

This chapter is organized into four main parts describing the four strategies network security managers need to protect their network from backdoor intrusions. Each part contains between two to six sub-parts explaining in more details the strategies and the relationship with backdoor intrusions. The objective of these four network defense strategy approaches is to defend the IT department against backdoor intrusions in the network system of the organization. Below is a short description of what backdoor intrusions mean.

Alexander (2017) stated that computing devices are becoming targets of backdoor intrusions (cyber-attacks), and, agencies are becoming dependent on secure network devices. Inside some network devices, there are integrated circuits vulnerable to malware code and botnets because the devices are creating backdoors that allow unauthorized access to information systems. For example, there are hardware devices that are designed to detect backdoors, but at the same time the hardware device ignores the presence of malicious logic software running inside the hardware device itself (Guo, Dutta, Mishra, & Jin, 2016); this is a contradiction causing backdoor intrusions to occur and also becoming an information assurance symptom that

affects networks. Another example is the Dual EC adopted as part of National Institute of Standards and Technology NIST SP 800-90A standard that might be intentional allowing backdoor access (Checkoway et al., 2016). Conventional scanning methods cannot see when this type of backdoor access has been executed.

According to Geramiparvar and Modiri (2016), cyber-attackers take advantage of four weaknesses, including design and implementation, innate and structural weaknesses, configurations, and human-made errors. Haider, Hu, Slay, Turnbull, and Xie (2017) described through his pre-simulation phase of an intrusion detection system that abnormal traffic can indeed detect a backdoor intrusion or cyber-attack but backdoor intrusions continue to occur despite the many layers of defense-in-depth strategies used. These backdoor intrusions suggested tools used in IT departments may not be adequate to prevent them.

Viruses often create backdoor intrusions that can trigger various effects including the denial-of-service or (DoS) attack because distributing a computer virus turn devices into zombies interfering with the normal functionality of computers (Downing, 2013). Dormann (2018) stated that a remote unauthenticated attacker might be able to trigger a denial-of-service condition on devices using CISCO products. Denial of service attacks can lead to a considerable amount of organizational expenses (Liu, Zhang, & Chen, 2014). The security issue for Network-on-Chips (NoCs) is a growing concern (Boraten & Kodi, 2018). One reason for the concern is because there are hidden codes implanted on these chips that can remotely trigger flood-based, latency inducing or denial of service attacks affecting the strategies of network managers to protect networks from backdoor intrusions. Thus, there may be stealth backdoors that IT tools like intrusion detection systems (IDS) cannot detect. This type of stealth backdoor attack is a dangerous gap in networks presenting vulnerability in IT departments.

Four Strategies to Defend and Secure IT networks from backdoor intrusions

Concerning the idea of a conceptual framework, Too and Weaver (2014) examined thoughts and concepts that can be used to improve performance and to enhance the value of an organization. The conceptual framework in this study brings four different types of network defense approaches that play an essential part of a secure network strategy from backdoor intrusions. The first approach is called the defense-in-depth strategy used by the organization. The second approach is called defense tools and best practices that the organization uses to secure its network. The third approach explored defense funding and staffing, and the last approach describes how the defense culture and awareness plays a vital role in the defense of network systems in IT departments.

Chapter 2 is organized into four parts that are related to defense used in systems against hacking from the IT management point of view. The literature review describes in more detail the network security strategies designed for IT systems based on four different defense approaches such as a) defense strategy, b) defense tools & practices, c) defense funding & staffing and, d) defense culture & awareness. Mavroeidakos et al. (2016) stated that the definition of multilayered security architecture is based on the defense-in- depth strategy. These approaches have the objective to defend networks against backdoor intrusions in IT departments. There is a lack of availability of or lack of real dataset to assess facts on intrusion detection systems (Haider et al., 2017); this lack of availability opens a gap in the information assurance field. The literature review presents evidence of strategies network security managers need to protect their networks from backdoor intrusions and describes what backdoor intrusions are.

A Brief History of Information Technology (IT) Network Security

During the mid-1960s the National Security Agency (NSA) was developing methods to apply cybersecurity techniques to computer network systems as one of many vital functions of

the industrial military complex infrastructure (Berg, Crawford, & Seymour, 2016). Rao and Nayak (2014) stated that during the 1960s and 70s telephone networks were a favorite mode of communication. The use of a modem device able to connect computers over telephone lines was introduced, and from the beginning, network computing security was weak.

Keegan et al. (2016) declared that at the beginning of the 1970s, system administrators were manually monitoring the activities of users while working on computer terminals. In 1974, during the development of the Transmission Routing Protocol, cybersecurity became a priority. In the 1980s, audit logs were the focus, but the monitoring task and audit log findings were not fast enough to pinpoint attacks which resulted in computer forensics identifying security incidents after backdoor intrusions were executed.

In the 1990s network traffic was growing with the introduction of the internet and the concept of network intrusion detection analysis evolved to diagnose and prevent backdoor intrusion attacks (Keegan et al., 2016). In the 1990s network connections were growing fast because in 1969 the Defense Advanced Research Projects Agency (DARPA) started to help develop Internet protocols known as Transmission Control Protocol /Internet Protocol (TCP/IP) and this protocol was tested in 1977 eventually leading to the growth of the Internet in 1983 (Fidler & Russell, 2018). In the 2000s real-time solutions emerged involving intrusion detection monitoring processes being applied to computer networks, combining more sophistication with the emerging need to define new classifications and frameworks that use two critical thoughts such as how the system behaves and what detection methods are appropriate (Keegan et al., 2016).

The origin of cyber-criminals having access to computer systems is due to defects in the software code itself which allows access to vulnerable points. Usually, for every one thousand

lines of code, there are roughly forty warnings (Beller, Bholanath, McIntosh, & Zaidman, 2016). Sensitive areas in the code are valuable to hackers, and those areas are susceptible to backdoor intrusions. Cybercriminals can make other attacks such as man-in-the-middle, impersonation, replay, de-synchronization, location tracking, and eavesdropping in the process of authentication. Because of such attacks, administrators must monitor the authentication process closer in order to avoid and defend the IT system against further attacks (Dhal, Basu, & Gupta, 2014).

Defense-in-Depth Strategy

Alexander (2017) declared that business and government entities often use defense-in-depth information assurance measures to strategically manage and plan IT security risks. Measures such as intrusion detection systems, passwords and the use of firewalls are some strategic examples for network security managers to consider. Dai, Xu, Huang, Qin, and Xu (2017) stated that the traditional Data Center Network (DCN) architecture is not supporting enough defenses against security attacks on virtualization applications that IT departments use in their daily operations. This security flaw is present in network systems that enterprises use in order to conduct their daily business. This defense gap allows backdoor intrusions to occur, thus weakening the defense strategy of the organization.

Network systems are still experiencing security challenges, and this phenomenon presents the need for security methods, which require every enterprise to further develop their IT security management (Wang, Anokhin, & Anderl, 2017). One approach to deterring backdoor intrusions is to map IT security requirements and assign security measures to vulnerabilities. This approach can be added as a defense-in-depth strategy for managers to adopt in their IT departments. However, this method alone may not prevent backdoor intrusions that occur through stealth backdoor attacks.

Defense strategies have existing technical challenges that are cost related due to current algorithms that are difficult to solve. Martin (2017) argues the security of encryption algorithms and addresses the concept of backdoors in encryption that can be bypassed. The same principle can be applied to other systems such as information technology networks located in the public, government and private institutions. This is another technical challenge that causes intrusions to the network interface of an enterprise because this interface depends on algorithms as part of the network operation.

Information assurance and the business objective of the enterprise must maintain balance in order to make sense. According to Ahmad and Maynard (2014), information security and strategic business management must be aligned to protect the function of the enterprise. Having a disconnection between cybersecurity and the mission of the business causes security gaps. This gap results in more expenses but if both concepts remain aligned it allowed the organization to benefit and have a competitive advantage.

Defense Countermeasures as a Strategy

Bouabdellah, Kaabouch, El Bouanani, and Ben-Azza (2018) mentioned different countermeasure techniques to offset backdoor intrusions such as intrusion prevention system (IPS), routing game, checking the bi-directionality of a link and neighbor authentication. In the case of an effect caused by backdoor intrusions called Distributed Denial-of-Service (DDoS) attacks defenders can customize defense countermeasures on their own (Wang, Zheng, Lou, & Hou, 2015). This ability to personalize countermeasures opens a wide variety of ways to apply defense mechanisms to network systems in the IT environment. For example, a Denial-of-Service attack makes it difficult for a user to access their computer or network. According to Hui, Kim, and Wang (2017), a survey conducted by IT professionals from 38 countries suggests 50% of businesses experience disruptions in their networks are due to Distributed Denial-of-

Service (DDoS) attacks. Certainly, customized countermeasures need to be implemented to avoid this type of backdoor intrusion effect.

There is another countermeasure technique called side-channel signal analysis that can detect backdoor intrusions embedded in integrated circuits built by untrusted foundries (Tehranipoor et al., 2014). This is an alternative method of responding to cyber-attacks to mitigate backdoor intrusions in the IT networks. Also, Walters (2014) proposed to use more cyber tools in order to improve investigatory capabilities. This technique is like an active self-defense mechanism. Li, Liu and Zhang (2016) categorized recent research advances in the countermeasure against backdoor intrusions since they can be implanted in security-weak parts on chips. Malicious code can be implanted in security-weak parts in a circuit inside a chip (Li et al., 2016). Rostami et al. (2014) stated that in order to provide proper countermeasures against backdoor intrusions, a well thought out threat model needs to be developed first.

Kotenko and Ulanov (2014) considered an approach to modeling and simulation of backdoor intrusions to gain insight in order to discover both weak and strong areas for decision-makers to decide the best course of action to win such digital wars. Computer simulations may produce ideas that can be used to further countermeasure techniques critical to the defense-in-depth strategy. Basic ideas were developed dealing with distributed denial of service (DDoS) attacks that can be applied to real-world situations and gain an advantage against hackers (Kotenko & Ulanov, 2014). It is possible that such countermeasures could be classified as active defense strategies and can be used as a last resort to mitigate backdoor intrusion epidemics (Miles et al., 2014).

Network Perimeter

Cleghorn (2013) expressed that if a hacker is inside the perimeter of the network, it is possible to penetrate the system and bypass most of the defense layers such as firewalls, the

demilitarized zone (DMZ), intrusion detection system (IDS) and network address translation (NAT) layers of security. Of course, each layer provides an obstacle for hackers, but it is easier to navigate from within networks allowing backdoor intrusions to take place. This penetration activity revealed that many perimeter defenses were clustered instead of the defense method being implemented and spread within the interior of the network.

Defending the network perimeter often points to packet-based attacks typically using a device called a firewall that is designed to stop bad packets. Wang, Kohno, and Blakley (2014) proposed a novel technique to block certain types of automation attacks on web applications. Web application firewall (WAF) vendors promote botnets creating an automation problem for backdoor intrusions to occur. Systems administrators or network security managers may be well-advised to take advantage of such technology while at the same time remaining aware of firewall vulnerabilities.

Enclave Boundary

The enclave boundary is a collection of various computer environments that work together as part of the whole network system control by a single organization or authority. When system logs are stored outside of the enclave boundary, those logs should not be trusted (Karande, Bauman, Lin, & Khan, 2017). Protecting the enclave boundary of a network against intrusions requires tools such as firewalls and guards. Enclave boundary protection is one element in the defense-in-depth strategy for enterprise network systems.

Host Computers

Host computers could become compromised when backdoor intrusions occur. Bukač, and Matyáš (2014) stated that host-based intrusion detection systems (HIDS) are computer programs designed to monitor a single host system, thereby providing identification of suspicious network

traffic or network activity that can be stopped. This intrusion detection technique can filter traffic attacks, thus minimizing unauthorized access.

Information Assurance Core Principles

Before mentioning the seven core principles of information assurance, the phenomenon of backdoor intrusions must be addressed. For instance, hardware-based Trojans can interfere with the availability of the network affecting the confidentiality of its infrastructure (Tehranipoor et al., 2014). The objective of information assurance is to enforce principles that enable blocking backdoor intrusion attempts to ensure that digital information that has been sent, in transit and received is reliable for the use of business. Another important function of the core principles of information assurance is to manage risk while information is being stored, while in transit, or being received within the nodes of the secure network. Nugraha, Brown, and Sastrosubroto (2016) wrote that from the cybersecurity risk point of view, a lack of security operations might be exploited by hackers while installing malicious code in software and hardware.

The following sections describe seven core principles of information assurance.

Confidentiality. Confidentiality ensures that the disclosure of information is accessible only by authorized personnel. Yao, Mu, and Yang (2016) stated an encryption method scheme as a way to ensure message confidentiality. He suggests that network systems administrators or network security managers need to consider impersonation intrusions because they can be mistakenly perceived as friendly when these impersonation intrusions are unauthorized users masquerading themselves as members of a legitimate group. Information assurance focuses on the confidentiality of network technology when dealing with the absence of unauthorized disclosure of information (Tehranipoor et al., 2014).

Integrity. Integrity protects network information against destruction or unauthorized modification. For instance, hardware can measure system integrity focusing on boot-time but

cannot consider runtime (Wei, Shi, Qin, & Liang, 2015). Assuring accuracy according to some set specifications is what integrity covers in information assurance. Browsers cannot check Hyper Text Transfer Protocol Secure (HTTPS) certificates on behalf of the users (Corbetta, Invernizzi, Kruegel, & Vigna, 2014). Backdoor intrusions can occur when the integrity of web browsers is not protected, thus allowing cyber-attacks to bypass HTTPS certificates.

Availability. According to Armando, Bezzi, Metoui and Sabetta (2015), the increase in availability of customer data and transactions helps enterprises to know their market and make predictions. For example, malicious attacks compromise the availability of devices, and there is no sound approach designed to detect the availability and vulnerability at the source code level (Fang, Liu, Zhang, Wang, & Wang, 2015). Availability is an attribute of information assurance that ensures authorized users can access the network in a timely and reliable manner.

Authentication. Authentication makes sure information has not been changing or been seen by unauthorized personnel using cloaking techniques. A cryptographic mechanism can be applied in the media access control address (MAC address) layer to provide authenticity in a network to protect against intrusions (Lee, Choi, Kim, Shin, & Kim, 2014). Authenticity is an information assurance property that claims what an entity is and it can be applied to different scenarios in the network security situation. For instance, in the code level of the network, the objects are secure without the possibility of an interception from untrusted code to establish that the code is authentic (Budianto, Jia, Dong, Saxena, & Liang, 2014). However, if there are interceptions or intrusions in the code object, therefore, authenticity is compromised.

Non-Repudiation. Non-repudiation is a property of data storage required when a data owner sends a request thru a cloud service provider, and the request is not denied either by neither the cloud provider nor the data owner. For example, this property is enforced during

online transactions use, especially when the network is accessing the internet (Krotsiani, & Spanoudakis, 2014). Distributed Denial-of-Service (DDoS) attacks are the most dangerous backdoor intrusions category to happen when adding security policies into the net allowing the IT department to become available for online services (Ahmim & Ghoualmi, 2015). Distributed Denial-of-Service (DDoS) intrusions cause delays to network operations and functions in the IT department where the availability of the network is affected. This is an example of adding the principle of non-repudiation to the IT department and its network information system.

Authorization. Access control systems can identify authorized users to prevent theft. Illegitimate users can disrupt services and resources allowing backdoor intrusions to occur (Pandeeswari & Kumar, 2016). Authorized use eliminates the threat of theft in the organization. Also using safeguard access techniques for expensive services helps decrease the cost to the enterprise. Safeguard is used somewhat interchangeably with control or countermeasure, all of which are measures that modify risk.

Privacy. Privacy is related to confidentiality but deserves its right as a principle of information assurance. According to Shahri, Ismail, and Mohanna (2016), results of a survey show that unauthorized intrusion of network systems is an organizational threat to hospital information systems invading the principle of privacy. Organizations must follow laws and regulations regarding the storing and using of personally identifiable information (PII).

Defense Tools & Practices Strategy

The field of information assurance covers areas such as auditing, computer forensics, intrusion detection, incident handling, hacker techniques, firewall design, and appropriate perimeter protection. In addition, Miraglia and Casenove (2016) argued the need for an active defense method using powerful active tools could be used on network systems to mitigate

backdoor epidemic intrusions. Examples of these defense tools are antidotes sometimes called botnets or malware. Another strategic example that systems administrators or network managers might consider is the use of anti-phishing tools designed to detect phishing attacks because these attacks cost businesses billions of dollars every year (Purkait, 2015). The following topics are some examples of strategic defense tools & practice those IT system administrators or network security managers may use to defend their network systems from backdoor intrusions.

Strategic Use of Many Security Technologies and Network Management Tools

The 11th International Conference on Information Security Practice was hosted in 2015. This conference provided new information strategic security technologies that can be integrated with IT systems (Lopez & Wu, 2015). Different security technologies and network operations management applications are available to IT departments. The network operations management applications provide tools to handle network systems such as Statistical Analysis System Information Technology Management (SAS IT Management) solutions, or, Microsoft System Center Operations Manager 2007. These security mechanisms need to be in place parallel to policies and procedures as strategic options to defend networks from backdoor intrusions.

Network intrusion detection systems tools. According to Wang, Liu, Pitsilis, and Zhang (2016), intrusion detection is a very important technique in the defense-in-depth framework. A typical plan of intrusion detection systems (IDS) is to assemble malware blacklists of endpoints; however, little is known on how useful these malware blacklists are (Kührer, Rossow, & Holz, 2014). Singaravelan, Arun, Arunshunmugam, Joy, and Murugan (2017) proposed an internal detection system based on data mining and forensic techniques to detect backdoor intrusions. Backdoor intrusions still attack network systems even when they are using

intrusion detection technology. It is possible that there is a gap where backdoor intrusions find hidden areas in computer systems devices used in IT departments.

Surti and Jinwala (2015) focused on a technique in which the original program code is compressed, and new random noise is added to monitor data flow currently taking place in Wireless Sensor Networks (WSNs) applications. This technique is used against compression attacks and develops an intrusion detection measure which is significant and yet reduces communication overhead. Such detection occurs in the physical layer due to tampering attempts directed at the contents of the memory of the node. Comparing current events to detect backdoor intrusions is another strategic technique even though there are many approaches proposed in network security (Surti & Jinwala, 2015).

Backdoor intrusions into network systems indicate there is a gap in regards to strategies used in network security. According to Keegan et al. (2016), the place where machine learning algorithms (MLAs) and cloud-based network intrusion detection meet there are opportunities to be found that could enhance the identification of backdoor intrusions. Backdoor intrusions invade the enterprise system networks in different forms and methods. It is possible for network systems administrators or network security managers to use intrusion detection systems tools using the cloud environment. This intrusion detection system uses machine learning algorithms (MLAs) where there are opportunities to identify threats and mitigate backdoor intrusions because researchers are beginning to harness this intrusion detection possibility (Keegan et al., 2016).

Antivirus software as a tool. In summer 2017 a virus allowed a backdoor intrusion attack estimated at $8 million in Ukraine (Gavrylenko, Babenko, & Ignatova, 2018). Virus programs have the ability to allow backdoor intrusions to happen affecting network systems.

Entities involved in electronic business (or e-business) transactions require information assurance enforcement methods due to real virus threats. There is an issue in preventing viruses in the business computer systems called immunization cost, which includes the potential loss as a secondary effect named infection loss. Such damage and loss related to information assurance are not always evident regarding money quantity (Liu et al., 2014). The strategic use of antivirus software benefits the network to avoid future losses in its information systems infrastructure. Some services are for free, and they work well. Also, the antivirus software is not that expensive to implement in the network, but when the organization is working there should be some time allotted for the antivirus to run a scan.

Operating system security policy tools. The use of security policy tools is an important function used by IT managers as a strategic approach against backdoor intrusions. According to Pappas, Polychronakis, and Keromytis (2014), hardening tools such as Microsoft EMET (enhance mitigation experience toolkit) do not support recent exploit mitigation technologies suggesting the high possibility of backdoor intrusions. Han, Cheng, Zhang, and Feng (2015) proposed a method using several host tools that generate attack graphs to evaluate vulnerability and to detect privilege escalation intrusions. The tools are MulVAL (Multihost, multistage Vulnerability Analysis), a logic-based, data-driven enterprise network security analyzer (Jing, Yong, Divakaran, & Thing, 2017). NETRA (NEtwork TRaffic Analysis) is another tool that can identify information flow vulnerabilities (Gupta & Muttoo, 2017). Another tool called VulSAN is used to analyze and compare the quality of protection offered by different MAC systems. The next tool is called WACCA which systematically analyzes Windows configurations. Finally, SEAL serves as a logic programming language for the analysis of dynamic access control systems (Han et al., 2015).

Since organizations use different modern operating systems, there is heterogeneity of their respective semantics, and when enforcing stable mandatory access control, it is prone to error (Amthor, 2015). This suggests more openings for backdoor intrusions to bypass mandatory access control protocols. All these software devices do not enhance security policy configurations in operating systems. In this case, backdoor intrusions are still a problem affecting the network infrastructure.

Snort tool. It is essential to find good and bad connections in the network as a strategy to deter backdoor intrusions. According to Alnabulsi, Islam, and Mamun (2014), snort tool is a packet sniffer or network intrusion detector that can monitor network traffic in real time that supports Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Protocol (IP) and Internet Control Message Protocol (ICMP) protocols. The bad links are called intrusions or attacks while the good connections are regular traffic. One concern is whether backdoor intrusions can be detected in a clear manner or if the snort tool might bypass stealth intrusions in a repeated fashion.

Network scanning tools. A number of network scanning tools are available that can help the IT department further defend the system. For example, Dawson, Omar, and Abramson (2015) stated that Nmap is a useful scanning tool that network administrators cannot afford to ignore because it can identify firewalls and it is free of charge. Other products besides Nmap are, Amap, Vmap, Unicornscan, Ttlscan, like-scan and Paketto. Hoque et al. (2014) stated that network scanning tools offer defense and prevention mechanisms that are available in the public domain. Organizations should consider using these network scanning tools to reduce cost and increase network security. The purpose of network scanning tools is to identify active hosts to either attack or to assess vulnerabilities.

False alarms. Meng (2013) stated that false alarms detected on intrusion detection systems (IDS) are problematic because they decrease the effectiveness of current information and communications technology (ICT). Systems administrators could spend unnecessary time reading or trying to analyze false alarms causing harm to their parent business affiliate. Also, false alarms do not help in the detection of hidden attacks such as backdoors. False alarms burden the system administrator causing a backlog and draining resources that would otherwise be used to detect and analyze real threats (Meng, 2013).

Guo et al. (2016) mentioned an attack model where a third party rogue agent can access the hardware description language (HDL) code by inserting malicious programs into critical registers. Then the backdoor can be triggered, thereby leaking sensitive information or causing a denial of service attack to specific hardware in the network. Arp, Spreitzenbarth, Hubner, Gascon, Rieck, and Siemens (2014) proposed a method that detects 94% of malware with few false alarms for android smartphone systems. Generating false signals in a network help to make sure the network intrusion detection system works fine. It could be important for IT departments to apply this method in the cases where the need for smartphones is part of the job description and where systems administrators can implement the plan (Arp et al., 2014).

Firewall Practice on Networks

Firewall weaknesses. In December 2015 researchers confirmed a backdoor password in Juniper firewall program code. This vulnerability was implemented in 2008, and no one but the United States had been able to exploit it (Checkoway et al., 2016). Malignant program codes or backdoors can be propagated through malicious URLs using search engines that are synchronized by hackers, thus allowing another type of backdoor intrusion (Nagaonkar & Kulkarni, 2016). IT departments must consider whether there is any backdoor defense gap

related to a lack of intrusion detection for firewall devices that weaken the defense-in-depth strategy, thus making networks unmanageable. Also, mobile malware allows backdoors to be opened on devices and the traffic generated on mobile devices can be infected with such malware (Nagaonkar & Kulkarni, 2016). Using a firewall device is an example of an information assurance layer to protect against unauthorized access while using the network on the Internet.

Network Operations Best Practices

IT outsourcing practice. IT departments may consider outsourcing parts of the network infrastructure for cost-effectiveness and network security purposes. Outsourcing is the agreement between a vendor that provides IT services and the client that need such services (Dhillon, Syed, & de Sá-Soares, 2017). Many models are available for outsourcing security for information systems. For example, security as a service is available at low cost offering many products designed to secure networks. IT departments must determine if information technology outsourcing should be considered a best practice against backdoor intrusions. If security is provided as a service, then outsourcing security might be a good idea in order to help defend the IT department against backdoor intrusions.

Risk analysis/management practice. Cavusoglu, Cavusoglu, Son, and Benbasat (2015) declared that risk is the chance of something happening to an organization affecting its information security domain. One way to become more effective is to do a risk assessment by assigning a team to a section of an IT department during a specified period and interviewing its employees. Use this information to assess risks and inform the managers and supervisors of predictions and trends of possible future threats. This can support organizational learning designed to help entities avoid risks in the early stage. There is always a chance that something is

going to go wrong, but organizations can still mitigate the situation as much as possible to avoid unnecessary damage and threats to the computer systems of the organization.

Defense Funding (Cost) & Staffing Strategy

Defense Funding Allocated for the Information Technology Department

Lam (2016) argued about concerns on investing in security software such as Kaspersky and Symantec companies because hackers often use exploits for unknown vulnerabilities. More than 75% of websites Symantec scanned have unpatched vulnerabilities in 2015 allowing many backdoor intrusions. Information security professionals are not necessarily in charge of the amount of funding allocated to their departments. For information technology outsourcing there is evidence that suggests that cost escalation is common (Bahli & Rivard, 2013). Funding assigned to the IT determined what key types of security decisions are used to avoiding repeating intrusions. For instance, one factor to be considered has to do with what type of hardware an organization could purchase where would not be easy to inject backdoor code. Also, departments would be well-advised to consider whether there is a correlation between defense funding, staffing issues, and backdoor intrusions into the network environment of an organization.

IT departments want to protect network information with its business parent entity with low-cost cybersecurity protection. Cherdantseva (2016) proposed a cost-effective information assurance program by combining the correct security countermeasures with the objectives of the information technology business parent. One way to ensure the efficiency and cost-effectiveness of an information assurance & security strategy is by selecting the correct security countermeasures achieving security goals specific to the organization (Cherdantseva, 2016).

Figure 1 represents an entity securing its network based on a low cost information assurance program.

*Figure 1. C*ost-effective Information Assurance Program.

Possible Lower Cost Solutions for Information Technology (IT) Departments

Network outsource funding options. IT departments in hospitals that do not engage too much in outsourcing show considerable productivity gains (Lee, 2017). Outsourcing methods do not work for all IT departments. For example, using malicious cloud servers to retrieve private information may provide fraudulent answers (Zhang & Safavi-Naini, 2014). This is a type of backdoor intrusion for those IT departments that outsource cloud services for their business. This kind of unwanted hacking comes from outside networks when the internal system is retrieving private information. Taneja, Singh, and Arora (2017) stated that most IT organizations are losing control of their technology due to Cloud computing being considered a method of outsourcing and causing new cybersecurity trends to emerge.

Public domain network scanning tools. Scanning network products such as Nmap, Amap, Vmap, Unicornscan, Ttlscan, like-scan and Paketto are available online and free to use. Hoque et al. (2014) stated that network scanning tools are defense and prevention mechanisms that are available in the public domain. Organizations should consider using these network scanning tools to reduce cost and increase network security.

Cost of Staffing and Devices

Cost of staffing. Balancing backdoor intrusion threats with the objectives of the organization related to cost control must achieve a ratio of cost-benefit that tips the scale in favor of being cost-effective. According to Langer, König, and Fitili (2018), reactions toward novel technologies could detrimentally affect applicants. A continuous review of network security processes and the cost of staffing could reduce costs by increasing technology support. Lowering the network cost benefits the enterprise in achieving a cost balance between staffing and network infrastructure. Also, there is a possibility that the organization has the challenge of having untrained personnel. Outsourcing might allow the IT staff to have proper training while third-party contractors take care of migration issues.

Cost of devices. The IT staff can easily be blamed for allowing unreliable hardware devices that enable backdoor intrusions to have access to the enterprise network. Tang, Sethumadhavan, and Stolfo (2014) proposed that hardware-supported low-level features are able to detect malware exploitation and zero days using unsupervised machine learning. This idea assists IT managers and administrators making them comfortable deterring backdoor intrusions. Machine learning techniques could learn possible hidden structures because these hidden-structures inject backdoors into the network (Tang et al., 2014). Backdoor attacks are stealth in nature, and machine learning could help mitigate the problem by helping to secure the system.

Defense Culture & Awareness Strategy

Importance of Ethics

Goolsby (2005) offers four guidelines for evaluation due to system defense funding has its ethical problems. First, the enterprise must support an ethical environment. Second, the people must have a need to understand the code of ethics and the reasons behind that code.

Third, the funding problem affects human conduct when dealing with unintended consequences and negative impacts to the organization. Finally, the implications to network security when personnel are working in a regulated environment can affect the intrusion issue present in network environments.

The process of managing information systems involves significant challenges including ethics and security (Laudon & Laudon, 2016). This process includes information system literacy for managers that can be embedded in the culture of the information systems departments. Ethical culture may enhance strategies with the intent of mitigating backdoor intrusions. Rocha Flores, Holm, Nohlberg, and Ekstedt (2015) concluded that if national culture contributes to resisting phishing intrusions employees will have the power to resist them.

Shared Culture Values

Glue the culture of insider members with technology. Insider members of any organization could potentially influence how effective the enforcement of information security is. Differences are identified between two different groups such as the insiders of the corporation and the experts (Posey, Roberts, Lowry, & Hightower, 2014). Members of an organization are a potent part of the entity in terms of educating them to protect the assets of the organization against cybercrimes and other criminal activities affecting computer systems and networks. Insider members can be a valuable asset if they are trained well and selected well in the recruiting process.

The combination of technology and corporate culture mentality contribute to the involvement in fighting network cyber-attacks adding network countermeasure against backdoor intrusions. Zhu (2015) stated the organizational culture plays an important factor in technology innovation and it is critical for end-users that are performing the work. Developing a corporate

culture against backdoor intrusions is an essential component in the defense-in-depth strategy for network security. Combining the performance of employees with a culture that teaches them to report intrusions can benefit the overall network operations of the organization.

Information Technology (IT) Best Practices

To share or not to share, that is the question. Best practices result from experiences and errors made by the organization that cost money. One effective management practice is to compare a cost-effective analysis between IT investments and outcomes at the outsourcing firm level (Lee, 2017). Suuronen and Bergenwall (2016) offered ideas that network security managers can use such as changing firewall filtering rules and updating the anti-virus software useful for network security strategies. Another best practice to consider is to keep root access to the network system to a minimum and only allow personnel with a need to know direct access. Such best practices should be shared with businesses for the enhancement of their IT department operations. Intrusions are reduced if access to the root directory is controlled. There are still difficulties in sharing data between enterprises since each one has their own autonomous network.

Sharing Intrusion Response System Techniques

The use of network defense countermeasures. An intrusion response system (IRS) is used to select countermeasures in handling intrusion alerts (GhasemiGol, Takabi, & Ghaemi-Bafghi, 2016). Hong, Xu, Wang, and Gu (2015) mentioned two types of countermeasures, static and dynamic, where the static countermeasures depend on the manual configuration in the network, and the dynamic countermeasures use an authentication method to add cryptographic public-key infrastructure mechanisms. To reinforce these countermeasures, the IT department can mitigate intrusions and reduce their impact by implementing a configuration strategy.

Information Security Awareness

Education to fight against backdoor intrusions. Information technology benefits organizations using information security protocols with the implementation of awareness programs that can reinforce protection against backdoor intrusions. Al Awawdeh and Tubaishat (2014) stated that having employees who are educated and trained plays a critical role in the IT work environment to minimize threats and misuse of the assets of the organization. An essential part of a network is the people who participate in the daily operations of the enterprise. For example, a study in Japan concluded that various training programs have become accessible since 2013 resulting in a significant increase in the skill level of IT and security professionals (Beuran, Chinen, Tan, & Shinoda, 2016). This case study serves as an example for US-based IT departments to adopt the strategy of training employees for them to adapt and to reinforce the defense-in-depth strategy and decrease backdoor intrusions into the network assets. Well trained personnel can make a difference in deterring backdoor intrusions and support the information assurance program of the IT department.

Webb, Ahmad, Maynard, and Shanks (2014) mentioned a model idea that could be applied to assure situational awareness (SA) in information security risk management (ISRM). Webb et al. (2014) supported the idea that it is essential to make a distinction between the term situational awareness and the method used to accomplish such a state of situational awareness. One way to enforce situational awareness is through training classes. These should be given every 90 days or when the opportunity presents itself without affecting productivity. Even supervisors can implement situational knowledge by talking to their employees briefly during the work day to enforce security. The method of delivering situational awareness as a training class might be an easy way to implement situational knowledge in a very well-organized way.

Human Behavior

Test human behavior before, during and after hiring. Understanding the behavioral aspects of human and technology interaction is an essential factor for the practice and study of information systems within the information assurance field (Saunders et al., 2017). IT managers have to deal with employee behavioral education issues to complement the training given to employees with the fight against backdoor intrusions to protect the network enterprise. Human behavior can be tested during the hiring process of the organization to minimize internal damages that can cause adverse intrusions into the network. This topic impacts the IT department infrastructure by promoting knowledge in favor of security and privacy issues. Human behavior can offer benefits to the information assurance program.

Public, corporate and government entities have the primary responsibility to conserve the confidentiality, integrity, and availability of their digital information means (Webb et al., 2014). Such liability must be shared with everybody within the organization from the highest executive to the lowest paid employee. Everyone needs to make a contribution related to information assurance enforcement to protect the availability, integrity, and confidentiality of the information systems. Protecting computer systems is something everyone needs to take into consideration.

The computer abuse behavior conducted by employees in the workplace either in the government or the business enterprise should be labeled as a crime related to computer use (Guo 2013). The enterprise should consider monitoring their employees, especially those subjects who become disgruntled because they can cause damage to computer information systems by inputting viruses or malware. Periodic checks are necessary to avoid employees misusing their workstations. One way to avoid computer abuse behavior is to keep employees busy doing their job with the help of supervisors monitoring them.

Ngoqo and Flowerday (2015) proposed a behavior profiling framework derived from quantifiable constructs based on mobile user information. The structure can map the level of security awareness that the subjects portrayed. The frame is based on three models called awareness map, theory of planned behavior, and two-factor taxonomy of end-user security behaviors. The methods can measure information security awareness levels based on the needs of the organization.

Lowry, Posey, Bennett, and Roberts (2015) stated that reactive computer abuse encourages behavior originating from the employee security threat point of view despite the many resources spent by organizations to deliver security programs and activities. For example, employees that are offended while doing their job are most likely to react in a negative way by misusing information systems in their workplace. Organizations might spend lots of money to protect their systems against abuse, but at the same time, they are not aware of the behavior of the employees causing damage at work due to adverse behavioral patterns.

Information Assurance and Enterprise Information Systems Awareness

Information assurance is part of the cybersecurity and information security field used to shield the computer systems of an organization (Von Solms, & Van Niekerk, 2013). Information assurance offers many layers of security depending on the area where vulnerabilities must be protected. For example, regarding physical security, a layer of protection could be the use of electronic card access that can be used to enter the building. Another function of information assurance is to catch cybercriminals.

According to Hink and Goseva-Popstojanova (2016), awareness-training educates employees regarding concepts such as cybersecurity threats and operational management controls that can protect enterprise systems (ES) resources. Unfortunately, there are many

websites that store passwords in plaintext (Bauman, Lu, & Lin, 2015). This issue can cause backdoor intrusions for many users. The information technology department is an entity that needs to be aware of enforcing information assurance principles to its people, operations, and technology to deliver secure network implementations to the information infrastructure of the enterprise. Information assurance depends on people, operations, and technology to meet the objective and business requirements of the industry.

People. Corbetta et al. (2014) proposed a game that can help people not to get scammed. Training sessions help educate people, so backdoor intrusions are stopped as much as possible to protect network systems. Also, information technology offers services to multiple people depending on the size of the organization, and each organization has its peculiar way to provide this service. White, Ekin, and Visinescu (2017) concluded that education and training to personnel increase the awareness employees and elevate the recognition of security incidents. Organizations can use this to protect the network against backdoor intrusions. Even employees that do not need to access the network root must be aware of limiting themselves to their duty descriptions and not cross lines to gain unauthorized access to other areas.

Operations. Privacy and security constructs must be part of the daily activities of the information technology department. Bansal (2017) argued that information assurance ties the following two constructs: privacy concerns and security concerns that elevate such constructs into a higher order. Part of the operations portion of the IT department is the integration of functional systems such as operations, finance, and accounting, also known as enterprise information systems (EIS) (Sun, Strang, & Firmin, 2017). Integrating new emergent technologies to support information assurance operations in the IT department allows the continuity of business of the parent organization.

Technology. Technology focuses on four defense-in-depth strategy areas such as network defense, enclave boundary, computing environment defense and the defense of infrastructures that support the overall network of the information technology department. Alsaleh and Al-Shaer (2016) declared that active cyber defense strategies could automatically reconfigure networks and hosts to mitigate potential intrusions. Active cyber defense can be used to defend against sophisticated attacks. Some organizations have employees working from home, and this situation poses a backdoor threat that can cause backdoor intrusions into the network.

The backdoor intrusion issue is created when technology network devices are built with the intent to access a device. Enabling backdoor remote access at the design stage impacts IT departments and their parent business organization. A way to alleviate this backdoor intrusion scenario is not to allow the attacker physical access to the machine (Fattori, Lanzi, Balzarotti, & Kirda, 2015). On the other hand, a powerful cyber intrusion can be operated within the kernel-level privilege of the operating system in virtual environments. Technology is capable of fixing backdoor intrusions against network infrastructure, but careful attention must be paid at the third party level of device creation.

Conceptual Framework

Goodyear et al. (2014) stated that a robust conceptual framework is needed in order to guide data collection and analysis. The conceptual framework in this study holds four defense strategies necessary in the field of information assurance to secure network systems from backdoor intrusions. The first strategy is to enforce an active information assurance defense-in-depth approach which balances three critical elements: people, technology, and operations. Xingguo et al. (2016) stated that active defense technologies work best against backdoor

intrusions versus passive defense technology because the active approach enables detection before the system gets compromised.

The second strategy is to include defense tools & practices to mitigate backdoor intrusions. Ji-Ho et al. (2016) recommended an intrusion prevention strategy using log file and password to overcome integrity check failed in most IDS tools. Parameshwarappa et al. (2018) studied attack strategies against rule-based intrusion detection system tools to prevent cyberattacks that can be useful for network security managers.

The third strategy is having defense funding and staffing available to enforce information assurance policies and procedures that can ensure personnel know their roles and responsibilities and that they are aware of their hardware device vulnerabilities to implement protection of those devices against backdoor attacks. Li and Zhang (2015) came up with an intrusion protection system making up for a firewall, a honeypot and an intrusion detection system based on a technique called correlation policy.

The fourth strategy is the defense culture and awareness strategy that should ensure that an organization has members with the ability to protect the network from hardware-based attacks and use countermeasures to defend against such intrusions. Farhaoui (2016) stated that human errors are the cause of internal faults into systems enabling backdoor intrusions. A defense culture concept must be enforced within all personnel in the information technology department spreading the idea of defending the network against backdoor intrusions. The objective of the conceptual framework was to enhance information assurance strategies for the use of information technology departments.

Figure 2 represents the conceptual framework and the research question of this study based on four strategic approaches designed to secure network systems against backdoor

intrusions. The defense-in-depth strategy is the core principle operating under the conceptual framework. The research question is what are the strategies network security managers need to protect their networks from backdoor intrusions?

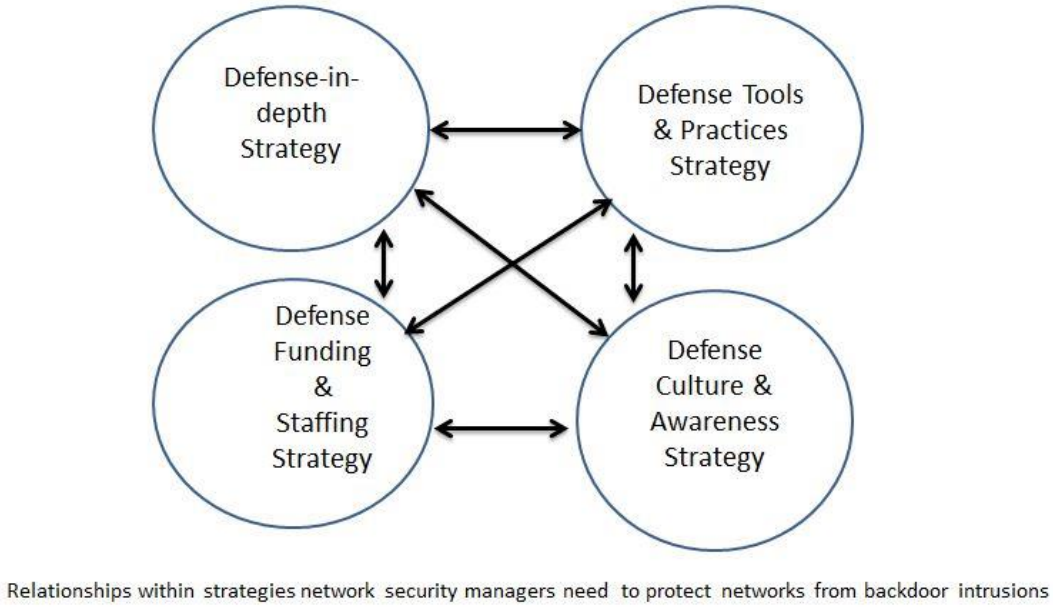

Figure 2. Conceptual Framework.

Summary of Literature Review

Chapter 2 reviewed literature related to four defense strategies needed to secure networks from backdoor intrusions. Orojloo and Azgomi (2017) defined defense-in-depth as a multiple layer security strategy. These four defense-in-depth approaches are the defense strategy, the defense tools & practices, the defense funding & staffing and the defense culture, and awareness strategies. The first approach describes what the network defense strategy used by the organization is. The second approach informs defense tools and best practices that the information technology department uses in its organization. The third approach of the conceptual framework is defense funding and staffing and the final approach addresses the defense culture and awareness of the IT department.

This study explored the strategies network security managers need to protect their networks from backdoor intrusions. Guo et al. (2016) stated that third party system-on-chip (SoC) platforms concentrate their intellectual property (IP) on functionality rather than trustworthiness opening access to modify the functionality. This open access leads to backdoor intrusions that are undetectable since third-party hardware focuses on intellectual property functionality rather than its trustworthiness. Therefore, integrated circuits located in network devices enable backdoor intrusions. This type of hardware-based cyber-attacks causes adverse ripple effects on information technology networks allowing backdoor intrusions. These computer hacks can be remotely triggered using programming codes that connect to the code embedded into the electronic circuits. This unchecked integrated circuit building process shows a contradiction or gap that affects network systems for future backdoor intrusions to occur.

Chapter 3 describes the methodology and design used in the study which is of qualitative nature and explores strategies systems administrators or network security managers need to protect their network systems against backdoor intrusions. For this qualitative study, the researcher was the key instrument to collect the data (Creswell & Poth, 2007). The data was collected through interviews. The methodology supported the investigation of how experienced IT system administrators or network security managers were protecting their organization network and if their defense methods were preventing backdoor intrusions.

CHAPTER THREE

The purpose of the qualitative study was to explore the strategies network security managers need to protect their networks from backdoor intrusions. Adding many types of security technologies to network systems not designed to work with the specific needs of the organization might add more problems than solutions to the network environment (Cleghorn, 2013). Rocha Flores et al. (2015) declared that another layer of defense would hopefully prevent a full breach, but Boggs et al. (2014) argued that few attacks could bypass the current defense-in-depth deployments because they are redundant. The network has devices that allow several malicious codes or enables backdoor intrusions on devices that are increasingly available on the internet (Lee et al., 2014). For instance, kernel rootkits hide malicious processes and thus backdoors can evade detection (Chen, Desmet, & Huygens, 2014). Adding many layers of defense into computer networks increases backdoor access, and this defense method might add vulnerabilities in the network infrastructure of information technology departments. It is not clear if systems administrators are aware that the defense concept applied to network systems is adding backdoor access for hackers and hacking machines to force backdoor intrusions into computer systems of the organization.

Chapter 3 identifies the research methodology employed to discuss the critical elements of an effective strategy for protecting network systems from backdoor intrusions. This chapter included (a) research tradition, (b) the research question, (c) research design, (d) population and sample (e) sampling procedure, (f) instrumentation, (g) validity, (h) reliability, (i) data collection, (j) data analysis, (k) ethical considerations, and (l) chapter 3 summary. Each section addressed the means in which the central research question was examined.

Research Tradition

In the late 1960s and early 1970s, qualitative inquiry was a new concept of evaluation with the intent of gathering and reporting data and developing the field of education (Goodyear et al., 2014). Since then, qualitative research has evolved. For example, management add benefits in research because they can refine research goals. Research goals can provide focus in the study to assist the researcher. The methods of qualitative research can evaluate information, generate new data, and it is insight-driven, providing more in-depth information on unexplored topics (Nunnally & Farkas (2016). Joyner, Rouse, and Glatthorn (2013) emphasized that the qualitative methodology is used in research to view the perception of individuals based on their experience. The study interviewed 12 participants that had experience in information technology managing or systems administration and how they mitigated backdoor intrusions.

A research design is used to make an inquiry within a chosen methodology whether qualitative, quantitative or mixed methods (Creswell, 2014). The qualitative methodology chosen for this study followed an exploratory direction and design. Exploratory studies can help clients understand how an innovative program works (Goodyear et al., 2014). This qualitative inquiry design explored backdoor intrusions with the intent to make a contribution to knowledge to strategies used in the field of cybersecurity and information assurance.

Mollick (2014) declared an exploratory study design follows a tradition of understanding first steps into a new phenomenon with the objective of developing initial evidence. The exploratory qualitative approach was appropriate for the study because it investigated the strategies network security managers need to protect their networks from backdoor intrusions in IT departments at the system administrator level, and if systems managers are mitigating backdoor intrusions. For example, backdoor intrusions can access the rights of the system administrators in the network, and a failure sequence can be initiated to start power outages on

electrical network systems (Goh, yi Sim, Mohamed, Mohamed, Ling, Chua, & Goh, 2017). Krombholz, Mayer, Schmiedecker, and Weippl (2017) suggested that a security deployment process is far too complex for experienced security auditors and that server configuration should have a stronger security protocol by default.

There were three design options considered during the development of this study: ethnography, phenomenology and case study. The ethnography design was not considered for the study because it is designed to inform future theory-driven evaluations to broaden its appeal, making the results of the research more relevant to management (Goodyear et al., 2014). Miles et al. (2014) expressed that the phenomenological design tends to look at data thematically to capture essential meanings of the participants, lending themselves to multiple interpretations, and this is the reason this design was not considered for the study. The case study design did not meet the criteria used in the research because it is not of a pre-experimental design nature nor does it depend on analogical reasoning (Willis, Jost, & Nilakanta, 2007). The quantitative methodology approach was not used for the study because Alexander (2017) conducted a quantitative study in information assurance defense-in-depth measures and recommended additional exploratory models to improve IT security.

Research Question

The central question of the study is what are the strategies network security managers need to protect their networks from backdoor intrusions?

Research Design

Lang and Howell (2017) stated research design involves a process of understanding the problem before coming up with a solution. The research design for the study was composed of a series of steps to acquire information derived from the research question. These steps were: population and sample, sampling procedure, instrumentation, validity, reliability, data collection,

data analysis, and ethical considerations. Following the study design helped to explore and discover information based on data obtained as a result of interviews with experienced IT systems administrators and network security managers designed to address the central research question. The research design chosen is described in the following sections.

Population and Sample

The target population in the study consisted of experienced network security managers or systems administrators involved in both Volusia and Orange counties from the state of Florida. Both counties included the cities of Deltona, Daytona Beach, Ormond Beach, Orlando and Apopka to name a few. The estimated size of the target population is about 2,970 network and computer systems administrators (Bureau of Labor Statistics, 2018). The population chosen for the study was appropriate because experienced IT system administrators and network managers are responsible for implementing security protocols in their IT departments in an effort to protect their proprietary data and personal information while also protecting the confidentiality, integrity, and availability of their computer systems against backdoor intrusions.

Nunnally and Farkas (2016) made it clear that qualitative methods are suitable for small sample sizes, especially when the researcher can travel to meet with participants in their environment. A sample is one of many possible ways to gather information that can be used by researchers for further studies (Goodyear et al., 2014). The sample size for the study consisted of 12 experienced IT system administrators or network security managers involved in detecting cyber-attacks and mitigating backdoor intrusions. In 2009 and 2016, the National Institute of Standards and Technology (NIST) conducted studies on topics related to network security where similar sample sizes were used (DePoy & Gitlin, 2016; Paulsen & Toth, 2016).

Sampling Procedure

A sampling procedure is a step that determines, describes and selects the characteristics of the participants (Grossoehme, 2014). For this qualitative exploratory study, purposeful sampling was used as the sampling procedure. Purposeful sampling allows for research participants to be carefully selected and gathers an in-depth understanding of information-rich cases and yield critical and timely insights (Goodyear et al., 2014). The purposeful sampling procedure was appropriate because it can help one better understand strategies experienced network managers used against backdoor intrusions (Creswell, 2014).

Before the participants were selected, a discussion of the letter of permission was presented to obtain approval and authorization from participating sites because the research needed to be approached with care (See Appendix C; Creswell, 2014). The letter of permission explained that the data collection, observations and recorded notes would remain the property of the researcher, and they are anonymous and strictly confidential (Creswell, 2014). The participants were given a reserved right to withdraw from the study at any time if circumstances were to change without the participants having any negative repercussions (Goodyear et al., 2014).

After the proposal and Institutional Review Board (IRB) were approved, an informed consent form was delivered to candidate participants, and they were contacted by phone or email to request their participation in the study. The contact information was obtained from public information at the Volusia and Orange counties and the Bureau of Labor Statistics websites. The appropriate selection criteria of the participants were based on the knowledge participants have in managing networks and their experience with strategies to secure networks from backdoor intrusions (Goodyear et al., 2014; Palys, 2008). Network managers and systems administrators were expected to have experience applying strategies to protect network systems from backdoor

intrusions. Network managers were contacted to request permission to participate in the study. Then, an informed consent form (See Appendix A) was sent to each participant. Once the informed consent was properly signed, the interview dates, times and locations with each study participant were scheduled following Institutional Review Board guidance (Longhofer, Floersch & Hoy, 2012).

Instrumentation

Miles et al. (2014) mentioned good qualities of a professional qualitative researcher-as-instrument such as familiarity with the setting and phenomenon, being comfortable with participants, and meticulous attention to detail. The researcher chose the exploratory qualitative method which affects how data is collected (Myers & Avison, 2002). In this qualitative study, the instrument responsible for collecting reliable data was the researcher (Knowles & Cole, 2008). Miles et al. (2014) announced that instrumentation includes a set of procedures with the purpose of collecting data and these procedures generate observations and record events. Goodyear et al. (2014) stated that researchers must adapt to local conditions in order to accommodate the needs of the management population. Most essential insights are generated with direct and open-ended semi-structured interview questions. Permission was not needed for this qualitative study in order to reuse or modify a pre-existing instrument because the researcher was the critical instrument to collect the data and the interview questions were written by the researcher (Creswell & Poth, 2007).

The investigator coordinated appointments and arrangements were made to schedule and review the consent form after participants were interested in being part of the study to answer the interview questions (Longhofer et al., 2012). Interviews lasted 20 to 40 minutes per participant based on the answers given from the interview questions (see Appendix B). Audio notes were recorded and transcribed using semi-structured questions that became the instrumentation

methods to collect valid and reliable data (Miles et al., 2014). The open-ended interview questions were designed to generate in-depth responses on the strategies that experienced network security managers use to protect networks from backdoor intrusions (Goodyear et al., 2014). The questions determined what the findings were, and based on the findings probing questions followed to find more details related to backdoor intrusions (Myers & Avison, 2002). Interviews took place at a date, place and time convenient for each participant.

Creswell (2014) stated that observations could be captured via handwritten notes and digital audio, combined with visual observations to record any speculation, feelings, ideas and other impressions. Labeling helps name categories with terms based on the actual language of the participant (Creswell, 2014). The researcher provided participants with the assurance that the organization will not be harmed by participating in the study (Myers & Avison, 2002).

Validity

Validity is when the results of the study reflect with precision what it is supposed to reflect, indicating the data is well grounded (Schwandt, 2015). Validity is important because it allows the reader to believe the results of the study are real (Willis, Jost, & Nilakanta, 2007). Lang and Howell (2017) compared validity as making trustworthy decisions based on the results of the study. Bauer and Gaskell (2000) argued that the validity of the data could be enhanced by making sure interviewees see the data in order to consent to, reject or correct the data to ensure the data is accurate.

Schwandt (2015) stated that Lincoln and Guba (1985; 1989) developed four criteria for judging the quality of a qualitative inquiry. First, credibility (internal validity) provides assurance between the views of the respondent and the inquirer. Credibility is important because it is vital to establish trust to the reader by describing some detail on how to report the results of the work (Myers & Avison, 2002). Second, transferability (external validity) is the responsibility of the

inquirer to make enough information available for the reader to transfer and use. Transferability is essential because it provides to other researchers a robust framework for comparison (Creswell, 2014). Third, dependability (reliability) focus that the study is logical, documented and traceable. Dependability measures to certain extent aspects of the quality of the interviews (Bauer & Gaskell, 2000). Fourth, confirmability (objectivity) is concerned with the factual interpretation of data and not a fantasy of the inquirer. Confirmability is important because it has the ability to reach consensus within the specialized community through reason (Schwandt, 2015).

Reliability

According to Schwandt (2015), reliability relates to the ability to generate and interpret data through careful documentation. Reliability is a traditional criterion that, to a certain extent, measures aspects of the quality of the interviews (Bauer & Gaskell, 2000). Reliability makes the study capable of being replicated, at least in principle, by another inquirer (Schwandt, 2015). Reliability is enhanced when the approach used by the researcher is consistent (Creswell, 2014). The reliability of interviews can be enhanced by a detailed analysis of the interview questions (Bauer & Gaskell, 2000). Member checking occurs when the participants are asked to provide their judgment and their major findings to the researcher (Miles et al., 2014). After reviewing the interview data, some adjustments may be necessary during the evaluation process (Goodyear et al., 2014).

The use of the triangulation method occurs when the research findings are corroborated and become similar based on different studies to establish credibility (Goodyear et al., 2014). The investigator did not use the triangulation method on this study because the analysis of the research question was not done from multiple perspectives; the analysis of the research question

was done only by the investigator without involving other colleagues within the field of information assurance.

Data Collection

Data collection is an essential research tool that opens up a view of key components of the role of the theory that has been investigated (Longhofer et al., 2012). The data was captured through the process of open-ended interview questions with participants working as managers from different information technology departments covering Volusia and Orange counties of Florida. The interviews were based on open-ended questions (Myers & Avison, 2002). The data collection method was conducted through face to face interviews that lasted less than an hour. The research question generated specific data to be collected for the investigation through related interview questions (Myers & Avison, 2002). Information such as the source of data and method of capture is gathered during the data collection process (Southekal, 2017). Advanced planning took the place of what data needed to be collected in the process of producing evidence in order to collect the right data in the right way (Lang & Howell, 2017).

The researcher was the main instrument in the data collection process (Creswell, 2014). Gilbert (2000) stated that data collection highly depends on the personal position of the researcher. The way questions are asked and how well the conversation went with interviewees determines how the data collection process will unfold (Goodyear et al., 2014). Analytic display formats can be developed during and after the data collection process (Miles et al., 2014). Although there are differences between data collection and data analysis, there is also some overlap.

Data Analysis

Human coding is a unique property of qualitative data analysis (Lazar, Feng, & Hochheiser, 2017). Goodyear et al. (2014) stated that data analysis emerges during the data

collection process and continues to evolve after the data has been collected. The feedback must be recorded to be able to use it, refine it, and to revise the data and present the analysis in a coherent form. There is a potential for management to influence the data with their own bias so ensuring professional standards of practice is advised (Goodyear et al., 2014). Data analysis was done manually. The investigator used a template divided into four columns. Column one had the transcripts, and the theme developing process was written in the remaining columns by using sentences, phrases or words to clarify specific themes emerging in the process and also categorizing each of the emerging themes in different lists.

Qualitative data analysis is descriptive and is used to draw conclusions from unstructured data like audio, images, video or text. Once qualitative data is arranged into categories, the next step is to quantify the values (Southekal, 2017). Lang and Howell (2017) suggested five phases as part of the data analysis process: make a plan, absorb data, find patterns, use patterns, and create the narrative.

Ethical Considerations

All research designs must seriously consider issues related to ethics concerning how the study is conducted and how human subjects are treated. The researcher has the expressed obligation to respect the rights of the informants (Creswell, 2014). Part of ethical duty is to ensure that the information collected is not disseminated (Gilbert, 2000). According to Goodyear et al. (2014), the Belmont Report provides guidance on ethical interaction and the treatment of human subjects in research. Ethical reviews help to make sure information discovered does not damage the interviewees (Miles et al., 2014). According to Willis, Jost, and Nilakanta (2007), ethical guidelines call for participants to provide informed consent to the study.

According to the Department of Health and Human Services (2014), The Belmont Report summarizes ethical principles and guidelines for researching human subjects. The report

summarizes boundaries between practice and research, basic ethical principles such as respect for persons, beneficence, and justice in order to protect human subjects and mitigate risk against harm. The report also describes the importance of having a signed informed consent form for each participant and an assessment of risks and benefits in the selection of subjects. There are serious ethical issues and considerations when doing research with human subjects, and the Belmont Report is the document that provides appropriate legal guidelines intended to be available for scientist and members of the Institutional Review Boards (IRB). In accordance with these ethical guidelines and principles, prior to the beginning of interviews, participants were presented with an informed consent form to read and sign. In addition, the interview protocol ensured that all participants were aware of their right to be part of a process that respects their safety and autonomy, including their right to terminate the interview process at any time and for any reason.

According to Pelleó and Reber (2016), research ethics covers many problems such as precautions to consider for preventing harm to human subjects or inappropriate behavior by researchers in the conduct of their work. Ethics and morals terms are often used interchangeably, and both terms indicate an area of concern related to what is bad or good (Pelleó & Reber 2016). The concern involving the use of machines and software where there are no humans involved is about making sure researchers are not causing harm to humans while using electronic software tools and machines in the research process. This also includes avoiding the misuse of private information and other breaches caused by electronic means (Department of Health, 2014). To meet this standard, the researcher took steps to ensure that participant responses, including names, were coded to protect their anonymity. All data collected is stored securely in password-

protected files. Data from the study remains securely held for three years, after which the records will be destroyed.

Summary of Chapter Three

Chapter 3 started with an introduction and presented the following sections: (a) research tradition, (b) research question, (c) research design, (d) population and sample (e) sampling procedure, (f) instrumentation, (g) validity, (h) reliability, (i) data collection, (j) data analysis, and, (k) ethical considerations. The intent of chapter 3 was to present the reader with a basic understanding of how this qualitative approach explored the research problem.

The framework of chapter 3 described the study participants, observation, location, and how data was collected and analyzed. Chapter 3 also reports the methodology used in the study. This chapter outlined sections with the purpose of exploring the strategies network security managers need to protect their networks from backdoor intrusions.

The objective of chapter 3 was to lay the groundwork for how evidence was processed and analyzed to provide information of an unexplored topic related to stealth backdoors and what experienced IT professionals were doing to manage such backdoor intrusion issues. The findings may contribute to the field of cybersecurity and information assurance. One-on-one qualitative interviewing is the most flexible approach to exploring how experienced IT system administrators and network managers are dealing with backdoor intrusion problems in network devices (Lang & Howell, 2017). Also, the exploratory research stressed the significance of context, setting, and the frame of reference of the participants (Gilbert, 2000). Miles et al. (2014) argued that heavy initial instrumentation or closed-ended devices are inappropriate for an exploratory inquiry.

CHAPTER FOUR

The purpose of the qualitative study was to explore the strategies network security managers need to protect their networks from backdoor intrusions. The research question explored on this qualitative research was “what are the strategies network security managers need to protect their networks from backdoor intrusions?" The fundamental problem was that backdoor intrusions are still affecting the IT departments despite the use of many protection layers in network systems as a strategic defense. Chapter 4 presents the results or findings of the research based on the answers given by 12 participants experienced in managing networks in their respective IT departments and organizations. Chapter 4 includes the data analysis collected from interviews, participant demographics, emerging themes, categories, and summary.

Participant Demographics

Participants were holding management or administrative positions for their respective IT departments. Each person was contacted either by email, phone calls or in person. The participants were given credentials about the investigator in order to get acquainted. Once the participants agreed to the interview, they were required to sign an Informed Consent (Appendix A). The average time to conduct the interview was approximately 30 minutes. The participants answered nine questions. The participants had experience as managers or systems administrators involved in IT departments covering the areas of Volusia and Orange counties located in the state of Florida. Ten organizations were selected for the study, with two organizations providing two participants each. Table 1 reports the participant demographics data. The table has three columns identifying twelve participants by identification number, gender, and position. Anonymity is established by identifying participant identification (PID) numbers 1 through 12.

Table 1

Participant Demographics

PID	Gender	Position
1	Male	Network administrator
2	Male	IT manager
3	Male	IT manager
4	Male	IT manager
5	Male	IT manager
6	Male	Systems administrator
7	Male	Network management
8	Male	Systems administration
9	Male	System administrator
10	Male	IT administrator
11	Male	Network administrator
12	Male	Network administrator

PID = Personal Identification

Table 2 presents additional statistics information from the twelve participants. The table has four columns reporting the type of industry of each participant, whether or not the participants had IT experience, their IT key position and the benefits they provide to their organization.

Table 2

Additional Statistics from Participants

Type of industry	IT experience	IT key position	Benefits of managing information systems
Government	Yes	Network administrator	Achieve efficiency
Healthcare	Yes	Chief information officer	Improves the quality of decisions
IT services	Yes	Company president	Provides data
IT services	Yes	Engineering	Identify strengths and weaknesses
City government	Yes	Director and records manager	Tells what is going on in the IT business
Education	Yes	Executive director	Operations and Management
City government	Yes	IT supervisor	Tells what is going on in the IT business
City government	Yes	IT administrator	Tells what is going on in the IT business
Cloud Services	Yes	InfoSec analyst / Engineer	Achieve efficiency
City government	Yes	IT manager	Tells what is going on in the IT business

City government	Yes	IT Manager	Tells what is going on in the IT business
City government	Yes	IT Administrator	Identify strengths and weaknesses

Presentation of the Data

Nine interview questions were asked of each of the 12 participants. The interview questions for this study were:

1. From your perspective as a manager of network security, what do you regard as the most effective network security monitoring strategies?
2. What is your protocol for determining if an intrusion to the perimeter-based security into the system has taken place? In other words, how do you know when you have a backdoor intrusion?
3. In your role as a network manager what has been the level of support for you and your staff to be able to implement the most effective strategies?, for instance, through staffing and funding?
4. When it becomes clear that the network has experienced a backdoor intrusion, what is the usual protocol or strategy that is employed to address the problem?
5. Could you please tell me as much as possible about the details of your experience selecting appropriate countermeasures as an IT manager working in the area of network security?
6. How does having the right kinds of staff members impact your ability to carry out an effective strategy for network protection?

7. What are your thoughts about the role of employees throughout the organization as part of the strategy of defending your network from backdoor intrusions?
8. The defense-in-depth strategy seems to be pretty widely accepted as the standard for network security. What is your perspective on the effectiveness of this strategy?
9. What other points would you like to make that we did not address during the interview that you think are key to an effective network security strategy?

The data collection process included that the interviewer selected network managers from different organizations that have an IT department. Twelve interviews were conducted for this qualitative exploratory study. Data saturation was reached after the twelfth interview. Each participant agreed with the interviewer to choose the location and interview times necessary to conduct the interviews. Participants granted permission to record their interviews by signing the informed consent form (Appendix A). The researcher took field notes while each interview was recorded. The interviewer transcribed all recorded audio, and the data was saved to an encrypted USB flash drive using Microsoft BitLocker. Once all 12 interviews were completed, the audio files were transcribed. For validity purposes, member checking was used to verify credibility, transferability, accuracy, and validation on the part of all respondents.

Next are the findings and analysis for each of the nine interview questions used on the interviews.

Interview Question 1

From your perspective as a manager of network security, what do you regard as the most effective network security monitoring strategies?

***Probe question* - please share an example?**

Aggregated data for Interview Question 1 yielded seven prominent themes: (a) protect data, (b) risk analysis, (c) recommend findings, (d) monitoring team, (e) internal message alerts (f) log notifications, and (g) third-party services. The number of responses to each of the prominent themes or topics for Interview Question 1 is shown in Table 3. Each of the indicated themes represents effective network security monitoring strategies by experienced network security managers and systems administrators. Monitoring of scheduling processes that occurred in operating systems is a complicated process in the case of end users, systems administrators or particular users on cloud systems and the requirements for effective monitoring tools are a challenge due to evolving attack vectors (Grzonka, Kołodziej, Tao, & Khan, 2015; Axon, Creese, Goldsmith, & Nurse, 2016).

Table 3

Themes for Interview Question 1

Themes	*n*
Protect data	4
Risk analysis	3
Recommend findings	3
Monitoring team	3
Internal message alerts	3

Log notifications	3
Third party services	2

Interview Question 1, Theme 1: Protect data. Protect data. For Theme 1 of Interview Question 1, 33% of the respondents indicated that besides monitoring data, the intent of protecting data should be included as an effective strategy. Respondents stress the importance of monitoring systems to prepare for defense strategies through end-user education and training to make the monitoring strategy of the network easier by providing well-founded recommendations to security personnel. Furthermore, it is essential to look for signatures in the logs or look for hash codes of suspected files that show unusual behavior and lastly monitor firewalls against internet traffic that is coming in with the intent of protecting data. Table 4 contains the Theme 1 responses for Interview Question 1.

Table 4

Interview Question 1, Theme 1 Responses: Protect Data

Responses
You want to have at each point of your network some kind of detection system and email detection system both on the gateway into the end user and network detection systems coming into your network.
Put as many deterrents between that attack vector and the goal that they are trying to get to prevent them from getting in or hopefully that they just give up and go somewhere else.
Others might want to do a more proactive monitoring approach where you are constantly calling and focusing on the security of clients.

Scanning the network and the educated end-user because that is really the easiest way to get into a network.

Interview Question 1, Theme 2: Risk analysis. For Theme 2 of Interview Question 1, 25% of the respondents indicated that the information derived from network monitoring services is essential for conducting a risk analysis. Network managers and system administrators suggest that the system logs need more analysis and automated checks to see clear trends that can point out behaviors. Participants need help from third parties to conduct risk analyses to detect traffic that is entering from the outside of the network and see what is happening in the system. Table 5 contains the Theme 2 responses for Interview Question 1.

Table 5

Interview Question 1, Theme 2 Responses: Risk Analysis

Responses
We did not want to have the company IP addresses being seen as going to those URLs so we would use a third party web site that would try to open it inside a virtual environment.
When it comes to monitoring, I would say the systems monitoring is really number one to us. We pull in all of our logs. We analyze those logs for trends automatically. If we see something amiss then we pursue it from there.
A good strategy as well as having like a really good alerting and monitoring just coming in from external but the thing is that you definitely do need to have internal or some kind of user behavior analytic type thing to see what is happening within.

Interview Question 1, Theme 3: Recommend findings. For Theme 3 of Interview Question 1, 25% of the respondents indicated that network managers and system administrators must make recommendations after analyzing the results from network monitoring tools. Participants indicated the importance of using intrusion prevention and intrusion detection systems for analysis in a contained virtual environment and to make recommendations to their network response team in order for them to take further actions. However, starting with clear policies and procedures is fundamental including proper documentation on what has been achieved keeping in mind to follow the requirements of the organization. Table 6 contains the Theme 3 responses for Interview Question 1.

Table 6

Interview Question 1, Theme 3 Responses: Recommend Findings

Responses
My primary responsibility was the monitoring of the intrusion prevention and intrusion detection systems and the event systems; trying to analyze the information they have provided us and send a recommendation to our network security response team.
Having well-defined policies and procedures is probably fundamental. Like that building block you have to have. You have to document exactly what you are trying to achieve based on what requirements.
They just are not numbers to see. The things are correlated very clearly so this amount of traffic coming in is coming from these IPs and these domains, so this is blocked.

Interview Question 1, Theme 4: Monitoring team. For Theme 4 of Interview Question 1, 25% of the respondents indicated that a well-trained monitoring team should be available in IT

departments to enhance protection. Network managers and systems administrators advised that users with a lack of knowledge can open malicious emails that could infect the network. Furthermore, teach people how to recognize phishing emails and scam emails to develop strong defenses against threats and keep up with the latest training updates. Table 7 contains the Theme 4 responses for Interview Question 1.

Table 7

Interview Question 1, Theme 4 Responses: Monitoring Team

Responses
If they pass the firewall if they pass software automation that is in place, like a scanning the network and so and so, the educated end-user because that is really the easiest way to get into a network and it is a social networking that folks use or lack of knowledge so you get the email and you click on it and by design those clicks will infect your network so educating the end-user is their best way of dealing with it.
It is just being aware of what is happening. I listen to various security podcast almost every week to hear what is new.
A good training base for people to understand phishing emails, scam emails, changing the password, do not use their birth dates or anniversary or names. Knowledge is one of your strongest defenses against any king of threat.

Interview Question 1, Theme 5: Internal message alerts. For Theme 5 of Interview Question 1, 25% of the respondents indicated that internal monitoring of the network should not be ignored and there is a need for message alerts that provide information on internal traffic behavior. Respondents stated that alerts must be comprehensive and at the same time, be easy to

read and understand. Also, software products can open those alerts and decide if the alert is a false positive or a false negative. A robust monitoring alert system can divide the alerts by categories within the intrusion detection systems. Lastly, the use of ping services to identify devices that are exceeding the threshold could enhance monitoring strategies. Table 8 contains the Theme 5 responses for Interview Question 1.

Table 8

Interview Question 1, Theme 5 Responses: Internal Message Alerts

Responses
The job mainly involved getting alerts from the network defense software, opening up those alerts, digging into them and trying to decide if the alert was a false positive, a false negative or an actual attack of some kind.
One of the most crucial, most fundamental is a simple pulling device that will pull the TCP to the device and alert you when it exceeds the threshold.
I think the most effective is having a very strong externally facing monitoring that alerts inward and gives very comprehensive reports that are easy to read.

Interview Question 1, Theme 6: Log notifications. For Theme 6 of Interview Question 1, 25% of the respondents indicated that systems log notifications should be provided in real time to have an accurate view of what is happening in the network in order to help in the decision making process and protect the information systems of the organization. These network managers indicated that a continuous monitoring system on the servers that are set up to look for isolated events could notify system administrators of important issues affecting the network. The next step is to see an event message that is scattered and might seem innocent, but when

combining them with other events brings a clear picture of the threat. Table 9 contains the Theme 6 responses for Interview Question 1.

Table 9

Interview Question 1, Theme 6 Responses: Log Notifications

Responses
We use something that continuously monitors all of our servers and all of our network traffic and looks for those isolated events. It sees if they are all happening at one point time, puts them all together then it starts to notify us and we start taking a deep dive into the issue.
Seeing the behavior of the connections and how suspicious the connections can be is one of the things that I understand is important.
Have an active live monitoring solution that is either continuously testing the policy or looking at the events within the policy to look for certain patterns and behaviors and failures of the BIOS messages.

Interview Question 1, Theme 7: Third party services. For Theme 7 of Interview Question 1, 17% of the respondents indicated that paying for third-party services helped with detecting threats and monitoring the network infrastructure in their departments. Participants shared that third-party assurance is a big deal because they provide websites that will do risk analysis and monitor financial transactions. Additionally, third-party services protect data for hospital services and provide overall transparency for the organization. Table 10 contains the Theme 7 responses for Interview Question 1.

Table 10

Interview Question 1, Theme 7 Responses: Third Party Services

Responses
We would use multiple third party websites that would do risk analyses on those URLs because we did not want to have the company IP addresses being seen.
The third party assurance thing is a pretty big deal because most hospitals have to send data somewhere else to have other folks do things for us.

Interview Question 2

What is your protocol for determining if an intrusion to the perimeter-based security into the system has taken place? In other words, how do you know when you have a backdoor intrusion?

***Probe question* - how you identify backdoor threats?**

Aggregated data for Interview Question 2 yielded seven prominent themes: (a) backdoor analysis, (b) brute force, (c) backdoor detection, (d) phishing emails, (e) compartmentalized email gateways, (f) zero-day, and (g) identifying backdoors. The number of responses to each of the prominent themes or topics for Interview Question 2 is shown in Table 11. Perimeter-based security is not enough for the zero-day exploit market. For instance, a Distributed Denial Of Service attack (DDoS) is an example of an effect caused by a backdoor intrusion that is hard to detect because to perform the attack an intrusion needs to be done to a set of computers prior to reaching the perimeter of the target network (Harasta, 2014; Kotenko & Ulanov, 2014).

Table 11

Themes for Interview Question 2

Themes	*n*
Backdoor analysis	5
Brute force	5
Backdoor detection	4
Phishing emails	3
Compartmentalized email gateways	3
Zero-day	3
Identifying backdoors	2

Interview Question 2, Theme 1: Backdoor analysis. For Theme 1 of Interview Question 2, 42% of the respondents indicated that a software and hardware backdoor analysis is necessary for the identification of backdoor threats. Furthermore, respondents stated that having an anti-hack or firewall including anti-phishing of software and hardware devices must notify by email or text to see any issues arriving in the system. Additionally, respondents further indicated proper software to alert behavior is crucial for in-depth analysis especially on webpage services should be part of the desired protocol to identify if an intrusion has taken place. Table 12 contains the Theme 1 responses for Interview Question 2.

Table 12

Interview Question 2, Theme 1 Responses: Backdoor Analysis

Responses
Usually you will have some kind of anti-hack or a firewall, anti-phishing some kind of software

or hardware device that if it is good, will notify you be it be by email or a text; something like that to let you know there is an issue going on.
If there is an incident that identifies some type of attack; either because an antivirus identified virus on a computer or is seeing some kind of errant behavior within the network.
How are you going to know if you do not have the proper software to alert on it?
We have our own software and hardware experts do a deep analysis on the equipment to make sure that there is nothing in there that could harm us.
We rely on some webpage services, security products and appliances to monitor intrusions.

Interview Question 2, Theme 2: Brute force. For Theme 2 of Interview Question 2, 42% of the respondents indicated the use of brute force at the perimeter area of the network is part of an excellent protocol to implement in the security of the network. These managers advised that having a penetration test team can enhance the protocols used to identify backdoor threats. Participants that have not experienced a brute force penetration test at the perimeter of the network depend on other devices or equipment at the perimeter that is more relevant to them because protocols have to adjust to the objective and limitations of their parent company. Table 13 contains the Theme 2 responses for Interview Question 2.

Table 13

Interview Question 2, Theme 2 Responses: Brute Force

Responses
Fortunately we have not experienced a penetration. I have in the past had to deal with a brute force attack or something like that. We have not had to deal with a brute force penetration.
A backdoor would be a piece of software or hardware installed into a device or software package

that allows the manufacturer or an outside source or outside individual to access it without permission.
Investigating a backdoor threat is not easy. We are talking about backdoor threats that are usually connections that are initiated by some user.
It is going to be a sys log review; Something is up if you start seeing anomalies in your traffic patterns.
Having a backdoor intrusion is really hard to detect. First of all, you want to have a strong security policy and regular reviews of network security based upon your policy.

Interview Question 2, Theme 3: Backdoor detection. For Theme 3 of Interview Question 2, 25% of the respondents indicated backdoors are challenging to detect. Respondents indicated that end users receive emails that look legitimate, but when they open the emails, backdoors are activated. However, firewalls are set up to send alerts through text or email messages even though are difficult to determine the threshold when receiving those alerts. Table 14 contains the Theme 3 responses for Interview Question 2.

Table 14

Interview Question 2, Theme 3 Responses: Backdoor Detection

Responses
For example, an email they receive, a page that is not supposed to enter they enter.
An email they receive, a page that is not supposed to enter they enter and then give them an ok that they do not have to enter.
We have our firewall set up to send us alerts through email or text message in case our email system is compromised.

What is very difficult is determining the threshold for where you want to receive alerts and that is where it is trial and error.

Interview Question 2, Theme 4: Phishing emails. For Theme 4 of Interview Question 2, 25% of the respondents indicated that detecting phishing emails at the perimeter should be a component of a protocol for determining if an intrusion has taken place. Network managers and system administrators suggest checking the user bandwidth for threats, downloads and streaming services that could potentially enable intrusions. Participants mentioned having email security service providers that are capable of detecting phishing emails. Additionally, having the perimeter secured inside its area that in order to avoid complete open access for attacks but at the same time separated from the network is a good strategy for detection of phishing emails. Table 15 contains the Theme 4 responses for Interview Question 2.

Table 15

Interview Question 2, Theme 4 Responses: Phishing Emails

Responses
The time stamp is actually parsed out to an actual date time and that can be visualized on a graph. We can use that to correlate it with other events at the same time so that helps us for determining if it is something in our perimeter.
We have email security vendors can detect phishing emails and things like that.
You want to have the perimeter inside its own secured area so that it is not open to every attack.

Interview Question 2, Theme 5: Compartmentalized email gateways. For Theme 5 of Interview Question 2, 25% of the respondents indicated that compartmentalizing email gateways

at the perimeter should be a component of a protocol for determining if an intrusion has taken place. Additionally, the email gateway must be outside for people to have access before the email is opened in order to stop a phishing email that has been detected. Participants need the education to recognize suspicious emails before they are opened in order to avoid a virus propagating into the system. Lastly, email logs could offer information about untrusted attachments that must not be clicked on to avoid intrusions. Table 16 contains the Theme 5 responses for Interview Question 2.

Table 16

Interview Question 2, Theme 5 Responses: Compartmentalized Email Gateways

Responses
You can have stuff in the perimeter. You might have an email gateway in the perimeter that is outside people have to access.
If you have a perimeter based security issue, you have a system in place that not only detected it but also stopped it.
Logs and archived arrival of an email for a participant employed within our network and then how it proliferated through; who it went to, attempts at containment that and remediation.

Interview Question 2, Theme 6: Zero-day. For Theme 6 of Interview Question 2, 25% of the respondents indicated one way to deal with zero-day problems is to get help from the end user that might notice any suspicious behavior in the computer while working at any given moment. Respondents suggest having an anti-hack or firewall device capable of notifying someone by email or text when a phishing attempt is occurring. Participants also stated that the end user is the number one deterrent that could notice any email attachments or links that are not

normal. Furthermore, the end user may contribute by noticing common zero-day issues such as zero-day viruses, attachments, or zero-day links allowing backdoor intrusions to affect the network. Table 17 contains the Theme 6 responses for Interview Question 2.

Table 17

Interview Question 2, Theme 6 Responses: Zero-Day

Responses
You still have zero day viruses. Attachments or links in phishing emails that those systems can not detect so our number one deterrent is our end user.
Usually you will have some kind of anti-hack or a firewall, anti-phishing, some kind of software or hardware device that, if it is good, will notify you by email or text to let you know there is an issue going on.
It is a combination of several different products that actively monitor the network traffic and look for specific signatures and patterns and then it alerts us accordingly.

Interview Question 2, Theme 7: Identifying backdoors. For Theme 7 of Interview Question 2, 17% of the respondents indicated different methods to test how their end-users behave when they are deciding to either click on a suspicious email attachment or go to websites that are not job-related and using this technique, the company can assess which users are more susceptible to allow backdoor intrusions to the systems. Respondents also pointed out fake phishing email tests to discover which employees need more training and whether or not they need to have their evaluation affected by their decision-making process when clicking on additional pages that they are not supposed to access. Furthermore, this protocol could help to control which emails should be allowed to enter or which ones should not in order to develop

some access control mechanism. Table 18 contains the Theme 7 responses for Interview Question 2.

Table 18

Interview Question 2, Theme 7 Responses: Identifying Backdoors

Responses
And so we spend a lot of time training. We also conduct fake phishing email tests.
If you do not have a threshold set at a good level, what you are going to end up with is not enough emails. It is kind of like when you are dealing with your spam filter; make it too strict.

Interview Question 3

In your role as a network manager what has been the level of support for you and your staff to be able to implement the most effective strategies?, for instance, through staffing and funding?

***Probe question* - could you elaborate on this a little?**

Aggregated data for Interview Question 3 yielded seven prominent themes: (a) executive, (b) organizational, (c) information technology, (d) client, (e) financial, (f) staffing, and (g) leadership. The number of responses of each of the prominent themes or topics for Interview Question 3 is shown in Table 19. Information security managers must be part in the decision-making process resulting on effective network strategies when investing is resources to support cybersecurity; funding programs in organizations are complex stages that needed expertise and is financially limited (Fielder, Panaousis, Malacaria, Hankin, & Smeraldi, 2016; Green et al., 2015).

Table 29

Themes for Interview Question 3

Themes	*n*
Executive	4
Organizational	4
Information technology	4
Client	4
Financial	4
Staffing	4
Leadership	3

Interview Question 3, Theme 1: Executive. For Theme 1 of Interview Question 3, 33% of the respondents indicated that having executive support has a significant impact on implementing effective strategies. However, respondents stated that they need buy-in support for security webinars or keynote training to enhance strategies within the IT department. Furthermore, there is miscommunication between the IT department and higher levels because the higher level is aware of the need for support, but the IT department thinks the opposite causing misunderstanding. Table 20 contains the Theme 1 responses for Interview Question 3.

Table 20

Interview Question 3, Theme 1 Responses: Executive

Responses
We have a whole department that supports us. Everybody has a different position and we all work together. Everybody has a certain role or priority so my main thing is the network.

I have our executive leadership support.
It is really hard and everywhere you go, every bit of webinar or keynote that you are going has a lot to do with getting executive management buy-in for security.
I think it is more commonplace, it is not just something that IT knows about. CEOs, finance, CFOs, board of commissioners; they all know about this type of thing so it is getting better.

Interview Question 3, Theme 2: Organizational. For Theme 2 of Interview Question 3, 33% of the respondents indicated the level of support for network managers and system administrators is always available. Respondents are confident they have the right amount of staff, and the organization is well aware of intrusion threats with the help of media news spreading information about the damage that companies face when they do not support their IT departments. Lastly, the IT department can get support from within when their employees are careful not to damage systems. For instance, staff members recognized not to click suspicious web pages; therefore the IT department helps itself. Table 21 contains the Theme 2 responses for Interview Question 3.

Table 21

Interview Question 3, Theme 2 Responses: Organizational

Responses
We have a whole department that supports staffing and funding.
Level of support was to welcome me with open arms when having issues with ransomware and scams.
The level of support depending on the organization is always medium to low.
Our organization is very supportive of it. I believe they realized that it is a real threat that

previously it was the business side telling the IT side here is your money, just make it work.

Interview Question 3, Theme 3: Information technology. For Theme 3 of Interview Question 3, 33% of the respondents indicated that they look for support within the staff of the IT department itself in order to implement strategies despite the shortage of staffing and funding. Network engineers indicated support from an assistant and the assistant gets support from database staff; participants do not influence funding or staffing, and they use all the help they can get from personnel that is currently available because the business still needs to operate. Table 22 contains the Theme 3 responses for Interview Question 3.

Table 22

Interview Question 3, Theme 3 Responses: Information Technology

Responses
We have the support, I am the network engineer and he has an assistant and then he also has other support staff.
I mostly focus on networking and security; my coworker, he does general support around here.
If I need additional assistance, I could go to my system administrator. He can come and help me out because he knows networking as well or I can go to my IT manager who was previously a network administrator. Between the three of us, we know the network and if there is anything that I need help with they are usually my right and left hand.
Yeah, I think I will just pass that.

Interview Question 3, Theme 4: Client. For Theme 4 of Interview Question 3, 33% of the respondents indicated that supporting clients help to implement effective strategies in the IT

department. Participants stated external companies are contracted to help protect the IT department and network services; these third-party services provide support to the IT department. The support goes back and forth, for example, the IT department helps their parent organization, and at the same time, third-party services support the security needs of the IT department. Table 23 contains the Theme 4 responses for Interview Question 3.

Table 23

Interview Question 3, Theme 4 Responses: Client

Responses
If there is a problem with the ORACLE system, we give them support. The company that provides the application also gives us support to see if there is a problem.
Currently right now, we are well staffed. In the eleven years that I have been with this organization, we have the most capable, most professional and most skilled team that this organization has had in my time here.
Those are the ones that cannot afford a security department, they cannot afford a specialist. If they cannot afford all those people the education for business owners of those levels is where the biggest risks are.
That challenge is not enough communications between us and the security guys. Where we should be working hand in hand and some might argue we should be part of the same department which was not our company.

Interview Question 3, Theme 5: Financial. For Theme 5 of Interview Question 3, 33% of the respondents indicated the IT funding support is limited and is one of the most significant issues affecting the implementation of effective strategies. Participants stated that there is a fear

of understanding the importance of staffing and funding support for security is short. Typically IT departments have not run into any major problems despite suggesting that there is an acceptable level of risk implied in their daily operations. Table 24 contains the Theme 5 responses for Interview Question 3.

Table 24

Interview Question 3, Theme 5 Responses: Financial

Responses
And I got those questions and with their help I was able to get the right resources but I think now get us to an adequate staff.
We want to fix features and in order to get sales we need to fix this security hold that is usually the only time we get funding because it is not so much of a buy because people think that security is an IT problem. We have to build this in from the business model.
To be able to implement effective strategies, generally they are very understanding about the importance of staffing and support funding. We typically have not run into any problems.
So this is definitely one of the biggest issues we face.

Interview Question 3, Theme 6: Staffing. For Theme 6 of Interview Question 3, 33% of the respondents indicated there is a shortage of cybersecurity staff. Therefore staffing support is limited. Respondents stated that it is difficult to obtain staffing support because the business objective is more sales driven and there is no return on investment for security. The limitation of competent network security administrators or network security engineers is positively supported by institutions offering degree programs to offer qualified staffing and possibly fill the shortage of cybersecurity staff. Table 25 contains the Theme 6 responses for Interview Question 3.

Table 25

Interview Question 3, Theme 6 Responses: Staffing

Responses
So it becomes easier and more accepting of any kind of changes you are going to make. There are always those people who would rather make it easy. And, in most cases they do not realized how easy it is to get to somebody.
Security is a business level problem that you are going to need to spend money on. The support for that is very hard to get because there is no return on investment for security.
It is just now becoming where the colleges are offering that type of curriculum and that type of degree path specifically in network security. I think it is going to get better as more students go through university and graduate with degrees in network security and it is going to be easier to find staff that are trained and experienced.
If you can imagine somebody that has a lawn business that has blown up and now they have a thousand employees and they are doing all the lawns in Florida chances are they do not have a good guy.

Interview Question 3, Theme 7: Leadership. For Theme 7 of Interview Question 3, 25% of the respondents indicated they received proper staffing and funding support, enhancing the role of the network manager. Participants stated that they have a departmental partner that dedicates their effort to provide qualified personnel and sources. These managers also established that there is a sort of fear to understand the implications of staff and funding shortage but news related to network intrusions affecting business help leaders to become more supportive. Table 26 contains the Theme 7 responses for Interview Question 3.

Table 36

Interview Question 3, Theme 7 Responses: Leadership

Responses
Staffing and funding; we have a whole department that supports us.
I think because of some of the compromises and big time business impacts that you have seen with X Company and Y Company, they have faced legal issues. Because of issues that they had with their network security; I think it is more public now.
To be able to implement effective strategies, generally understanding the importance of staffing and support funding to do what we need to do, we have not run into any problems.

Interview Question 4

When it becomes clear that the network has experienced a backdoor intrusion, what is the usual protocol or strategy that is employed to address the problem?

***Probe question* - do you have an example you could share?**

Aggregated data for Interview Question 4 yielded six prominent themes: (a) notify upper management, (b) systems update, (c) collecting evidence, (d) isolate devices, (e) backdoor issue, and (f) firmware. The number of responses of each of the prominent themes or topics for Interview Question 4 is shown in Table 27. Passive defense technologies are not strategically efficient when dealing with backdoor threats; for instance, malware generating PDF documents allows hackers to read confidential information (Goldman, Burstein, Benton, Kuter, Mueller, Robertson, ... Bobrow, 2015; Xingguo et al., 2016).

Table 27

Themes for Interview Question 4

Themes	*n*
Notify upper management	4
Systems update	4
Collecting evidence	4
Isolate devices	4
Backdoor issue	3
Firmware	3

Interview Question 4, Theme 1: Notify upper management. For Theme 1 of Interview Question 4, 33% of the respondents indicated keeping upper management informed is the usual protocol if the network has experienced a backdoor intrusion. Respondents indicated that the findings are presented to upper management to help them make further decisions. Furthermore, respondents indicated that calling for meetings can initiate further investigation in order to help clarify the backdoor intrusion issue. Table 28 contains the Theme 1 responses for Interview Question 4.

Table 28

Interview Question 4, Theme 1 Responses: Notify Upper Management

Responses
What he did was notify the majority of the vendors and secretly let them know first and gave them time to come out with an update.
I am going to call a government authority and they are going to come in and take over an

investigation for us.
We called an emergency meeting with information technology staff and upper management staff and explained the issue in layman terms.
We combined that with our findings, presented it once again to upper management then the decision was made to bring everything back online and there was no issue.

Interview Question 4, Theme 2: Systems update. For Theme 2 of Interview Question 4, 33% of the respondents indicated that the use of updates for the network systems could help resolve backdoor problems. Respondents stated that in order to fix the backdoor exploit, they work on patching the network. Respondents further indicated that discrete notification to the vendors allows for the development of new updates in order to fix the issue as soon as possible. Table 29 contains the Theme 2 responses for Interview Question 4.

Table 29

Interview Question 4, Theme 2 Responses: Systems Update

Responses
The one incident we have identified what vulnerability, what the exploit was and now we take that to fix the exploit. In some cases those are patches from the vendors.
What he did was notify the majority of the vendors and secretly let them know first and gave them time to come out with an update.
We manage the server and network settings; they install and update the software.
If there is something simple, like an update to the software on the actual access point; if I did not update it and the attacker took advantage of the export because I am running an old firmware, now I know I have to update it to prevent this type of situation in the future.

Interview Question 4, Theme 3: Collecting evidence. For Theme 3 of Interview Question 4, 33% of the respondents indicated when it becomes clear that the network has experienced a backdoor intrusion; usually, they collect as much evidence related to the incident as possible. Respondents indicated they could see backdoors with the help of detection methods and analyzing backdoors is part of the protocol to address the problem. Respondents also stated that generating a chain of custody document to record the intrusion in chronological order is part of the protocol employed. Respondents also stated that the amount of evidence plays a key factor when addressing the backdoor intrusion problem. Table 30 contains the Theme 3 responses for Interview Question 4.

Table 30

Interview Question 4, Theme 3 Responses: Collecting Evidence

Responses
Based on a backdoor intrusion, the amount of evidence that you collect is going to be important. We would have to analyze it ourselves for any kind of back door that could potentially intrude or open up a security risk to our network.
We have detection methods to seal traffic and any device so we can see backdoors.
This organization had a data breach. Credit card information was exposed because of this backdoor intrusion. When realizing that we run the same software and it is exposed to the internet, we called an emergency meeting with information technology staff and upper management staff explain the issue kind of in layman terms meanwhile we were doing.

Interview Question 4, Theme 4: Isolate devices. For Theme 4 of Interview Question 4, 33% of the respondents indicated that when it becomes clear that the network has experienced a

backdoor intrusion, they must isolate all devices containing backdoor intrusions. Respondents indicated that backdoors are tough to defend because backdoors are built into the devices. Respondents also stated that not trying to cover up the intrusion and roll back the network to a prior state is an excellent strategy to defend against backdoor intrusions. Table 31 contains the Theme 4 responses for Interview Question 4.

Table 31

Interview Question 4, Theme 4 Responses: Isolate Devices

Responses
I think when you have seen intrusions happen, it makes it ten times worse if you try to cover it up without being transparent.
We would have to analyze it ourselves for any kind of back door that could potentially intrude or open up a security risk to our network.
If you are in doubt of the intrusions or you see symptoms of it, you would roll back to a known phase of the network or your data.
We have identified that our set up process is either augmented or somebody did not follow it properly and then take you know uh disciplinary steps.

Interview Question 4, Theme 5: Backdoor issue. For Theme 5 of Interview Question 4, 25% of the respondents indicated backdoor intrusions are a severe problem for the organization. Network managers and systems administrators stated that to address the backdoor intrusion issue, they notify the Federal Bureau of Investigation (FBI) as a strategic option. However, disclosing information is part of the requirement and dialogue must include to not spreading confidential information to avoid leaked or compromised. Furthermore, the organization must be

careful not to spread confidential information. Table 32 contains the Theme 5 responses for Interview Question 4.

Table 32

Interview Question 4, Theme 5 Responses: Backdoor Issue

Responses
If I have a serious issue and we know that we had an intrusion, I am going to call the FBI. Make sure that you have that dialogue and everything is out in the open as much as can be without divulging any sort of confidential information.
We do not believe in paying ransomware, the best way to deal with it is to go to a backup.

Interview Question 4, Theme 6: Firmware. For Theme 6 of Interview Question 4, 33% of the respondents indicated that firmware embedded into the hardware of specific network devices allows backdoor intrusions. Furthermore, simple firmware updates can allow backdoor intrusions to access points in the network. Additionally, there is a need to update policies to prevent firmware updates from spreading backdoors. Table 33 contains the Theme 6 responses for Interview Question 4.

Table 33

Interview Question 4, Theme 6 Responses: Firmware

Responses
If there is something simple like an update to the software on the actual access point some cases those fixes are patches from the vendors; firmware updates, software updates, web updates those kinds of things other times it is configuration changes on a firewall on a switch.
Case is opened with CISCO so that they can verify what is happening and if they have to update

something in their systems to give us support.

We manage the server and network settings; they install and update the software.

Interview Question 5

Could you please tell me as much as possible about the details of your experience selecting appropriate countermeasures as an IT manager working in the area of network security?

***Probe question* - how disruptions in the network are handled?**

Aggregated data for Interview Question 5 yielded seven prominent themes: (a) educate and share, (b) investigate network sections, (c) disabling traffic, (d) counter-intrusion service, (e) isolate software, (f) identify anomalies, and (g) stopping traffic. The number of responses of each of the prominent themes or topics for Interview Question 5 is shown in Table 34. There are algorithms designed to analyze network traffic and to detect backdoor intrusions; another defense strategy includes static and dynamic countermeasures which are the two major types of defense strategies for network systems (Powers, 2015; Hong et al., 2015).

Table 34

Themes for Interview Question 5

Themes	*n*
Educate and share	5
Investigate network sections	4
Disabling traffic	3
Counter intrusion service	3
Isolate software	3

Identify anomalies	3
Stopping traffic	3

Interview Question 5, Theme 1: Educate and share. For Theme 1 of Interview Question 5, 42% of the respondents indicated that sharing incidents within the organization helps the department to develop better countermeasures. Respondents indicated that they emulate attacks in the network and have training sessions to teach personnel. Furthermore, respondents indicated that they use information shared by the Department of Homeland Security to developed knowledgeable members and enhance countermeasures against intrusions. Table 35 contains the Theme 1 responses for Interview Question 5.

Table 35

Interview Question 5, Theme 1 Responses: Educate and Share

Responses
Our approach is to emulate these attacks and have training sessions to train the employees. We have our conference room and we put out email bulletins that say if you want to, please attend this training; and it is something that we do citywide.
I think one of the most important things is there is a lot of organizations out there to share information. That is, a good countermeasure to have. One of the organizations that we belong to is called multi-state information sharing… I do not remember the last two, but it is MS-ISAC. It is funded by the Department Homeland Security; it is free for all private and public organizations.
You start swinging back and you do not know what you are doing, you are shadow boxing. You know, you are swinging in the dark and there may be one hundred of them in there; they are

going to whip you (self-training).
You want to let people know what happened. So again, it goes back to the knowledge base of your end user. The people, who are using the equipment, say hey this is what just happened, this is what it cost, and this is how to try to avoid it.
Any other information we can get out of it and then then reporting it up to the proper channels whether it is you know our intruding detection system; letting them know hey, you guys did not pick this up here you go, here is the IP please do something about it but whether is an anti-virus or firewall or Semantic we say hey, you did not discover this so can you please add this signature?

Interview Question 5, Theme 2: Investigate network sections. For Theme 2 of Interview Question 5, 33% of the respondents indicated that investigations of different sections of the network serve as a countermeasure against intrusions. Furthermore, respondents identified that a network without segmentation allowed for easy and rapid damage from cyber-attacks. Additionally, respondents further indicated that once the network is isolated, the next step is to investigate those segregated sections located in different areas of the network while restoring other sections of the system from backups to restore network operation. Table 36 contains the Theme 2 responses for Interview Question 5.

Table 36

Interview Question 5, Theme 2 Responses: Investigate Network Sections

Responses
They just found the X company credentials and were able to use them and go into X network and unfortunately X company network was flat so it did not have any segmentation to it and once

they were in they have got everything.
You are going to do isolation and then investigation and repair. Alright, you want to stop what is happening immediately.
We did not shut down the entire file server because it was only spread to that one department container, it had not spread to any other departments because they did not have access to that so the server itself we were able to leave online but we disabled access to the user and wiped their computer clean and then we started restoring from backups.
And then the other thing a lot of hospitals do is use firewalls internally to micro-segment to better protect uh the golden data.

Interview Question 5, Theme 3: Disabling traffic. For Theme 3 of Interview Question 5, 33% of the respondents indicated that the network must shut down to counter-intrusion attacks. Participants stated to take the network off right away for investigation purposes. Participants thought that disabling user access to the server allows information to be accessible and stop intrusions to cause more damage to the network. Participants also thought and alleged that sometimes you do not even realize a vulnerability and need to turn off the network traffic to prevent more exploits to occur. Table 37 contains the Theme 3 responses for Interview Question 5.

Table 37

Interview Question 5, Theme 3 Responses: Disabling Traffic

Responses
Yes, countermeasure in this context it is just plugging the hole. Sometimes you do not even realize vulnerability until it is exploited so a countermeasure would just be going back and

forth in that hole; maybe turning off TCP.
I would just shut it down. Just remain silent and shut it down.
Try to take it off the network right away. You want to make a work around for it and then finally investigate it and put your resolution in there. If you have a disruption, you go right for finding what that is and then you take it off the network.

Interview Question 5, Theme 4: Counter intrusion service. For Theme 4 of Interview Question 5, 17% of the respondents indicated that third-party services could be used to counter intrusions alleviating the overload to network managers and systems administrators. According to the respondents, using two-factor authentication adds a layer of defense and protection to the network environment. However, third-party services have access to the systems, and they also need the two-factor authentication added; therefore, vendors can fix elements from inside the network domain. Furthermore, third-party cybersecurity consultants can benefit the organization by using their expertise; therefore, third-party services can add defense mechanisms to counter backdoor intrusions. Table 38 contains the Theme 4 responses for Interview Question 5.

Table 38

Interview Question 5, Theme 4 Responses: Counter Intrusion Service

Responses
You have vendors that may be fixing gear for you inside your domain.
I think they are a great organization and that is a good countermeasure to have because what they will also do is if you do not have funding for or have your own third party cybersecurity consultants, you can also send them as much information as you want or as little information as you want and they will actually have their experts look at it and determine whether you

might have a real issue or not.
And so you know one of the ways that health care prevents that today is the use of two-factor authentication or your third-party vendors that access your system so it is not only the username and password but it is another factor that they have to have in order to get in.

Interview Question 5, Theme 5: Isolate software. For Theme 5 of Interview Question 5, 25% of the respondents indicated that isolating the network software without being noticed by the attacker can be used as a good countermeasure against intrusions. Respondents also pointed out that being silent and shutting down the network helps isolate compromised software. Respondents further indicated that staying quiet helps to not let the attacker know that they are aware of being attacked in order to take advantage of the intrusion to develop better countermeasures. Table 39 contains the Theme 5 responses for Interview Question 5.

Table 39

Interview Question 5, Theme 5 Responses: Isolate Software

Responses
I would just shut it down. Just remain silent and shut it down.
You want to make sure that no one is using any kind of shareware program or other junk they are not supposed to be using at work.
We did not want them to know that we knew they were attacking us. We wanted to be able to stop it without their knowing because we want them to keep trying the same attacks we have already got defenses against; we do not want them to try something new.

Interview Question 5, Theme 6: Identify anomalies. For Theme 6 of Interview Question 5, 25% of the respondents indicated that the identification of anomalies in the network

serves as a countermeasure strategy. Respondents indicated that anti-virus software helps to identify intrusion signatures that are not normal during regular network traffic. Respondents also stated the reports generated by intrusion detection and intrusion protection systems enable countermeasure strategies to protect networks from backdoor intrusions. Respondents also indicated that identifying the source of IP address can be used to engage the party that is trying to gain access. Table 40 contains the Theme 6 responses for Interview Question 5.

Table 40

Interview Question 5, Theme 6 Responses: Identify Anomalies

Responses
Yes there are some viruses that the software automatically will identify the signature on it. It would either quarantine it or block it. So the countermeasure would be going through the network and running scans to identify any known signatures.
Not as far as engaging the party that is trying to gain access or trying to do harm. It is more just identifying maybe the source of the IP.
Host based intrusion protection systems and intrusion detection systems are good that report back to a managed console. So for me, that is a good countermeasure or even active port switching, like something starts having an issue or goes outside of its regular network traffic the port will shut down.

Interview Question 5, Theme 7: Stopping traffic. For Theme 7 of Interview Question 5, 25% of the respondents indicated that stopping the network traffic during a backdoor intrusion is a good countermeasure. Respondents indicated that you do not realize vulnerable areas while using the internet and turning off the transmission control protocol (TCP) is a countermeasure to

consider. Respondents also stated that investigating and making resolutions during network disruptions must be taken into account as a countermeasure against backdoor intrusions. Table 41 contains the Theme 7 responses for Interview Question 5.

Table 41

Interview Question 5, Theme 7 Responses: Stopping Traffic

Responses
Yes, countermeasure probably in this context it is just plugging the hole. Sometimes you do not even realize vulnerability until it is exploited so a countermeasure would just going back and forth in that hole whatever may be turning off TCP.
Truly not, you should in particular that I am in I would just shut it down. Just remain silent and shut it down.
Try to take it off the network right away, right? So you want to make a work around for it and then finally investigate it and put your resolution in there. So for me, if you have a disruption, you go right for finding what that is and then you take it off the network.

Interview Question 6

How does having the "right" kinds of staff members impact your ability to carry out an effective strategy for network protection?

***Probe question* - what is the key to this strategy working?**

Aggregated data for Interview Question 6 yielded seven prominent themes: (a) certifications, (b) awareness, (c) expertise, (d) culture, (e) teamwork, (f) weakest link, and (g) network protocol analysis. The number of responses of each of the prominent themes or topics

for Interview Question 6 is shown in Table 42. Each of the indicated themes represents that staff must have a clear understanding of security procedures and processes and the IT systems must follow defined policies rules enforcement in real-time in order to impact an effective strategy for network protection (Safa, Sookhak, Von Solms, Furnell, Ghani, & Herawan, 2015; Ghai, Sharma, & Jain, 2015).

Table 42

Themes for Interview Question 6

Themes	*n*
Certifications	9
Awareness	5
Expertise	5
Culture	4
Teamwork	4
Weakest link	4
Network protocol analysis	2

Interview Question 6, Theme 1: Certifications. For Theme 1 of Interview Question 6, 75% of the respondents indicated that having staff members that pay attention to the agreements they sign and are willing to handle problems and find solutions carry out an effective strategy for network protection. Furthermore, respondents identified staff that has certifications such as CompTIA, network plus and security plus or CISSP level show confidence that allow companies to hire personnel. Additionally, respondents further indicated that staff with extensive knowledge in network architecture, skill in technical areas, a willingness to continue to learn and that have a

passion or desire in the field would impact your ability to carry out an effective strategy for network protection. Table 43 contains the Theme 1 responses for Interview Question 6.

Table 43

Interview Question 6, Theme 1 Responses: Certifications

Responses
Actually paying attention to training; paying attention to the agreements they signed. I know everyone just initials it and goes off, nobody pays attention.
We like to look for people that want to make this a career; they want to be around. So as long as they have at least a COMPTIA, network plus, security plus of some kind it would enter into the entry level position.
You need to have people that are willing to handle things the same way that everybody else is handling them; not trying to be a maverick or rogue or anything like that.
It has to be a person who has extensive knowledge in networking and architecture of the system.
Absolutely crucial, absolutely crucial. People are number one.
I definitely say the people. Just having persons who have an aptitude to continue to learn; so continuing education. But also just some form of a passion or desire in the field.
Having the right people impact your ability as far as if it is effective, how fast they can do it so there is not going to be everybody who is perfect at everything, so having the right staff members that you need to find out who is good.
The biggest vulnerability in any business or institution is people. We do have people here who do not know computers at all they will click on an e mail and training in that instance is such a big thing.
Good HR departments work with the IT department together to try to screen these people and

figure out okay, which is the right personality, and who has the right skill set.

Interview Question 6, Theme 2: Awareness. For Theme 2 of Interview Question 6, 42% of the respondents indicated that staff must know what the requirements are for the end-user. Participants stated to make sure policies and procedures are carried out. Participants thought that an engaging staff provides strength to the organization. Participants also thought and alleged that they need staff that wants to have a career in the networking field with minimum entry level certifications. Table 44 contains the Theme 2 responses for Interview Question 6.

Table 44

Interview Question 6, Theme 2 Responses: Awareness

Responses
Some kind of check on learning for that level of employees would be really good. That way they understand what the requirements are for the end user; it is all about understanding.
You need the right mentality of staff. If you get people who think they know it all or had experience with it and do not want to do what is being set forth as the policies and procedures of how you do things, that can become an issue.
Yes. So we have been named one of the best places to work in IT for the last four years in a row; we have a very engaged staff.
We look for people that want to make this a career. They want to be around, so as long as they have at least a COMPTIA, network plus, security plus of some kind they would enter into the entry level position.
Apart from the certifications you may have, you have to have work in the street because these are situations that are given daily and the certifications help in terms of the theory and

understanding what is happening, but nothing is over experience at work.

Interview Question 6, Theme 3: Expertise. For Theme 3 of Interview Question 6, 42% of the respondents indicated the staff needs extensive knowledge of the network architecture. Respondents indicated their staff needs to have a security mentality whether as a professional coder or a developer. Furthermore, respondents indicated the staff members make jobs easier if they are trained on network threats and also if they take care of all those threat issues. Lastly, knowledge is one aspect of what a staff member needs, but also we need the right people that meet other criteria required by the organization. Table 45 contains the Theme 3 responses for Interview Question 6.

Table 45

Interview Question 6, Theme 3 Responses: Expertise

Responses
You need to be just like any other experts in their field and they need to be at the very forefront of their field.
Having staff is everything; you got to have the right people. Obviously, they have to be knowledgeable, but having the knowledge itself is one aspect.
We want to make sure that our people were trained. People who are trained and are aware of those issues and care about those issues make our job easier.
You definitely want to have security minded people for that.
First it has to be a person who has extensive knowledge in networking and architecture of the system.

Interview Question 6, Theme 4: Culture. For Theme 4 of Interview Question 6, 42% of the respondents indicated that staff is a powerful force in the organization that needs to be handled with caution. According to the respondents, the company faces danger by not knowing the background of the staff members, for example, having the right network equipment in the wrong hands can compromise the network. However, staff needs overlap training to strengthen weak areas; therefore, staff needs to take ownership and accountability of the network. Furthermore, the staff needs to be screened in order to mold them to the vision of the organization. Table 46 contains the Theme 4 responses for Interview Question 6.

Table 46

Interview Question 6, Theme 4 Responses: Culture

Responses
They may know something more than you do, but it is when these people go outside the realm of the standard of the norm that it becomes an issue.
You could have the right product in the wrong hands and it means nothing; whereas you could have a lesser of a product, but in the right hands can be leveraged, very effectively.
Having the right people impact your ability as far as if it is effective, how fast they can do it so there is not going to be everybody who is perfect at everything, so having the right staff members that you need to find out right who is good at A, B & C and we can train them on D & E where you also have other people who are great that C, D & E we got to train them on A & B or you put them in overlapping areas.
You know that is probably one of the key aspects I think the right type of staff that you want to surround yourself with are those that take ownership and accountability of the network.
Have a good HR department work with the IT department together to try to screen these people

and figure out which is the right personality, and who has the right skill set? Which character is more moldable that I can train and shape; some personalities are not flexible.

Interview Question 6, Theme 5: Teamwork. For Theme 5 of Interview Question 6, 33% of the respondents indicated that the staff needs to work together and share responsibilities. Respondents also pointed out that employees need to get things done and engage with each other as members of the team. Respondents further indicated the employees need to take ownership of the network and also be held accountable for their actions and thus treat the network as part of the family. Table 47 contains the Theme 5 responses for Interview Question 6.

Table 47

Interview Question 6, Theme 5 Responses: Teamwork

Responses
You need people who can work together to get things done. Security guy shows presentation guy and presentation guy teaches everyone else.
Another aspect is just having everybody working together.
We have been named one of the best places to work in IT for the last four years in a row; we have a very engaged staff.
I think the right type of staff that you want to surround yourself with are those that take ownership and accountability of the network. You have to almost see it as it is your baby; you take care of it and it takes care of you.

Interview Question 6, Theme 6: Weakest link. For Theme 6 of Interview Question 6, 33% of the respondents indicated people play a role in the network being weak or strong.

Respondents indicated that besides being knowledgeable on networking topics, people need to know how computers process information. Respondents stated that people that are accountable and take ownership play a vital role in network operations; also, with the right kind of people in the right hands the network could work effectively. Table 48 contains the Theme 6 responses for Interview Question 6.

Table 48

Interview Question 6, Theme 6 Responses: Weakest Link

Responses
When you say no, people try to still make things happen and most of the time it affects your service ability and can create vulnerabilities in your network.
Logically, you can have a person who has a great knowledge of networking but does not know how things are processed in a computer then you have a problem. Must have knowledge in both elements.
Absolutely crucial, people are number one; you could have the right product in the wrong hands and it means nothing, whereas you could have a lesser of a product, but in the right hands can be leveraged, very effectively.
The right types of staff are those that take ownership and accountability of the network.

Interview Question 6, Theme 7: Network protocol analysis. For Theme 7 of Interview Question 6, 17% of the respondents indicated the need of personnel that are good in understanding analysis and network protocols. Respondents indicated that personnel who have a flexible personality can adapt better to the network environment. Respondents also stated that they do not want people that are too smart that think they know everything. Respondents also

indicated they do not want people that want only to be told their tasks or are too submissive. Table 49 contains the Theme 7 responses for Interview Question 6.

Table 49

Interview Question 6, Theme 7 Responses: Network Protocol Analysis

Responses
You are going to need somebody who is really good at network protocol analysis.
I need a good flexible personality, but not too smart, where he becomes Mr. Know it all. Or I will not be told anything, because he knows everything. You know, you do not want those, either.

Interview Question 7

What are your thoughts about the role of employees throughout the organization as part of the strategy of defending your network from backdoor intrusions?

***Probe question* - What is your role in this process?**

Aggregated data for Interview Question 7 yielded seven prominent themes: (a) dynamic awareness, (b) understanding defense, (c) network security, (d) understanding threats, (e) human factor, (f) enforcing defense, and (g) defense tasks. The number of responses of each of the prominent themes or topics for Interview Question 7 is shown in Table 50. The use of phishing emails is an example of an Advanced Persistent Threat, and security awareness training plays a vital role in defending the network; in addition, the feelings and behavior of employees should be taking into account as an essential human factor within information security (Chen et al., 2014; Bucak, 2016).

Table 50

Themes for Interview Question 7

Themes	*n*
Dynamic awareness	5
Understanding defense	5
Network security	5
Understanding threats	4
Human factor	4
Enforcing defense	4
Defense tasks	3

Interview Question 7, Theme 1: Dynamic awareness. For Theme 1 of Interview Question 7, 42% of the respondents indicated that security awareness must be part of the role of defending the network from backdoor intrusions. According to the respondents, employees need to know that awareness starts from the moment they access the system and while surfing Websites. However, they recommend that training is a mechanism that contributes to security awareness for employees, network security managers, and system administrators. Table 51 contains the Theme 1 responses for Interview Question 7.

Table 51

Interview Question 7, Theme 1 Responses: Dynamic Awareness

Responses
I have to train these people not to do stupid things. Training just to do the right thing.
It is down to everybody to know about things and that is where information security awareness training, strong password training; even picking up USB or anything else, web surfing

trainings are highly important.
We not only view our internal IT staff as important to the defense but we also view that every employee here in our organization plays a key role so about a year and a half ago what we did is we put together a cyber security training for all staff. All staff is required to take it as part of when they are hired by the organization.
Number one orientation; they have what is called security awareness. I can block a lot of pages but if the employee is not aware that if he has inserted a thumb drive with content from his house, or if is opening an email that does not necessarily come from reliable places because it is a continuous orientation process.
Crucial, again crucial. User awareness of the threats.

Interview Question 7, Theme 2: Understanding defense. For Theme 2 of Interview Question 7, 42% of the respondents indicated that understanding network defense roles could strength the strategy of defending the network. Respondents indicated that workers could combat attacks without even knowing they have been attacked. Respondents also stated that being complacent affects the understanding of who has the role of defending the network. Respondents also indicated that the role of defending the network from backdoor intrusions is not clear. Table 52 contains the Theme 2 responses for Interview Question 7.

Table 52

Interview Question 7, Theme 2 Responses: Understanding Defense

Responses
People are your front line of network defense; combatting attacks and do not even know it.
Overcoming that mindset that they are actually the operators of a terminal on a network that has access to data, be a financial, word documents, excel documents, databases; what have you.

Email systems, things like this that they can do real damage by their complacency, or lack of basic operational, business, computer systems; operational knowledge is huge.
X company put out a report about how they are addressing phishing issues and I mean phishing that goes beyond DDOS, beyond worms, and all the stuff getting us out of the network.
The roles of employees in an organization for defending network from backdoors intrusion have to have some awareness at some point.
You have to be involved from a management standpoint any time that there is an incident or that you are making decisions about how you are going to defend your network from compromise.

Interview Question 7, Theme 3: Network security. For Theme 3 of Interview Question 7, 42% of the respondents indicated the role of employees is crucial in defending the network from backdoor intrusions. Respondents indicated that if upper management does not care about security, then employees are not going to care either. Respondents also stated that safeguarding employees is significant in defending the network. Table 53 contains the Theme 3 responses for Interview Question 7.

Table 53

Interview Question 7, Theme 3 Responses: Network Security

Responses
They are getting junk emails in that are scam emails or phishing emails, or that are Trojan horses and their knowledge of what is coming or their understanding of how things work gives them the weapons to protect your network. So they play a crucial, crucial part in any network security; employees are your first line of defense.
Sometimes you find organizations where the upper management is not so interested in investing

money in security and then if you are up there in the head does not have that importance because the employees are not going to care.
The fact a company as large as X, that they did that it shows the significance in the importance of making sure your employees are safeguarded as well at all levels.
The role of employees in an organization for defending the network against backdoor intrusion is somebody has; everybody has to have some awareness at some point.
If an employee does something they are not supposed to and they get their computer infected or they get our network affected, even worse, then they not only are subjected to cyber security awareness training, but it also goes on the personnel record, if it happens again and even again, it starts to result in written reprimands all the way up to possible termination.

Interview Question 7, Theme 4: Understanding threats. For Theme 4 of Interview Question 7, 33% of the respondents indicated that understanding what the threats are can shape the role of employees to defend the network from backdoor intrusions. Participants stated that depending on automation tools involved in the daily operations of the network affects the role of the individual. Participants thought that employees need to understand how phishing email works and use that knowledge as a weapon to protect the network. Table 54 contains the Theme 4 responses for Interview Question 7.

Table 54

Interview Question 7, Theme 4 Responses: Understanding Threats

Responses
When you see a role, most of those tasks are automated so the role would be reading alerts from the monitoring software.

You know, they are getting junk emails in that are scam emails or phishing emails, or that are Trojan horses and their knowledge of what is coming or their understanding of how things work gives them the weapons to protect your network. So they play a crucial, crucial part in any network security.
I think it is huge. I think their role is just as significant as an IT security engineer.
Whose role is it to maintain security or trying to be secure within an organization? Everyone.

Interview Question 7, Theme 5: Human factor. For Theme 5 of Interview Question 7, 33% of the respondents indicated that employees and their network security managers or system administrators play a role in the network defense process. Respondents indicated that part of defending the network is to open case tickets in the IT department that initiate the problem-solving process. Furthermore, respondents indicated that they use services provided by other companies to help defend the network from backdoor intrusions. Table 55 contains the Theme 5 responses for Interview Question 7.

Table 45

Interview Question 7, Theme 5 Responses: Human Factor

Responses
I am here to push these buttons today and if my computer breaks then we will just open a ticket with IT, you know and they will fix that. You know or we have people for that.
People who are brand new into the organization may be you not that familiar with computers. Maybe their job role does not require them to be and Company X introduced a two-factor authentication but it is the way that they are doing it that has successfully allowed them for the past two years to not have an incident of phishing or breaching.

The most responsible person for network security, which is the people who write the checks.
Where we see most of our issues of possible breaches is through email. People sending email.

Interview Question 7, Theme 6: Enforcing defense. For Theme 6 of Interview Question 7, 33% of the respondents indicated that employees and their network security managers or system administrators play a role in enforcing network defense strategies. Respondents also pointed out that they play a crucial part in network security. Respondents further indicated defending the network is a process that everyone should be a part of; thus, not only security personnel should get involved in the process, but even end-users should share in the responsibilities. Table 56 contains the Theme 6 responses for Interview Question 7.

Table 56

Interview Question 7, Theme 6 Responses: Enforcing Defense

Responses
Security should be the job of everyone and we should talk to them that training was part of the process.
They play a crucial, crucial part in any network security.
I think their role is just as significant as an IT security engineers.
You know whose role is it to maintain security within an organization? Everyone.

Interview Question 7, Theme 7: Defense tasks. For Theme 7 of Interview Question 7, 25% of the respondents indicated that adding roles to defend the network is vital for employees and their network security manager or system administrators as part of the strategy of defending the network from back door intrusions. Furthermore, respondents identified that employees are

the front line of defense. Additionally, respondents further indicated that everybody is responsible for the security of the network. Table 57 contains the Theme 7 responses for Interview Question 7.

Table 57

Interview Question 7, Theme 7 Responses: Defense Tasks

Responses
Security should be job of everyone.
They are your front line of defense really. They are the people who are combatting attacks and do not even know it, so they play a crucial, crucial part in any network security.
Everybody here is responsible for our security.

Interview Question 8

The defense-in-depth strategy seems to be pretty widely accepted as the standard for network security. What is your perspective on the effectiveness of this strategy?

***Probe question* - what would a different approach look like?**

Aggregated data for Interview Question 8 yielded seven prominent themes: (a) weak network sections, (b) network layers, (c) access points, (d) defense-in-depth, (e) network segmentation, (f) internal network defense, and (g) strategic value. The number of responses of each of the prominent themes or topics for Interview Question 8 is shown in Table 58. Defense-in-depth mechanisms are practical and feasible, and the coordinated used of multiple security layers protects the integrity of information assets of the organization and manages IT security risks (Levillain, Gourdin, & Debar, 2015; Alexander, 2017).

Table 58

Themes for Interview Question 8

Themes	*n*
Weak network sections	6
Network layers	6
Access points	6
Defense-in-depth	4
Network segmentation	4
Internal network defense	2
Strategic value	2

Interview Question 8, Theme 1: Weak network sections. For Theme 1 of Interview Question 8, 50% of the respondents indicated that adding many layers of security can make it difficult for intrusions to occur. Participants stated that many layers of defense serve as a deterrence method. Participants also thought and alleged that if a single layer gets breached, the intrusion affects the network. Table 59 contains the Theme 1 responses for Interview Question 8.

Table 59

Interview Question 8, Theme 1 Responses: Weak Network Sections

Responses
We use a lot of different layers, but I am not going to talk about what we actually utilize. Basically, any security system is going to have multiple layers, whether it is network or access or anything like that.
It is effective because the more layers you create, the more problematic you make it for the

attacker to access a system.

So my perspective when you have all these layers put in place with firewalls, File Allocation Table (FAT) translations, Audit Command Language (ACLs) and network segments and then on top of that you have load balancers that do all sorts of security and then on top you have the monitoring with all sorts of alerts allowed to it with just layer after layer.

It just requires all of these layers to be in place, because if one of those single things gets breached I do not want it to roll down.

You have to think of all these seven layers, how can I break in each layer? How can I prevent those break ins? What vulnerabilities do we have on these layers, how can I secure each of these layers?

Interview Question 8, Theme 2: Network layers. For Theme 2 of Interview Question 8, 50% of the respondents indicated that defense in depth must be applied not only to the exterior of the network but the interior of the network as well including the small points where the system is still vulnerable. According to the respondents, dividing and isolating the network is useful. However, do not underestimate the access points where intrusions are most likely to occur; therefore, the principle of defense-in-depth is still the de facto standard that network managers and system administrator trust. Table 60 contains the Theme 2 responses for Interview Question 8.

Table 60

Interview Question 8, Theme 2 Responses: Network Layers

Responses
As I mentioned to you our area concentration is our businesses by dividing sub netting the

network; they would isolate the possibility of risks.

Any security system is going to have multiple layers, whether it is network or access or anything like that.

You need to have that layered approach. It is essential if you want to have any confidence in the security of your network.

You have all these layers put in place with firewalls, File Allocation Table (FAT) translations, Audit Command Language (ACLs) and network segments and then on top of that you have load balancers that do all sorts of security.

Systems access control systems, anything that is really hooked up to our network and even some things that are not; we have to have defense there at every single point. We do not just do the crunchy exterior and the soft gooey interior we try to protect all points.

You cannot just look at your perimeter; you also have to look everywhere else in your network. You also do not want to have all of your eggs in one basket per se.

Interview Question 8, Theme 3: Access points. For Theme 3 of Interview Question 8, 50% of the respondents indicated that accessing the network is critical where the defense-in-depth strategy needs to be implemented. Respondents also pointed out that having multiple layers of security is a primary function of network defense. Respondents further indicated that one way to gain secure access to the network is via a virtual private network (VPN); thus, cloud services as third party entities are another effective strategic approach used in IT departments. Table 61 contains the Theme 3 responses for Interview Question 8.

Table 51

Interview Question 8, Theme 3 Responses: Access Points

Responses
Any security system is going to have multiple layers, whether it is network or access or anything like that.
Logically that is beneficial from the point of view if I am going to make a remote data attack trying to gain access to a remote system.
Were it not for that layered approach, it could have been the files of everyone.
From training or protecting your devices that connect your end user devices to you know protecting the server that the data that exists on the resources that the users are going to access to protecting how the users access the resources like you need to have that layered approach it is, it is essential if you want to have any confidence in the security of your network.
Cloud access security brokers and things like that really allow you, if you have a cloud service it actually is a third party that you get your traffic sent to.
Specifically as an external VPN. Our users use the VPN, they get in so it must be accessible on the outside but we do not allow anything else, so it gives us the nice, crunchy exterior that we, we check the firmware all the time on the firewall to make sure there is nothing.

Interview Question 8, Theme 4: Defense-in-depth. For Theme 4 of Interview Question 8, 33% of the respondents indicated that the defense-in-depth method prevents breaches because it protects every point that could be accessed. Furthermore, respondents identified that the defense-in-depth strategy still prevails even under changing conditions where more sophisticated types of attacks keep emerging. Additionally, respondents further indicated that the defense-in-

depth method should be implemented at the level of the Open Systems Interconnection model (OSI model). Table 62 contains the Theme 4 responses for Interview Question 8.

Table 62

Interview Question 8, Theme 4 Responses: Defense-in-Depth

Responses
Defense in depth should have been there as something that will prevent breaches at a higher level than having just open source things out on the perimeter.
I mean it all kind of comes together. Still it is defense in depth us is that we have to assume that our network as always breached. There is somebody always on our network and thus we must protect every point that could be accessed.
You know that defense in depth strategy that you mentioned is very important; I think that really is the standard. I know things change every single day but currently that is the strategy that we follow here, and until I see something different, that is the one we will continue to use.
I think it is the best, I think it is the standard that everybody uses; I think it is a good one. And, you know I think you have to think of, okay, all these seven layers, how can I break in each layer?

Interview Question 8, Theme 5: Network segmentation. For Theme 5 of Interview Question 8, 33% of the respondents indicated that security is needed at every segment of the network. Respondents indicated that security must be divided into small sections of the network in order to be effective. Furthermore, respondents indicated that backup solutions play a part of the defense-in-depth method. Table 63 contains the Theme 5 responses for Interview Question 8.

Table 63

Interview Question 8, Theme 5 Responses: Network Segmentation

Responses
The multiple layers are a good idea because it is multiple protection points.
Were it not for that layered approach, it could have been the file of everyone.
We have to assume that our network is always breached. We look at who is there is somebody always on our network and thus we must protect every point that could be accessed.
You know all the way, like I mentioned before it from your end point protection from what is on your PC, monitoring that PC to what is monitoring the traffic internal to your network that is monitoring traffic coming and going.

Interview Question 8, Theme 6: Internal network defense. For Theme 6 of Interview Question 8, 17% of the respondents indicated that the defense-in-depth strategy should be implemented not only at the perimeter of the network but inside the network as well. Respondents indicated that the strategy prevents breaches at higher levels of the network. Respondents also stated the strategy is needed in all sections of the network to be more effective. Table 64 contains the Theme 6 responses for Interview Question 8.

Table 64

Interview Question 8, Theme 6 Responses: Internal Network Defense

Responses
So defense in depth should have been there is something that will prevent breaches at a higher level than having just open source things out on the perimeter.
So back to number eight um yeah so I, I believe in that strategy and I think I kind of spoke on it

earlier that you do not want you cannot just look at your perimeter.

Interview Question 8, Theme 7: Strategic value. For Theme 7 of Interview Question 8, 17% of the respondents indicated that the defense-in-depth strategy is an effective strategy. Respondents indicated that the defense-in-depth strategy is the standard that many companies follow. Respondents also stated that this defense standard is the best option to secure the network. Table 65 contains the Theme 7 responses for Interview Question 8.

Table 65

Interview Question 8, Theme 7 Responses: Strategic Value

Responses
I think that is where you know that defense in depth strategy that you mentioned is very important I think that really is the standard.
I think it is the best, I think it is the standard that everybody uses; I think it is a good one.

Interview Question 9

What other points would you like to make that we did not address during the interview that you think are key to an effective network security strategy?

Aggregated data for Interview Question 9 yielded seven prominent themes: (a) internet security, (b) risk assessment team, (c) management, (d) ethical hacking, (e) administrative policies, (f) cloud security, and (g) wireless security. The number of responses of each of the prominent themes or topics for Interview Question 9 is shown in Table 66. Each of the indicated themes represents additional points that network security managers or system administrators commented as crucial areas for an effective network security strategy needed to protect the

network from backdoor intrusions. Internet Security including Policy is a responsibility shared by managers (Abrahams & Mbanaso, 2017).

Table 66

Themes for Interview Question 9

Themes	*n*
Internet security	7
Risk assessment team	6
Management	4
Ethical hacking	4
Administrative policies	3
Cloud security	3
Wireless security	2

Interview Question 9, Theme 1: Internet security. For Theme 1 of Interview Question 9, 58% of the respondents indicated that an assessment on Internet or cloud services is key to an effective network security strategy. Furthermore, respondents identified that there are security gaps when combining different operating systems that need to work together in the same network. Additionally, respondents further indicated that risk assessments must be conducted not just internally but outside the network as well (from an outside source). Table 67 contains the Theme 1 responses for Interview Question 9.

Table 67

Interview Question 9, Theme 1 Responses: Internet Security

Responses

I think and research on back doors I think most of that is it is going to be national agencies doing that, you know, like the NSA requires backdoors on internet service providers.

Whoever gets in that field has to constantly have their hands on the poles of networks primarily the internet even do in the network you secure it all.

There is going to be vulnerability, someone is going to defeat that. But at the end of the day I think the most important is going to be physical security.

I think what one strategy that I do not know why but you know it I find it often gets overlooked is physical security.

And then encrypting data between those systems if it is applicable right, because some systems like Linux or Window systems it is hard to get them to communicate on a higher level of security where you know backwards compatibility to low security usually works great. A little bit difficult to configure do, so I think that is a good one to put on there.

I think all organizations should conduct some level of a risk assessment of their systems and not just, you can do it internally, I would recommend having someone external come look at it.

The only thing that I think we did not touch would be probably the cloud. Because that is the big thing now, the cloud. Putting everything in the cloud.

Interview Question 9, Theme 2: Risk assessment team. For Theme 2 of Interview Question 9, 50% of the respondents indicated that having an outside company evaluating and watching network activity is key to an active network security strategy. Respondents also pointed out that those third-party personnel can provide a new perspective on how well or how poorly the security in the network is operating. Respondents further indicated the use of virtual LANs and

isolation of wireless network are valid strategies. Table 68 contains the Theme 2 responses for Interview Question 9.

Table 68

Interview Question 9, Theme 2 Responses: Risk Assessment Team

Responses
It is good practice to use ethical hackers in order to test your network security.
Whoever gets in that field has to constantly have their hands on the poles of networks primarily the internet even do in the network you secure it all.
Have virtual LANs and you have isolation between your wireless network.
That has nothing to do with getting through network security, making the software; script keys nothing to do with it. That is just somebody they can see what you are doing.
You could put as much stuff as you want in network security, but if you have people that just open the door for a burglar you pretty much have circumvented all of that.
Any organization is going to have some sort of risk when it comes to your network security. I think it just shows you areas that you need to improve on and I think, you are constantly improving; no one is going to be one hundred percent on top so I think by doing a risk assessment it shows you where you are where you need to improve on but also shows you where you are good at you know.

Interview Question 9, Theme 3: Management. For Theme 3 of Interview Question 9, 33% of the respondents indicated that an effort to discover backdoors from other nations including tools available in the dark web is key to an active network security strategy. Participants stated that managers must be involved in looking for different types of threats.

Participants thought that understanding new threats can improve the procedures taken when facing an intrusion. Table 69 contains the Theme 3 responses for Interview Question 9.

Table 69

Interview Question 9, Theme 3 Responses: Management

Responses
So any research in the back doors have to be like one nation discovering back doors that another nation created or companies finding backdoors that nations created so that is not something I have any information on.
Ok, now we go to the dark web. In the dark web you have exploits tools that are not published in these other security applications that call the penetration testing tools.
But any other nation state out there right so but if you are not just looking at different types of threats you got to look at the risk as a whole in different sections of it, right?
I think another thing that is pretty important is you want to be sure that the key managers in the organization that are involved in any sort of emergency management or disaster recovery understand the procedures you take when there is an intrusion.

Interview Question 9, Theme 4: Ethical hacking. For Theme 4 of Interview Question 9, 33% of the respondents indicated that having a security team to test their network is key to having an effective network security strategy. Respondents indicated that spending money on penetration testing teams can help determine if policies created to protect the network can be breached. Respondents also stated that even someone without malicious intent can still breach the network accidentally. Respondents also indicated that the administration level can implement

effective policies to help in improving the defensive strategy. Table 70 contains the Theme 4 responses for Interview Question 9.

Table 60

Interview Question 9, Theme 4 Responses: Ethical Hacking

Responses
That is probably the best money spent in cyber security is ethical hacking because you are actually practically testing everything you created.
Somebody threw a couple USBs around and people would just grab it to see what is in it. You know, maybe with the intention of finding their rightful owner to return it to them. But again, those were proof that how easily people could be gullible and get hacked per se.
In the dark web you have exploits tools that are not published in these other security applications that call the penetration testing tools.
For research, to me just looking at network, everything I hear says security strategies. On top of that you are going to need to add administrative step strategies such as effective policies.

Interview Question 9, Theme 5: Administrative policies. For Theme 5 of Interview Question 9, 25% of the respondents indicated that having effective administrative policies is key to having an effective network security strategy. Respondents indicated that they need emergency management and disaster recovery teams that understand backdoor intrusions. Furthermore, respondents indicated that following compliance based on National Institute of Standards and Technology NIST 800-53 and the Center for Internet Security (CIS) can improve network security performance. Table 71 contains the Theme 5 responses for Interview Question 9.

Table 71

Interview Question 9, Theme 5 Responses: Administrative Policies

Responses
The most effective way to manage cyber security is to have someone else test it for you.
On top of that you are going to need to add administrative step strategies such as effective policies; you are going to need to make sure the people have standards that they follow which would be some kind of compliance regulation of hardening or control such as National Institute of Standards and Technology NIST 800-53 or some kind of Center of Internet Security (CIS) controls or disks that have the strategic technology.
I think another thing is you want to be sure that effective managers in the organization that are involved in any sort of emergency management or disaster recovery understand the procedures you take when there is an intrusion.

Interview Question 9, Theme 6: Cloud security. For Theme 6 of Interview Question 9, 25% of the respondents indicated that physical security is key to having an effective network security strategy. Respondents indicated that they trust third-party security cloud services even though nothing is secured one hundred percent. Respondents also stated that physical security should not be overlooked. Table 72 contains the Theme 6 responses for Interview Question 9.

Table 72

Interview Question 9, Theme 6 Response: Cloud Security

Responses
I think what one strategy that I find often gets overlooked is physical security.
So but what if they have a breach, okay, somebody breaks into their cloud? So now I have to

trust all of them but they got a good strategy and they have a better security than me. But you know what, nothing is a hundred percent secure.
At the end of the day, the physical security cannot be overlooked.

Interview Question 9, Theme 7: Wireless security. For Theme 7 of Interview Question 9, 17% of the respondents indicated that vulnerabilities on wireless access networks need to be addressed as part of an effective network security strategy. According to the respondents, separating the primary wireless network from the guest network improves security. There are still security gaps, however, in wireless access points, presenting vulnerabilities and affecting the performance of the network in IT departments. Table 73 contains the Theme 7 responses for Interview Question 9.

Table 73

Interview Question 9, Theme 7 Responses: Wireless Security

Responses
It is those points where it happens and there is a breach between two different parts. So that is why I believe wholeheartedly having your wireless network separate from the rest of your important information; especially the guest network. I am a big promoter of that one.
In the end again, wireless access points. You know things like this have a feature now that does not allow peer to peer devices. Let us say that this is a wireless access point and this is a client that wireless access points will not allow this client to peer to that client at all.

Presentation and Discussion of Findings

Table 74 indicates all themes and topics emerging from twelve interviews; the first column presents the theme and the second column indicate the number of responses per participant indicated the frequency of reference related to interview question one to interview question nine. The total of interview questions were nine (See Appendix B). The first column indicates emerging themes generated from the answers of the twelve participants and the second column is the frequency of reference for each theme related to the interview question using n as the number of responses supporting each theme. Complete descriptions of the results of these findings are discussed in Chapter 5.

Table 74

Themes and Topics Emerging from the 12 Interviews

Themes	*n*
Frequency of reference for themes related to Interview Question 1	
Protect data	4
Risk analysis	3
Recommend findings	3
Monitoring team	3
Internal message alerts	3
Log notifications	3
Third party services	2
Frequency of reference for themes related to Interview Question 2	
Backdoor analysis	5
Brute force	5

Backdoor detection	4
Phishing emails	3
Compartmentalized email gateways	3
Zero-day	3
Identifying backdoors	2
Frequency of reference for themes related to Interview Question 3	
Executive	4
Organizational	4
Information technology	4
Client	4
Financial	4
Staffing	4
Leadership	3
Frequency of reference for themes related to Interview Question 4	
Notify upper management	4
Systems update	4
Collecting evidence	4
Isolate devices	4
Backdoor issue	3
Firmware	3
Frequency of reference for themes related to Interview Question 5	
Educate and share	5
Investigate network sections	4

Disabling traffic	3
Counter intrusion service	3
Isolate software	3
Identify anomalies	3
Stopping traffic	3
Frequency of reference for themes related to Interview Question 6	
Certifications	9
Awareness	5
Expertise	5
Culture	4
Teamwork	4
Weakest link	4
Network protocol analysis	2
Frequency of reference for themes related to Interview Question 7	
Dynamic awareness	5
Understanding defense	5
Network security	5
Understanding threats	4
Human factor	4
Enforcing defense	4
Defense tasks	3
Frequency of reference for themes related to Interview Question 8	
Weak network sections	6

Network layers	6
Access points	6
Defense-in-depth	4
Network segmentation	4
Internal network defense	2
Strategic value	2
Frequency of reference for themes related to Interview Question 9	
Internet security	7
Risk assessment team	6
Management	4
Ethical hacking	4
Administrative policies	3
Cloud security	3
Wireless security	2
Cumulative number of responses	241

Table 75 contains the aggregated theme data from all nine interview questions. Once the data was analyzed, the categories of major themes and prominent topics were created. The major themes category contains the ideas which were very popular among interview participants. The prominent topics, while less popular, are still significant. The four major themes were (a) human factor, (b) defense-in-depth strategies, (c) backdoor detection techniques, and (d) network monitoring strategies. The three prominent topics were (a) involvement of management, (b) effective administrative policies, and (c) ethical hacking services. The major themes and

prominent topics that emerged from the data suggested these are strategies that should be implemented by network security managers to protect their network. The findings are directly related to the current literature used for researching strategies to protect networks from backdoor intrusions.

Table 75

Major Themes and Prominent Topics of Research Data

Major Themes and Prominent Topics	
Major Themes	
Human factor	79
Defense-in-depth strategies	30
Backdoor detection techniques	22
Network monitoring strategies	21
Prominent Topics	
Involvement of management	4
Effective administrative policies	3
Ethical hacking services	4
Total of Major Themes and Prominent Topics	163

The original transcripts were verified by interviewed participants to ensure the validity of the raw data. Data saturation was reached after the twelfth interview. The researcher conducted a thorough review of the raw data and then began coding by looking for themes, patterns, and experiences. One transcript had to be translated due to a language preference from the participant. Once the data was coded, and saturation was reached, the data were analyzed to look

for major themes and prominent topics. The data was analyzed a second time ensuring a thorough and unbiased assessment had been achieved. From the unbiased assessment of data, four major themes and three prominent topics emerged from the responses of each participant providing a clear understanding of the phenomenon. The participants answered each of the nine interview questions resulting in a compilation of four major themes as well as three prominent topics.

These findings indicate that many strategies are needed to be implemented simultaneously to protect networks from backdoor intrusions. Backdoor intrusions are a complex problem due to their stealth nature embedded into circuits of network devices. The responses show that despite the complexity of backdoor intrusions there are many strategies that still can be implemented. Additionally, the major themes and prominent topics support the findings. Network managers face a challenge, and they need all the help they can get during their daily network operations. The literature correlates with the responses of each participant and supports the findings in this study.

Summary of Chapter Four

Chapter 4 included the findings and analysis of the data collected from the participants. The analysis resulted in four major themes and three prominent topics emerging from the aggregated theme data and the nine interview questions. Chapter 5 presents interpretations from the results found in chapter 4. Recommendations and future research also are included in chapter 5.

CHAPTER FIVE

The problem addressed in the study was the strategies network security managers need to protect their networks from backdoor intrusions. The purpose of this qualitative study was to explore the strategies network security managers need to protect their networks from backdoor intrusions. The research design study selected was the qualitative methodology approach to explore the views of research participants (Creswell, 2014). The first step was to select 12 participants that had experience in managing or administrating network security in IT departments to explore the strategies needed to protect networks from backdoor intrusions. The investigator served as the instrument in the research study, and he focused on the process and events to be studied using a digital audio recorder and took notes to record the events (Miles et al., 2014). The second step was to collect the data through the process of interviewing the participants. The investigator adapted to local conditions in order to accommodate the needs of the management population while generating insights via open-end communication with experienced network managers or systems administrators (Goodyear et al., 2014). The third step was analyzing the data manually. Goodyear et al. (2014) declared that after data has been collected, the analysis continues to evolve.

According to Simon and Goes (2013), limitations are permanent characteristics of method and design and cannot be controlled by the investigator. The first limitation of this study was the time constraint. The second limitation was not knowing how the business objective of each organization affects the defense strategies against backdoor intrusions. Lastly, not knowing how the budget of each IT department influences the defense strategies used by network security managers was the third and final limitation.

The investigator had an obligation to be mindful and respect the rights of the informants (Creswell, 2014). It is ethical to ensure that the information collected is not disseminated inappropriately (Gilbert, 2000). The Belmont Report provides guidelines for research on how to treat human subjects (Goodyear et al., 2014); the report also outlines the importance of having a signed informed consent form for each participant. Ethical assessments make sure information found does not harm the interviewees (Miles et al., 2014). Willis, Jost, and Nilakanta (2007) stated that ethical guidelines give participants the opportunity for them to provide informed consent to the study. Finally, ethics prevent harm to human subjects or inappropriate behavior in part of the investigator conducting the research work.

Chapter 5 includes the following sections: findings and conclusions, limitations of the study, implications for practice, implications of the study and recommendations for future studies, and, conclusion. The investigator interpreted conclusions comparing the literature review in chapter 2, the analysis in chapter 4, and, the methodology in chapter 3 taking into consideration the research question and problem statement to present the results of the research in a coherent form.

Findings and Conclusions

According to Miles et al. (2014), member checking occurs when the participants are asked to provide their judgment and their major findings to the researcher. For validity purposes, member checking was used to verify credibility, transferability, accuracy, and validation in part of all respondents. This section presents findings and conclusions derived from nine interview questions used for the interviews.

The investigator compiled raw data generated from the following nine semi-structured interview questions:

1. From your perspective as a manager of network security, what do you regard as the most effective network security monitoring strategies?

   Probe question - Please share an example?

2. What is your protocol for determining if an intrusion to the perimeter-based security into the system has taken place? In other words, how do you know when you have a backdoor intrusion?

   Probe question - How you identify backdoor threats?

3. In your role as a network manager what has been the level of support for you and your staff to be able to implement the most effective strategies?, for instance, through staffing and funding?

   Probe question - Could you elaborate on this a little?

4. When it becomes clear that the network has experienced a backdoor intrusion, what is the usual protocol or strategy that is employed to address the problem?

   Probe question - Do you have an example you could share?

5. Could you please tell me as much as possible about the details of your experience selecting appropriate countermeasures as an IT manager working in the area of network security?

   Probe question - How disruptions in the network are handled?

6. How does having the "right" kinds of staff members impact your ability to carry out an effective strategy for network protection?

   Probe question - What is the key to this strategy working?

7. What are your thoughts about the role of employees throughout the organization as part of the strategy of defending your network from backdoor intrusions?

   Probe question - What is your role in this process?

8. The defense-in-depth strategy seems to be pretty widely accepted as the standard for network security. What is your perspective on the effectiveness of this strategy?

   Probe question - What would a different approach looks like?

9. What other points would you like to make that we did not address during the interview that you think are key to an effective network security strategy?

For interview question 1, the current literature identifies that intrusion detection is a fundamental technique in the defense-in-depth framework (Wang et al., 2016). The requirements to use monitoring tools effectively are a challenge because backdoor attacks are evolving (Grzonka et al., 2015; Axon et al., 2016). After analyzing the data in Chapter 4, the investigator found that information gathered from intrusion detection systems for both external and internal parts of the network can still be used for risk analysis. Monitoring firewall devices against traffic coming from the internet can be a strategy to use to protect data. An active monitoring alert system dividing the alerts into categories should be easy to understand for personnel involved in monitoring the system. The conclusion drawn from the answers given by 12 participants from interview question 1 is that network monitoring tools help for risk analysis processes and the results can be forwarded to upper management. Another point participants brought up is that monitoring results can be used with the intent of protecting data and that there exists a need for a team that is responsible for checking the results is necessary. In addition, third-party services can provide monitoring message alerts and real-time log notifications providing information that

could potentially help in the discovery of backdoor intrusions. The importance of this for network managers is that the use of monitoring tools serves as a strategy needed to protect network systems from intrusions.

For interview question 2, the current literature identifies that if a backdoor intrusion penetrates the perimeter of the network, it is possible to bypass firewalls, intrusion detection systems (IDS) and network address translation (NAT) layers of security (Cleghorn, 2013). After analyzing the data in Chapter 4, the investigator found that detecting phishing emails at the perimeter section of the network should be part of the protocol to determine if a backdoor intrusion has taken place. The perimeter section should be separated from the network in order to isolate phishing emails in a secured containment. The conclusion drawn from the answers given by the participants for interview question 2 is the idea of detecting phishing emails at the perimeter of the network and compartmentalized email gateways is an alternative to avoid intrusions. Other tasks such as checking brute force at the perimeter and relying on end-users for zero-day issues could be effective strategies. The importance for network managers is that by doing checks at the perimeter, it is possible to avoid email threats carrying backdoors that could be opened by the end user.

For interview question 3, the current literature identifies concerns about investing in security software because hackers often use exploits for unknown vulnerabilities (Lam 2016); and according to Langer et al. (2018), reactions towards novel technologies could detrimentally affect staff members. After analyzing the data in Chapter 4, the investigator found that funding support for IT departments is limited; this issue affects the implementation of effective strategies. A fear was perceived regarding the understanding of the importance of staffing and funding. Funding support for network security is low, affecting personnel performance when dealing with

backdoor intrusions. The conclusion drawn from the answers given by the participants for interview question 3 is that leadership is responsible for the support that can influence network strategies. For instance, organizational support can help staff and support IT personnel. Although staffing support is limited, the financial support depends on the business objective of the organization. The meaning for network security managers is that communication is essential to enforce cybersecurity not as an isolated task but as a team effort with the help of everyone in the organization.

For interview question 4 the current literature identifies that active defense methods using powerful active tools on network systems might mitigate backdoor intrusions (Miraglia & Casenove, 2016). After analyzing the data in Chapter 4, the investigator found that collecting as much evidence as possible related to backdoor intrusions is a strategy that can address the problem. With the help of detection methods, personnel are able to see certain types of backdoor intrusions. Another active approach is to keep upper management informed and call for meetings to initiate an investigation and clarify backdoor issues. The conclusion drawn from the answers given for interview question 4 is that collecting evidence is essential in order to defend the network because backdoor intrusions are a serious issue. For example, firmware allows backdoor intrusions to occur. Without notifying upper management about backdoor intrusion evidence eventually will affect network operations. The importance for network managers is that knowing and documenting evidence of possible backdoor attacks could serve as a good strategy to enhance protocols for addressing the problem.

For interview question 5, the current literature identifies different countermeasure techniques to offset backdoor intrusions such as intrusion prevention system (IPS), routing game, checking the bi-directionality of a link, and neighbor authentication (Bouabdellah et al., 2018).

After analyzing the data in Chapter 4, the investigator found that network traffic anomalies should be identified prior to disabling the network in order to stop the traffic. Another countermeasure is to use antivirus software to help identify backdoor intrusion signatures. The conclusion drawn from the answers given by the participants for interview question 5 is that there are several possible countermeasures to take against backdoor intrusions. The following countermeasures suggested by the participants were: a) stopping and disabling network traffic in order to avoid malware to spread and for the computer forensics team to analyze the intrusion, b) using third-party services to allow time for IT departments to focus on other internal issues related to network vulnerabilities, c) investigating specific sections of the network will tell network managers what is going on in their networks to enhance counter measures, d) sharing of knowledge will keep the communication link between employees to keep awareness present in the work environment , e) isolating software will assist computer forensics in finding evidence to have it ready for the court of law proceedings, f) staying quiet might deceived the attacker to keep attacking and understand better their types of attacks, and finally, g) identifying traffic anomalies provides information that can identify potential backdoor intrusions. The significance for systems administrators is that these countermeasures offer strategic value to the IT department.

For interview question 6, the current literature identifies that employees have the power to resist phishing intrusions contributed by enforcing policies as part of the culture of the organization (Rocha Flores et al., 2015). After analyzing the data in Chapter 4, the investigator found that staff members who comply with policies and procedures can positively impact the vision of the organization. Organizations trust employees that have professional security certifications and are willing to learn. The culture mentality of the IT department impacts the

ability of the organization to employ effective strategies. The conclusion drawn from the answers given by the participants for interview question 6 is that having proper qualified staff members promotes the following: a) staff security awareness, b) company rules and needs, c) staff willingness to adjust to the work culture, d) staff certifications, e) staff expertise in their field, and f) teamwork. What this means for network security managers is that having the right kind of staff members is an essential strategy for IT departments.

For interview question 7, the current literature identifies that it is essential to understand human behavior and technology interaction for practicing and studying information systems within the information assurance field (Saunders et al., 2017). After analyzing the data in Chapter 4, the investigator found that understanding what threats are can shape the role of employees and the way they behave. The behavior of employees, network managers, systems administrators, and upper management plays a role in the network defense process. The conclusion drawn from the answers given for interview question 7 is the following roles can be adapted by personnel as another strategy to defend the network: a) understanding how cyber threats affects the organization, and b) adding defense role tasks such as identifying phishing email or not opening web pages that does not have to do with the daily business of the organization. The importance of this for network managers is that assigning roles to employees that have to do with defending the network can serve as a dynamic strategy against backdoor intrusions.

For interview question 8, the current literature identifies that business and government entities often use defense-in-depth information assurance measures to strategically manage and plan for IT security risks (Alexander 2017). After analyzing the data in Chapter 4, the investigator found that having many layers of defense serves as a deterrence method contrary to

Cleghorn (2013) that adding many security technologies causes to the network more problems than solutions. In addition isolating and segmenting the network are effective strategies. In addition, the defense-in-depth strategy should be implemented at the level of the Open Systems Interconnection model (OSI model) where IT departments connect to the internet world. Even though stealth backdoors still penetrating networks, the conclusion drawn from the answers given by the participants for interview question 8 is that defense-in-depth serves of strategic importance and must be enforced in many levels of the network. The strategy could be applied to weak sections of the network, within layers of the computer systems and at every wireless access point. The significance for systems administrators is that meticulously applying defense-in-depth principles in different sections of the network brings strategic value against backdoor intrusions.

For interview question 9, the current literature identifies that organizations use different modern operating systems leading to errors when enforcing stable mandatory access control (Amthor, 2015). After analyzing the data in Chapter 4, the investigator found that indeed there are security errors when combining different operating systems used in the IT department. For example, using encrypting data between Windows machines and Linux environments causes communication problems between the operating systems. The conclusion drawn from the answers for interview question 9 brought up additional strategic ideas for defending the network from intrusions. For instance, the involvement of management, wireless network security, Internet, operating systems and physical security, effective administration, use of risk assessment teams, the use of ethical hacking services and the application of cybersecurity at the cloud level must all be taken into consideration as ideas for network defense strategies. What this means for network security managers is that there are many strategic functions that can help to secure the

network and they can be personalized depending on the business objective of the parent organization.

Major Theme 1: Human Factor

The major theme of human factor was voiced by 100% of the participants. For instance, network security managers must play a part in the decision-making process to support IT network security (Fielder et al., 2016; Green et al., 2015). IT staff must understand security procedures and policies during real-time operations as an effective protection strategy (Safa et al., 2015; Ghai et al., 2015). The organization must not underestimate the behavior and feelings of employees as a vital human factor within information security (Chen et al., 2014; Bucak, 2016). Also, network managers need support from upper management as well as their employees. Personnel need to play security roles to protect the networks, and well-trained staff can help network managers secure network operations. The investigator noticed during the interviews that participants verbalized the need for involvement of people to support the IT department and parent organization. Network managers working together with their employees and upper management can help strengthen strategies needed to protect the network from backdoor intrusions. Respondents mentioned the need of having employees that speak up if something is wrong and that care having the network environment secure and providing employees with knowledge to protect network against phishing email. Another example of human factor is when business executives heard about news related to cybersecurity intrusions resulting to review their security strategies on IT departments.

Major Theme 2: Defense-in-Depth Strategies

The major theme of defense-in-depth strategies was voiced by 83% of the participants. Respondents agree that adding security layers is essential in network defense. According to

Levillain et al., (2015), multiple security layers protect information and manages IT risks. Alexander (2017) stated defense-in-depth approaches are effective. Participants recommended the use of third party services to test traffic safety before allowing it on the network working environment. However, the investigator found many gaps based on the responses. Number one was gaps between layers in the network; number two was gaps in weak network sections such as wireless access points; and number three was a gap inside the IT network itself where backdoor intrusions manage to infiltrate in many forms. For example, phishing emails can reach the end-user, and if opened the backdoor intrusion will succeed. Respondents stated to follow a mesh topology network and not put the network in one location because once breach you can lose everything. Without layered security one breach can destroy the whole network. Participants mentioned that defense-in-depth is the standard until advancements of artificial intelligence might offer better defense alternatives. Participants declared that defense-in-depth should be applied outside the network to prevent breaches with the implementation of two-factor authentication in order to protect every point that could be accessed.

Major Theme 3: Backdoor Detection Techniques

The major theme of backdoor detection techniques was voiced by 100% of the participants. Participants were aware of backdoor intrusions and they rely on tools they have available to detect them. For example, the use of firewall devices, intrusion detection systems and the use of systems logs. However, backdoors are hard to detect because, in the case of Distributed Denial Of Service attack (DDoS), the intrusions have been executed prior to reaching the perimeter of the target network (Harasta, 2014 ; Kotenko & Ulanov, 2014). Passive defense strategies are not efficient regarding backdoor intrusions; for example, malware generating PDF files enable attackers to read private data (Goldman et al., 2015; Xingguo et al., 2016). Backdoor

detection techniques deserve careful attention due to the stealth nature of backdoor intrusions. For instance, opening a file that looks like a PDF file can trigger an executable code to open a Trojan Horse backdoor and the only technique to defuse this situation is to alert the user if the PDF file has anomalies before the end-user opens the file. Identifying backdoor threats and what protocols are used to address the backdoor intrusion problem is not easy to determine; especially for those backdoor intrusions that are stealth in nature and impossible to detect due to the code being embedded deep in the binary level of the components of the network itself.

Major Theme 4: Network Monitoring Strategies

The major theme of network monitoring strategies was voiced by 75% of the participants. Respondents stated the importance of using intrusion detection systems to look for anomalies. Now, network monitoring tools have their own particular weaknesses. For example, scheduling processes that occur while operating systems are running in the network are difficult to monitor because backdoor vectors are evolving (Grzonka et al., 2015; Axon et al., 2016). The best network managers can do is to use the tools that they choose to achieve desirable results. In addition, participants point out that system logs need more analysis as well as the need for automated checks in order to see clear trends that can point to behaviors related to backdoor intrusions. Respondents stated to have intrusion detection systems monitoring traffic coming in the network and use third party monitoring services to do the risk analysis and provide recommendations based on findings. In addition, monitoring the end-user provides information related to intrusions that might be trigger by users. Another area of monitoring is to look at firewalls which most of the viruses are coming from accessing the internet. The use of active live monitoring can be used to continuously test policies or locking events to look for patterns and behaviors related to backdoor intrusions.

Prominent Topic 1: Involvement of Management

The prominent topic of involvement of management was voiced by 33% of the participants. Respondents indicated that an effort to discover backdoors from other nations including tools available on the dark web is key to an effective network security strategy. Participants stated that managers must be involved in looking for different types of threats. Participants thought that understanding new threats can improve the procedures taken when facing an intrusion. Network managers point out to make sure that key leaders in the organization are involved in any sort of emergency management and disaster recovery planning and have a good relationship with managers. Furthermore, IT personnel must look for different types of threats. Participants mentioned the need of leaders to specify budget in security. Upper management need to understand what backdoor intrusions are in order for them to consider reviewing network security protocol steps and enhance strategies to protect their data.

Prominent Topic 2: Effective Administrative Policies

The prominent topic of effective administrative policy was voiced by 25% of the respondents. Participants indicated that having effective administrative policies is key to having an effective network security strategy. Respondents indicated that they need emergency management and disaster recovery teams that understand backdoor intrusions. Furthermore, respondents indicated that following compliance based on National Institute of Standards and Technology NIST 800-53 and the Center for Internet Security (CIS) can improve network security performance. Well defined policies and procedures is probably the fundamental building block to protect data and have process documented. Participants recommend frequent policy tests at least monthly to verify if policies are doing what they are supposed to do. Also, policies need the support of leadership to provide proper technologies for adequate functioning. For example,

have policies related with clicking emails for employee performance evaluation purposes and define policies regarding proper use of networks.

Prominent Topic 3: Ethical Hacking Services

The prominent topic regarding the use of ethical hacking services was voiced by 33% of the respondents. Participants indicated that having a security team to test their network positively impacts the network security strategy. Respondents also indicated that spending money on penetration testing teams can help determine if policies created to protect the network can be breached. Respondents stated that even someone without malicious intent can still breach the network accidentally. Participants also indicated that the administration level could implement effective policies to help in improving the defensive strategy. Penetration testing teams can influence strategies that can positively impact network security protocols. According to respondents there are free penetration testing services help to see get a vantage point of the network. At least annual penetration tests were recommended by participants because it shows a different perspective to view network vulnerabilities in a different way and use such findings to have an advantage from the strategic point of view.

Limitations of the Study

The study had three limitations. The first limitation was participants were from only one geographic area and business climate. The second limitation was that the investigator did not obtain data on the business objective of each IT department parental organization that might constrain the strategies needed against backdoor intrusions. Finally, limitation three was not being aware that the budget of each IT department may cause an impact on the research results.

Additional limitations emerged during the data collection process. The investigator did not have specific experience as a network security manager or systems administrator and was forced to rely on what was learned on the basis of the literature review. The conceptual

framework relied on the defense-in-depth strategy and added other concepts that the investigator thinks are important to help protect networks from backdoor intrusions.

The investigator had four key assumptions. The first was that the defense-in-depth strategy helps network managers assure the system works safely. The second assumption was that IT managers or administrators are required to work on issues if expected results are not delivered. The third assumption was that IT departments are well financed, and the fourth that staff members had mandatory training as part of their job. The investigator learned that defense-in-depth serves as an important strategy that makes difficult to hackers entering the network and works as a well deterrent method. IT departments count on their members to solved security issues in real-time and communication is essential in the process of managing risks. The investigator did not learn much about the relationship between budget allowing IT departments to protect their environment and definitely training sessions are conducted in a regular basis.

This study also had two delimitations; first delimitation was the time constraint allowing up to an hour for each of the interviews. The second delimitation was the geographical area selected can affect the findings due to data being restricted in one location. During the execution of the study, the investigator found that the data collection process took about 12 weeks. The investigator prioritized a considerable amount of time concentrating on finishing the data collection process before proceeding to analyze the data. The investigator interviewed a total of 12 participants.

Implications for Practice

The problem addressed in the study was the strategies network security managers need to protect their networks from backdoor intrusions. The results of the study are relevant for IT network managers and systems administrators or other practitioners in the field of cybersecurity and information assurance. According to Bou-Harb et al. (2014), current network detection

strategies still have serious challenges due to cyber scanning campaigns that render current detection techniques impractical.

Recommendation 1

This recommendation is for professionals involved in managing or administrating IT departments and for cybersecurity and information assurance practitioners. People are the key factor that can make a difference in securing networks from intrusions. Investing in resources to support information systems security can be a complex task. Executive support buy-in is needed for IT support. In addition, help from developers and systems engineers enhances the strategy of securing the network from backdoor intrusions. Proper training for all organizational staff plays a crucial part in network security.

Recommendation 2

The defense-in-depth strategy has strong and weak layers of security. From accessing the network to having layers of protection on firewalls and the File Allocation Table (FAT) with the purpose of deterrence are some examples of finding weak and strong areas in locations where backdoor intrusions could penetrate. Attention must be paid not only to the exterior section of the network but the interior level as well, especially in critical points of the network where traffic is entering the system. Another point that might interest practitioners is the prevention of breaches at the upper level in the demilitarized zone of the network including every point that could be accessed.

Recommendation 3

Another attribute of backdoors is that manufacturer implant hardware and software that results in accessing network systems without permission. This access in the wrong hands could potentially damage networks. Since IT departments need more help in preventing backdoor

intrusions, the analysis of backdoors by software and hardware experts could bring ideas to develop methods beneficial for network managers or systems administrators in their IT departments. Backdoors are hard to detect, but the use of firewalls that can send alerts by text or email messages may provide some help to personnel involved in the information technology business. Since backdoors are tough to defend against, it is essential to use the best tools available, keep upper management informed, spread the word to law enforcement organizations and avoid ignoring the backdoor problem.

Recommendation 4

It is crucial to use intrusion prevention and detection systems to monitor traffic coming into the network. In addition, using third-party services to do the risk analysis improved defense strategies used to secure the systems. Analyzing monitoring findings and providing recommendations to the proper authorities can provide vital information. There is a need to have a reliable external monitoring alert system that can provide comprehensive reports that need to be easy to read. Network managers and system administrators suggested the systems logs need more analysis as well as a need for automated checks in order to see clear trends that can point out behaviors.

Implications of Study and Recommendations for Future Research

The future step to provide continuity of this study is to research IT budget and the effects the budget has in network security strategies. In order to conduct future research on this topic the investigator would need to have access to upper management and their IT department. The use of a qualitative method with a case study approach might be appropriate. (Fagnan et al., 2018) stated that practices for large-scale businesses require quality improvement transformation initiatives, but they can be difficult and costly.

Another step to compliment this study is to conduct a qualitative study in order to investigate gaps between information technology departments and the business objective of the IT parent organization. For instance, research on business informatics is recommended because IT departments affect parent business organizations with its network security issues. This recommendation might bring strategic network security knowledge that could be beneficial for organizations and their IT departments. Business informatics is a combination of business studies and information science (Paul, Bhuimali, Aithal, & Bhowmick 2018).

Finally, another step to continue contributing to the body of knowledge following this study is to do a quantitative study to analyze systems logs, hidden parameters, exposed configuration data or other types of backdoors affecting networks. The investigator may set up a self-contained laboratory representing a network, and perhaps using a series of virtual environments with different operating systems. This idea might offer a closer look at how backdoor intrusions behave. Lei, Yang, Ma, Sun, Zhou, and Ma (2018) proposed an improved vulnerability scoring method for home internets.

Conclusion

The importance of this study emphasizes that strategies employed to protect networks from backdoor intrusions need improvement and clarification. Returning to the question posed at the beginning of this study," what are the strategies network security managers need to protect their networks from backdoor intrusions?", it is now possible to state that the strategies are complex, dynamic in nature and that challenges are still present. The level of support the organization has to offer concerning whether or not the organization can afford adequate staff and funding to provide resources and services from third-party vendors is an essential component of strategic value. The role of each staff member is interconnected with effective strategies.

Human involvement in securing network operations is a challenge. The need of sharing responsibilities is necessary to offset the shortage of cybersecurity support. For example delegating responsibilities to employees might be an alternate method of sharing tasks to enhance network security strategies. The organization can benefit from adding up the latest security updates against backdoor intrusions. Backdoor intrusions attack in multiple directions, from the first line in defense to different parts of the network including devices and software. The study set out to explore the influence of network managers or systems administration in dealing with backdoor intrusions. Their experience is connected with themes found by the investigator such as the use of consulting services, antivirus software, systems logs analysis, systems back up, firewall devices and reporting forensic evidence to legal authorities as some of the strategies that help deter backdoor intrusions. These themes suggests ways connected to understand how backdoor intrusions behave and how we can implement strategies to defend against such threats.

The study has examined the relationship between these strategies and the impact they have on IT departments and their parent organizations. This study has raised important questions about the stealth nature of backdoor intrusions and their effects on the strategies needed to deter such attacks. For example, comprehensive alerts and transmission control protocol (TCP) reports can provide internal network information on what is happening inside IT department systems where network security managers can have a better understanding of the importance of defending the network from backdoor intrusions.

The insights gained from this study may be of assistance to network managers, systems administrators, and their upper management. This is the first study to report an association between backdoor intrusions and strategies used by IT departments to help not only the parent

organization but to attempt to discover different strategic approaches that could be beneficial for IT departments. The study was important for furthering our understanding of the role of network security managers and systems administrators and the strategic value they can offer.

Although the findings should be interpreted with caution, this study has several strengths. Participants shared their experience in order to provide their point of view in exploring the relationship between backdoor intrusions and network defense. This study intended to bring awareness to the organization regarding the importance of enhancing security strategies in IT departments from backdoor intrusions.

Below is a summary of the major findings:

Human Factor

Managers play a key role in cybersecurity investment decisions with regards to allocating funds and resources for cybersecurity. Support from technical experts can address upgrades and security needs for the organization. For example, investing in cyber insurance could potentially provide another strategy option to protect networks from backdoor intrusions that could damage IT devices (Fielder et al., 2016; Green et al., 2015). Support from enforcement components and firms may reduce data breaches in organizations (Safa et al., 2015). Bucak (2016) stated that management commonly does not listen to employees but rather commands them, enabling insider threats. For instance, a backdoor intrusion may be initiated by disgruntled employees inserting USB devices that contain malware into the computers. Also, intrusion detection systems can be used to detect anomalies and offer another different strategic approach against backdoor intrusions.

Defense-in-Depth Strategies

Defense-in-depth is a strategy with multiple methodologies that can fit the needs of the organization. Keeping an active approach decreases the risk of networks being harmed from

threats that are continually evolving. Among many examples, a strategy called masking techniques could be used as a defense-in-depth countermeasure. This approach can be applied to Hyper Text Transfer Protocol Secure (HTTPS) applications (Levillain et al., 2015). The argument on this study is defense-in-depth strategy presents vulnerabilities, for instance, end-users accessing unauthorized internet sites at the workplace enable backdoor intrusions. Despite its weaknesses, defense-in-depth is still the de-facto standard in the cybersecurity and information assurance field. Disabling the section of the network being attack by shutting down the system is a way to counteract backdoor intrusions. Adding security layers, using third-party services, and using two-factor authentication adds an additional layer of defense and protection. Identifying events, signatures, IP address and ports and stopping the traffic can add strategic value to deter backdoor intrusions.

Backdoor Detection Techniques

The use of email opens opportunities for compromising the network. The end-user plays a critical role in detecting this backdoor intrusion approach. The best technique for deterring the fake email that can damage the machine is to simply not open it. Another possible technique to detect backdoor intrusions is the process of archiving evidence at the perimeter of the network in order to stop and prevent intrusions. Another strategy called mimic defense technology has been already put into practice in routers and web servers deterring and decreasing the backdoor threat. In terms of detecting stealth backdoors, the investigator did not find any indication of possible strategies either because more research is needed or because stealth backdoors are impossible to detect. Finally, systems backups offer a solution to minimize the risk from backdoor intrusions in the case where the system is backed up prior to use.

Law enforcement agencies and intelligence services require backdoors to ease their investigations, but this can lead to cyber insecurities. This issue might require new backdoor

detection techniques or the involvement of qualified personnel to rethink new cybersecurity policies in order to protect networks from backdoor intrusions (Harasta, 2014). On the other hand, DDOS attacks are hard to detect and become more complex affecting the defense of the network. Goldman et al. (2015) presented an active approach that has the likelihood of accurate detection helping systems administrators or network security managers reduce the effect of having too many false warnings which may aid in detecting "zero-day" attacks, but it is not clear how this method detects backdoor intrusions. Xingguo et al. (2016) proposed a strategy to help solve the backdoor intrusion issue.

Network Monitoring Strategies

Grzonka et al. (2015) presented a strategy that monitors the schedule executions for cloud and grid computing that could be beneficial for IT managers to adopt. Axon et al. (2016) proposed another monitoring strategy using a method called "sonification" that may improve current monitoring capabilities. The use of monitoring software in IT departments could enhance detection of backdoor intrusions, and reporting the results to legal authorities provides opportunities for researchers to explore such evidence. Network security managers may consider learning about the latest automation scanning systems and firewall technologies and apply these strategies to their internal section of the network in order to record and study traffic behavior. In addition, conducting risk analysis is another strategy available to help understand how backdoor intrusions behave; also the process of isolating suspicious events, messages, and infected files prevent some backdoor intrusions from spreading within the system.

REFERENCES

Abrahams, L., & Mbanaso, U. (2017, May). *State of Internet Security and Policy in Africa.* Paper presented at The First African Academic Network on Internet Policy in The International Institute of tropical Agriculture (IITA) Nigeria, Africa.

Acquaviva, J., Mahon, M., Einfalt, B., & LaPorta, T. (2017, September). *Optimal Cyber-Defense Strategies for Advanced Persistent Threats: A Game Theoretical Analysis. In Reliable Distributed Systems (SRDS),* 2017 IEEE 36th Symposium, Hong Kong, China. doi: 10.1109/SRDS.2017.29

Ahmad, A., & Maynard, S. (2014). Teaching information security management: reflections and experiences. *Information Management & Computer Security*, *22*(5), 513-536. doi: 10.1108/IMCS-08-2013-0058

Ahmim, A., & Ghoualmi Zine, N. (2015). A new hierarchical intrusion detection system based on a binary tree of classifiers. *Information & Computer Security*, *23*(1), 31-57. doi: 10.1108/ICS-04-2013-0031

Akhmetov, B., Lakhno, V., Boiko, Y., & Mishchenko, A. (2017). Designing a decision support system for the weakly formalized problems in the provision of cybersecurity. *Восточно-Европейский журнал передовых технологий*, *1*(2), 4-15. doi: 10.15587/1729-4061.2017.90506

Akhunzada, A., Ahmed, E., Gani, A., Khan, M. K., Imran, M., & Guizani, S. (2015). Securing software defined networks: taxonomy, requirements, and open issues. *IEEE Communications Magazine*, *53*(4), 36-44. doi: 10.1109/MCOM.2015.7081073

Al Awawdeh, S., & Tubaishat, A. (2014, April). *An information security awareness program to address common security concerns in IT unit*. Presented at the 11th International Conference on Information Technology: New Generations, Las Vegas, NV. doi: 10.1109/ITNG.2014.67

Alexander, R. (2017). *Solving Information Assurance Issues using Defense in Depth Measures and The Analytical Hiearchy Process*. Denver, CO. Outskirts Press.

Alexander, R. (2017). Using the Analytical Hierarchy Process Model in the Prioritization of Information Assurance Defense In-Depth Measures?—A Quantitative Study. *Journal of Information Security*, *8*(03), 166. doi: 10.4236/jis.2017.83011

Alexander, R. T. (2017). *Can the analytical hierarchy process model be effectively applied in the prioritization of information assurance defense in-depth measures? -a quantitative study* (Doctoral dissertation, Capella University). Retrieved from ProQuest Dissertations and Theses Database. (10257625)

Almorsy, M., Grundy, J., & Ibrahim, A. S. (2013, May). Automated software architecture security risk analysis using formalized signatures. In Proceedings of the 2013 International Conference on Software Engineering, San Francisco, CA. doi: 10.1109/ICSE.2013.6606612

Alnabulsi, H., Islam, M. R., & Mamun, Q. (2014, November). Detecting SQL injection attacks using SNORT IDS. In *Computer Science and Engineering (APWC on CSE)*, 2014 Asia-Pacific World Congress, Nadi, Fiji. doi: 10.1109/APWCCSE.2014.7053873

Alsaleh, M. N., & Al-Shaer, E. (2016, October). Towards Automated Verification of Active Cyber Defense Strategies on Software Defined Networks. In Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, Vienna, Austria. doi: 10.1145/2994475.2994482

Amthor, P. (2015, July). A uniform modeling pattern for operating systems access control policies with an application to SELinux. In e-Business and Telecommunications (ICETE), 2015 12th International Joint Conference, Colmar, France. doi: 10.5220/0005551000880099

Armando, A., Bezzi, M., Metoui, N., & Sabetta, A. (2015). Risk-aware information disclosure. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, 8872*, 266-276. Springer, Cham. doi: 10.1007/978-3-319-17016-9_17

Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H., Rieck, K., & Siemens, C. E. R. T. (2014, February). DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket. In *NDSS*, *14*, 23-26. doi: 10.14722/ndss.2014.23247

Awan, J. H., Memon, S., Khan, R. A., Noonari, A. Q., Hussain, Z., & Usman, M. (2017). Security strategies to overcome cyber measures, factors and barriers. *Eng. Sci. Technol. Int. Res. J*, *1*(1), 51-58. Retrieved from https://www.researchgate.net/publication/321012672_Security_strategies_to_overcome_cyber_measures_factors_and_barriers

Axon, L., Creese, S., Goldsmith, M., & Nurse, J. (2016, July). *Reflecting on the use of sonification for network monitoring.* Paper presented at the 10th International Conference on emerging Security Information, Systems and Technologies, Nice, France.

Bahli, B., & Rivard, S. (2013). Cost escalation in information technology outsourcing: A moderated mediation study. *Decision Support Systems*, *56*, 37-47. doi: 10.1016/j.dss.2013.04.007

Balaman, Ş. Y., Wright, D. G., Scott, J., & Matopoulos, A. (2018). Network design and technology management for waste to energy production: An integrated optimization framework under the principles of circular economy. *Energy*, *143*, 911-933. doi: 10.1016/j.energy.2017.11.058

Bansal, G. (2017). Distinguishing between Privacy and Security Concerns: An Empirical Examination and Scale Validation. *Journal of Computer Information Systems*, *57*(4), 330-343. doi: 10.1080/08874417.2016.1232981

Bauer, M. W., & Gaskell, G. (Eds.). (2000). *Qualitative researching with text, image and sound: A practical handbook for social research*. Los Angeles, CA: Sage.

Bauman, E., Lu, Y., & Lin, Z. (2015). Half a century of practice: Who is still storing plaintext passwords? In *Information Security Practice and Experience 9065*, 253-267. Springer, Cham. doi: 10.1007/978-3-319-17533-1_18

Beller, M., Bholanath, R., McIntosh, S., & Zaidman, A. (2016, March). Analyzing the state of static analysis: A large-scale evaluation in open source software. In *2016 IEEE 23rd International Conference on Software Analysis, Evolution, and Reengineering (SANER), Osaka, Japan.* doi: 10.1109/saner.2016.105

Berg, K., Crawford, J. N., & Seymour, T. (2016). Unbreakable: A concise overview of cybersecurity. *Issues in Information Systems*, *17*(4), 208-221. Retrieved from http://www.iacis.org/iis/2016/4_iis_2016_208-221.pdf

Beuran, R., Chinen, K. I., Tan, Y., & Shinoda, Y. (2016). Towards effective cybersecurity education and training. *School of Information Science, Graduate School of Advanced Science and Technology, Japan Advanced Institute of Science and Technology*, Retrieved from http://hdl.handle.net/10119/13769

Boggs, N., Du, S., & Stolfo, S. J. (2014, September). Measuring drive-by download defense in depth. In *International Workshop on Recent Advances in Intrusion Detection 8688*, 172-191. Springer, Cham. doi: 10.1007/978-3-319-11379-1_9

Boraten, T., & Kodi, A. (2018). Mitigation of Hardware Trojan based Denial-of-Service attack for secure NoCs. *Journal of Parallel and Distributed Computing*, *111*, 24-38. doi: 10.1016/j.jpdc.2017.06.014

Bouabdellah, M., Kaabouch, N., El Bouanani, F., & Ben-Azza, H. (2018). Network layer attacks and countermeasures in cognitive radio networks: A survey. *Journal of Information Security and Applications*, *38*, 40-49. Retrieved from https://www.researchgate.net/publication/321642631_Network_layer_attacks_and_countermeasures_in_cognitive_radio_networks_A_survey

Bou-Harb, E., Debbabi, M., & Assi, C. (2014). Cyber scanning: a comprehensive survey. *IEEE Communications Surveys & Tutorials*, *16*(3), 1496-1519. doi: 10.1016/j.jisa.2017.11.010

Bragg, S. M. (2016). *Cost accounting fundamentals*. Colorado, CO: Accounting Tools, Incorporation.

Bucak, I. O. (2016). An Extended Human Threats Taxonomy To Identify Information Security Breaches. *International Journal of Advances in Computer Networks and Its Security, 6*(1), 29-34. doi: 10.15224/978-1-63248-064-4-07

Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018). Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition. *Computers & Security, 73,* 114-136. doi: 10.1016/j.cose.2017.10.013

Budianto, E., Jia, Y., Dong, X., Saxena, P., & Liang, Z. (2014, September). You can't be me: Enabling trusted paths and user sub-origins in web browsers. In *International Workshop on Recent Advances in Intrusion Detection, 8688,* 150-171. Springer, Cham. doi: 10.1007/978-3-319-11379-1_8

Bukač, V., & Matyáš, V. (2014). Host–Based Intrusion Detection Systems: Architectures, Solutions, and Challenges. In *Architectures and Protocols for Secure Information Technology Infrastructures* (pp. 184-213). doi: 10.4018/978-1-4666-4514-1.ch007

Bureau of Labor Statistics, U.S. Department of Labor, (2018). *Occupational Outlook Handbook,* Retrieved from: https://www.bls.gov/ooh/computer-and-information-technology/network-and-computer-systems-administrators.htm

Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & management, 52*(4), 385-400. doi: 10.1016/j.im.2014.12.004

Checkoway, S., Maskiewicz, J., Garman, C., Fried, J., Cohney, S., Green, M., ... Shacham, H. (2016, October). A systematic analysis of the Juniper Dual EC incident. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria. doi: 10.1145/2976749.2978395

Chen, P., Desmet, L., & Huygens, C. (2014, September). A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security, 8735,*63-72. Springer, Berlin, Heidelberg. doi: 10.1007/978-3-662-44885-4_5

Chen, X., Liu, C., Li, B., Lu, K., & Song, D. (2017). Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning. *arXiv preprint arXiv:1712.05526.* Retrieved from https://arxiv.org/abs/1712.05526

Cherdantseva, Y., Hilton, J., Rana, O., & Ivins, W. (2016). A multifaceted evaluation of the reference model of information assurance & security. *Computers & Security, 63*, 45-66. doi: 10.1016/j.cose.2016.09.007

Choi, B., & Cho, K. (2013). Two-step hierarchical scheme for detecting detoured attacks to the web server. *Computer Science and Information Systems, 10*(2), 633-649. doi: 10.2298/csis120908026c

Cleghorn, L. (2013). Network defense methodology: A comparison of defense in depth and defense in breadth. *Journal of Information Security, 4*(03), 144. doi: 10.4236/jis.2013.43017

Corbetta, J., Invernizzi, L., Kruegel, C., & Vigna, G. (2014, September). Eyes of a human, eyes of a program: Leveraging different views of the web for analysis and detection. In *International Workshop on Recent Advances in Intrusion Detection, 8688,* 130-149. Springer, Cham. doi: 10.1007/978-3-319-11379-1_7

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Los Angeles, CA: Sage.

Creswell, J. W., & Poth, C. N. (2007). Qualitative inquiry and research design: Choosing among five approaches. Los Angeles, CA: Sage.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, *45*(4), 51-71. doi: 10.1145/2691517.2691521

Da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *computers & security, 70*, 72-94. doi: 10.1016/j.cose.2017.05.002

Dai, B., Xu, G., Huang, B., Qin, P., & Xu, Y. (2017). Enabling network innovation in data center networks with software defined networking: A survey. *Journal of Network and Computer Applications, 94*, 33-49. doi: 10.1016/j.jnca.2017.07.004

Dainotti, A., King, A., Claffy, K., Papale, F., & Pescapé, A. (2015). Analysis of a/0 stealth scan from a botnet. *IEEE/ACM Transactions on Networking (TON), 23*(2), 341-354. doi: 10.1145/2398776.2398778

Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the methods behind cyber terrorism. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549). IGI Global. doi: 10.4018/978-1-4666-5888-2.ch147

Department of Health, (2014). The Belmont Report. Ethical principles and guidelines for the protection of human subjects of research. *The Journal of the American College of Dentists, 81*(3), 4.

DePoy, E., Gitlin, L. N. (2016). *Introduction to Research - E-Book: Understanding and Applying Multiple Strategies*. St. Louis, MO: Elsevier Inc.

Dhal, S., Basu, A., & Gupta, I. S. (2014). Managing Authentication and Detection Probability in Multi-tag RFID System. *Journal of Information Assurance & Security*, *9*(7), 316-328. Retrieved from https://web.a.ebscohost.com/

Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management*, *54*(4), 452-464. doi: 10.1016/j.im.2016.10.002

Dormann, W. (2018). *Cisco ASA and FTD SIP Inspection denial-of-service vulnerability*. Software Engineering Institute. CERT Coordination Center. Vulnerability Note VU#339704. Retrieved from https://kb.cert.org/vuls/id/339704/#

Downing, D. (2013). *Dictionary of computer and internet terms*. S.l. Woodbury, NY: Barrons Educational Series.

Fagnan, L. J., Walunas, T. L., Parchman, M. L., Dickinson, C. L., Murphy, K. M., Howell, R., ... Kho, A. N. (2018). *Engaging Primary Care Practices in Studies of Improvement: Did You Budget Enough for Practice Recruitment?.* The Annals of Family Medicine, 16(Suppl 1), S72-S79. doi: 10.1370/afm.2199

Fang, Z., Liu, Q., Zhang, Y., Wang, K., & Wang, Z. (2015). IVDroid: Static detection for input validation vulnerability in Android inter-component communication. In *Information Security Practice and Experience, 9065,* 378-392. Springer, Cham. doi: 10.1007/978-3-319-17533-1_26

Farhaoui, Y. (2016). How to secure web servers by the intrusion prevention system (IPS)?. *International Journal of Advanced Computer Research*, *6*(23), 65. doi: 10.19101/ijacr.2016.623028

Fattori, A., Lanzi, A., Balzarotti, D., & Kirda, E. (2015). Hypervisor-based malware protection with accessminer. *Computers & Security*, *52*, 33-50. doi: 10.1016/j.cose.2015.03.007

Fidler, B., & Russell, A. L. (2018). Infrastructure and Maintenance at the Defense Communications Agency: Recasting Computer Networks in Histories of Technology. *Technology and Culture*, *59*(4). Retrieved from https://www.press.jhu.edu/journals/technology-and-culture

Fielder, A., Li, T., & Hankin, C. (2016, August). Defense-in-depth vs. Critical Component Defense for Industrial Control Systems. Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research 2016. Belfast, Northern Ireland doi: 10.14236/ewic/ics2016.1

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13-23. doi: 10.1016/j.dss.2016.02.012

Gavrylenko, S., Babenko, O., & Ignatova, E. (2018, April). Development of the disable software reporting system on the basis of the neural network. In *Journal of Physics: Conference Series* (Vol. 998, No. 1, p. 012009). IOP Publishing. doi: 10.1088/1742-6596/998/1/012009

Geramiparvar, M. S., & Modiri, N. (2016). An Approach to Counteracting the Common Cyber-attacks According to the Metric-Based Model. *International Journal of Computer Science and Network Security (IJCSNS), 16*(1), 81. Retrieved from http://paper.ijcsns.org/07_book/201601/20160112.pdf

Ghai, V., Sharma, S., & Jain, A. (2015). *U.S. Patent No. 9,111,088*. Washington, DC: U.S. Patent and Trademark Office.

GhasemiGol, M., Takabi, H., & Ghaemi-Bafghi, A. (2016). A foresight model for intrusion response management. *computers & security, 62*, 73-94. doi: 10.1016/j.cose.2016.06.005

Gilbert, K. (Ed.). (2000). *The emotional nature of qualitative research*. Boca Raton, FL., CRC Press.

Goh, H. H., yi Sim, S., Mohamed, O. A., Mohamed, A. F., Ling, C. W., Chua, Q. S., & Goh, K. C. (2017). Assessment of Power System Risk in Cyber-Attacks in View of the Role Protection Systems. *Indonesian Journal of Electrical Engineering and Computer Science*, *8*(1), 184-191. Retrieved from https://www.iaescore.com/journals/index.php/IJEECS

Goldman, R. P., Burstein, M., Benton, J., Kuter, U., Mueller, J., Robertson, P., ... Bobrow, R. (2015, September). Active Perception for Cyber Intrusion Detection and Defense. In *Self-Adaptive and Self-Organizing Systems Workshops (SASOW), 2015 IEEE International Conference,* Cambridge, MA, USA. doi: 10.1109/sasow.2015.20

Goodyear, L., Barela, E., Jewiss, J., & Usinger, J. (Eds.). (2014). *Qualitative inquiry in evaluation: From theory to practice* (Vol. 29). San Francisco, CA: John Wiley & Sons.

Goolsby, R. (2005). Ethics and defense agency funding: some considerations. *Social networks*, *27*(2), 95-106. doi: 10.1016/j.socnet.2005.01.003

Goztepe, K., Kilic, R., & Kayaalp, A. (2014). Cyber Defense in Depth: Designing Cyber Security Agency Organization for Turkey. *Journal of Naval Science and Engineering*, *10*(1), 1-24. Retrieved from http://dergipark.gov.tr/jnse

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of health care chaplaincy, 20*(3), 109-122. doi: 10.1080/08854726.2014.925660

Green, L. A., Potworowski, G., Day, A., May-Gentile, R., Vibbert, D., Maki, B., & Kiesel, L. (2015). Sustaining "meaningful use" of health information technology in low-resource practices. *The Annals of Family Medicine, 13*(1), 17-22. doi: 10.1370/afm.1740

Grzonka, D., Kołodziej, J., Tao, J., & Khan, S. U. (2015). Artificial Neural Network support to monitoring of the evolutionary driven security aware scheduling in computational distributed environments. *Future Generation Computer Systems, 51*, 72-86. doi: 10.1016/j.future.2014.10.031

Gui, Q., Jin, Z., & Xu, W. (2014, December). Exploring EEG-based biometrics for user identification and authentication. In *Signal Processing in Medicine and Biology Symposium (SPMB), 2014 IEEE*, Philadelphia, PA. doi: 10.1109/spmb.2014.7002950

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32,* 242-251. doi: 10.1016/j.cose.2012.10.003

Guo, X., Dutta, R. G., Mishra, P., & Jin, Y. (2016, December). Automatic RTL-to-formal code converter for IP security formal verification. In *Microprocessor and SOC Test and Verification (MTV), 2016 17th International Workshop*, Austin, TX. doi: 10.1109/mtv.2016.23

Guo, X., Dutta, R. G., Mishra, P., & Jin, Y. (2016, May). Scalable SoC trust verification using integrated theorem proving and model checking. In *Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium*, McLean, VA, USA. doi: 10.1109/hst.2016.7495569

Gupta, R., & Muttoo, S. K. (2017). Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA. *Network Protocols and Algorithms, 8*(4), 1-28. doi: 10.5296/npa.v8i4.10179

Haider, W., Hu, J., Slay, J., Turnbull, B. P., & Xie, Y. (2017). Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. *Journal of Network and Computer Applications*, *87,* 185-192. doi: 10.1016/j.jnca.2017.03.018

Hamed, T., Dara, R., & Kremer, S. C. (2018). Network intrusion detection system based on recursive feature addition and bigram technique. *Computers & Security*, *73*, 137-155. doi: 10.1016/j.cose.2017.10.011

Han, Z., Cheng, L., Zhang, Y., & Feng, D. (2015). Operating System Security Policy Hardening via Capability Dependency Graphs. In *Information Security Practice and Experience, 9065,* 3-17. Springer, Cham. doi: 10.1007/978-3-319-17533-1_1

Harasta, J. (2014). Cyber Security of Tomorrow & Personal Data of Yesterday. *Masaryk UJL & Tech.*, *8*, 171.

He, J. (2017, May). The research of computer network security and protection strategy. In *AIP Conference Proceedings* (Vol. 1839, No. 1, p. 020173). AIP Publishing. doi: 10.1063/1.4982538

Hink, R. C. B., & Goseva-Popstojanova, K. (2016, January). Characterization of Cyberattacks Aimed at Integrated Industrial Control and Enterprise Systems: A Case Study. In *High Assurance Systems Engineering (HASE), 2016 IEEE 17th International Symposium*, Orlando, FL. doi 10.1109/hase.2016.49

Hong, S., Xu, L., Wang, H., & Gu, G. (2015, February). Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures. In *NDSS 15*, 8-11. doi: 10.14722/ndss.2015.23283

Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications, 40*, 307-324. doi: 10.1016/j.jnca.2013.08.001

Hui, K. L., Kim, S. H., & Wang, Q. H. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *Mis Quarterly*, *41*(2), 497. doi: 10.25300/misq/2017/41.2.08

Hyden, P., Moskowitz, I. S., & Russell, S. (2016, March). *Fortification through topological dominance: Using hop distance and randomized topology strategies to enhance network security*. In AAAI Spring Symposium Series Palo Alto, CA.

Ji-Ho, C. H. O., Han, L. E. E., & Geuk, L. E. E. (2016). Intrusion Prevention Method on LKM (Loadable Kernel Module) Backdoor Attack. *DEStech Transactions on Engineering and Technology Research*, (icamm) p.65-64. doi: 10.12783/dtetr/icamm2016/7344

Jing, J. T. W., Yong, L. W., Divakaran, D. M., & Thing, V. L. (2017, November). Augmenting MulVAL with automated extraction of vulnerabilities descriptions. In *Region 10 Conference, TENCON 2017-2017 IEEE*, Penang, Malaysia. doi: 10.1109/tencon.2017.8227911

Joyner, R. L., Rouse, W. A., & Glatthorn, A. A. (2013). *Writing the winning thesis or dissertation: A step-by-step guide*. Thousand Oaks, CA: Corwin, Sage.

Khan, R., & Hasan, M. (2017). Network threats, attacks and security measures: A review. *International Journal*, *8*(8). doi: 10.26483/ijarcs.v8i8.4641

Karande, V., Bauman, E., Lin, Z., & Khan, L. (2017, April). Sgx-log: Securing system logs with sgx. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Abu Dhabi, UAE. doi: 10.1145/3052973.3053034

Keegan, N., Ji, S. Y., Chaudhary, A., Concolato, C., Yu, B., & Jeong, D. H. (2016). A survey of cloud-based network intrusion detection analysis. *Human-centric Computing and Information Sciences*, *6*(1), 19. doi: 10.1186/s13673-016-0076-z

Khaldi, A., Karoui, K., & Ghezala, H. B. (2014, January). *Framework to detect and repair distributed intrusions based on mobile agent in hybrid cloud.* In Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications, Athens. Retrieved from https://search.proquest.com/openview/3473e193878e868d2f6fad885fe256e3/1?pq-origsite=gscholar&cbl=1976343

Kim, H., & Feamster, N. (2013). Improving network management with software defined networking. *IEEE Communications Magazine, 51*(2), 114-119. doi: 10.1109/mcom.2013.6461195

Knowles, J. G., & Cole, A. L. (2008). *Handbook of the arts in qualitative research: Perspectives, methodologies, examples, and issues*. Thousand Oaks, CA: Sage.

Kotenko, I., & Ulanov, A. (2014). Agent-based simulation of DDOS attacks and defense mechanisms. *International Journal of Computing*, *4*(2), 113-123.

Krombholz, K., Mayer, W., Schmiedecker, M., & Weippl, E. (2017, August). "I Have No Idea What I am Doing"-On the Usability of Deploying HTTPS. In *Proc. of the 26th USENIX Security Symposium*, Vancouver, BC, Canada.

Krotsiani, M., & Spanoudakis, G. (2014, September). Continuous certification of non-repudiation in cloud storage services. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference*, Beijing, China. doi: 10.1109/trustcom.2014.122

Kührer, M., Rossow, C., & Holz, T. (2014, September). Paint it black: Evaluating the effectiveness of malware blacklists. In *International Workshop on Recent Advances in Intrusion Detection, 8688,* 1-21. Springer, Cham. doi: 10.1007/978-3-319-11379-1_1

Lam, W. M. W. (2016). Attack-prevention and damage-control investments in cybersecurity. *Information Economics and Policy*, *37*, 42-51. doi: 10.1016/j.infoecopol.2016.10.003

Lang, J., & Howell, E. (2017). *Researching UX: User Research*. VIC Australia: Sitepoint.

Langer, M., König, C. J., & Fitili, A. (2018). Information as a double-edged sword: The role of computer experience and information on applicant reactions towards novel technologies for personnel selection. *Computers in Human Behavior*, *81*, 19-30. doi: 10.1016/j.chb.2017.11.036

Laudon, K. C., & Laudon, J. P. (2016). *Management information system*. India: Pearson Education.

Lazar, J., Feng, J. H., & Hochheiser, H. (2017). *Research methods in human-computer interaction*. Cambridge, MA: Morgan Kaufmann.

Lee, I. G., Choi, H., Kim, Y., Shin, S., & Kim, M. (2014, September). Run Away If You Can: Persistent Jamming Attacks against Channel Hopping. In *Research in Attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden, September 17-19, 2014, Proceedings*(Vol. 8688, p. 362). Springer. doi: 10.1007/978-3-319-11379-1_18

Lee, J. (2017). Strategic risk analysis for information technology outsourcing in hospitals. *Information & Management*, *54*(8), 1049-1058. doi: 10.1016/j.im.2017.02.010

Lei, M., Yang, Y., Ma, N., Sun, H., Zhou, C., & Ma, M. (2018 Nov, 2017). *Dynamically enabled defense effectiveness evaluation of a home Internet based on vulnerability analysis and attack layer measurement.* Personal and Ubiquitous Computing, 22(1), 153-162. doi: 10.1007/s00779-017-1084-3

Levillain, O., Gourdin, B., & Debar, H. (2015, April). TLS record protocol: Security analysis and defense-in-depth countermeasures for HTTPS. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, Singapour, Singapore. doi: 10.1145/2714576.2714592

Li, H., Liu, Q., & Zhang, J. (2016). A survey of hardware Trojan threat and defense. *Integration, the VLSI journal*, *55*, 426-437. doi: 10.1016/j.vlsi.2016.01.004

Li, S., & Zhang, Q. (2015). Research of intrusion protection system using correlation policy. *International Conference on Matrials Engineering and Information Technology Applications (MEITA)*. doi:10.2991/meita-15.2015.117

Liu, G., Zhang, J., & Chen, G. (2014). An approach to finding the cost-effective immunization targets for information assurance. *Decision Support Systems, 67*, 40-52. doi: 10.1016/j.dss.2014.08.002

Longhofer, J., Floersch, J., & Hoy, J. (2012). *Qualitative methods for practice research*. New York, NY: Oxford University Press.

Lopez, J., & Wu, Y. (2015, May). *Information Security Practice and Experience*, 11th International Conference, ISPEC 2015, Beijing, China, May 5-8, 2015 Springer. Retrieved from https://doi.org/10.1007/978-3-319-17533-1

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193-273. doi: doi.org/10.1111/isj.12063

Mansfield-Devine, S. (2016). The death of defence in depth. *Computer Fraud & Security*, *2016*(6), 16-20. doi: 10.1016/s1361-3723(15)30048-8

Martin, J. A. (2017). Encryption Backdoors: A Discussion of Feasibility, Ethics, and the Future of Cryptography. *Honors Project,* p. 69. Retrieved from https://digitalcommons.spu.edu/honorsprojects/69

Mavroeidakos, T., Michalas, A., & Vergados, D. D. (2016, April). Security architecture based on defense in depth for Cloud Computing environment. In *Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference*, San Francisco, CA doi: 10.1109/infcomw.2016.7562097

Meng, Y. & Kwok, L. (2013). Enhancing intrusion detection systems using intelligent false alarm filter: Selecting the best machine learning algorithm. In *Architectures and Protocols for Secure Information Technology Infrastructures* (pp. 214-236). IGI Global. doi: 10.4018/978-1-4666-4514-1.ch008

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). Qualitative data analysis: A method sourcebook. Thousand Oaks, CA: Sage.

Miraglia, A., & Casenove, M. (2016). Fight fire with fire: the ultimate active defence. *Information & Computer Security, 24*(3), 288-296. doi: 10.1108/ics-01-2015-0004

Mollick, E. (2014). The dynamics of crowdfunding: An exploratory study. *Journal of business venturing*, *29*(1), 1-16. doi: 10.1016/j.jbusvent.2013.06.005

Moustafa, N., & Slay, J. (2015, November). UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *Military Communications and Information Systems Conference (MilCIS),* Canberra, ACT, Australia. IEEE. doi: 10.1109/milcis.2015.7348942

Myers, M. D., & Avison, D. (Eds.). (2002). *Qualitative research in information systems: a reader*. Thousand Oaks, CA: Sage.

Nagaonkar, A. R., & Kulkarni, U. L. (2016, March). Finding the malicious URLs using search engines. *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom),* (pp. 3692-3694). Retrieved from https://ieeexplore.ieee.org/document/7724951

Ngoqo, B., & Flowerday, S. V. (2015). Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users. *computers & security*, *53*, 132-142. doi: 10.1016/j.cose.2015.05.011

Nugraha, Y., Brown, I., & Sastrosubroto, A. S. (2016). An adaptive wideband delphi method to study state cyber-defence requirements. *IEEE Transactions on Emerging Topics in Computing*, *4*(1), 47-59. doi: 10.1109/tetc.2015.2389661

Nunnally, B., & Farkas, D. (2016). *UX Research: Practical Techniques for Designing Better Products*. Sebastopol, CA., O'Reilly Media, Inc.

Orojloo, H., & Azgomi, M. A. (2017). A method for evaluating the consequence propagation of security attacks in cyber–physical systems. *Future Generation Computer Systems, 67*, 57-71. doi: 10.1016/j.future.2016.07.016

Palys, T. (2008). Purposive sampling. In L. M. Given (Ed.) *The Sage encyclopedia of qualitative research methods*. (Vol.2). Los Angeles, Ca: Sage doi: 10.4135/9781412963909.n349

Pandeeswari, N., & Kumar, G. (2016). Anomaly detection system in cloud environment using fuzzy clustering based ANN. *Mobile Networks and Applications, 21*(3), 494-505. doi: 10.1007/s11036-015-0644-x

Pant, R., & Khairnar, C. N. (2014). A cumulative security metric for an information network. *International Journal of Application or Innovation in Engineering & Management (IJAIEM), 3*(4). Retrieved from http://www.ijaiem.org

Pappas, V., Polychronakis, M., & Keromytis, A. D. (2014, September). Dynamic reconstruction of relocation information for stripped binaries. In *International Workshop on Recent Advances in Intrusion Detection, 8688*, 68-87. Springer, Cham. doi: 10.1007/978-3-319-11379-1_4

Parameshwarappa, P., Chen, Z., & Gangopadhyay, A. (2018, January). Analyzing attack strategies against rule-based intrusion detection systems. In *Proceedings of the Workshop Program of the 19th International Conference on Distributed Computing and Networking* (p. 1). New York, NY: ACM doi: 10.1145/3170521.3170522

Paul, P., Bhuimali, A., Aithal, P. S., & Bhowmick, S. (2018). Business Information Sciences emphasizing Digital Marketing as an emerging field of Business & IT: A Study of Indian Private Universities. *IRA International Journal of Management & Social Sciences, 10*(2), 63-73 doi: 10.21013/jmss.v10.n2.p1

Paulsen, C., Toth, P. (2016) Small business information security: The fundamentals. *National Institute of Standards and Technology* National Institute of Standards and Technology, Report 7621 Revision 1. doi:10.6028/NIST.IR.7621r1

Pellé, S., & Reber, B. (2016). *From Ethical Review to Responsible Research and Innovation*. Hoboken, NJ: John Wiley & Sons.

Pierson, G., & DeHaan, J. (2015). *U.S. Patent No. 9,203,837*. Washington, DC: U.S. Patent and Trademark Office.

Poonia, A. S. (2014). Cyber Crime: Challenges and its Classification. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 3(6), 119-121* Retrieved from http://www.ijettcs.org

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & management, 51*(5), 551-567. doi: 10.2139/ssrn.2418233

Powers, J. (2015). *U.S. Patent No. 9,083,741*. Washington, DC: U.S. Patent and Trademark Office.

Purkait, S. (2015). Examining the effectiveness of phishing filters against DNS based phishing attacks. *Information & Computer Security*, *23*(3), 333-346. doi: 10.1108/ics-02-2013-0009

Rao, U. H., & Nayak, U. (2014). History of Computer Security. In *The InfoSec Handbook* (pp. 13-25). Apress, Berkeley, CA. doi: 10.1007/978-1-4302-6383-8_2

Ren, X., Blanton, R. D., & Tavares, V. G. (2016). A Learning-based Approach to Secure JTAG against Unseen Scan-based Attacks. *2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Pittsburgh, PA. doi: 10.1109/isvlsi.2016.107

Rocha Flores, W., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security*, *23*(2), 178-199. doi: 10.1108/ics-05-2014-0029

Rostami, M., Koushanfar, F., & Karri, R. (2014). A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, *102*(8), 1283-1295. doi: 10.1109/jproc.2014.2335155

Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: a comprehensive study. *International journal of computer networks and communications security*, *4*(6), 165-176. doi: 10.1109/icccf.2016.7740434

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78. doi: 10.1016/j.cose.2015.05.012

Santoro, D., Escudero-Andreu, G., Kyriakopoulos, K. G., Aparicio-Navarro, F. J., Parish, D. J., & Vadursi, M. (2017). A hybrid intrusion detection system for virtual jamming attacks on wireless networks. *Measurement*, *109*, 79-87. doi: 10.1016/j.measurement.2017.05.034

Saunders, C., Bygstad, B., Ferran, C., Liang, T. P., Recker, J., Brown, S. A., ... Sarker, S. (2017). Goals, Values, and Expectations of the AIS Family of Journals. *Journal of the Association for Information Systems*, *18*(9), 633-647. doi: 10.17705/1cais.04116

Schwandt, T. A. (2015). *The Sage dictionary of qualitative inquiry*. Los Angeles, CA: Sage.

Sethumadhavan, L., & Waksman, A. (2015). *U.S. Patent No. 9,037,895*. Washington, DC: U.S. Patent and Trademark Office.

Shahri, A. B., Ismail, Z., & Mohanna, S. (2016). The Impact of the Security Competency on "Self-Efficacy in Information Security" for Effective Health Information Security in Iran. *Journal of medical systems*, *40*(11), 241. doi: 10.1007/978-3-319-31307-8_6

Simon, M. K., & Goes, J. (2013). Assumptions, limitations, delimitations, and scope of the study. Retrieved from http://www.dissertationrecipes.com/

Singaravelan, S., Arun, R., Arunshunmugam, D., Joy, S. J. C., & Murugan, D. (2017). Inner Interruption Discovery and Defense System by using Data Mining. *Journal of King Saud University-Computer and Information Sciences*. doi: 10.1016/j.jksuci.2017.09.009

Smith, M., & Green, M. (2017). A Discussion of Surveillance Backdoors: Effectiveness, Collateral Damage, and Ethics. *International Security in the 21st Century:* 131-142 doi: 10.14220/9783737007627.131

Song, W., Choi, H., Kim, J., Kim, E., Kim, Y., & Kim, J. (2016, August). *PIkit: A New Kernel-Independent Processor-Interconnect Rootkit.* In USENIX Security Symposium, Austin, TX

Southekal, P. H. (2017). *Data for business performance: the Goal-Question-Metric (GQM) model to transform business data into an enterprise asset*. Basking Ridge, NJ: Technics Publications.

Sun, Z., Strang, K., & Firmin, S. (2017). Business analytics-based enterprise information systems. *Journal of Computer Information Systems*, *57*(2), 169-178. doi: 10.1080/08874417.2016.1183977

Surti, N. A., & Jinwala, D. C. (2015). Code Attestation Based Intrusion Detection System for Compression Attack in Wireless Sensor Networks. *Journal of Information Assurance & Security*, *10*(5). doi: 10.5120/21167-4234

Suuronen, J., & Bergenwall, M. (2016). *U.S. Patent No. 9,392,002*. Washington, DC: U.S. Patent and Trademark Office.

Taneja, S., Singh, V. V., & Arora, J. (2017). Role of Cloud computing in the Era of cyber security. *IITM Journal of Management and IT*, *8*(1), 71-74. Retrieved from http://www.indianjournals.com/ijor.aspx?target=ijor:iitmjmit&type=home

Tang, A., Sethumadhavan, S., & Stolfo, S. J. (2014, September). Unsupervised anomaly-based malware detection using hardware features. In *International Workshop on Recent Advances in Intrusion Detection*, Gothenburg, Sweden, *8688*, 109-129. Springer, Cham. doi: 10.1007/978-3-319-11379-1_6

Tehranipoor, M., Salmani, H., & Zhang, X. (2014). *Integrated circuit authentication*. Switzerland: Springer, Cham. doi: 10.1007/978-3-319-00816-5

Teo, W. T., Toh, T. K., & Chung, H. H. (2015). *U.S. Patent No. 9,112,897*. Washington, DC: U.S. Patent and Trademark Office.

Too, E. G., & Weaver, P. (2014). The management of project management: A conceptual framework for project governance. *International Journal of Project Management*, *32*(8), 1382-1394. doi: 10.1016/j.ijproman.2013.07.006

Trouw, A., Rangel, A., & Cable, J. (2018). *Security Risks and Mitigations.*San Diego, CA: XYO Network. Retrieved from http://docs.xyo.network/XYO-Red-Paper.pdf

Vasiu, I., & Vasiu, L. (2017). Backdoor Man: A Radiograph of Computer Source Code Theft Cases. *The Journal of High Technology Law Volume XVIII Number 1.* Retrieved from https://sites.suffolk.edu/jhtl/?s=Backdoor+Man%3A+A+Radiograph+of+Computer+Source+Code+Theft+

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. doi: 10.1016/j.cose.2013.04.004

Walters, R. (2014). Cyber attacks on US companies in 2014. *The Heritage Foundation*, *4289*, 1-5. Retrieved from http://www.heritage.org/research/reports/2014/10/cyber-attacks-on-us-companies-in-2014

Wang, B., Zheng, Y., Lou, W., & Hou, Y. T. (2015). DDoS attack protection in the era of cloud computing and software-defined networking. *Computer Networks*, *81*, 308-319. doi: 10.1016/j.comnet.2015.02.026

Wang, W., Liu, J., Pitsilis, G., & Zhang, X. (2016). Abstracting massive data for lightweight intrusion detection in computer networks. *Information Sciences*, *433*, 417-430 doi: 10.1016/j.ins.2016.10.023

Wang, X., Kohno, T., & Blakley, B. (2014, June). Polymorphism as a defense for automated attack of websites. In *International Conference on Applied Cryptography and Network Security*, Lausanne, Switzerland, *8479*, 513-530. Springer, Cham. doi: 10.1007/978-3-319-07536-5_30

Wang, Y., Anokhin, O., & Anderl, R. (2017). Concept and use case driven approach for mapping it security requirements on system assets and processes in industrie 4.0. *Procedia CIRP*, *63*(1), 207-212. doi: 10.1016/j.procir.2017.03.142

Watkins, L., Beck, S., Zook, J., Buczak, A., Chavis, J., Robinson, W. H., Mishra, S. (2017, January). Using semi-supervised machine learning to address the Big Data problem in DNS networks. *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV. doi: 10.1109/ccwc.2017.7868376

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, *44*, 1-15. doi: 10.1016/j.cose.2014.04.005

Wei, C., Shi, W., Qin, B., & Liang, B. (2015). Expanding an Operating System's Working Space with a New Mode to Support Trust Measurement. In *Information Security Practice and Experience*, *9065*, 18-32. doi: 10.1007/978-3-319-17533-1_2

White, G., Ekin, T., & Visinescu, L. (2017). Analysis of Protective Behavior and Security Incidents for Home Computers. *Journal of Computer Information Systems*, *57*(4), 353-363. doi: 10.1080/08874417.2016.1232991

Willis, J. W., Jost, M., & Nilakanta, R. (2007). *Foundations of qualitative research: Interpretive and critical approaches*. Thousand Oaks, CA: Sage.

Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems*, *33*(2), 597-620. doi: 10.1080/07421222.2016.1205934

Wu, S. P. J., Straub, D. W., & Liang, T. P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. *MIS Quarterly*, *39*(2), 497-518. doi: 10.25300/misq/2015/39.2.10

Wu, T. F., Ganesan, K., Hu, Y. A., Wong, H. S. P., Wong, S., & Mitra, S. (2016). Tpad: Hardware trojan prevention and detection for trusted integrated circuits. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *35*(4), 521-534. doi: 10.1109/tcad.2015.2474373

Xingguo, L., Qing, T., Zheng, Z., & Jiangxing, W. (2016). Mimic defense technology. *Strategic Study of Chinese Academy of Engineering*, *18*(6), 69-73. doi: 10.15302/j-sscae-2016.06.014

Yao, Z., Mu, Y., & Yang, G. (2016, November). A privacy preserving source verifiable encryption scheme. *International Conference on Information Security Practice and Experience*, Zhangjiajie, China, *10060*, 182-193. Springer, Cham. doi: 10.1007/978-3-319-49151-6_13

Yu, Y., Li, M., Li, X., Zhao, J. L., & Zhao, D. (2017). Effects of entrepreneurship and IT fashion on SMEs' transformation toward cloud service through mediation of trust. *Information & Management, 55*(2), 245-257. doi.org/10.1016/j.im.2017.07.001

Zhang, L. F., & Safavi-Naini, R. (2014, June). Verifiable multi-server private information retrieval. In *International Conference on Applied Cryptography and Network Security*, *8479*, 62-79. doi: 10.1007/978-3-319-07536-5_5

Zhu, C. (2015). Organisational culture and technology-enhanced innovation in higher education. *Technology, Pedagogy and Education, 24*(1), 65-79. doi: 10.1080/1475939x.2013.822414

APPENDIX A

Informed Consent

Title of Study: EXPLORING THE STRATEGIES NETWORK SECURITY MANAGERS NEED TO PROTECT THEIR NETWORKS FROM BACKDOOR INTRUSIONS

Investigator: Luis Rivera-Lopez

Contact Number: (786) 877-2289

Purpose of the Study

You are invited to participate in a research study. The purpose of this study is to explore the strategies network security managers need to protect their networks from backdoor intrusions.

Participants

You are being asked to participate in the study because your experience in network security strategies can add new perspectives and knowledge to the field of cybersecurity and information assurance. Your insights with respect to the research question are critical to enhance cybersecurity strategies needed in IT departments and help the parent business.

Procedures

If you volunteer to participate in this study, you will be asked to do the following: agree to make arrangements for an appointment for a face-to-face meeting and interview to review and sign the consent form and answer the interview questions. The process will take no more than an hour. An audio recorder will be used during the interview and some notes will also be taken.

Benefits of Participation

There may/may not be direct benefits to you as a participant in this study. However, we hope to learn from your knowledge and experience strategies network security managers need to protect their network from backdoor intrusions for the advancement of the information assurance and cybersecurity field.

Risks of Participation

There are risks involved in all research studies. This study is estimated to involve minimal risk. An example of this risk is feeling uncomfortable answering questions about your organization.

Cost/Compensation

This will be no financial cost to you to participate in this study. The study will take up to an hour for the interview process at a location chosen by you and at your convenience. You will not be compensated for your time. *Colorado Technical University will not provide compensation or free medical care for an unanticipated injury sustained as a result of participating in this research study.*

Contact Information

If you have any questions or concerns about the study, you may contact the investigator, Luis Rivera-Lopez (786) 877-2289, luis.riveralopez4@student.ctuonline.edu or the research supervisor, Dr. Debra Burrington (310) 592-0854, DBurrington@coloradotech.edu For questions regarding the rights of research subjects, any complaints or comments regarding the manner in which the study is being conducted, you may contact Colorado Technical University – Doctoral Programs at 719-598-0200.

Voluntary Participation

Your participation in this study is voluntary. You may refuse to participate in this study or in any part of this study. You may withdraw at any time without prejudice. You are encouraged to ask questions about this study at the beginning or at any time during the research study.

Confidentiality

Data collected such as recorded audio mp3 files and scanned handwritten notes will be stored in an encrypted flash drive using the Microsoft bitlocker function. Participants will not be identified by name in inerview transcripts. The handwritten notes will be destroyed inmediately after the study using an office schredder. The flash drive will be destroyed after the dissertation has been approved no later than October 2018.

Participant Consent

I have read the above information and agree to participate in this study. I am at least 18 years of age. A copy of this form has been given to me.

_____ _____

Signature of Participant Date

_____

Participant Name (Please Print)

APPENDIX B

Interview Questions

Research question: What are the strategies network security managers need to protect their networks from backdoor intrusions?

According to Miles et al., (2014), the research questions start working the conceptual framework explaining better the theoretical assumptions. The research interview question will test the knowledge of experienced IT managers and awareness of whether networks have been compromised due to stealth cyber-attacks, thus causing the computer systems to become vulnerable to backdoor intrusions.

Below are the interview questions for the purpose data collection process:

1. From your perspective as a manager of network security, what do you regard as the most effective two to three strategies for protecting a computer network?
2. What is your protocol for determining if an intrusion into the system has taken place? In other words, how do you know when you have an intruder?
3. In your role as a network manager what has been the level of support (for instance through staffing and funding) for you and your staff to be able to implement the most effective strategies?
4. When it becomes clear that the network has experienced a backdoor intrusion, what is the usual protocol or strategy that is employed to address the problem? (Probes: Does strategy vary depending upon the type of intrusion? In your experience what has been the level of success in implementing a strategy for addressing backdoor intrusions? How about a specific example?)

5. What are some of the biggest challenges you face as a network manager to ensure necessary funding for security strategies is maintained over time?
6. How does having the "right" kinds of staff members impact your ability to carry out an effective strategy for network protection?
7. What are your thoughts about the role of employees throughout the organization as part of the strategy of defending your network from backdoor intrusions?
8. The defense-in-depth strategy seems to be pretty widely accepted as the standard for network security. What is your perspective on the effectiveness of this strategy? (Probe: What are your thoughts about whether networks could be defended more effectively through a different strategy? What would a different approach look like?)
9. What other points would you like to make that we did not address during the interview that you think are key to an effective network security strategy?

Interview Protocol

1. Make participants aware that the purpose of the study is to explore the strategies network security managers need to protect their networks from backdoor intrusions.
2. Assure participant confidentiality and have the participant sign the informed consent agreement form. Ensure all participants are aware they can terminate the interview at any time and for any reason.
3. Address participant physical comfort concerns (lighting, room temperature, chair, and ambient noise distraction, make water available.
4. Record the number of the subject on the top of the interview field notes.
5. Encourage participants to open up about their experiences.
6. Monitor participant body language to minimize influencing subject answers.
7. Precisely record participant responses and annotate any non-verbal responses.
8. Audio record and assign a chronological number to each interview.
9. Ask interview questions in order and ask follow-on questions for clarification.

    Interview and follow-on questions:

    1. From your perspective as a manager of network security, what do you regard as the most effective two to three strategies for protecting a computer network?

        a. Follow-on question 1: From your perspective as a manager of network security, what is the most effective approach to protecting a network?
        b. Follow-on question 2: Please share an example?
        c. Follow-on question 3: Are other departments besides IT involved?

    2. What is your protocol for determining if an intrusion into the system has taken place? In other words, how do you know when you have an intruder?

a. Follow-on question 1: What steps are taken in your organization once an intrusion has been detected?
b. Follow-on question 2: Could you provide a bit more detail, please
c. Follow-on question 3: How have you seen this approach in practice?
d. Follow-on question 4: From your perspective as a manager of network security, what is the most effective approach to protecting a network?

3. In your role as a network manager what has been the level of support (for instance through staffing and funding) for you and your staff to be able to implement the most effective strategies?
    a. Follow-on Probing question 1: In other words, has it been relatively easy to get support for the strategies you feel are best? Or not so easy?
    b. Follow-on question 2: What are some of the biggest challenges you face as a network manager in obtaining necessary funding to maintain ongoing network security?
    c. Follow-on question 3: Are there tell-tale signs you can identify?
    d. Follow-on question 4: Could you elaborate on this a little?
4. When it becomes clear that the network has experienced a backdoor intrusion, what is the usual protocol or strategy that is employed to address the problem? (Probes: Does strategy vary depending upon the type of intrusion? In your experience what has been the level of success in implementing a strategy for addressing backdoor intrusions? How about a specific example?)
    a. Follow-on question 1: What is your assessment of whether security threats can ever be completely eliminated as opposed to reduced?

b. Follow-on question 2: How do you identify threats to the enterprise?

c. Follow-on question 3: Describe the process of selecting appropriate countermeasures?

d. Follow-on question 4: Do you have an example you could share?

5. What are some of the biggest challenges you face as a network manager to ensure necessary funding for security strategies is maintained over time?

    a. Follow-on question 1: What involvement do you have in hiring?

    b. Follow-on question 2: What is your role in the training of new staff?

6. How does having the "right" kinds of staff members impact your ability to carry out an effective strategy for network protection?

    a. Follow-on question 1: What difficulties, if any, do you have in ensuring you have the most skilled network security staff you can find?

    b. Follow-on question 2: How do you ensure that all employees in your organization are security-minded?

    c. Follow-on question 3: Could you clarify what you mean by _____?

    d. Follow-on question 4: What is the key to this strategy working?

7. What are your thoughts about the role of employees throughout the organization as part of the strategy of defending your network from backdoor intrusions?

    a. Follow-on question 1: What is your role in this process?

    b. Follow-on question 2: What is an example of employees exhibiting a culture of security-mindedness?

8. The defense-in-depth strategy seems to be pretty widely accepted as the standard for network security. What is your perspective on the effectiveness of this strategy?

(Probe: What are your thoughts about whether networks could be defended more effectively through a different strategy? What would a different approach look like?)

   a. Follow-on question 1: Does your organization have a comprehensive security strategy? If so, please describe it to me?
   b. Follow-on question 2: In your experience, what are the benefits and risks of using multiple layers of security tools for defending your network?
   c. Follow-on question 3: Where your network is concerned, what is the level of effectiveness of having multiple layers of security tools for defending your network against backdoor intrusions?
   d. Follow-on question 4: What is an example of a key benefit
   e. Follow-on question 5: What is an example of a key risk?

9. What other points would you like to make that we did not address during the interview that you think are key to an effective network security strategy?
   a. Follow-on question 1: Could you clarify what you mean by _____?
10. Thank each subject for his or her participation in the study at the end of the interview.
11. Inform participants that a transcript of their interview will be made available to them when transcription is complete, and ensure participants understand they will have a final opportunity to clarify or add to responses.(i.e. Can you tell me if this looks accurate to you?)

APPENDIX C

Letter of Permission to Use Site - Records Template

13 May 2018

Dear Luis Rivera-Lopez

Based on my review of your intended research, I grant permission for you to conduct your research entitled EXPLORING THE STRATEGIES NETWORK SECURITY MANAGERS NEED TO PROTECT THEIR NETWORKS FROM BACKDOOR INTRUSIONS within information technology departments within Volusia and Orange counties in the state of Florida. I authorize you to perform recruitment, data collection, member checking, and other necessary contact strategies to conduct the research. Individual participation will be voluntary and at their own discretion.

I understand our organization has the responsibility to include you to follow regulations and policies in accordance to the rules of the IRB board. We reserve the right to withdraw from the study at any time if our circumstances change.

I confirm that I am authorized to approve the research specified above in IT departments within the area of Volusia and Orange counties and the research plan does not violate our company policies.

I understand the collected data and/or records will remain strictly confidential and will not be provided to anyone besides the student and his supervising faculty/committee members without permission from Colorado Technical University Institutional Review Board.

Sincerely,

Authorizing Official Name, Title, and Signature

Contact Information