2020

Denial of Service Attacks: Difference in Rates, Duration, and Financial Damages and the Relationship Between Company Assets and Revenues

Abebe Gebreyes
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral dissertation by

Abebe Gebreyes

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Robert Haussmann, Committee Chairperson,
Applied Management and Decision Sciences Faculty

Dr. Kenneth Levitt, Committee Member,
Applied Management and Decision Sciences Faculty

Dr. Keri Heitner, University Reviewer
Applied Management and Decision Sciences Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Denial of Service Attacks: Difference in Rates, Duration, and Financial Damages and the Relationship Between Company Assets and Revenues

by

Abebe Gebreyes

MPhil, Walden University, 2020

MS, American University, 2003

MA, Howard University, 1996

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

October 2020

Abstract

Denial-of-service/distributed denial-of-service (DoS) attacks on network connectivity are a threat to businesses that academics and professionals have attempted to address through cyber-security practices. However, currently there are no metrics to determine how attackers target certain businesses. The purpose of this quantitative study was to address this problem by, first, determining differences among business sectors in rates and duration of attacks and financial damages from attacks and, second, examining relationship among assets and/or revenues and duration of attacks and financial damages. Cohen and Felson's routine activity theory and Cornish and Clarke's rational choice theory served as frameworks as they address the motivations and choices within criminal targeted attacks. Using the Kruskal-Wallis test and Spearman's correlation analysis, data, compiled from online database, on 100 U.S. businesses that were attacked in a 19-year period were analyzed. Kruskal-Wallis test indicated financial and informational sectors had higher attack rates; educational and informational sectors experienced longer attacks; and retail and informational sectors suffered greater financial damages. Results of Spearman's correlation showed that there was a significant negative relationship between duration and assets across all sectors but a significant positive relationship between duration and assets within the financial sector. A key recommendation is for cyber security professionals to better understand DoS attacks and to develop protections targeted business sectors. The implications of positive social change include the potential for security professionals to improve their security defenses from targeted attacks and trigger scholars to further research using the issues presented in the study.

Denial of Service Attacks: Difference in Rates, Duration, and Financial Damages and the Relationship Between Company Assets and Revenues

by

Abebe Gebreyes

MPhil, Walden University, 2020

MS, American University, 2003

MA, Howard University, 1996

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

October 2020

Dedication

First and foremost, I would like to give honor to my God (Elohim) almighty for giving me the never-ending perseverance and strength to deal with this strenuous process. This study is dedicated to my mother, Zenebech Wondim who encouraged me to get education. I would also like to honor, acknowledge, and dedicate this study to my family, Emaways Assefa, Abel, Ethael, and Bruk Abebe who endured my long journey for this doctoral research: I thank you for your support and patience with me during this protracted journey. I also thank my sister (Yeshi), brothers (Arega, Moges, Getachew, Teklu, Zewdu, Alemayehu) and relatives for their encouragement and assistance through this doctoral research process: you contributed everything in your power to make sure I had the proper resources I need to accomplish my dissertation. I could not have reached this point without all of you.

Acknowledgments

In this dissertation process, I would like to express my sincere appreciation and gratefulness to my chairperson, Dr. Robert Haussmann. Dr. Haussmann, I thank you enormously for your guidance throughout my long journey. I have learnt wisdom and vision from your immediate and valuable feedback to my research. I give thanks also to Dr. Ken Levitt my second committee member and methodology expert. Thank you for accepting my request during a difficult time. Thanks to all of you for ensuring that my dissertation met the University's rigorous requirements

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

Internet technology has grown from an academic curiosity into a means of communication, media distribution (Kende, 2014), knowledge warehousing, and business activities (Hunter, 2016). The Internet has become the medium through which denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks on businesses take place (Harris & Maymi, 2016; Lee, 2013). Since the late 1990s, the growth of complex DoS attacks on business sectors has corresponded directly with the growth of the Internet and its use within diverse services. DoS attacks targeted the availability of services, disrupted online access, disabled computer functions, and controlled computing systems remotely (Harris & Maymi, 2016).Growth in the number of Internet-enabled devices and Internet connectivity across businesses has led to an increase in DoS attacks (Harris & Maymi, 2016; Sood & Enbody, 2014). Protecting companies from targeted DoS attacks is a challenging task that requires diligence and ingenuity, as those who would attack Internet-connected systems continue to probe for vulnerabilities and devise new attacks (Somal & Virk, 2014).

DoS attacks have become the most common types of cyber-security attacks in business sectors (Conrad, Misenar, & Feldman, 2015). From 2000 to 2019, many companies faced repeated challenges to cyber-security from DoS attacks. DoS attacks deplete the availability of the targeted companies' computer systems, whereas a virus breaches the systems to search through sensitive data and interrupt normal computing operations. DoS attacks are harmful for companies' networks because they block services and prevent authorized users from controlling the system (Harris & Maymi, 2016).

By combining different components of DoS attacks, attackers invade a targeted company's computer systems. Some DoS assaults allow intruders to install malicious code onto the target's systems (Stewart, Chapple, & Gibson, 2015). By using multiple and differing vectors, attackers increase their chances of success. The more sophisticated the methods used by attackers, the greater their chances of bypassing cyber-security defense mechanisms.

Since 1990, the study of cyber-attacks has emerged as a crucial and developing area in the field of cyber-security. According to Mancuso, Strang, Funke, and Finomore (2014), cyber-security research is dominated by operational and attack perspectives. Operational perspectives focus on comprehending and expanding cyber-security protection. Research within the attack perspective typically focuses on attackers' principles. Some researchers suggested that operational perspectives dominate existing research. For example, according to Mulligan and Schneider (2011), most cyber-security researchers focused on technological (operational) ways to achieve security. Similarly, Jyothsna, Prasad, and Prasad (2011), Ballora, Giacobe, McNeese, and Hall (2012), and Langton and Baker (2013) argued that while cyber-security researchers gave attention to technical aspects, targeting attacks and attackers received little attention. Uma and Padmavathi (2013) highlighted the absence of a common understanding of various forms of cyber-attacks, features, and probable outcomes, suggesting a lack of focus on attack perspective research. Regardless of whether the operational perspective or attack perspective has received more attention, both have limitations as they do not examine the metrics of targeted DoS attacks.

Despite the abundance of literature on cyber-attacks, including research on targeted business sectors types, researchers have generally not examined the relationships among DoS attacks, assets, and revenues within specific business sectors (Shakarian, Shakarian, & Ruef, 2013). Although few scholars indicated additional research is needed (Harris & Maymi, 2016; Yadav & Gour, 2014), the claim of a research gap is supported in the literature review where the I describe the existing research on attack metrics in detail. I examined the differences among business sectors in attack rates, duration of attacks, and financial damages resulting from attacks as well as the relationship between company revenues and assets and the duration of attacks and resulting financial damages. The study involved compiling and analyzing archival data to identify whether these factors were part of candidate targeting metrics, thereby helping cyber-security professionals, practitioners, and researchers create higher-level protection and management of DoS attacks. The findings from this study on DoS attacks could enlighten security professionals, contribute to the advancement of cyber-security theory, and enrich the availability of empirical writings on cyber-security. The evolving nature of DoS attacks requires continuous vigilance for both large and small businesses (Harris & Maymi, 2016). Better understanding of the factors related to DoS attacks (including business sector types, assets, and revenues) produced information that could assist future research.

In Chapter 1, I present the background of the study, problem statement, purpose of the study, research questions and hypotheses. I also present the theoretical framework,

nature of the study, definitions, assumptions, scope and delimitations, limitations, significance of the study, and summary.

Background of the Study

Targeted computer systems attacks did not begin with the creation of Internet. Business sector security attacks started with wiretapping in the 1970s. Attacks on computer systems came later, as technology advanced (Moore, 2015). In the 1980s, the attacker 414 assaulted as many as 60 different computer systems for unlawful gains (Middleton, 2017). Cyber-security attacks of companies continued to increase throughout the 1980s (Yar, 2013). A trend of tapping into e-mail systems at both Digital Equipment Corp and MCI Communications Corporation emerged, and attackers stole $70 million by targeting the financial sector, including the National Bank of Chicago (Middleton, 2017). Following the rise in computer system attacks, another trend emerged: virtually injecting computers with viruses. By 1991, there were more than 1,000 known viruses in computer systems (Yar, 2006). The Melissa virus, which was spread through e-mail messages, triggered $500 million in financial damages. Targeted companies and organizations included AT&T, Griffith Air Force Base, National Aeronautics and Space Administration (NASA), and the Korean Atomic Research Institute. In the 1990s, attackers breached the computer security systems of the Department of Justice, Central Intelligence Agency (CIA), and Department of Defense (Hill & Marion, 2016).

After the 1990s, DoS attackers shifted their focus to attacking the websites of company sectors and institutions. A new form of cyber-security attacks surfaced. DoS attackers utilized Transmission Control (TCP), Internet Protocol (IP), and User Datagram

Protocol for launching attacks. Attackers launched DoS attacks from multiple sources (Stewart et al., 2015). The DoS attacks on cyber-security systems were serious in the 1990s, but the situation worsened in the 2000s when the Internet took center stage in technological development and advancement. Attackers coordinated a chain of DoS attacks against many e-commerce sites, including AOL, Yahoo!, Amazon, and eBay (Bosworth, Kabay, & Whyne, 2014). Cyber-attacks led to financial losses of $8 billion in the United States and an average of $1 trillion in cyber-related thefts occurred globally each year (Yar, 2006). In contrast, business sector attackers carried out attacks with low cost and with advanced technology (Harris & Maymi, 2016). Since 2000, DoS and its variant DDoS attacked availability of services on the Internet. Whereas a DoS attack uses a single computer and an Internet link to flood a targeted system with packets (unit of data), a DDoS attack involves using multiple computers and Internet connections (Bosworth & Kabay, 2002; Harris & Maymi, 2016).

In the 2000s, attackers refined their strategies to target companies by using zombie computers (a compromised computer connected to the Internet, used to forward transmissions to other computers) to mask the source of the attacks; as many as 37,000 attempted attacks occurred on the government and private companies (Radware, 2017). In the first quarter of 2009, McAfee researchers detected more than 12 million zombies (McAfee, 2009). In 2015, over 430 million new malware instances were detected (Symantec, 2015). In 2016, CryptoLocker ransomware attacks, which can find and encrypt files (see page 31 for a more complete definition and explanation of this kind of cyber-attack), were higher than 2015 and the types of ransomware increased by 752%

(TrendLabs, 2017). Examining and recording the amount of new malicious code samples each day is overwhelming.

Attackers with malware targeted the Epsilon system, made their way into the e-mail servers, and obtained the names and e-mails of thousands of clients (Bonner, 2012; Vijayan, 2011). Attackers accessed Lockheed Martin's files and stole information (Schwartz, 2011) and breached Target, JPMorgan, and Home Depot security defenses (Walters, 2014). Most businesses in the United States continue to fall victim to cyber-attacks with DoS. The CNN, Yahoo, and Amazon targeted attack rates were around 1 Gb per second (Harrison, 2000). In 2013, the DoS attack rate grew to 300 Gb per second (Kaur, Kumar, & Bhandari, 2017; Yu, 2014). In the fourth quarter of 2014, DoS attacks increased by 57% compared to 2013 (Brenner, 2015). The 2016 DoS attack brought down many Internet connections. The magnitude of attack was 1.2 Tbps (York, 2017). According to the Kaspersky report (2019), the number of DoS attacks mounted by 84%, with the major growth in the number of attacks lasting over 60 minutes. The average duration of attacks enlarged by 4.21 times. The size of attacks is larger than ever before. The conventional information technology security system offers little protection from cyber-criminals using advanced DoS and malware targeted methods to bypass security systems.

The sophistication and growth of cyber-security targeted attacks led scholars to examine the applicability of various cyber-security theories, including prevention, risk management (Salim, 2014), and general deterrents (Hassan, Reza, & Farkhad, 2015). These traditional approaches focused on the nature of attack prevention (Whitman &

Mattord, 2016) and have potential limitations. For cyber-crime, researchers (e.g., Holt & Bossler, 2014; Leukfeldt, 2014; Holt, 2017) increasingly used Cohen and Felson's (1979) routine activity theory (RAT); the theory is traditionally used to highlight crimes in relation to opportunity and action. Researchers also use rational choice theory (RCT) in cyber-crime research (e.g., Claude & Siponen, 2014; Exum & Layana, 2016; Homans, 1961; Hostettler, 2011). The theory derived from an economic principle designed by Cornish and Clarke (1987) and examines attackers' choices from a risk/benefit perspective in relation to gains and losses.

Problem Statement

The growth of Internet connectivity across the globe has led to an increase in DoS targeted attacks (Arora, Kumar, & Sachdeva, 2011; Harris & Maymi, 2016). Since 2000, in the United States, business sectors were targeted with DoS attacks at an increasing rate of occurrence and cost (Mahjabin, Xiao, Sun, & Jiang, 2017; Nakashima, 2014). Fighting cyber-attacks costs organizations over $100 billion annually (Nakashima, 2014), which is an unsustainable loss. Further, these attacks continue to threaten organizations with billions of dollars in damages (Singer & Friedman, 2014), also unsustainable.

Although DoS attacks have become the problem of the security of business sectors, researchers have focused on examining risks and problems of cyber-security (Andress & Winterfeld, 2014; Mulligan & Schneider, 2011). Understanding that cyber-security has continued to be an emergent area of study, Warkentin and Willison (2009) called for the addition of new lenses for criminological studies. Although researchers examined risks, cyber-security problems, and DoS attacks (Harris & Maymi, 2016;

Sanghvi & Dahiya, 2013; Sood & Enbody, 2014; Whitman & Mattord, 2016), at the time of this study, there were no published research papers that specifically addressed the differences among business sector types and rates, duration, and financial damages of DoS attacks nor the relationship between company assets and revenues and the duration of attacks and the financial damages due to attacks. Knowing the patterns among business sector types, company assets and revenues, and the rates and severity of attacks would help to address this research gap.

Existing research on the rates and severity of attacks across business sectors (such as Amoroso, 2011; Mahjabin et al., 2017; Tajalizadehkhoob, Asghari, Ganan, & van Eeten, 2014) does not focus solely on DoS attacks and has not examined rates and severity of attacks beyond a 3-year period (Tajalizadehkhoob et al., 2014), making a DoS-focused study that addresses a longer period especially necessary. Such knowledge could enable cyber-security professionals to identify targeted sectors and customize their approaches in cyber-defense. The general problem for businesses and cyber-security professionals is that the continuation of DoS targeting attacks damages business sector values financially. The specific problem is that cyber security professions currently clearly do not know the metrics that determine how attackers collectively target business sectors with DoS and have been unable to protect business from attacks.

To address this problem, I used quantitative methods to examine the differences among business sector types in attack rates, duration of attacks, and financial damages resulting from attacks as well as the relationship among company assets and revenues and duration of attacks and financial damages. The findings from this study, particularly the

findings on differences among business sector types in attack rates, duration of attacks, and financial damages, can provide security professionals with information they need to more effectively target their attention and spending.

Purpose of the Study

The purpose of this study was to examine the difference of attack rates, duration of attacks, and their resulting financial damages among business sectors over a 19-year period as well as the relationship among company revenues and assets and the duration of attacks and the relationship among company revenues and assets and the financial damages from attacks, also over a 19-year period. The results of the statistical analyses address the research gap and help scholars and cyber-security professionals identify the most likely targets of attacks, particularly those that are most damaging in terms of duration and financial loss. This study contributes to knowledge about risk factors for DoS attacks that could allow cyber security professionals to focus their efforts on organizations that are most likely to suffer a DoS attack and to provide possible suggestions for organizations to minimize their attractiveness as targets of DoS attacks.

Research Questions and Hypotheses

The research questions for this study were specific and formulated based upon reliable theoretical analysis. Designing research questions requires a combination of practicality and relevancy as the study needs to be testable, suitable for data collection, and likely to lead to a useful answer (Singleton & Straits, 2017). Newman and Covrig (2013) stated that research questions must be coherent with the purpose of study and problem statement. Further, although there is no single best approach to testing a

hypothesis, the research hypothesis should be measurable, suitable for intended study, and reflect different aspects (Singleton & Straits, 2017). The first three research questions (RQs 1, 2, and 3) and hypotheses (e.g., $H_0$1: null and H_a1: alternative) for this study deal with differences in DoS attacks among business sectors:

(RQ1): Between 2000–2019, were there significant differences among business sectors in the rate of DoS attacks?

($H_0$1): Between 2000–2019, there were no significant differences among business sectors in the rate of DoS attacks.

(H_a1): Between 2000–2019, there were significant differences among business sectors in the rate of DoS attacks.

RQ2: Between 2000–2019, were there significant differences among business sectors in the duration of DoS attacks?

$H_0$2: Between 2000–2019, there were no significant differences among business sectors in the duration of DoS attacks.

H_a2: Between 2000–2019, there were significant differences among business sectors in the duration of DoS attacks.

RQ3: Between 2000–2019, were there significant differences among business sectors in the financial damage per DoS attack?

$H_0$3: Between 2000–2019, there were no significant differences among business sectors in the financial damage per DoS attack.

H_a3: Between 2000–2019, there were significant differences among business sectors in the financial damage per DoS attack.

The remaining two research questions and hypotheses (e.g., $H_0$4: null and H_a4, H_b4: alternative) for this study deal with the relationship between company assets and revenues and attack duration and financial damages:

RQ4: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and duration of DoS attacks?

$H_0$4: Between 2000–2019, within sectors, there were no significant relationships between company assets and/or revenues and the duration of DoS attacks.

H_a4: Between 2000–2019, within sectors, there was a significant relationship between company assets and the duration of DoS attacks.

H_b4: Between 2000–2019, within sectors, there was a significant relationship between company revenues and the duration of DoS attacks.

RQ5: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and the financial damage resulting from DoS attacks?

$H_0$5: Between 2000–2019, within sectors, there were no significant relationships between company assets and/or revenues and the financial damage of DoS attacks.

H_a5: Between 2000–2019, within sectors, there was a significant relationship between company assets and the financial damage resulting from DoS attacks.

H_b5: Between 2000–2019, within sectors, there was a significant relationship between company revenues and the financial damage resulting from DoS attacks.

Theoretical Framework

A theoretical framework is the incorporation and fusion of thoughts that researchers distinguish to depict and explain a particular phenomenon (Imenda, 2014). I used RAT and RCT, and cyber-attack (DoS) theory developed by Yar (2005), Mandelcorn, Modarres, and Mosle (2013), Tajalizadehkhoob et al. (2014), and Reyns (2016) as the theoretical framework for this study. These researchers developed a theory to address the gap, limited depth, and absence of other cyber-attack or DoS attack theory. Given the similarity between cybercrime or attacks in businesses and social settings, the theories advanced in the criminology literature are appropriate for cyber-security research, specifically RAT and RCT.

I used this theoretical framework to examine the research problem in this study. This framework has been established as effective in cyber-crime research (Exum & Layana, 2016). Researchers use theoretical frameworks to introduce, depict, and illustrate the research problem and the significance of the intended practical approach for their study. In this study I used a combination of RAT designed by Cohen and Felson (1979) and RCT by Cornish and Clarke (1986), to address my assumption that DoS attackers are motivated by, and make decisions based on, an evaluation of gains and losses and the lack of security defenses. As cyber attacks are multifaceted and their sources are unlikely to be adequately described by a single theory, multiple theories can provide more effective insight than a single theory. I used RAT and RCT to provide knowledge about target attractiveness factors, which could help in developing future cyber-security approaches.

RAT has traditionally been used to analyze crime based on the premise of an attractive target and the opportunity for crime; RCT examines the rational decisions that comprise crime or attacks based on costs and benefits or risks and rewards. Combined, the use of RAT and RCT allows researchers to examine factors that might influence attackers' choices, particularly as they pertain to choosing targets. This section includes a brief synopsis of why RAT and RCT models are appropriate for analyzing DoS attacks on targeted companies. A more detailed explanation of the theoretical framework is provided in Chapter 2.

Routine Activity Theory

The RAT is a branch of crime theory that focuses on the conditions of crimes and the elements of crimes that occur. Cohen and Felson (1979), who developed RAT, argued that an attack or crime occurs at the convergence of a motivated attacker and an appropriate target that is in some way attractive or susceptible. This theory provides a macroperception of crime. Attacks are neither unintentional nor frivolous actions, and choosing suitable targets is a rational calculation (Cohen & Felson, 1979). The theory explains the convergence of motivated attackers with the goal of committing a crime against the target. The RAT is an appropriate framework for the study to explain cyber-attacks. The theory calls for analysis of the specific circumstances for crimes; in the terms of this study, an attack occurs when a motivated cyber-attacker and targeted business sector are present. In this study, I used RAT to examine the targeted business sector types, revenues, and assets, attack rates, durations of attacks and resulting financial damages.

RAT is an analytical method suited for use in real-life situations (Hollis, Felson, & Welsh, 2013). According to the theory, a potential attacker must be motivated to commit the cyber-crime. The target needs to be the right target from an attacker's perspective and lack effective guardianship, making it vulnerable enough to be a potential target. In practical testing of the theory, scholars indicated that it is a good fit in a variety of cyber-attacks (Downess, Rock, & McLaughlin, 2016; Felson & Boba, 2010). Researchers applied the theory to research on cyber-attacks in virtual spaces (Bolden & Nalla, 2014; Holt & Bosler, 2013; Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011). RAT is valuable for describing an attacker's rationale of scanning vulnerable targets to deny access using DoS. Further, using RAT as a framework provided an understanding of both suitable targets and lack of security.

Rational Choice Theory

While RAT can be a useful analytical tool for studying the factors that might predispose companies to a cyber-attack, the focus of RCT is choice and decisions pertaining to the actual crime (Cornish & Clarke, 1986, 2008). The theory includes an assumption that attackers premeditate their actions before they decide to commit an attack and that an attack or crime is purposive, intentional, and for the attacker's benefit (Clarke & Cornish, 2001). More specifically, attackers select their targeted sectors to fulfill financial or social status desires (Cornish & Clarke, 2008). When applying theories from other disciplines to cyber DoS attacks, it is important to seriously consider the context to refine the theory for the study setting. As such, I used RCT to study DoS attacks by focusing on the attacker perspective (attacker and choice of target).

Three main premises of RCT (agent, choice, and opportunity to take action) (Cameron & Kornhauser, 2015) were relevant to the current research project because they address the elements needed for a cyber-attack to occur in the business sector. The RCT first identifies the agent/attackers; specifically, it defines preferences of an attacker. Second, it distinguishes the set of choices accessible to the attacker. Third, it detects the situation in which the attacker acts (Cornish & Clarke, 1986). Further, Vance and Siponen (2012) expanded the RCT for their theoretical model and described that RCT can be a good fit for explaining intentional cyber-security crimes and target accessibility.

As a theoretical foundation, RCT can be used to explain targeting patterns in DoS attack rates, as it helps explain the targeting factors such as business sector types and values (assets and revenues) in relation to attack rates and duration, and financial damages of DoS attacks. Theoretically, businesses that are more attractive will experience higher rates, longer durations and greater losses, providing the ideal underpinnings for this research. I determined differences among business sectors in attack rates, duration of attacks, and financial damages resulting from attacks. I also examined the relationship between company assets and revenues and the duration of attacks as well as the financial damages resulting from attacks. RAT and RCT was used as the theoretical foundation for explaining the results in relation to target value attractiveness.

Nature of the Study

This quantitative study involved investigating DoS attacks in the United States from 2000 to 2019. Research projects fall into three categories: quantitative, qualitative, or mixed methods (Bryman & Bell, 2015). Quantitative methods measure variables and

statistically analyze numerical data; qualitative techniques identify and explore meanings and interpretations about particular phenomena, including human behaviors (Neuman, 2011); and mixed method examine various features of a phenomena (Long, 2014). The goal of this study is not to explore phenomenon to reveal meanings. Thus, neither a qualitative nor mixed method approach was appropriate.

Quantitative research applies numerical data to focus on particular research questions and answer research questions (Neuman, 2011), which was appropriate for this study, Quantitative descriptive design was applicable for this research in that I used numerical means to determine statistically significant differences between categorical variables and answer research questions 1-3. A quantitative correlational design was applicable to determine the degree of relationship between variables and answer research questions 4 and 5. This quantitative study was not designed to use control groups, the manipulation of predicted relationships between variables (Neuman, 2011), randomization, or manipulation to predict relationships between variables. This quantitative study is neither an experimental nor a quasi-experimental design; neither of those approaches were appropriate for this study because it was designed to analyze numerical, archival data utilizing computational data methods.

Based on Singleton and Straits' (2017) research approach, I used a systematic method to gather data on the following five business sectors: educational, financial, informational, insurance, and retail. I compiled the data for this study from the following archival databases: Computerworld, McAfee, Privacyrights.org, Idtheftcenter.org, Avtest.org, IC3, Federal Bureau of Investigation (FBI), U.S. Department of Justice, and

Department of Homeland Security reports, Department of Commerce, Library of Congress. Archival documents refer to existing data recorded or reported information that gives researchers valuable sources of measurement (Singleton & Straits, 2017).

When randomization and manipulation of independent variable is not possible, ex post facto design is suitable to examine the relationship between the dependent and independent variables (Ary, Jacobs, & Sorenen, 2010). Ex post facto is a type of nonexperimental research in which the researcher measures the statistical differences between variables with no way to control extraneous variables. Employing an ex post facto research design was necessary for this study because examining DoS attacks in real time, would have required collecting data over a very long time span in order to examine enough instances to draw conclusions. I examined differences among business sectors in attack rates, duration of attacks, and financial damages resulting from attacks, which required three the Kruskal-Wallis tests with sector as the independent variable and rate of attacks, duration of attacks, and financial damage resulting from attacks as the three dependent variables. Correlational research is a type of research in which the researcher measures the statistical relationship among variables. I examined the relationship between company assets and revenues and the duration of attacks and the relationship between company assets and revenues and the financial damages resulting from attacks, which required four Spearman correlations with assets and revenues as the independent variables and duration of attacks, and financial damage resulting from attacks as the three dependent variables. Data was analyzed using Statistical Packages of

the Social Sciences (SPSS) version 24, which includes Kruskal-Wallis tests and Spearman correlation analyses.

By examining the difference of attack rates, duration of attacks, and financial damages resulting from attacks among business sectors over a 19-year period as well as the relationship among company assets and revenues and the duration of attacks and the relationship among company assets and revenues and financial damages, the study was designed to respond to the problem of cyber security professionals not having adequate metrics to determine how attackers target businesses with DoS attacks. The findings from this study could enlighten security professionals, contribute to the advancement of cyber-security theory, and enrich the availability of empirical writings on cyber-security.

Definitions

Thorough knowledge of the terms and acronyms used in cyber-security research is crucial for understanding the topic. In the field of cyber-security, scholars and professionals used several terms to define and describe their activities. To sustain methodological accuracy, this section includes key definitions. The main terms for this study include the following.

Attack: An attack is a deliberate effort to launch an assault to exploit a weakness of a company's defense structure to bring destruction, failure, and disrupt normal traffic or to make normal network resource unavailable (Stewart et al., 2015).

Asset: An asset is everything of monetary value retained by a business that is grouped as capital/fixed, current, tangible or intangible and stated in terms of their cash value on financial accounts (The Farlex Financial Dictionary, 2017).

Business sectors: For this study, businesses are classified as falling into the following business sectors: educational, financial, informational, insurance, and retail sectors (Langager, 2019).

Breach: A breach is an act of breaking the defense system of organizations or penetrating the system by an attacker (Stewart et al., 2015).

Damage: Damage refers to a negative effect on the asset values by denying services and it includes both the tangible losses, lost revenue, and other types of damages (Palekiene, Bruneckiene, & Simanaviciene, 2014). For this study, I used total damages to a company measured by monetary value caused by DoS online business interruption. Damage was operationalized as the cost of an individual DoS attack. If there had been more than one attack on a given company, the duration was recorded as the average of the attacks on that company.

Denial-of-Service (DoS): A DoS is a malicious attack that denies an access of network connection of a company, making it inaccessible to its intended operators and cause the target system to crash, by transmitting a large number of packets from Internet protocol address (Soltanian & Amiri, 2016).

Distributed Denial-of-Service: Is a sophisticated version of DoS and dangerous Internet connection attacks with the capability to overwhelm a web server, thereby decelerating it down and possibly taking it down entirely (Jaafar, Abdullah, & Ismail, 2019).

Duration of DoS attack: Duration refers to the time, in hours and minutes that a DoS takes the system offline and the total legitimate traffic drop and that can be enough

to inflict damage at the target site (NSFOCUS, 2017). Duration was operationalized as the amount of time of an individual DoS attack, during which the system was offline. If there had been more than one attack on a given company, the duration was recorded as the average duration of the attacks on that company.

Hacking: Hacking is the "illegal intrusion into a computer system without the permission of the computer owner or user" (Vacca & Rudolph, 2011, p. 22).

Rate of DoS attacks: Rate was operationalized as the number of attacks on a given company (Zhenxin, 2014). For the purpose of this study, because it would be nearly impossible to come up with a credible total number of companies in the retail industry, the researcher examined the 100 companies (as measured by total workforce) in each of the five sectors and "rate" refers to the number attacks on each of those 100 companies in the time period under consideration.

Reconnaissance: Reconnaissance is the act of an unlawful attacker exploring to obtain as much information about the computer connection for further potential attacks (Agbogun & Ejiga, 2013).

Revenue: Revenue is the total amount of income that a given company generated from sale of goods and services during a specific period or the amount, in monetary units, received during in a given time (Carcello, 2008).

System compromise: Unlawful admittance to the computer structure or stored data (Stewart et al., 2015).

Vulnerability: A flaw in a computer system that provides easy access to compromise security system (Harris & Maymi, 2016).

Assumptions

One of the vital assumptions for this research is the accuracy of the archival data obtained on DoS attacks from Computerworld, McAfee, Privacyrights.org, Idtheftcenter.org, Avtest.org, Internet Crime Compliant Center (IC3), FBI, U.S. Department of Justice, U.S. Department of Homeland Security reports, and business values. The inquiry dataset for this study included data compiled from published reports and categorized by year, from 2000 to 2019. The quality of the dataset was dependent on the precision of coding. To ensure that the data was accurate, I included a quality management mechanism. Coding error detection techniques were in place to ensure the reduction of inaccuracies. Privacyrights.org, IC3, and FBI provide data considered by some researchers to be more precise and reliable than data gained by surveys, under the assumption that the data collected from business sectors only apply to DoS attacks. Another assumption, directly related to the theoretical framework of this study is that DoS attackers identify their targeted business sectors based on business factors.

Scope and Delimitations

The scope of this dissertation study is bounded by DoS attacks within selected business sectors in the United States over a 19-year period. The data were compiled from the databases listed above and company websites. I included only the five business sectors identified as having suffered DoS attacks and examined only external DoS attacks that directly interrupted networking. To answer the research questions, I compiled a dataset from archival reports on DoS attacks and company financial assets and values.

As delimitations denote prearranged constraints to manage data (Sampson et al., 2014), to be feasible this quantitative study required certain delimitations. The most important delimitation was that I only examined the 100 organizations in each sector. This resulted in examination of 500 organizations, 100 that had experienced DoS attacks and 400 that had not. Within the insurance sector, only two organizations had been attacked, which excluded this sector from some of the analyses. Because some sectors, such as retail, include thousands of organizations, many of them very small, it was impractical to randomly select organizations for inclusion in the study.

A second delimitation was that the study included only five business sectors and so generalizations could not be extended to other business sectors. Specifically, other types of malicious code attacks and techniques, such as Cross-site Script, Structural Query Language injection, phishing, sniffing, spoofing, eavesdropping, Data breach, and ransomware attacks were beyond the scope of this study. Further, because of the vastness of the topic, this study included a background paradigm limited to that which is useful to understanding the research questions. In this study, the potential issues of generalizability were properly addressed. To ensure generalizability, several facets of measurement error were isolated and eliminated.

Limitations

Limitations are weak points that a researcher cannot control and inappropriately influence the result of the study (Yin, 2014). Although this study deals with DoS attacks for a 19-year period, this does not include unsuccessful attempts at DoS attacks, it only deals with successful DoS attacks that disrupted systems and caused financial loss.

Businesses targeted with attempted DOS attacks do not always make their reports available to the public.

I employed ex post facto research, which is a type of nonexperimental research in which the researcher studies events that have already happened with no way to control extraneous variables. The study was also limited to the archival data of the business sectors with DoS attacks during 2000- 2019 in the United States. Another possible limitation of the study is that the data sources may not have contained information about all DoS attacks occurred in the U.S. There is a possibility that an important variable was missing. A final limitation is that this is an archival study, and so it looked backward at the relationships between the dependent and independent variables in the past (2000-2019). The continuing relationships was ultimately needed to be verified with data obtained from future DoS attacks.

Significance of the Study

While there is a large quantity of literature on cyber-attacks, this research adds to the literature by filling a gap in network and security management literature with regard to DoS targeted attacks analysis. The findings from this research are applicable to researchers, government agencies, and organizations. The study findings include information valuable to organizations, cyber-security professionals, practitioners, and researchers about DoS targeted attacks. I determined differences among business sectors in attack rates, duration of attacks, and financial damages resulting from attacks. I also examined the relationship between company assets and revenues and the duration of attacks as well as the relationship between company assets and the financial damages

resulting from attacks. This information could serve as a reference for industry practitioners and academic researchers in the field of cyber-security attacks. Addressing a research gap in a field that lacks a unified theory pertaining to cyber-attacks is useful in real-world applications. By increasing the specificity of the dependent variables beyond those used in previous studies, this study provides a clearer picture of attack rates, duration, and financial loss across business sector types and in relation to company variables, such as revenues and assets. This increased knowledge is a step toward successful development of holistic approaches to understand types of sectors likely to be targeted and to identify specific businesses within sectors that are more likely to be a victim of financial damages.

The findings from this study can inform business managers, information technology specialists as well as researchers at large. Studying DoS attacks helps build knowledge necessary for developing appropriate defense and reducing the risks of attacks. The study's significance extends further to expand identifying targeted business sectors and rates of attack per sector for 19 years. The relatively long time period for this study was chosen because DoS attacks are somewhat infrequent. With five business sectors, the 19-year period was necessary in order to have a base of 100 DoS attacks to examine.

Significance to Theory

The paradigms for this study were RAT and RCT, which are basic theoretical methods in criminology. These theories provided an appropriate framework for studying the DoS-targeted business sectors attacks as they can be used to examine factors related

to attackers, target attractiveness, and lack of guardians. I used the selected theories for this study to explain differences among business sectors in attack rates, duration of attacks, and financial damages resulting from attacks as well as the relationship between company assets and revenues and the duration of attacks and financial damages resulting from attacks. I used RAT and RCT to interpret findings concerning target attractiveness and rates of DoS attacks, duration of the attacks, and the financial damages resulting from these attacks. Previous RAT and RCT studies often focus on motivation in relation to gaining money, status, and benefits on targeted attacks. While all RAT and RCT propositions are essentially hypotheses themselves, only selecting the targeted industries and companies lends itself to more explicit and better testable hypotheses when employed in the context of DoS attacks.

While assets and revenues are both standard attractiveness factors, this researcher also considers whether these factors vary in significance by sector. I expanded the theories by considering other types of motivations on DoS targeted attacks and underlining the specificity of RCT and RAT in terms of cyber-security attack artifact in theory development. A new approach using RAT and RCT expands these theories to cyber-attacks so others can use them differently in the future.

Significance to Practice

Modern cyber-attackers are patient and remain in the system as long as they can without being noticed; these attacks differ from traditional crime activities where the offender would conduct the offense and disappear as soon as possible. In this case, the contemporary criminals follow procedures that are difficult to understand. The current

cyber-crime threat is persistent (Harris & Maymi, 2016). Applying theories to the changing nature of attacks provides practical knowledge.

I advanced practical awareness by investigating the cyber-attacks from the attacker's standpoint in relation to target attractiveness. The findings assist a cyber-security investigator in knowing what kinds of targets are likely to be perceived as suitable. Others could use these findings to prevent future cyber-crimes. Business leaders and information security specialists who manage cyber-security risks could use the findings from this research to identify targeted sector types and improve security practices. Business owners could utilize findings from this research to devise new approaches to handling strategic priorities related to DoS attacks building more effective layered defenses.

Significance to Social Change

This research study is important to various parts of society, particularly to cyber-security practitioners. The combined theories of RAT and RCT can be used to interpret findings in relation to targeted business sectors. This knowledge can assist cyber-security practitioners in reducing cyber-criminal activities, increasing company defense system control measures, and minimizing the likelihood of a cyber-attack happening. The information and knowledge obtained as an outcome of this research could improve information systems management's understanding of the risk of attack for targeted business sectors and holds the potential for positive social change through decreasing DoS attacks. This study is useful for security professionals to gain knowledge that could help them build their security defenses and reduce the likelihood of attacks.

Summary

DoS attacks are more complicated and threatening than previously thought. These attacks will increase in speed, diffusion, and power if action does not take place. The dynamism of these attacks continues to be the biggest threat to cyber-security in business, as it is almost impossible to know how to design an effective defense. Even though researchers studied DoS attacks incidents for years, no clear-cut solution has appeared.

Researchers and organizational leaders attempted to find ways to protect companies' cyber-infrastructure from DoS attacks. However, no line of defense emerged as entirely effective. It is important to understand differences among business sectors in attack rates, duration of attacks, and financial damages resulting from attacks as well as the relationship between company assets and revenues and the duration of attacks and the relationship between company assets and revenues and the financial damages resulting from attacks.

This chapter included a review of the threats posed by DoS attacks and several challenges faced by academics and cyber-security professionals looking to understand and mitigate these attacks. The chapter also included the research questions. Chapter 2 will include a comprehensive review of the literature surrounding DoS attacks and the theoretical frames. Chapter 3 will include the research design, data collection method, and strategy for data analysis. Chapter 4 will include the results of the analysis of DoS attacks and an interpretation of the statistical findings. Chapter 5 will include the rationale of this study and the interpretation of the outcomes. This final chapter will also

include implications for social change based on the study of DoS attacks in cyber-security and recommendations for future study.

Chapter 2: Literature Review

Introduction

My goal for this literature review is to describe the existing research on targeted business sector attacks with DoS. This review includes a comparison of the findings from previous DoS attack literature (including attackers) with specific attention to types of attacks, financial damages, and theoretical foundations. This chapter includes a discussion of DoS attacks and cyber-security in order to demonstrate a need for the current study and to show a connection to the problem statement and purpose presented in Chapter 1.

This review includes literature on business sector cyber-security attacks with DoS and background information on attacks, attackers, the attacking process, and cyber-security in general. I also include an outline of existing research on targeted attacks, the motivation of attacks, target attractiveness, targeted business sectors, and financial damages. Finally, I describe existing attack metrics. In this review, I explore all these components in terms of potential DoS attacks in targeting business sectors' values. A number of related topics about denial of service and data breach attacks are included. These topics contained network, computer, and vulnerability attacks and the nature of DoS and their attack systems. Pertinent literature on DoS, including categories, techniques, types, targets, and tools of attacks are reviewed and synthesized. I assess and compare the similarities and differences of researchers' approaches and offer an extended review of the two theoretical frames of this study: RAT and RCT. This subsection of the chapter includes information about the background of these theories, their key premises,

and their application to both cyber-crime and this study in particular. Finally, this chapter includes highlights of the benefit of using these theories in combination.

As researchers conduct literature reviews "to identify theories, and findings [and] gaps in knowledge in that research area" (Bhattacherjee, 2012, p. 21), this chapter includes a systematic investigation of theories, findings, and gaps in the literature on DoS attacks based on an evaluation of ideas promoted by Singleton and Straits (2017). These authors recommended using logic to review literature related to a research problem, the purpose of a study, and the research questions and to explore and analyze basic account information. The literature review also includes recent scholarly works that include the theoretical and methodological input.

As cyber-security has become a new field of study, finding theoretically and empirically advanced, well-researched, and unified literature on this research topic is challenging. The focus is on academic and peer-reviewed articles from various sources, with attention to taxonomies of DoS attacks. The theoretical background for this literature review includes recent literature pertinent to cyber-security attacks. I used the Library of Congress (books, peer-reviewed articles, journals, newspapers), local university libraries, and computerized databases and resources, such as EBSCO, ProQuest Dissertations, and the Google search engine to find applicable materials on the topic of DoS attacks. Key search terms were used *cyber-attack, DoS, data breach, information systems attacks*, *network security attacks, security incidents, routine activity theory, rational choice theory attackers,* and *targeted business sector.*

Cyber-Attacks

The developers of RAT), Cohen and Felson (1979), stated that attacks occur when there is an attacker and a target in the absence of security. But one question that arises when conducting research on targeting business sectors with DoS attacks is what an attack or cyber-attack entails. In general, a cyber-attack is an assault launched from a single computer or multiple computer systems against another computer system\ to disrupt communications or to gain data. In 2009, analysts at the National Research Council presented a description of attacks as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks" (p. 1). Kesan and Hayes (2012) attempted to offer insight into the legal issues related to attacks and found that researchers felt uneasy about expressing the differences between cyber-attacks, cyber-exploitation, or cyber-intrusion. Hathaway et al. (2012) defined a cyber-attack with DoS as an attack that encompasses any engagement to destabilize the operation of a communication system for a government or public protection principle. According to Uma and Padmavathi (2013), a cyber-attack is any technique used to disrupt the Internet communication or structure. Uma and Padmavathi's understanding of an attack included the breakdown of a computer defense network structure.

From a more technical point of view, Conrad et al. (2015) referred to an attack as an intentional act against computer components or a computer system that aims to destroy, deny access to, or degrade the system. An attack with DoS is a deliberate attempt to manipulate computer systems and networks (making these attacks well-suited to

analysis using the RCT and the result of the action may be cyber-crimes. Harris and Maymi (2016) focused on process when describing an attack as the deliberate act of tracking someone's movements without his or her authorization or knowledge that leads to a breach in the information system. The skills and technology employed in executing attacks are similar to those used in cyber-exploitation, yet the objectives of each action are different. Attacks result in dysfunction, as attackers try to render the computer system and networks untrustworthy and unavailable.

Attacks with DoS are asymmetric, stealthy, and evolving; an individual, group, or state located anywhere on the globe can deny access to, or breach, the computer system. According to Clarke and Knake (2010), attacks exist in a global system, and they can occur quickly at any time. Clarke and Knake stressed the ability of an attack to obliterate private and government computer infrastructures by providing examples of attack scenarios triggered by DoS. Although Clarke and Knake made some important points, it is difficult to confirm the credibility of their assertions or to know the source of an attack. The explanation for attacks is inadequate for real-world applications. Despite these limitations, scholars make similar arguments, including that no private or government cyber-infrastructure has protection from multifaceted attacks in the electronic era (Yu, 2014). Part of the complication of protecting against attacks can be tied to questions of responsibility. Sales (2013) noted that researchers had not sufficiently tackled the issue of cyber-security because "most scholars understand cyber-attacks as a problem of either the criminal law or the law of armed conflict" (p. 1503). The focus of most research is on attack behavior rather than the metrics and mechanism of cyber-attack target choices. An

attack can be separated into two forms or categories: an attack in which the aim is to impede the target computers or one in which the aim is to breach the systems to get information from the computer.

Type of Attacks

To understand how attackers target companies with DoS, it is necessary to classify the various types of attacks. Attacks on the cyber-security systems of organizations can take many different forms. This study involved examining DoS attacks, which form most attacks against businesses. To find a solution to computer and network insecurity, scholars proposed taxonomy systems for attacks.

Hansman and Hunt (2005) developed a taxonomy comprised of four computer attack dimensions. The first dimension deals with the attack vector or the path by which malicious code gets to its targets. The second dimension, attack target, indicates whether the attack is aimed at hardware or software targets. The third dimension consists of the type of vulnerability that attackers exploit. The final dimension is the attack payload, which refers to the risk or effect associated with the attack. Chabinsky (2010) examined the attack vector on its own and classified attacks into supply chain, remote access, and proximity access based on the type of access that the attackers use to gain unauthorized entry into a system or network.

Kjaerland (2005) classified attacks based on incident reports. The first category is the attack's source area, such as .com or .gov (Kjaerland, 2005). The second category is the techniques of the attack, such as a virus or DoS (Kjaerland, 2005). The third category is the impact that the attack has on the system, and the fourth is the services targeted by

the attack (Kjaerland, 2005). Harris and Maymi (2016) suggested adding Domain Name System cache poisoning to the list of the types of cyber-attacks because that type of attack interrupts a service and damages systems.

Researchers attempted to classify DoS security attacks on companies more precisely, including bandwidth flooding attacks, penetration attacks, cyber-infrastructure attacks, and electronic warfare attacks (Conrad et al., 2015; Harris & Maymi, 2016). Somal and Virk (2014) examined the history, trends, and strategies of a wide range of DoS attacks across and categorized these attacks by level of mechanization, the assault pace, and the attack impact. The study highlighted how DoS attacks became a complex and serious problem for businesses and identified various approaches proposed to counter them. Harris and Maymi (2016) and Conrad et al. (2015) also addressed the attacks that come from DoS, virus, and worm attacks. Because researchers do not use one common taxonomy to address business sector attacks, this study included the models that Harris and Maymi (2016) and Conrad et al. (2015) used to classify the different types of DoS attacks and other types of cyber attacks.

Malware Attacks

Like a DoS attack, a malware attack is a type of cyber-security attack against a company's values. Malicious software attacks involve attempts to identify targets' components and infect their systems. Both Harris and Maymi (2016) and Conrad et al. (2015) described malware as a generic term that comprises all types of harmful software, including computer viruses, worms, Trojan horses, spyware, logic bombs, key loggers, shareware, backdoors, botnet code, and root kits. Attackers can use various types of

malware viruses and worms to manage a system (Conrad et al., 2015; Harris & Maymi, 2016). The malware works by affecting the integrity of stored data or information, as well as the entire system (Conrad et al., 2015; Harris & Maymi, 2016). Malware attackers put destructive software into use to conduct activities that can harm electronic communication.

Unlike a DoS attack, malware resources can customize content delivery to a victim. The complexity of malware is increasing, and it can often access its target system without detection to gather information. According to Rajab, Zarfoss, Monrose, and Terzis (2006) and Pinguelo and Muller (2011), malware programs gather personal data, store and distribute illegal content, and attack computer and network systems. Beyond personal computers, malware programs can also attack and cripple infrastructures.

Cryptolocker

Cryptolocker is one of the most popular types of ransomware that launches attacks on business computer systems via spam messages, drive-by downloads, watering hole, and spear phishing (Jarvis, 2014; Stewart et al., 2015). Spammed messages come with attachments, which contain Cryptolocker malware. The malware installs into the computer through downloading the file attachments (Pathak, 2016). Upon launching an attack on a computer, every file and document in the infected computer becomes encrypted, blocking the normal user access. This is followed up with a message pop-up, detailing potential damage to the documents and files; the rightful computer owner has to pay a ransom in order to be issued the decryption key (Thakkar, 2014). Patil (2017) acknowledged that Cryptolocker, an active Trojan horse, was the initial cyber-attack that

used public-key encryption. According to Kansagra, Kumhar, and Jha (2016), Cryptolocker functions by integrating RSA-2048 and AES-256 encryption to lock files and documents of victims. The use of RSA-2048 encryption makes it a difficult for rightful computer users to obtain the RSA-2048 key as it takes approximately 6.4 quadrillion years to crack the key.

Cryptolocker attackers lock files and documents rather than focusing on system destruction. After inhibiting file access, the criminals then demand the users to pay a sum of money; failure to pay results in obliteration of the encryption key to permanently erase the user's data (Stewart et al., 2015). According to Patil (2017), the cyber-attackers withhold the decryption keys as they demand sum of money to be paid via MoneyPak or Bitcoin within the time limit, after which they assert to destroy the decryption keys. Pathak (2016) explained that Cryptolocker attackers, as other cyber-criminals, mainly target business organizations by launching attacks through spam e-mails. These e-mails are often sent as complaints by customers. Cryptolocker inhibits users from accessing the computer system unlike DoS, which blocks the networking system of the users. In the wake of increasing cyber-security threats, the business community is at risk of losing data that are the backbone of everyday business operations and organizational success. As such, information system specialists face the challenge of developing decryption keys to the encryption algorithm used by malwares such as Cryptolocker.

Denial-of-Services/Distributed Denial-of-Services Attack

DoS attacks are one kind of cyber-security attack used against business sectors. For several years, DoS attacks did not receive attention. However, the trend changed in 2011 as attackers began using DoS as one of their main attack methods (Kesan & Hayes, 2012; Patil & Kulkarni, 2011). By 2012, DoS attacks became a part of the cyber-security landscape. In 2017, 6.9 million attacks by DoS, which were not at all selective and cut across all sectors, were registered; in October of that year 22,622 attacks were registered per day (Whalen, 2017). The present study dealt only with the tiny fraction of those attempts that actually resulted in denial of service.

DoS attack operations have several vectors and often occur over an extended period. Their advanced and multifarious nature has produced security challenges for companies. Attackers use various methods to attack and gain control of computers. Traditional security devices such as firewalls, IDSs, and antivirus software programs are not effective in defending against DoS attacks that forward extra traffic to a network address (Harris & Maymi, 2016).

Harris and Maymi (2016) addressed some similarities and differences between DoS and DDoS. Whereas a DoS attack involves using a single computer and an Internet link to flood a server with packets, a DDoS attack involves using multiple computers and Internet connections, which makes it more difficult to deflect. Harris and Maymi noted that DDoS attacks send voluminous packets in large numbers to consume a larger part of the network's bandwidth. DoS attacks do not depend on an Internet protocol. The most widespread type of DoS attack is the packet flooding attack. Flooding attacks consume

the target resources by flooding the system with an overwhelming number of packets (Harris & Maymi, 2016). Arora et al. (2011) and Conrad et al. (2015) indicated that the common goal of DoS attacks is to use up the target system's availability to legitimate users. The danger of DoS attacks is higher in a DDoS attack because DDoS attacks include massive botnets (Imperva, 2012).

DoS attacks against companies' systems have become more complex. Anstee (2013) described escalating attacks over the years. These attacks occur at a speed greater than 10 and 20 gigabytes per second (Gbps), and they take place numerous times each day. Schwartz's (2013) description of the growth of DoS attacks aligned with Anstee's description: the average speed of attacks has increased from 6 Gbps to 48 Gbps, and 10% of all DoS attacks exceed 60 Gbps. The growth in number and severity of DoS attacks may result in financial damage to companies. Usually, DoS attackers focus on sending a flood of packets rather than breaching the privacy and integrity of the data (Kashyap & Jena, 2012).

Even though researchers agreed that DoS attacks involve the interruption of servers, they examined the nature of DoS in various ways. Mahjabin et al. (2017) discussed the different forms, strategies, and processes of DoS and examined architectures used in attacks, but it was Patel and Borisagar (2012) who designed the DoS taxonomy. Conrad et al. (2015) and Harris and Maymi (2016) reviewed functional mechanisms of DoS attacks. In a larger context, Yu (2014) provided an understanding of the emerging issues in the field of DoS attacks and information relating to how DoS attackers accomplish their mission.

Smurf Attack

The smurf attack is one common type of DoS attack against companies' network systems. Smurf attacks can prevent legitimate traffic by creating an overwhelming number of pings and resulting echoes directed toward the victim's IP address. According to Conrad et al. (2015), to perform a smurf attack, an attacker pings a directed broadcast address on the Internet with the address forged as being from the victim. The computer then becomes unresponsive due to the creation of high computer network traffic on the victim's network. Smurf attacks flood the target with Internet control message protocol (ICMP) echo packets. The spoofed network packet sent from the smurf program includes an ICMP ping. There are similarities between Harris and Maymi's (2016) and Conrad et al. (2015)'s research on the nature of smurf attacks. However, Harris and Maymi added the attacker, the victim, and the amplifying network to their research.

Fraggle Attack

Like the smurf attack, the fraggle attack is a type of flooding attack. Attackers of both types of attacks send packets to a network amplifier. However, fraggle attacks use user datagram protocol (UDP) echo packets instead of the ICMP echo used by the smurf attack (Conrad et al., 2015; Harris & Maymi, 2016). A fraggle attack is a DoS attack that works when attackers broadcast a spoofed UDP packet to the amplifying network, which responds by replying to the victim's system (Harris & Maymi, 2016).

SYN Flood Attack

Like smurf and fraggle attacks, synchronization (SYN) attacks involve flooding. A SYN flood attack depletes protocol data construction on the server side by sending a

constant stream of requests to the transfer control protocol (TCP) link from external hosts. In this manner, the servers must match resources to every new connection, thereby using all of its resources (Conrad et al., 2015). A SYN flooding attack involves constantly sending packets to each port on the server using a bogus IP address to exhaust the connection resources. In this situation, a hostile user may exploit a half-open connection and gain access to the target's server. Smurf, fraggle, and SYN flood attacks involve attempts to disable the target networks. In these attacks, the server loses or cannot process a real connection.

The Ping-of-Death Attack

The ping of death involves sending a malformed ping to a computer with an intent to attack the destination host server. Conrad et al. (2015) and Harris and Maymi (2016) provided similar descriptions of the nature of the ping-of-death attack. A typical server attack involves the flooding of ping traffic on a single server in such a way that the regular traffic fails to reach the target computer system (Conrad et al., 2015; Harris & Maymi, 2016). According to Stewart et al. (2015), sending a ping larger than the TCP/IP requirement packet size (65,535) could crush the destination server. The ICMP echo requests of a packet size greater than the standard IP packet size cripple the victim's server, and the victim cannot reassemble the packets. The ping-of-death attack is easy to implement using the ping application packaged with any operating system.

The Teardrop Attack

Teardrop attacks generally involve manipulating fragmented IP packages. According to Conrad et al. (2015) and Harris and Maymi (2016), teardrop attacks usually

exploit the overlapping fragment bug on computers with operating systems such as Windows NT and Windows 95. The bug causes the IP fragmentation assembly code to malfunction by failing to coordinate the overlapping IP fragments. Severe damage can occur because computer users fail to save their data in open applications. Teardrop attacks can crash the systems and there is a chance of losing unsaved data on the affected computer.

Launching DDoS Attacks

The complexity of attacks and the volume of traffic necessary to block and control a target system increased. The Mariposa and Kroxxu botnets are just two of the many hundreds of similar botnets, and the scale of similar botnets can run to 10s of millions of hosts. The Mariposa botnet, for instance, infected over 13 million computers (McMillan, 2010). In 2016, a massive flooded DoS attack occurred. A domain name service business was flooded by 1.2 Tbps of traffic, the most massive of DoS traffic ever documented (McAfee, 2017).

Alomari, Manickam, Gupta, Karuppayah, and Alfaris (2012) and Yu (2014) explained forms and launching techniques of DDoS attacks. The bandwidth depletion attack involves sending harmful traffic to a target's system to prevent the target from accessing the legal traffic. This type of attack can be categorized into amplification and flood attacks. Further, according to Malik (2016), the amplification assault includes sending the message to a broadcast IP address to cause harmful traffic resulting from messages being sent via broadcast in the target's system. As the harmful traffic increases, the target's bandwidth becomes low. The attackers send large floods of traffic to the

target's system bandwidth using robots (zombies) to cause congestion in the network and with the traffic of the IP. Because the bandwidth is saturated, the target's network becomes slow or crashes. Amplification attack is associated with an attacker or zombies sending packets to scattered IP addresses. These attacks cause all network systems on the subnet to be accessible by the multiple user IP locations to access packets to the target's network. Somal and Virk (2014) stated that the flooding attack increases unwanted network traffic that leads to a reduction in the victim system's bandwidth. User datagram protocol (UDP) and Internet control message protocol (ICMP) packets are used to launch this type of attack. In the UDP method of flood attack, a large number of packets are randomly sent to the target's network, and the system tries to respond to the packets as incoming requests. If the target's system is not running any applications on the port, a message of the port not being reachable is sent by ICMP packet.

Alomari et al. (2012) and Malik (2016) described that a resource attack is achieved through limiting the user's requirements to access the network. This type of attack is aimed at the core of a network where all processes are done. An attacker sends messages that include the guiding communications in a network. Requirements for usage in the network are shut down. In attacks in TCP SYN, the initiator of the attack is the one who sends instructions and directions to the user's system so that the requests by the user are not responded to. IP address packets consist of similar message sources and destinations of the recipient addresses. This type of attack leads to confusion in the victim's system, which can result in the system crashing.

DoS crushes the targeted system by sending packets to the system of the victim. DoS attacks are performed by using large volumes of traffic to deplete the bandwidth, OS, and computing power of victim systems. The quality of the victim system is degraded, which prevents legitimate clients from being able to access the system. The depletion attack is hard to control or manage compared to the bandwidth attack.

In order to launch DoS attacks, attackers need to set up attack network connection systems with compromised systems. To set up an attack network, DoS attackers use scanning tools to search unprotected computer systems or hosts on the Internet. Alomari et al. (2012), Yu (2014), and Stewart et al. (2015) explained how DoS attackers set up botnets (robot networks) to coordinate launching from botnets in compromised systems. The attacker launches bots, which are small scripts for performing automated functions to secondary targets that send other entities to the primary target. Before organizing a botnet, attackers access the potential targets using the Internet and run scripts to get into the compromised systems. The attackers then install harmful software to the target's computer using a virus, worm, attachments, and other methods. After installing the harmful software into compromised systems, the attacker uses the weakness of various layers of the network (i.e., SYN, UDP, and ICMP flooding) to make the system a secondary victim and use it as a robot in accessing the primary targets. The command and control server act as the headquarters of a botnet by communicating with the bots to update the attack order and tools. The control servers are set by the programmers to have intermediate nodes between them and the bots to maintain them. The messages in the communication of the control server and the bots are encrypted to encroach on the

network bandwidth and resources of the target, hence facilitating denial of legitimate access by clients to the servers hence no service.

A large volume of botnets will shut down the targeted systems. To make sure that all bots get into contact with their various call command and control servers, the relevant IP addresses of the central command centers must keep changing to prevent trace and detection for elimination. To remain undetected, attackers separate botnet activities to prevent them from being removed or detected. Techniques such as reflectors, IP tricking, code confusion, and memeory coding are used by attackers to make sure their bots survive. The masters or owners of botnets avoid detection and elimination by changing servers and IP of command and control while still maintaining the communication between the bots and the command and control servers (Yu, 2014).

Commonly Used Attack Tools

Attackers use common tools to perform DoS attacks. Radware (2013) provided information about attack tools used by attackers. Attackers use some of these tools to launch application layer, volume-based, and protocol DoS attacks.

Trinoo

Tripathi, Gupta, Almomani, Mishra, and Veluru (2013) referred to several resources that described how attackers use Trinoo to accomplish flooding attacks against a combination of several IP addresses. Trinoo commands the master and agent computers to send DoS flooding (see Figure 1). In such a scenario, DoS attackers use sizeable UDP packets to manipulate some ports on victims' computers, and attackers are able to access

information by using application vulnerabilities on the victims' computers (Radware, 2013).

Tribe Flood Network Tool

Behal and Kumar (2017) described the Tribe Flood Network (TFN) tool, which consists of a combination of computer programs that attackers use to execute smurf attacks, UDP floods, and ICMP floods. This set of computer programs uses master–slave architecture to manipulate random ports at the victims' computers. To execute a TFN attack, the TFN master station sends a command package to several TFN servers. On command, the sent signals generate a predefined DoS attack against the target systems (see Figure 1). Attackers can both randomize the source ports and hide the source IP address to make the DoS attack more widespread. To avoid detection, attackers vary the sizes of packets by using packet crafting tools like Loki to communicate to the master servers. The ICMP echo reply packets play a role in controlling TFN agents from a remote location.

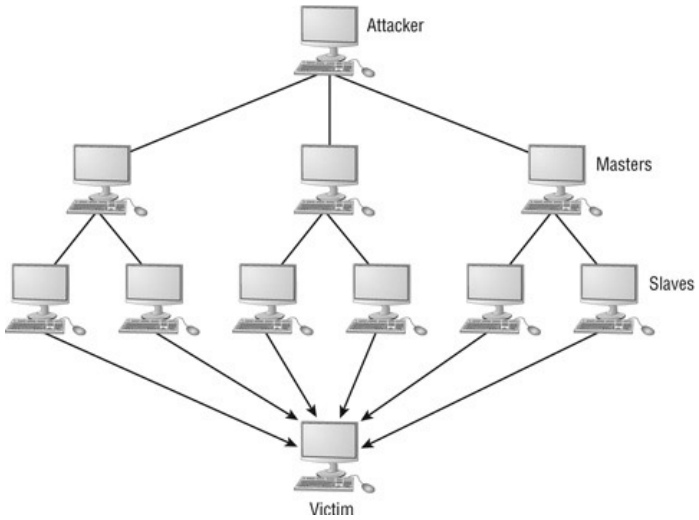

Figure 1. Master slave botnet attacks.

Somal and Virk (2014) indicated that the TFN 2000 has various techniques for overflowing in conjunction with other exploits to carry out DoS attacks. Hoque, Bhuyan, Baishya, Bhattacharyya, and Kalita (2014) described how the tool could operate in distributed mode by connecting various computer systems to the Internet for an attack on a single computer system. Due to its distributed mode of operation, the tool comprises two modules including a server and a client module. The user of the program must supply a password to initiate and terminate a TFN 2000 attack. Communication between the servers and the clients involves using ICMP echo reply packets. As a result, network users find it hard to detect the attack due to the absence of port numbers.

Stacheldraht Tool

In addition to the TFN tool, Behal and Kumar (2017) examined the Stacheldraht tool. Stacheldraht consists of a set of computer programs initially designed by Solaris and Lixus. This set of programs plays the role of a DoS agent. The DoS agent combines some elements of Trinoo with TFN. Stacheldraht can add some encryption between the attackers and the master. The tool can also add updates of the agent code to enhance the efficiency of attacks on the victim's computer systems. This tool enables source address IP spoofing and renewals (Radware, 2013). Stacheldraht executes several DoS attacks, including smurf attacks, UDP floods, TCP SYN floods, and ICMP floods. Stacheldraht can also use TCP to communicate between the master systems and the agents.

Shaft

Another advanced tool for DoS attack is Shaft. Shaft belongs in the same category as Trinoo and Stacheldraht. Behal and Kumar (2017) noted that the Shaft tool brings back

statistical information from agent to handler. Its DoS attack involves collecting statistical information from the victim machine (Radware, 2013). The tool has some additional elements, such as the capability to turn on master servers and master ports on the fly. Shaft consists of one or more shaft masters and several sets of shaft agents. The attacker uses the client to interact with the handlers. To achieve communication between handlers and agents, the attacker uses the unreliable IP protocol UDP. Switching master servers and master ports disrupts detection. Tenet connections from the attacker to the master provide better conditions for remote control. Attackers can incorporate passwords and tickets in the command codes to the agents *(*Dietrich, Long, & Dittrich, 2000).

Mstream

According to Hoque et al. (2014), Mstream acts as a classic point-to-point DoS attack tool. This program can affect users connected to a network with several agents. Attackers can use a password-protected interactive login to control the master servers remotely. Attackers can conceal their identity by setting up the program on both handler and agent systems. The Mstream tool also spoofs the source IP addresses and randomizes the client ports. The communication process occurs in TCP and UDP packets, which makes it hard to encrypt.

Trinity

Behal and Kumar (2017), Mohiuddin, Uddin, and Someswar (2014) described Trinity as a more sophisticated DoS tool for flooding attacks (UDP, TCP, IP fragment used to initiate a massive IP flood against several victims' computer systems). Trinity operates the same way as other DoS tools, such as TFN and Trinoo. Alomari et al. (2012)

claimed that Trinity has become one of the advanced Internet relay chat (IRC)-based DoS tools. Attackers can secretly control the hacked servers from a remote location with the help of the IRC channel. The chat feature hides the identity of the attacker and makes the attacker's operations undetected.

Attackers

Although the term *hacker* refers to all individuals and groups engaged in cyber-attacks with malicious code that target companies, categorizing all cyber-security attackers into a single group creates conceptual problems. Several investigators noted that hackers are not a homogeneous class (Harris & Maymi, 2016; Prasad, 2014). Calling a cyber-attacker a hacker can lead to confusion, vagueness, and misconceptions. Early in the conceptualization of cyber-attackers, Rogers (2001) noted that researchers should name groups of attackers for research to take place. Harris and Maymi (2016) claimed that subgroups of hackers join groups depending on what they want to achieve in their hacking attempts. Different types of attackers, including script kiddies, crackers, and hackers, can assault and target the values of companies. All three types of attackers are skillful in system identification, and engaging in such activities is illegal, as they obtain access to systems without the owners' knowledge (Harris & Maymi, 2016). Different groups of attackers might also end up attacking a single cyber-site or system at the same time but for different reasons.

Script Kiddies

In examining the script kiddies or attackers who focus on cyber-intrusions without destroying data or gaining system knowledge, Harris and Maymi (2016) explained that

this group is unsophisticated and unskillful in hacking, as they do not follow the normal guidelines for cyber-security attack activity. Professional hacking entails having knowledge, being skillful, and having the mindset of learning more about the system while pursuing the act of attacking. However, script kiddies are impatient in their use of malicious code. Their actions are quick, and they take many shortcuts, which results in superficial hacking. Conrad et al. (2015) claimed that script kiddies use the hacking guidelines established by professional hackers to launch their cyber-attacks; they do not establish their own. As much as script kiddies lack experience and are unknowledgeable, the damage they cause to a computer system is just as serious as the damage caused by other attackers. Rittinghouse and Hancock (2003) noted this group's tendency to use programs written by professional hackers to do their work. Script kiddies copy and paste codes used by others to gain access to systems (Lemos, 2000). Members of this group do not have their own ideas about breaching companies' security systems. They engage in cyber-attacks to show that they can do it successfully.

Crackers

Crackers are cyber-security attackers who target companies with DoS and malware. The attackers in this group obtain access to a company's computer system illegally with the motive to destroy, steal from, and introduce viruses into the system. Crackers target credit cards, files, and the computer systems to corrupt them (Harris & Maymi, 2016). People confused the terms *cracker* and *hacker*, as both groups of attackers use some of the same skills to access a computer system and cause destruction (Conrad et al., 2015). Raymond (1996) supported the idea of applying the term cracker to everyone

who engages in computer attacks illegally. In referring to the computer breaching criminal activity of crackers, Clifford (2011) noted that crackers only gain access to a system to cause malicious destruction of the system.

Hackers

Hackers use various methods to block cyber-security systems with DoS. According to Moore (2015), the terms *script kiddies* and *crackers* made it more complicated to understand the term hacker. The term hacker has lost a lot of its original meaning, which used to refer to someone knowledgeable about computer efficiency, creativity, and compact computer programming (Levy, 1984). Schell and Melnychuk (2011) noted that this positive meaning has been diluted because the hackers under the first definition enjoyed cognitive challenges. An association used to exist between hackers and the satisfaction they derived from exploring and overcoming intellectual barriers. Hackers need to show their skills as they go about gaining illegal access to computer systems. Harris and Maymi (2016) also tried to clarify this term and discovered that it fits into two categories of expert programmers: the black hats or illegal hackers and the white hats, or those associated with attacking a computer system in a planned manner.

Researchers in the field of cultural studies described the category of hackers. According to Wark (2004), early hackers created a class that was similar to the capitalists' class. The relevance of class analysis has withstood the test of dispute posited by Fuchs (2010), where most of the world's population depends on some type of wage earning activity to survive. Conversely, by examining the hacker culture, Coleman (2013) noted that hackers felt motivated by several driving forces. Most of their motives reflect a

commitment to “productive freedom” (p. 3) or to libertarian ideas. Kelty (2008) noted hackers’ ability to overturn preexisting concepts and established modes of representation. Hackers use various methods to flood the target network with information and breach security systems. To accomplish that feat, hackers commonly use clocking software to control logs, logger files, and stamps.

Script kiddies, crackers, and hackers are all cyber-security attackers who use malicious code, and they attack the same network or computer systems. To avoid confusion, just as Stewart et al. (2011) did, the researcher used the term *attackers* in this study to refer to the following three existing categories: script kiddies, crackers, and hackers. Members of these subgroups all use the same means to illegally block communication, gain access to a system, and preserve their access.

Attacking Process

Business sector attackers use techniques to reach their targets to perform DoS attacks. Harris and Maymi (2016) and Conrad et al. (2015) portrayed cyber-security attack phases to reach company values in various ways. Skoudis and Zeltser (2006) also categorized attack techniques. The stages of the cyber-security attacks with DoS often involve reconnaissance, scanning, and enumeration, in which the attackers try to seek as much information about the target’s system as possible. They search for this information using web browsers, employing tools to send packets to spot hosts, and detecting services run on the target computer of the company. The attackers’ next step is to gain access to the system. The final phase is to gain control of the machine to plunder information.

Reconnaissance

The initial phase of cyber-security attacking is reconnaissance. In an analogy to a traditional criminal attack, this stage is similar to walking into a crime site through the DNS tables and using nlookup to conduct domain zone transfers (Sanghvi & Dahiya, 2013). Liu and Cheng (2009) described manipulations of the host system's domain to gain Internet-accessible names. Disguised as common users, attackers search for domain names to look for information concerning the target network. These reconnaissance techniques provide preliminary information about the target structure to break into the system infrastructure. Reconnaissance includes intent reaching, social engineering, location mapping of systems, dumpster diving, domain name management, querying who is, and eavesdropping.

Researchers often described DoS attacks against companies using analogies similar to traditional crime methods (Sanghvi & Dahiya, 2013) because the attack procedure follows an organized process. Wiles, Gudaitis, Jabbusch, Rogers, and Lowther (2012) explained how advanced attackers have become in their approach, using sophisticated but unexpected methods to obtain access to victims' information systems. Sanghvi and Dahiya (2013) noted that active reconnaissance and passive reconnaissance are common in modern methods of attack. In active reconnaissance, the idea is to target the IP address, packet route, and ports using different technologies, including ping, trace route, and netcat. In contrast, the aim of passive reconnaissance is to intrude systems without the victim noticing the entry due to minimal correspondence with the target. The intention of passive reconnaissance is to avoid all forms of observation or traces of print,

and another term for the method is footprinting (Harris & Maymi, 2016). In the process of reconnaissance, attackers also try to gain general information about the organization in question. Attackers access the companies' profile for scanning the target security. Attackers use accumulated data for targeting an organization's security to reveal system vulnerability.

Scanning

After reconnaissance phases, attackers can use automated apparatuses to scan nodes and find open and active ports of the target. The scanning phase is a logical expansion of the active reconnaissance. By scanning, attackers can determine which services are operating on the chosen node. During this process, attackers can find targeted organizational firewalls, intrusion detections systems, routing, and networking typology. The scanning phase also includes war driving, ping sweeps, and war dialing to discover the system connections (Stewart, 2011).

Attackers developed remote attacks using DoS to target businesses. Harris and Maymi (2016) described remote hacking tools and the techniques that attackers use. As knowledge of the port used by a target is important in the success rate of an attack on a system, attackers employ strategies to scan targets' ports. Using these strategies, it becomes possible to connect to the target's system or port, such as port 21 (FTP) or port 80 (HTTP). Port scanning and operating system fingerprinting are two means of gaining access to victims' systems. Attackers used these techniques to overcome various forms of defenses. Sanghvi and Dahiya (2013) described some of the most common system tools (ie., Snort, Nmap, and TCP Dump) that attackers can use to collect data and make port

detections. Stewart et al. (2015) focused on Nmap scanning tools that are used to detect the existing state of each network port and IP protocols, as well as tools that make use of timing options, remote operating system detection, port filtering, and parallel scanning. By scanning ports, attackers gain access to aspects of the targeted system exposed to attack, and they identify those that they cannot attack. Researchers have not examined several new tools, including Wireshark, and attackers are developing new tools that create challenges for cyber-defense.

Wireshark is a software tool that can read the organization of various networking protocols. Security professionals used Wireshark for defensive mechanisms such as an IDS (Banerjee, Vashishtha, & Saxena, 2010). Others used it to seize the packets (TCP/UDP) from networks, whether wired or wireless. Wireshark acts as a wire sniffer and penetrates the operational scopes of various network protocols. Wireshark is able to access TCP streams of the network on which the system operates. It is a sniffer because it can read all the operational movements of a browser and determine all the processes taking place on the browser, which includes all forms of clear-text passwords that the browser may have. Orebaugh, Burke, Perce, Wright, and Morris (2007) noted that Wireshark's power stems from its ability to overpower data packets found on the network interface in which it operates.

Enumeration

Enumeration is the process of collecting information about targeted companies' systems by linking to the systems and managing queries. The enumeration phase includes performing tests to discover weaknesses and to create holes in a system. Once the link

has been established, the victim system could send notice of connection proof. The confirmation banner can comprise information about product name and version number of the facility. From a security service, hackers can obtain valuable data. In this phase, attackers identify operating systems and applications to mine information. Attackers can extract information about service from the systems, user names, computer systems, and network resources. Attackers make a link with targeted systems to execute command queries. The information provides possible attack steps. In the enumeration phase, several attack programs exist that allow unauthorized access (Harris & Maymi, 2016). Attackers enumerate the following: network sources, user names and groups, applications and banners, IP table, routing tables, simple network management protocol (SNMP), and DNS details. Enumeration is the process of uncovering vulnerabilities of targeted business sectors to perform successful attacks.

Attacking

Groundwork gives the attackers information on how to successfully attack the systems. If attackers successfully breach the systems, this process is ephemeral. If they do not successfully breach the systems, attackers modify the exploit, adjust payload, retune the vector, and relaunch system attack. Attackers perform virus attacks, password cracking, and other unauthorized processes on target systems to ensure systems function and respond in a manner that suits the attacker rather than the host (Harris & Maymi, 2016).

In an attacking phase, attackers can install malicious software to launch DoS attack. Conrad et al. (2015) and Harris and Maymi (2016) mentioned that after attackers

gain entry into a system through hacking, they can introduce all forms of malicious software to gain total control over the system. Attackers can gain access to files and programs on the system and try to use these in such a way that there is no trace of their activity. Attackers can also replace programs running on the host system with harmful applications, commonly Trojan horses and other malicious software. Although the IDSs frequently sense the modified system file, experienced attackers generally escape detection by concealing traces of their presence (Stewart, 2011).

DoS attackers achieve their success by using several attackers and controlled or breached computer systems as the basis to attack Internet traffic. DoS attacks make the business services unreachable for the service to be delivered.

Cyber-Security

DoS are agents that attackers use to attack business cyber-security systems. To understand the extant writing on cyber-security and DoS attacks, it is important to understand cyber-security in the field of cyber-security attacks. Despite the near ubiquitous use of the term cyber-security, there is no agreement on a precise conceptual understanding of the term. According to the Cyber Security Enhancement Act (2005), cyber-security is "the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (p. 3). The focus of this approach is on the protection, prevention, and restoration of a company's values. The National Institute of Standards and Technology (NIST, 2011)

described cyber-security as the skill to secure or guard the operation of Internet communication from attacks. Sheldon and McDonald (2012) viewed cyber-security as an appropriately installed software system that neutralizes cyber-security attacks with DoS or malware and employs secure measures to safeguard confidentiality, integrity, and availability. An advanced cyber-security software system or a defense tool is a technique that can be used to secure information and network systems from attackers using DoS. Cyber-security involves taking action to protect and safeguard a computer system against attacks.

A lack of consensus around the conceptual understanding of cyber-security could cause confusion. That confusion often leads to different cyber-security approaches and prevents nations from using common strategies to protect information systems. Despite this ambiguity, cyber-security is a body of different processes, practices, and technologies created to protect organizational computers, data, networks, and personal databases from DoS or malicious attackers. The function of cyber-security is to guarantee the confidentiality, integrity, and availability of data (Harris & Maymi, 2016) and to provide protection to computer-related components and software so that unauthorized personnel do not have access to stored data (Stewart et al., 2015).

Current State of Guardianship

Defensive or guardian systems used by businesses to prevent DoS attacks generally fall into three categories: firewalls, IDS, and antimalware programs.

Firewalls. A firewall is network protection mechanism that verifies the traffic going into and out of a network. It is a part of network security because of the functions

that it performs in a given network (Conrad et al., 2015). According to Harris and Maymi (2016), firewalls come in either software or hardware forms, and they are suitable for analyzing the data packets flowing into and out of networks. A firewall creates a permission forum that only allows approved programs to pass through the network. Harris and Maymi described the nature and functions of firewalls used to create secure and trusted networks.

The dynamic nature by which traffic-related network attacks take place makes it necessary for firewalls to have variable functionality. Depending upon the nature of the attack, a firewall may need to operate in different formats. Harris and Maymi (2016) described various types of firewalls. The first carries out filtering at the IP packet level, ensuring that attackers do not hack the IP address of the network under surveillance in the first place. A second type of firewall filter is at the TCP session level, and it ensures that even if the hacker succeeds in bypassing the IP, the TCP will be secure against further entry. The last kind of firewall filters are at the application level and clear all incoming programs to ensure the elimination of unsafe ones (Stewart et al., 2015). Even with these different types of firewalls, attackers continue to devise means of gaining entry. Such attackers send ICMP packets to overpower DoS defenses, virtual private networks, and web security, thereby blocking communication between a targeted system and its peers. Stewart et al. (2015) endorsed the need to ping vulnerable systems with ICMP Echo Request.

Sanghvi and Dahiya (2013) indicated several methods for detection that can also act as pre-attack mechanisms to stop port scanning from succeeding. However, attackers

are developing means to bypass firewall policies. Some of the new versions of attacks include e-mail-based Trojan horse attacks and stealth scanning techniques. Attackers who bypass firewall and virtual private network defenses have often been able to disable permitted protocols. Thus, they can use port scanning techniques to gain access to otherwise robust and secure network systems (Harris & Maymi, 2016). Firewalls cannot perfectly protect systems from breaches by attackers.

Intrusion detection systems. Unlike conventional firewall systems, which monitor network traffic, the aim of an IDS is to detect security penetration. Harris and Maymi (2016) and Kesan and Hayes (2012) considered an IDS to be an active detective defense tool that helps to determine whether attackers breached the system. Three conventional elements of IDS are a sensor that gathers traffic data, an analyzer that examines attempted or completed suspicious activity, and a user who forwards alerts to the security manager (Harris & Maymi, 2016; Kesan & Hayes, 2012). The interaction between the intruder malware and the IDS forms a game in which the virus tries to infect a system undetected while the IDS tries to alert networks to malicious activity.

Harris and Maymi (2016) and Conrad et al. (2015) described different types of IDSs. Network-based IDSs are software or hardware that monitor network traffic and examine packet payloads before they go to the target. Host-based IDS (HIDS) tools are installed on servers to detect malicious action, scrutinize systems data, and monitor changes. HIDS are used to identify abnormalities on the host systems that network-based IDS cannot detect. Rule-based IDSs are used to detect attack activities. Statistical IDSs are used for anomaly detection mode and to establish a learning manner to make a profile

of normal activity. These IDSs identify unusual activities, inspect trial files, and identify suspicious attempts by employing a blend of pattern matching and guidelines. A signature-based IDS compares data in packet headers to known attacks stored in a database. Signature IDSs have two weaknesses: comparing the large flow of traffic with every signature in the database and detecting new forms of attacks.

An IDS is a sophisticated auditing log and traffic monitoring tool that reveals many malicious actions. However, an IDS does not represent total protection of the system of a company from DoS attacks. Malware developers intensify their efforts to infect computer systems as a part of the game between the malware and the IDS.

Intrusion prevention systems. Intrusion detection systems have become powerful and sophisticated and often incorporate prevention mechanisms that changed cyber-security for businesses. Like Trost (2010), Harris and Maymi (2016) examined how IDS's and intrusion prevention systems (IPS) work in intrusion analysis. IPS can use these systems for attack analysis, damage mitigation, and attacker tracking. Much of the work done by Trost involves techniques and business drivers of intrusion detection and prevention and an assessment of the strengths and weaknesses associated with mainstream monitoring tools. The use of IPS technologies and attack graphs for mapping the path of network vulnerability serves as a means of achieving the proactive prevention of intrusion. According to Harris and Maymi, IPS is an extension of IDS and detects both traffic and activities. IPS's hinder detected invasions. Despite this breakthrough in new defense tools, no device prevents all DoS attacks; the game is ongoing.

Antimalware. Antimalware is the general term for programs that users employ to prevent, detect, and eliminate hazardous programs such as DoS malware bots or botnet, viruses, and worms (Harris & Maymi, 2016). Harris and Maymi (2016) also provided methods for defending against each type of attack. A botnet is a kind of malware that installs itself on many computers through infected e-mails, Trojan horses, and shared media. This type of virus uses to perform DoS attacks.

To identify various types of antimalware, signature detection is one of the most effective techniques (Harris & Maymi, 2016; Silnov, 2013). This technique evaluates the contents of the files stored in databases against identified malware signatures or code sequences. Antivirus software examines e-mails and files, compares them with the signatures, and stores them in the system's database. When they match, the antivirus software detects the viruses within the files. Although Silnov (2013) and Harris and Maymi (2016) agreed that this technique is effective; they also observed that it responds slowly to new attacks. To protect companies from DoS botnet malware attacks and overcome this weakness in the signature detection technique, information security practitioners and researchers introduced heuristic techniques (Harris & Maymi, 2016). Security professionals use heuristic techniques to scrutinize the structure of malware code, evaluate the instructions of the code, and assess the probability of malevolence. Heuristic techniques exhibit high performance, although they often have a high rate of false positives that result in flagging files that contain no malware. Although the false positive rate is high, heuristic software may have difficulty detecting newly developed malicious code (Kaspersky, 2013).

According to Harris and Maymi (2016), in contrast to the signature-based or heuristic scanning technique, behavior blocking software integrates itself into the operating system of the main (host) system and examines the entire system to prevent malicious activities. The system monitors and screens the interaction and compatibility of the malicious code with the system's operating system. When the behavior blocking software finds that the malicious code is about to affect the integrity of the system, it blocks and restricts the actions of the harmful codes. Continuous monitoring requires high levels of proficiency, as well as organizational and system resources.

Signature-based is not effective for safeguarding a company's systems with regard to identifying new malware. This performance is also a weakness of behavior blocking antimalware. Amro and Alkhalifah (2015) questioned why viruses spread and bypass antivirus defense software without detection. Attackers use more system-adaptable malicious code, and cyber-security breaches have become more complex and harder to detect. Antimalware installations scan and detect malware at networking access points but were ineffective for more complex malware designed to avoid this sort of detection (Harris & Maymi, 2016). Despite firewalls, IDSs, and antimalware, attackers attack organizational cyber-security systems successfully.

Guardianship Actions

Cyber-security defense involves a variety of different measures based on the type of attack. Several cyber-security defenders used a countermeasures model to protect their infrastructures from DoS attacks. The focus of defenses is on risk reduction through increasing effective cyber-security systems. There is often one corresponding

countermeasure for every available attack (Harris & Maymi, 2016). Countermeasures operate by detecting, preventing, and mitigating threats (Harris & Maymi, 2016); countermeasure should be able to cope with new technological innovation.

Passive versus active defense. Cyber-security systems use both passive and active techniques to counteract DoS attacks. These systems have several inadequacies with regard to protecting information. Kesan and Hayes (2012) studied passive systems in comparison to the level of threat that comes from modern cyber-security attackers found deficiencies in defensive capabilities versus cyber-attack capabilities. Active defenses are suitable because users can trace and actively respond to threats posed by an attack, in addition to targeting the attack itself. Kesan and Hayes noted that defense generally involves interrupting a pending attack and active defenses work via a mitigation process. The mechanism by which active defense operates on attacks is active threat neutralization, which includes offensive actions that neutralize threats but do not necessarily retaliate against the threats or attacks. Although this may sound convincing in terms of improving cyber-security, further research is necessary to verify the confidence levels of the trace-backs performed by the active defense to ensure their accuracy.

Detection. Detection is the most important measure in the incident reaction. In Conrad et al. (2015)'s assumptions, cyber-security experts use the detection phase to decide whether an event has occurred. This process involves identifying any security breaches that take place within a system as used in information security systems. When prevention fails in security systems, detection can fill the gap. According to Straub and Nance (1990), finding computer misuse involves three methods: unintentional finding,

finding in the course of internal system managements, and finding focused on revealing actions. Hoffer and Straub (1989) pointed out that most company security professionals do not carry out this form of detection. Consequently, the discovery of most cyber-attacks with malware is accidental or through normal system control.

Prevention. As a security measure, prevention refers to a means of not experiencing an attack with DoS. Prevention has several forms, including using guards, authentication devices, identifying traffic patterns, and firewalls (Harris & Maymi, 2016). Prevention ensures threats do not surface at all. Harris and Maymi (2016) and Conrad et al. (2015) stressed that prevention is a commonly used cyber-security system. Preventive efforts can be effective for cyber-security.

Problems for Guardianship

Attempts to have an all-in-one security solution to protect against Internet-based DoS attacks include several additional factors, including the nature of different institutions; diverse security needs across companies and departments; and the number of different applications commonly used by businesses, including e-mail, electronic commerce, and databases (Andress, 2011). The various current applications and systems posed a challenge for system administrators to secure the confidentiality, integrity, and availability of all services. Overarching security solutions make it difficult to protect companies' information systems in multiple application systems. When diverse computer systems lack a common approach to cyber-security, it becomes difficult to create a corresponding, all-in-one security solution (Harris & Maymi, 2016).

The diversity of computer platforms, operating systems, and architectures has inspired an equally diverse array of tactics, schemes, and strategies for disabling or compromising them from remote areas of the world (Stewart et al., 2015). Complicated types of cyber-attacks with DoS occurred at various levels and regions of the world against every kind of computer system in existence (Amoroso, 2011). In information systems with many diverse components, DoS attackers can block networks, inhibit access for businesses, and lurk in the system (Conrad et al., 2015).

Targeted Attacks

Targeted attacks pose several threats to the financial sector, as they jeopardize network accessibility, performance, and discretion. The attacks can also destroy the communication infrastructure through service sabotage and breaching of systems. Targeted attacks cause damage to their victims because of the care that attackers take in planning and execution (Adomi, 2011). Attackers launch attacks to break down the network's infrastructure to grant intruders easy and prolonged access to enhance data theft. The threat posed by targeted attacks is large (Villeneuve, 2011). According to Chapple and Seidl (2015), opportunistic attacks are less lethal than targeted attacks because the latter entails infiltrating a particular target with the primary intent to malign a firm's targeted business.

DoS attacks can target any business that uses a Website. According to the Trend Micro (2015) study, the following traits qualify an attack as being targeted: (a) foremost, the culprits bear in mind a particular potential victim, perform their background checks on the target and invest a substantial amount of energy towards developing the attack and

executing it; (b) a great volume of DoS attacks are ensured by the creation of botnets by the attack; and (c) the culprits spend a substantial amount of energy in actualizing the attack and carrying it out over and over again. A focused attack is, therefore, one where a particular company is targeted. Seeing as the actions and moves made by the attackers in a targeted attack are tweaked to accomplish the mission in particular, they are more harmful and cause more damage. Targeted attacks entail meticulous layout of strategy; they take place as soon as the attacker chooses; they focus on a particular target in order that they can attain their desired goal; and the attackers are able to knock the victims off using DoS as opposed to illegally acquiring information.

One of the largest forms of cyber-threats is the targeted attack, as was revealed in Trend Micro (2015) research in the contemporary Internet-linked world. All websites, online business servers or networks are prone to DoS attacks with a loss of reputation and monetary standing being considered the worst that a targeted corporation stands to lose. Some of the main reasons why targeted attacks are launched include control maintenance, unwarranted usage of systems, target infections, and collection of intelligence. According to Sood and Enbody (2014), when launched, a targeted attack is classified as one that is after a particular entity, be it a user, an organization or a company, in order that it can either gain access to its crucial assets or corrupt its networks.

O'Leary et al. (2017) argued that a targeted attack had to have a scope, an element of persistence, and effort, similar in terms of the nature of the targeted attacks and their characteristics. Scope, persistence, and level of effort were defined as follows: (a) scope: the attackers narrow down to a specific entity; (b) persistence: effort is made to

coordinate the activities being carried out in order that particular aims are realized as opposed to rushing the attack with the aim of bypassing the security threats in place; and (c) level of effort: A substantial amount of time, effort, and resources are applied in order to enact the attack. By stating characteristics of targeted attacks as being intentional, having a directive, and being tenacious, O'Leary et al. showed the importance of stratifying the different types of attacks according to whether they are targeted or not. There are high chances that an attack is targeted if it is identified as being aimed at a particular target or an assortment of targets with similar characteristics (for example companies in a common sector), leading to a conclusion that attacks that are targeted, to some extent, have an inclination toward monetary gain. Application of various styles and technology may be evident, and the attacker could apply different means as necessary to accomplish their mission.

Bendovschi, Al-Nemrat, and Ionescu (2016) gathered and studied numerical data of cyber-attacks collected by Verizon, a prominent company in the international security sector. The data included information about 4,785 attacks and the targets, the culprit, the weaknesses that made it possible for the ambush to occur, the consequence of the attack, and the approximate incurred damages. Their study led to a conclusion drawn by the National Cyber Security Center (2016) that attacks that were not targeted did not pose as critical a threat as those that were targeted, simply because by targeting, the attack is customized to inflict more damage as opposed to a stray attack. Unleashing of botnets is an example of an attack that is targeted.

With reference to the description of targeted attacks, several researchers (Bendovschi, 2015; Bendovschi et al., 2016; Whalen, 2017; Wueest, 2014) examined the relationship between business sectors and DoS attacks. However, this body of work does not give attention to, or include in their studies, the relationship between the rate of attacks and business sector or generated revenues and assets. Indeed, differences among business sectors in attack rates, duration of attacks, and financial damages resulting from attacks has not been examined in previous studies. Nor did they examine the relationships between company assets and revenues and the duration of attacks as well as the financial damages resulting from attacks. The criteria of targeted attacks (O'Leary et al., 2017; Trend Micro, 2015) can be considered relevant and significant to this study: having a specific target in mind, creating botnets to increase volume of DoS attacks, and focusing on specific organizations within an industry.

Motivation

The most apparent result of DoS attacks is unavailability of the service to the authentic customers; however, the objectives of the culprits are rarely clear and may vary significantly. Nonetheless, according to the lion's share of researchers, while causing damage to the victim is among the aims of DoS attacks, as is affluence within the hacker community, the main agenda is barricading the present resources, or performance degradation of the service needed by the machine that is targeted, to achieve material gain.

Sood and Enbody (2014) suggested that targeted attacks aim at corrupting business proceedings and are not solely for industrial espionage and monetary gain.

However, Semantic's (2015) indicated that the bulk of focused attacks in the financial sector are highly probable to be geared towards financial gain by the attackers. This research grouped attack motivation into three categories: financial motivation, espionage motivation, and political motivation. Exposure of banks to 'mass market' attacks was just as frequent as with other organizations making them, as well as other financial sectors, more susceptible to targeted attacks spanning IT security domains.

Regarding the motivation of DoS attacks Amoroso (2013), indicated that the need to demonstrate their prowess and achieve financial gains motivates attackers. In other words, hackers are motivated by the desire for fame and recognition. Supporting these findings, Prasad, Reddy, and Rao (2014) noted that financial gain, reputation, philosophical belief, and retaliation are the key drivers. Further, Madarie (2017) noticed that attackers want to demonstrate their ability to overcome hurdles using creativity and innovative computer skills. Sociocultural and political gain are two motivations that are beyond the scope of this study. Security experts found several reasons for cyber-intrusions, including theft of data and money, disruption of network functioning, blackmail, and economic sabotage (Lawrence et al., 2017). Regardless of the driving force behind them, new DoS attacks target companies' networks on a regular basis. However, researchers have not located any common factors that influence the targeting of companies and their holdings.

For many researchers, the leading indicators for attacks remain perplexing, particularly because the main aims of DoS attacks often remain unknown, despite the attacker's claims of responsibility (Shakarian et al., 2013). For example, according to *The*

Economist (2014), the motivation for targeting the financial sector remains unknown. Several theories emerged to explain the attacks, including hackers employed by nation states to retaliate against laws or to acquire critical data. Some network hacking could be the result of foreign countries colluding with individuals to obtain financial information. Notably, theft of data for monetary gains has emerged as a driving factor behind network attacks. Various business sectors were victims of financially targeted attacks.

Looking at attacks in the context of targeting company assets and other holdings produces a more useful picture. Van Beveren and Falkinder (2005) explained that malware often exists to make a financial profit or otherwise exploit lucrative situations. Harris and Maymi (2016) noted the financial motive as well, but they also indicated that attackers use DoS to inflict chaos, which can range from being beneficial to the hackers to being destructive. Hackers target a range of assets, from individual users to government institutions and multinational corporations.

The frequency of cyber-attacks with DoS varies between different sectors and companies within each sector. This variation could be due to differences in asset and revenue values. One of the limitations of previous studies is that they were not longitudinal. They rested on short-term reports and case studies rather than examining a company's assets and revenues over decades. Further, the scholars could not identify whether financial profiles, fame or reputation, or other cultural situations serve as motivations for DoS attacks. Researchers have not studied DoS attacks targeting companies based on their sector types, assets or revenues.

Targeted Business Sectors

Because there are several avenues to attack company computer systems, there are many motivations to attack. Although the motivations behind DoS attacks against targets are not known, certain business sectors seem to be vulnerable. From 2009 to 2013, cyber-infiltration in the healthcare and insurance sectors increased. McGee (2014) noted that healthcare-related companies are vulnerable to attackers because of the sensitive information on their networks. In their cyber-attack study, Sood and Enbody (2014) claimed that insurance firms became targets for cyber-attacks. Unauthorized intrusions expose medical firms to blackmail risks because patient information (i.e., identifying details, medical records, and financial status) may enter the public domain.

The Identity Theft Resource Center (2014) reported that the financial, insurance, education, and business sectors are the most attractive for targeted cyber-attacks. Akamai (2015) reported the gaming industry as being the most widely attacked by DoS threats as compared to any other sector during the Q1 of 2015 and in the same manner, as from Q2 of 2014.

On the other hand, Rivalhost Managed Web Hosting (2013) identified the finance sector as the most targeted. Verisign (2014) reported that in the second quarter of 2014, media represented 43% of all targeted attacks, closely followed by IT services at 41% of the attacks. Verisign also reported telecommunication service, institutions of finance, and the public sector as targeted sectors. Akamai (2015) indicated that the gaming sector, software, and media were the most threatened sectors by the DoS flood attacks. Yadav and Gour (2014) identified web-based business (financial services, retail, travel) as the

main targeted sector. They also stated that no field is spared from DoS threats. Clearly, there is no consensus among researchers on the most commonly targeted sectors types.

In addition to examining the most targeted business industries, researchers also examined the industries most threatened by DoS attacks in terms of what they stand to lose. On the Internet hosting provider DoS attacks, Rivalhost Managed Web Hosting's (2013) study indicated that one of the highest rated victims of DoS attacks being Internet service providers with such attacks being complicated and set on precise websites leading to a spread in the network causing its impacts to be felt by different customers. As a result, sites that deal in Ecommerce are in a position to lose much more from such attacks. The researchers found that the DoS attacks continues to be a problem for businesses large and small. Similarly, Yadav and Gour (2014) reported that the industries most threatened by DoS were those dealing in web-based transactions, the likes of telecom services, financial services, travel, retail, and IT. Wueest (2014) identified the energy sector as a field with great risk as attacks would result in catastrophic disorder and a chain of effects whose eventuality would be monetary loss.

Over the 3 years of Bendovschi's (2015) study of patterns and trends in cybercrime, a compelling relationship was established between the kinds of industries in question and the kinds of threats experienced, which led to the conclusion that cyber-crime was a menace to all types of business regardless of the public domain being the most sought-after target. Specifically, Bendovschi showed that most sectors are targeted with DoS attacks and identified DoS as being the threat most frequent type of attack from the array of the many in existence. Cyber-attacks became a threat to all sector scales

(private companies, Internet and online services, retail education, online services, finance, not-for-profit organizations). Those conducting the attacks are primarily targeting information that could be of value. Their aim is to gain access to information with the capability of earning either them or the associated sponsors great benefits. Through the process of reviewing Verizon's data, Bendovschi et al. (2016) revealed that they could identify relationships between the attacks carried out.

Financial Damages

On the consequence of financial damage with DoS attacks, Anderson et al. (2013) classified damage or loss into direct and indirect damages. The line of reasoning was the direct loses comprise of infrastructural downtime, loss of online traffic, paid ransom and customer compensation among others while indirect damage is when the reputation or the stock price is damaged. An unavailability of networking access for users can result in financial loss for targeted business sectors. In addition to financial loss, the consequences of DoS attacks can embrace brand and reputation damage, loss if investor confidence, and violation of service agreement.

Though attacks that deny computer access result in financial loss in the business sector, Pau (2013) asserted that there is minimal body of evidence on assessment of damage. According to his study, companies are unable to approximate the kind of loss they incur when their systems are infiltrated whether successfully or unsuccessfully. He thus proposed that it is imperative to take into consideration the relationship of other targets and the bodies affected by the targeted system and its related bodies and how an infiltration affects the sustainability of the entire organization. Considering finance and

economics, a critical question is on the allocation of assets when aiming at some performance goals.

Anderson et al. (2012) focused on different business organizations such as online retailers, business to business hubs, online marketplaces, Internet-based advertisers, streaming media services, and Internet commerce business. These kinds of organizations incur direct forms of revenue loss from any form of disruption whether the infiltration is successful or unsuccessful. A common feature within these organizations is that the mode of receiving revenue is in minutes or even seconds. Profits cannot be attained when there is a disruption or can be reduced in the course of a disruption (Anderson et al., 2013). Previous researchers did not focus on revenues and assets, but the research that focuses on business sector attractiveness and targets, damages, and sector types are valuable support to this research project.

Business Values

As businesses or industries are categorized according to the type of their economic activities, assets and revenues are fundamental elements of business sectors. Assets are resources with economic value that the business owns and that are recorded in companies' balance sheets (Siegel, Dauber, & Shim, 2005). Assets represent the value of a sector or possession that can be transformed into cash. Assets can be largely classified into current, fixed, financial investment, and intangible assets. Current assets are short-term economic resources that can be changed into cash within a year period; Current assets include cash, accounts receivable, and other resources. Compared to current assets, fixed assets are long-term sources that include plant, equipment, and

buildings (CFI, 2018). According to Bragg (2017), fixed assets are items that generate economic benefits over a long period of time. However, accounting for fixed assets is not uniform throughout the world. Financial assets represent investments, such as banks, stocks, and bonds, whose values derive from contractual claim of what they represent. Further, intangible assets are economic resources that have no tangible presence, including patent, trademark, intellectual property, and copyright. Reilly and Schweihs (2014) stated that intangible assets' value comes from the ability to exploit the legal rights related to the asset. Assets are recorded in reports, such as those compiled by Forbes. As an example, according to the most recent Forbes (2018) report, JPMorgan Chase has $2,609.8 billion assets and Amazon has $131.3 B. Prudential was the largest insurance business sector in the United States with assets amounting $596 billion (Statista, 2017).

Revenues are the income that a business sector received from its business activity (Bondarenko, 2014). Most revenue comes from sales of goods or services, as such revenue is also referred to as sales or turnover. Revenue depends upon business activities, for some businesses, interest royalties or other types of fees are revenues (Carcello, 2008). For several businesses, such as manufacturing, retail, or grocery, revenues come from the sale of goods. Service businesses receive most of their revenue from rendering services. Banks receive revenue from fees and interest generated by lending assets. In general, revenue is the amount of income a business sector is generating from sales of products or services. The more revenue a sector generates, the more money the sector owns. In 2016, 500 United States businesses generated $12 trillion in combined revenue.

In addition, the social media sector has rapidly increased its revenues by 44% in 2015 compared to its 2014 revenues (Frohlich & Comen, 2016).

In relation to this study, Leukfeldt and Yar (2016) noticed that value has a financial character and cyber-attackers are interested in assigned value. The concept of a suitable target in RAT is a combination of value, and attackers are interested in assigned value. As such, assets and revenue might likely play a role in the risk for DoS targeted attacks. However, Cayubit et al. (2017) indicated that little research has endeavored to determine hackers' motivations because the motives behind the acts of attacking are often obscure.

Attack Targeted Metrics

The body of literature about DoS attacks on companies' information networks includes scholarship about targeting companies' assets and other holdings (Camillo, 2017), detecting attacks (Jasiul, Szpyrka, & Sliwa, 2014; Raj Kumar & Selvakumar, 2011; Xuan, Shin, Thai, & Znati, 2010), protecting against security breaches (Dzurenda, 2015; Rajesh, 2013; Ramesh, 2013), making efforts to mitigate the effects of cyber-attacks (Patil & Kulkarni, 2011), studying system vulnerability (Harris & Maymi, 2016; Villeneuve, 2011), and exploring hackers' motivations (Amoroso, 2013; Hughes & Cybenko, 2013). However, researchers have not addressed the metrics how and why attackers choose their targets. In particular, researchers have not investigated the role of financial metrics in determining business sectors and target candidates for cyber-attack. Tajalizadehkhoob et al. (2014) drew upon RAT (a motivated offender, a suitable target, and the absence of guardian) to describe why criminals go after a certain target and

examined DoS attacks through the lens of the economics of crime, but they did not categorize targets by assets or revenues. I attempted to address this gap by searching for a relationship between a business's financial value and the duration of DoS attacks against it and resulting financial damages.

The concept of metrics entails the allocation of values to objects, while the procedure that is employed in approximating an object's qualities is known as a measurement. Often, measurement is categorized into groups: nominal, ordinal, interval, or ratio measurement which is the topmost form of measurement. Metrics are considered integral in creating security systems because of the ability to denote cause-effect relationships between cyber-attacks. Several cyber-security attack researchers (Behal & Kumar, 2017; Mateski et al., 2012; Mishra & Saini, 2013; Verendel, 2009; Savola, 2009) used various metrics to measure cyber-attacks, including technical, operational weakness volumetric attack-oriented, attacks taxonomy, business targeted types, and scale of security metrics-nominal, ordinal and interval. In quantitative studies on cyber security, Verendel (2009) grouped different kinds of literature based on the methods used for validation, perspective, and assumptions made regarding the quantitative security and, lastly, based on the targets. One rare study that developed a DoS attack metrics was conducted by Savola (2009), who used a holistic approach based on the fundamentals of security metrics. Savola's metrics categorized goals into control areas and targeted users. To fill the research gaps in studies conducted by Verendel (2009) and Mishra and Saini (2013), this study employed a holistic perspective to categorize system-wide DoS attacks based on differences of rates of attacks, duration of attacks, and financial damages across

business sector types and to categorize the relationship of DoS attack duration and financial damages to assets and revenues.

Other researchers (Tajalizadehkhoob et al., 2014) examined target selection attacks (attack choices) to ascertain the advancement of attacks metrics. According to Tajalizadehkhoob et al. (2014), security metrics can be divided based on several factors. Some of the factors integral in this classification are the goals for providing security, vulnerable areas, targeted systems, and temporal dimension. Mateski et al. (2012) focused on threat actions identified that the most commonly used security metrics are threat metrics (target no specific entity, high values entities, critical assets, specific single entity), taxonomy attacks, volumetric attack results, goal and business targeted metrics. In this study, the researcher identified whether some sectors are targeted more frequently than others, providing information about whether some sectors are more attractive than others to be targeted.

In examining other researchers' attack metrics, Romanosky (2016) identified that banks are the most vulnerable organizations when it comes to attacks though some are targeted more frequently compared to others. Online banks were found to be more vulnerable than physical banks. Data network organizations also were found to be vulnerable to these attacks. Attackers use DoS attacks as a strategy to attack organizational systems and target financial services. Trend Micro (2019) also confirmed the notion that banks are more likely to be DoS targets. Tajalizadehkhoob et al. (2014) used metrics based on RAT to determine a selection of cyber-crime targets. The model indicates that there are three key factors that explain why criminals chose targets:

motivation, suitability of a target, and the lack of proper protection. Tajalizadehkhoob et al. used metrics to examine the number of botnets that attacked a given domain in a one week. This helped in evaluating the size and attractiveness of different banks in the United States. However, Tajalizadehkhoob et al. faced a challenge in collecting existing data to examine targeted choice patterns. As a result, the current study's variable was business sector types to examine DoS targeted attacks and to contribute to previous studies' findings that attackers tend to favor certain financial services over others.

Theoretical Foundation

Modern criminology has begun perceiving the emergence of cyber-crime as new crime activity; scholarly research into cyber-crime increased over the last 20 years. This introduces a challenge to the scholars of effectively applying the knowledge, skills, and concepts used in a normal world setting into the cyber-attacks. To address the issues of cyber-crime attacks, in a breadth and depth viewpoint, identifying the relevance and efficacy of criminological theories that apply to DoS attacks helps to distinguish the association of targeted attacks and the value (assets, revenues) of businesses sector types.

The theoretical foundation of this study was based on Cohen and Felson's (1979) RAT and Cornish and Clarke's (1987) RCT. These two theories serve as a foundation for cyber-security attack in literature. It is important to identify attackers' targeted attacks using DoS, as well as to understand attackers' choices regarding which companies or organizations to target. In this study, the researcher used RAT to explain findings regarding target suitability (Navarro & Jasinski, 2012); the researcher used RCT to consider the findings in relation to the decision-making process of attackers based on a

determination of rewards and to explain how DoS attacks target specific business sectors with particular financial values.

The remainder of this chapter includes a review of RAT and RCT, including descriptions of the theories, examples of how researchers use the models, empirical outcomes of research using these models, the application of these theories to the research of cyber-attack crime, and discussion of the framework and variables that best explain business sector value attack with DoS.

Routine Activity Theory (RAT)

Application to crime. The RAT has been used in the field of criminology to analyze deviance and crime structures since its inception in 1979 by Cohen and Felson. According to Cohen and Felson (1979), the wealth of modern society provides increased opportunities for crime to occur, and an attack can be carried out by anyone who has the opportunity. They identified a natural offender as a component of the environment, noting that an attack must convene in the space and time of potential criminals, easy targets, and a lack of guardians. Cohen and Felson's premise was that postmodernity had facilitated the junction in space and time of motivated offenders with potential targets. Their idea was that the opportunity of the crime depends on offender, target and the absence of guardian. The theory is an attempt to identify attacker activities and their patterns through elucidation of alterations in crime rate trends. According to Leukfeldt and Yar (2016), the concepts and applications of the RAT theory vary across research projects and researchers. However, key components are common to all variations: once an attacker is motivated, they are in a position to commit a crime at the slightest of

opportunities; when the target is vulnerable and too exposed, the attacker is further motivated to commit the crime. Therefore, the offender, the target, and the absence of a guardian in an enabling environment form the components of crime according to RAT.

Application to cyber-crime. The expansion of computers caused a shift in the nature of traditional crime. An attacker can commit an attack from anywhere in the world, block access, and extract information digitally. Reyns, Henson, and Fisher (2011), Holt (2013), and Reyns (2016) indicated that proper timing and place, coupled with proper conditions (i.e., a lack of guardianship, availability of target, and motivated attacker) lead to attack (see Figure 2). In cyber-crime, defense software and firewalls act in the guardianship role (Harris & Maymi, 2016). According to Décary-Hetú and Dupont (2012), attackers target companies' software and find security weaknesses in software while sharing their findings through online forums. Bendovschi (2015) indicated that cyber-space has become a platform for an attacker to attack potential targets.

Figure 2. Elements of routine activity theory.

There is disagreement among scholars on how to apply traditional criminological theory to the study of cyber-crime. Some argue that cyber-crime is a new crime which is

unique in the sense that the two parties involved may never have contact and, therefore, require new analytical approaches. For example, Hollis et al. (2013) and Holt (2017) explained the complexity of employing traditional crime theory to cyber-attack crimes. Likewise, Holt (2013) described the suitability of RAT to predict some aspects of the online crimes but also noted its limitations in other aspects of cyber-crime. However, recently, several scholars applied RAT to examine technology-enabled (cyber-attacks) attacks (Leukfeldt, 2014; Holt & Bossler, 2014) as an analytical framework to study cybercrime and found that RAT elements are more applicable to the study. There is data that supports the use of RAT to analyze cyber-crime (Felson 1986, 1987; Felson & Boba, 2010). RAT has been successfully applied to virtual settings involving social media, computer networks, and online gaming.

The first scholar to effectively apply the principles of RAT to cyber-attack crime was Yar in 2005. Yar applied all the main elements of RAT to the virtual world: the online-motivated offenders mainly comprised of the hackers, and the targets included personal information and proprietary data. In essence, the more time a person spends on the Internet, the more likely they may be targeted by the online offenders. As businesses utilize Internet, they become potential cyber-attack targets. The enabling environment for such online criminal attack activities is accelerated by data which is not secured online. Hutchings and Hayes (2009) also examined online activity in relation to phishing, using RAT as a theoretical foundation for their explanatory studies. Their quantitative cross-sectional survey approach revealed that Internet banking users were more often victims of cyber-attackers. Also, examining existing survey data in combination with RAT

assumptions, Yucedal (2010) compared home users' and business users' online victimization. In addition to RAT, Yucedal used lifestyle exposure theory for his theoretical framework, and he framed his findings in relation to individual perceptions of victimization, cyber-crime, and spyware.

Similarly, applying RAT to cyber-fraud, Pratt et al. (2010) found that vulnerability to cyber-attack was a result of online exposure. Reyns (2013) studied identify theft using RAT and found that the use of the Internet for banking and also, the constant use and forwarding of online messages through emails increased the risk of cyber-attacks. Specifically, his findings indicated that the risk for cyber-attack of people who regularly use these online facilities is almost 50% higher compared to those who rarely use such online services.

Researchers also used RAT to examine approaches to cyber-crime. For example, Chu and Holt (2015) found that attackers use botnets to attack networks and to scan vulnerable networks to exploit information. In addition, Chu and Ahn (2010) conducted a crucial study regarding cyber-trespass, which showed that hackers do not target individuals but go for bigger populations of Internet users where they use botnets to attack the computers. Botnets represent groups of computers that are infected (zombies), and usually more than one hacker can use the botnets for their own ends (Symantec, 2014). Zombies created by attackers are used to carry out large volume of DoS attacks. Chu et al. (2010) advocated for the application of RAT to these cyber-crimes.

The Symantec (2014) study and the findings from Chu et al. (2010) fit into the components of the RAT: the hackers, in this case, are the motivated offenders or attacker

in the study; the potential targets by the cyber-attackers are all the business computers which are connected networks; the guards are anti-virus software and intrusion detection systems that are installed on business computers. In other words, there are various ways to tailor RAT to suit the Internet environment when analyzing cyber-attacks.

Leukfeldt and Yar (2016) studied the suitability of RAT in explaining cyber-attacks. According to their findings, they revealed that some aspects of RAT better allow for an understanding of cyber-attack crime than others. Just as financial values are especially likely to play a role in on-line offense, visibility clearly plays a role in cyber-crime victimization. Therefore, value and visibility, as discussed by Leukfeldt and Yar, reflect an important aspect of business sector targeted studies.

Application to DoS attacks. I employed the components of RAT that examine attackers, attack targets (business sector as a target and business assets and revenue as a target), and the victim (duration of attack and financial damage). The intention is to apply RAT in a manner that suits the environment of DoS attacks to develop more measures of linking intent with attractiveness through an extended examination of DoS targeted attacks.

While RAT is valuable for examining the attractiveness of targets that could result in an attack, RCT complements RAT by recognizing that the occurrence of crime is a progressive outcome—not a one-time decision—facilitated by the interaction of potential offenders and potential victims, as well as the tradeoffs of opportunity, situational factors, and constraints to the crime committed (Cornish & Clarke, 2008).

Rational Choice Theory (RCT)

According to Jennings and Beaudry-Cyr (2014), RCT is one of the most fundamental criminological theories, establishing that the process of rational decision making enables people to independently decide to take part in criminal activities. Essentially, people act rationally by measuring the advantages and disadvantages of participating in criminal activities to find the most advantageous move. Should the advantages of committing a crime outweigh the disadvantages, then criminals will decide to take part.

According to Hostettler (2011), the origins of RCT date back to the 18th century and the utilitarian social philosopher, Cesare Beccaria, who examined the role of people's perceptions of pain and pleasure in their decision making. Since Beccaria's original influence on RCT, the theory has been extended (Freilich, 2015). A variety of theorists contributed to the establishment of RCT, including Homans (1961), who created a basic theoretical framework associated with the exchange theory derived from behaviorist psychology and analyzed how people carry out their activities. Blau (1964), Coleman (1973), and Cook (1977) expanded Homan's work and made RCT applicable to math application. Until recently, RCT has been the leading method within the social sciences of conceptualizing the actions of people.

There are various approaches to RCT because there are numerous variations of the theory customized for different fields. Claude and Siponen (2014) observed that these variations of RCT had been put into various uses in different fields such as criminology, political science, sociology, and even the field of economics. Regardless of the field in

which RCTs were established, they were based on a common assumption of differences in rationality, starting with total rationality, bounded rationality, and the systematic rationality to social rationality. Participants seek to fully utilize their resources when committing their crime by depending on the knowledge they have. Attackers usually have their own projections, and they work their way out to establish the hidden facts through their various objectively misconstrued but sensible efforts

While RCT is used in many fields, it has been a dominating paradigm in Economics, where it is referred to as the neoclassical paradigm. Although RCT has been tremendously criticized, including critiques of its empirical and conceptual limitations (Burns & Roszkowska, 2016), it continues to be used in economic research. Apart from economics, RCT is also largely used in criminology (Steele, 2016).

Application to crime. RCT first was used in criminology studies in 1970s, drawing on Becker's (1968) conceptualization of RCT as a way to examine attackers' decisions of whether or not to attack. Indeed, the classical criminological theory was founded on the basic principle of actions and decisions that are taken by an individual. The theory of rational choice is meant to explain how people make their choices; it highlights that crime is a matter of choice that is intended for benefiting the attacker. According to RCT, attackers commit a crime after analyzing their options and making a decision to commit the crime. Cornish and Clarke (2008) noted that individuals committing crimes make rational decisions prior to making their moves. Attackers are active decision makers in the process of evaluating alternatives, which indicates that

attackers are criminals who evaluate rational factors to decide whether and how to commit crimes (Cornish & Clarke, 2008).

Initial studies in criminology using RCT received empirical backing from many researchers (D'arcy & Hovav, 2009; Ransbotham & Mitra, 2009; Wilson & Herrnstein, 1985). When RCT was still under development, its sole purpose was to explain particular types of crime. This was the main intention of Cornish and Clarke during its development when it received their support for studying sexual harassment cases, theft, and academic fraud (Exum & Layana, 2016). In the 1980s, Clarke and Cornish (1985) developed three lenses, which they elaborated on a year later (Cornish and Clarke, 1986), through which to view human criminal behaviors.

First, crime would be committed by people who perceived the real value in those acts of crime; they would commit a crime if they saw more pros than cons in their act. As noted by Steele (2016), the criminal act involves a process of making decisions to establish advantages and disadvantages, and the decision-making process is often hampered by the insufficient or lack of information regarding those acts of crime.

Second, decisions about committing crimes are made based on sets of information and variations in that information. This focus highlighted situations or frameworks of acts of crime as opposed to focusing the attention on specific people. The focus also allowed for getting idiosyncrasies of various requirements that came in line with the crime.

Third, criminal acts hinge on decisions made by a particular person in order for them to take part in committing a crime. The attacker decides to take part in criminal activities or not through the process of criminal involvement in which the decision had to

be made from a substantially informed position. This process of decision making does not rely on an individual's character; instead, it relies on various levels of information. More recently, Burns and Roszkowska (2016) updated the three components of RCT: agent, accessibility to the target, and the opportunity to take action. These components are similar to the RAT elements of offenders, suitable targets, and absence of guardian.

In 2006, Buldas, Laud, Priisalu, Saarepera, and Willemson created a sequence of reasoning to analyze an attacker's decisions. They postulated that any rational attacker would not go through with committing that crime if it was not beneficial to them. Again, they stated that attackers will always choose the approaches that will result in the greatest rewards. In their model of their attacker's thinking process, Buldas et al. argued that the attacker needs to have an idea of all his measures and then applies a combination of his measures to establish a strategic attacking plan. Attackers then assess the profitability of their plans to see if they will move forward with them. The attackers decide to take part in the attack as a game. At this point, they put in place all the necessary requirements and launch their assault on the given system.

Cornish and Clarke (2008) contributed to RCT by stating that crime is intended to meet attackers' needs, such as status or money. Attackers must have a motive directing their focus. Due to varying levels of crime, attackers commit different crimes based on the returns, risks, and purposes of a crime. Thus, the decision to commit an attack is an outcome of the factors associated with the nature of each crime. This theoretical view is essential in the analysis of an attacker's rational choice related to the criteria of the companies targeted, the method of attack, and the ability to beat the security

countermeasures already in place. The RCT theory can serve as a framework to address the decision of which targets to choose in cyber-attacks.

Application to cyber-crime. Cyber-crime is often quite distinct from a normal crime whether the attack is on physical entities or targeting information systems, and as result, it can be difficult to examine or predict. Attackers have countless ways of launching attacks by involving their rational thinking; hackers weigh several options and are very methodical when they are carrying out their operations with caution. As such, using RCT to examine cyber-crime can be challenging. However, there are various criminal and economic types of RCTs that cyber-security researchers used (Paternoster, Jaynes, & Wilson, 2017). For example, Bachmann (2010) used RCT to study the activity of cyber-attackers, measuring cyber-interruption and malicious code dissemination activities as a way to examine cyber-attacker decision-making activities. Bachmann used analysis to test the effect of rationality and risk propensity (independent variable) on the total amount of hacking incidents (dependent variable).

Similarly, using RCT, Hutchings (2014) found that most attackers commit cyber-crimes because they are more motivated by the thought that they cannot be arrested. These attackers sacrifice their time and engage in the crime only to the point when they deem it to be no longer beneficial. The benefits that come from committing attacks vary depending on the nature of the crime; common offenses usually come with financial benefits.

Mandelcorn, Modarres, and Mosleh (2016) developed an RCT-informed cyber-attack model, which examined cyber-attacks and their relationship with criminology

theory. They found that the random attacks they studied were very opportunistic in nature, and they were carried out without a plan, unlike the planned attacks which were very strategic and very deliberate. The planned attacks usually involved the attackers choosing targets and outcomes, such as targeting financial sector by denying access and further acquiring the confidential information. According to Mandelcorn et al.'s implementation of cyber-security should be carried out from an attacker's point of view. Their model focused on the usefulness of RCT in understanding the attacker's simple goals and decision-making process.

Application to DoS attacks. Cyber-attack with DoS is a relatively new phenomenon, which is still under researched due to its complexity. However, RCT is well-suited to studying DoS attacks because attackers, who likely have everything needed for an attack at their disposal, employ rational thinking to determine the approach that is likely to lead to the best results. This study used RCT as a theoretical approach in order to understand targeted business sector attacks with DoS. Specifically, RCT provided a framework for analyzing the patterns of attack rates in relation to business sectors and their values, offering insight into how attackers choose their targets in relation to expected financial benefits.

Combining two theories. RAT and RCT have, for some time, added value to the theoretical understanding of the various forms of cyber-crimes. Researchers used the theories as tools of analyses to examine the motivations of cyber-crimes through their propositions that when a motivated offender, suitable target, and lack of a capable guardian converge at a particular time, then cyber-attacks are likely to take place.

Combining RAT and RCT expanded the scope of understanding of the topic. Specifically, the focus of RAT is on the required components for an attack to take place (i.e., attacker, target, and lack of security) while the focus of RCT is on the rational choices in which the attacker weighs the odds and considers the costs and the benefits. Although RAT is suitable for a large scale or a macro level, RCT is more suitable for the small or micro level.

There are various models of RAT and RCT that researchers used to analyze crime. The model used in this study focused on the targets of DoS attacks; it assumed that it is possible to apply the RAT and RCT models used to study crime to cyber-crime. The rationale for employing two theories in this study was that combining two theories can explain how DoS attacks target specific business sectors and can contribute to a better awareness of attack in relation to costs and benefits. Two theories, with their variations, can be used as multi-agent modeling to examine cyber-attack variants.

Summary and Conclusions

In Chapter 2, I reviewed the literature that supports the problem statement and the theoretical foundation as stated in Chapter 1. I discussed the literature on cyber-attacks, cyber-security, targeted attacks, attack metrics, and the theoretical framework for this study. In addition to the underlying literature on the historical and theoretical background for this DoS attack inquiry, this review included several other references and resources. Harris and Maymi (2016) and Conrad et al. (2015) noted that attackers (which can be script kiddies, crackers, or hackers) used DoS attacks to consume bandwidth and to bypass firewall and IDSs and IPSs. The dynamic nature and complexities of attack

systems make it difficult to protect companies from DoS attackers. Attackers often use reconnaissance techniques to gather as much information about a target's system as possible, which could include searching for information using web browsers, using particular tools to send packets to spot hosts, and detecting services run on the target computers. The possible dangers of these attacks are network communications interruptions and cyber-security breaches. Targeted attacks may operate to maximize attackers' opportunity to prevent access (Harris & Maymi, 2019; Stewart et al., 2015).

Some researchers of DoS attacks (Conrad et al., 2015; Harris & Maymi, 2016; Mahjabin et al., 2017) examined categories of attacks, techniques of attackers, defense mechanisms against attacks, and motivations of attacks. However, studies with different conclusions exist within the DoS targeted attack literature (e.g., Alomari et al., 2012; Bendovschi, 2015; Yu, 2014). Several researchers examined the relationship between business sector and DoS attacks. However, discrepancies exist as a result of metholodical diffirences; failure to recognize the need to use the business sector as an independent variable. The rate, duration, and financial damages were not specifically accounted for in these correlational studies. Recently, Bendovschi et al. (2016), Leukfeldt and Yar (2016), and O'Leary et al. (2017) endeavored to address the relationships between DoS targeted attack and business sector. With the exception of these three studies, there is a gap in the research literature whether attackers target some business sectors with DoS more than they target others and on whether there is a relationship between targeted attacks and a company's generated revenues and assets.

In Chapter 3, I discuss the purpose of quantitative research and the rationale for choosing this research approach. I include a description of the research design selected for this investigation. Most significantly, Chapter 3 includes the details of how the researcher determined differences among business sectors in attack rates, duration of attacks, and financial damages resulting from attacks and determined the relationship between company assets and revenues and the duration of attacks as well as the relationship between company assets and revenues and the financial damages resulting from attacks. The chapter includes a detailed explanation of, and justification for, the research design, including data collection, data analysis, and ethical considerations.

Chapter 3: Research Method

The literature review in Chapter 2 included an examination and comparison of various types of DoS attacks, malicious activities and motivations that intensified over time, existing research on DoS attacks, and the theoretical foundation for this study. Although researchers provided information about cyber-security, gaps exist in the literature regarding targeted attacks on companies with DoS and target attractiveness in relation to business sectors and values. In this study, I conducted the research to fill the gap. This chapter includes a discussion on the research method, study design and rational, sampling and sample procedures, instrument design, data collection, and data analysis.

As research is a process of collecting, analyzing, and interpreting data to understand events and uncover new information (Williman, 2011), it requires an appropriate methodology. To select an applicable method of inquiry described by its procedure (Lapan, Quartaroli, & Riemer, 2012) and to gain reliable and valid results to answer the research questions for a study of DoS attacks, the researcher examined and compared various theoretical methods of inquiry and selected a quantitative method. I used a quantitative, nonexperimental methodology to investigate the patterns that could explain how attackers collectively target business sectors and companies with DoS attacks. In order to include enough incidents of successful DoS attacks to allow the researcher to draw conclusions, the researcher included DoS attacks that occurred during the 19-year time span from 2000–2019. This provided enough information to determine differences among the five sectors and to examine the relationships between companies'

assets and revenues and duration of attacks as well as the financial damages resulting from attacks. I used the quantitative research method to answer the research questions.

Research Design and Rational

Researchers may choose qualitative or quantitative research approaches (Singleton & Straits, 2017). Quantitative designs include survey research, experimental, quasi-experimental, nonexperimental, correlational and causal-comparative designs (Turner, Balmer, & Coverdale, 2013). In nonexperimental designs, researchers can utilize correlational design to identify the relationship between variables (Turner et al., 2013) and examine variables using numerical or statistics (Holosko, Jolivette, & Houchins, 2014). I selected a quantitative analysis approach for this study.

Utilizing a quantitative approach, I also examined the relationship between company assets and revenues and the duration of attacks and relationship between company assets and revenues and the financial damages resulting from attacks. I compiled and analyzed archival data for attack rates, duration, and damages between 2000 to 2019. I analyzed the data to test the hypotheses generated by the research questions.

The research design for this study on DoS attacks was nonexperimental. Nonexperimental research designs are suitable for studies that involve no manipulation of the independent variable (Carter & Lubinsky, 2016), no control, and no randomization. When randomization and manipulation of variables is not possible, ex post facto design is useful to examine the differences and relationship between variables (Ary, et al., 2010). The focus of these designs is on measuring independent and dependent variables and

determining relationships among variables. The goal is to describe phenomena and to explore and explain relationships among variables (Edmonds & Kennedy, 2013).

I used a dataset compiled from archival reports that include other scholars' research, as well as reports from network administrators, information security officers, government agencies, and private companies. The dataset was also compiled from incident reports on companies obtained from online, publicly accessible incident and crime reports from 2000 to 2019. Compared with survey research, utilizing a dataset created from archival data has the advantage of increased accuracy and objectivity. The major sources of the data for this study were: ComputerWorld, McAfee, Privacyrights.org, Idtheftcenter.org, IC3, Avtest.org, FBI websites, and Library of Congress. After the collection of data, I entered into a computer database. I studied differences among business sectors using the Kruskal-Wallis test to evaluate the dependent variables across the five sectors. I studied the relationship among assets, revenues and duration of attacks as well as the financial damages from attacks using Spearman correlational tests.

Methodology

The research methodology is a systematic way to investigate the research questions and acquire new understanding (Singleton & Straits, 2017). In this methodological section, I explain how the Kruskal-Wallis tests and Spearman correlation analysis were used to determine the differences of attack rates, duration of attacks, and financial damages resulting from attacks among sectors as well as to examine the relationship among assets and revenues and the duration of attacks as well as the financial

damages from attacks. I then describe how the research questions that derived from the theoretical foundation and literature review were tested and how the research was conducted. I used quantitative statistical analyses, specifically Kruskal-Wallis tests and Spearman correlation, to analyze data (number of attacks, length of attacks, financial damages, assets, and revenues) and to answer the research questions so that other investigators can replicate the findings. In general, the purpose of a quantitative study is to examine hypotheses (Morgan, 2015) using an objective procedure. For more detail, this section is organized in the following subsections: population; sampling and sampling procedures; procedures for recruitment, participation, and data collection; archival data; and instrumentation and operationalization of constructs.

Population

The study included the 100 largest U.S. companies within each of the business sectors (educational, financial, informational, insurance, and retail sectors) whether they experienced DoS attacks between the years of 2000 and 2019 or not. Business sectors and companies outside of the United States were excluded.

Sampling and Sampling Procedures

Based on Singleton and Straits' (2017) research approach, I used a systematic method to gather data on five business sectors from the United States, as categorized by the North American Industry Classification System (NAICS). I compiled a complete database of DoS attacks focusing on the 100 companies within each of the business sectors for the specified 19-year period (100 attacks across the 500 sampled organizations).

I performed a power analysis for the Kruskal-Wallis tests using G*Power (McDonald 2014; Perugini, Gallucci, & Costantini, 2018) with $f = .25$, $p = .05$, and power = .80. I performed a second power analysis for the Spearman correlations using G*Power with $f^2 = .15$, $p = .05$, power = .80, and number of predictors = 1. The results indicated that a total sample size across the five groups should be at least 200 for the Kruskal-Wallis tests s and fewer would be required for the correlations. By including 100 companies in each sector, the total sample size was 500. This suggests that the sample size had a greater than 80% chance of finding significant differences across sectors and relationships between financial variables and duration and financial damages if they exist in the larger population.

Procedures for Recruitment, Participation, and Data Collection

Archival documents refer to existing data recorded or reported information that gives researchers valuable sources of measurement (Singleton & Straits, 2017). This archival data collection includes: DoS attacks from government and business reports and assets and revenues from business report database for the years 2000–2019. I used and evaluated the Information on DoS attacks from Symantec and McAfee monitoring research databases. Retrieving data sets from online archives and government reports involved key word searches using terms such as *cyber-attack, network attack, security breach, hacker,* and *DoS attacks*. The study involved gathering archival documents, studies, and record and incident reports and interpreting them into categories for the five business sector types.

The data included the following information: (a) DoS attacks, (b) types (names) of targeted business sectors, (c) year of attack, (d) financial loss/damages, (e) business assets and revenues of attacked business, and (f) duration of attacks. See Table 1 for a listing of the data that were compiled to answer each research question along with the sources for the data. I used these data (business sector types, value of assets and revenue of businesses at the period of the attacks) as the independent variables for this research. Asset includes any values owned by business, and revenue is total income of a business sector over a specific period or year. For the purpose of the correlation analyses, assets and revenues were operationalized as the assets and revenues for the company as reported the year of the attack.

Data extraction involved using the TextEdit application or Microsoft Excel. After extracting the data for each year into text format, I uploaded data categorized by financial loss due to DoS attacks, sector types, assets, revenues, duration of attack and year into the SPSS version 24 system. This procedure was repeated for each year of the data set and aggregated across the 19 years included in this study, and I examined whether the data correctly fit to the research questions. To avoid bias while extracting information from books, articles, and reports, the researcher employed strategies such as examining source integrity and reliability. Table 1 includes a summary of the data required to answer each of the research questions and the databases from which data were extracted.

Table 1
Data Types and Sources

Research Question	Data	Data Sources
RQ1: Between 2000–2019, were there significant differences among business sectors in the rate of DoS attacks?	Rate of DoS attacks on each of 100 companies in each industry in the 19-year period. Business sector type (educational, financial, informational, insurance, and retail)	Arbor network, Norton report, McAFee report, NAICS, Privacyrights.org, Idtheftcenter.org, IC3, Avtest.org, FBI websites, and Library of Congress, U.S. Department of Justice, Carnegie Mellon, Computer Security Institute, university libraries, Internet, Homeland security, NSA, and journals.
RQ2: Between 2000–2019, were there significant differences among business sectors in the duration of DoS attacks?	Duration of DoS attacks in 19-year period. Business sector type (educational, financial, informational, insurance, and retail)	Arbor network, Norton report, McAFee report, NAICS, Privacyrights.org, Idtheftcenter.org, IC3, Avtest.org, FBI websites, and Library of Congress, U.S. Department of Justice, Carnegie Mellon, Computer Security Institute, university libraries, Internet, Homeland security, NSA, and journals.
RQ3: Between 2000–2019, were there significant differences among business sectors in the financial damage per DoS attack?	Financial damage resulting from DoS attacks in 19-year period. Business sector type (educational, financial, informational, insurance, and retail)	Journal of Business & Economic Statistics, Bureau of labor statistics, Arbor network, Norton report, McAFee report, NAICS, Privacyrights.org, Idtheftcenter.org, IC3, Avtest.org, FBI websites, and Library of Congress, U.S. Department of Justice, Carnegie Mellon, Computer Security Institute, university libraries, Internet, Homeland security, NSA, and journals.
RQ4: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and duration of DoS attacks?	Duration of DoS attacks in 19-year period. Business sector type. Company assets and revenues.	Journal of Business & Economic Statistics, Bureau of labor statistics, Arbor network, Norton report, McAFee report, NAICS, Privacyrights.org, Idtheftcenter.org, IC3, Avtest.org, FBI websites, and Library of Congress, U.S. Department of Justice, Carnegie Mellon, Computer Security Institute, university libraries, Internet, Homeland security, NSA, and journals.
RQ5: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and the financial damage resulting from DoS attacks?	Financial damage resulting from DoS attacks in 19-year period. Business sector type. Company assets and revenues.	Journal of Business & Economic Statistics, Bureau of labor statistics, Arbor network, Norton report, McAFee report, NAICS, Privacyrights.org, Idtheftcenter.org, IC3, Avtest.org, FBI websites, and Library of Congress, U.S. Department of Justice, Carnegie Mellon, Computer Security Institute, university libraries, Internet, Homeland security, NSA, and journals.

Archival Data

I only used secondary data to answer the research questions. As the original data collection process is separated from me, my aims and views cannot distort the collected data. Data are less likely to be influenced by preconceived notions. Instead, when compiling archival data, researchers must ensure completeness, accuracy, accessibility of reliable measurements, and in cases of quantitative studies such as this one, appropriateness of statistical techniques to analyze the compiled data.

Archival/available data studies compile data from a variety of different types of documents (Moore, Salter, Stanley, & Tamboukou, 2017). These available data include public and private documents and incident reports. Compared with a survey study, creating an archival dataset has the advantage of increased accuracy. Business leaders can omit valuable information when responding to surveys for fear of losing customer trust and potential client investments (White, 2016). Archival research reduces the likelihood such omissions because it relies on data that were submitted to the federal government, for which there are serious legal consequences to falsification or omission. Every method of data collection has drawbacks and there are several advantages and problems related to the use of available data (Singleton & Straits, 2017). For example, in cases where the response rate is poor and past events need reexamining, using existing archival data appears to be the most viable option for researchers. To avoid any shortcomings and to maintain reliability and validity, I compared across data sources to confirm the integrity

of the available data. I checked the compiled data for accuracy by visually inspecting data and checking invalid and missing data against the original archival data.

DoS attack reports on business sectors come from databases of government agencies (FBI, Homeland Security), private companies, and the Internet. Both government and organizational databases are public domain resources, and no special permissions are required for acquisition of such data. I verified (cross-checking, evaluating) Internet sites and determined whether the information was from legitimate government, organizations, businesses, and institutions sources.

Instrumentation and Operationalization of Constructs

Instruments are often used in the data collection procedure as a means of measuring research variables (Singleton & Straits, 2017). However, I did not include any surveys or similar instruments because archival data were used.

In this quantitative study, I employ operationalization as defined by Singleton and Straits (2017) as the means of defining variables into testable and measurable elements. To ensure reliability, I inspected the study to retest the congruency between the operational definition and the research questions. I used Kruskal-Wallis tests to determine whether there are significant differences across sectors on: rate of attacks, duration of attacks, and financial damages resulting from attacks. I also used four Spearman correlation analyses to determine whether there is a relationship within a given sector between a company's assets and/or revenues and the duration of attacks as well as the financial damages resulting from attacks.

Operationalization of Independent and Dependent Variables

Rate of DoS attacks. Rate is operationalized as the average number of attacks per company in each industry. For the purpose of this study, because it would be nearly impossible to come up with a credible total number of companies in the retail industry, for example, I examined the 100 companies (as measured by total workforce) in each of the five sectors and "rate" referred to the average number attacks on those 100 companies in the time period under consideration.

Duration of DoS attack. Duration was operationalized as the hours and minutes that a DoS takes the system offline (block the communication) and that can be enough to inflict damage at the target site (NSFOCUS, 2017).

Financial damage. Damage refers a negative effect on the asset values by denying services and it includes tangible losses, lost revenue, and other types of damages (Palekiene et al., 2014). For this study damages were operationalized as the monetary value of losses caused by DoS online business interruption.

Sector. Five business sectors were included in this analysis: educational, financial, informational, insurance, and retail.

Asset. An asset is everything of monetary value retained by a business that is grouped as capital/fixed, current, tangible or intangible and stated in terms of their cash value on financial accounts (The Farlex Financial Dictionary, 2017).

Revenue. Revenue is the total amount of income that a business sector generated from sale of goods and services during a specific period or the amount, in monetary unit, received during in a given time (Carcello, 2008).

Data Analysis Plan

Scholars conduct both primary and secondary research. Secondary research depends on existing data sources collected by others for various objectives (Anderson & Paterson, 2015). I used two analytical methods to test the hypotheses about cyber-security attacks with DoS. In the first analysis, I tested differences across sectors in DoS attack rates, duration of attacks, and financial damages resulting from the attacks for the period from 2000 to 2019. The second phase of analysis included determining whether there was a statistically significant relationship between company assets and/or revenues and duration of DoS attacks and the financial damage resulting from DoS attacks within the period from 2000 to 2019. Table 2 includes the data analysis plan, indicating the dependent and independent variables for each research question as well as the statistical technique that was used to test each hypothesis.

Table 2
Summary of Data Analysis Approach Per Research Question

Research Questions	Independent Variable(s)	Dependent Variable(s)	Analysis
RQ1: Between 2000–2019, were there significant differences among business sectors in the rate of DoS attacks?	Business sector type (educational, financial, informational, insurance, and retail)	Rate of DoS attacks from databases (IC3, FBI, The U.S. Bureau of Labor Statistics and U.S. Bureau of Economic Analysis, journals) tracking number of attacks in each sector type	Kruskal-Wallis tests with 4 categories (insurance excluded) and rate of DoS attacks on each company as DV.
RQ2: Between 2000–2019, were there significant differences among business sectors in the duration of DoS attacks?	Business sector	Duration of DoS attacks from databases tracking number of attacks in relation to value of assets held per employee within each sector (IV)	Kruskal-Wallis tests with 4 categories (insurance excluded) and Duration of DoS attacks as DV
RQ3: Between 2000–2019, were there significant differences among business sectors in the financial damage per DoS attack?	Business sector	Financial damages from DoS attacks from databases tracking number of attacks in relation to revenue at the time of the attack (IV)	Kruskal-Wallis tests with 4 categories (insurance excluded) and Financial Damages resulting from DoS attacks as DV
RQ4: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and duration of DoS attacks?	Business sector Value of assets Revenue of businesses at the period of attacks	Financial damages due to DoS attacks.	Eight Spearman rank-order correlations (r_s), two for each sector (insurance excluded), Value of Assets and Revenues as IVs and Duration of attack as DV.)
RQ5: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and the financial damage resulting from DoS attacks?	Business sector Value of assets Revenue of businesses at the period of attacks		Eight Spearman rank-order correlations (r_s), two for each sector (insurance excluded) Value of Assets and Revenues as IVs and financial damage resulting from attack as DV.

Kruskal-Wallis Test

Analysis of Variance (ANOVA) is an analysis used to evaluate statistical differences. This study originally planned to use ANOVA to determine which of the differences among the variables were significant. Using this test allows a researcher to test whether means are statistically different from each other. The closer in value the means are, the more likely the assumption of equal means will be true when conducting the test. However, there was a lack of normal distribution across business sectors. Thus, for the first, second, and third research questions, I used the Kruskal-Wallis test, a nonparametric test that can be used as alternative to the one-way ANOVA when groups of independent variables are not equal in population. While previous research has suggested that the financial services sector might be more subject to DoS attacks (Tariq, 2018), I used the post hoc tests to looks at all possible differences among the five sectors.

Researchers (DePoy & Gitlin, 2011; Hinton, McMurray, & Brownlow, 2014) use an error bar plot prior to the independent sample test as a preliminary determination of whether there is no difference in the means and variances between the groups. The *x* axis represents the sectors (educational, financial, informational, insurance, and retail), and the *y* axis represents the mean value of the dependent variable. In each error bar, the dot represents the mean of the group. Reading the mean involves placing a horizontal line across to the left to the *y* axis and reading the value for that group. The vertical distance between the two horizontal lines in each error bar is the variance (Carter & Lubinsky, 2016).

Kruskal-Wallis test is used to identify whether there are statistically significant differences among independent and dependent variables. Kruskal-Wallis *H* test is a nonparametric test that is used to determine significant differences on continuous dependent variable by categorizing independent variable when the requirements are not met for one -way ANOVAs.

Kruskal-Wallis assumption of variance indicate whether the difference in the level of variance between the two groups is significant using an *H* test. In addition, each dependent variable was examined for violations of normality and outliers. Normality was evaluated by measuring skewness and kurtosis for each quantitative variable. Violations of normality were corrected, through a transformation of the nonnormal variable and/or by removing outliers from the data base. Testing the hypotheses involves using a $p < .05$ level of significance (Neuman, 2011).

For Research Question 1, Research Question 2, and Research Question 3, the independent variable was business sector (educational, financial, informational, insurance, and retail). The dependent variables were rate of DoS target attacks for the period from 2000-2019, the duration of the attacks, and the financial damages resulting from these attacks. Tajalizadehkhoob et al. (2014) and Tariq (2018) demonstrated some businesses are more attractive for DoS attack actors than others. For example, gathering data from secondary sources from the period of 2010-2018 and utilizing descriptive statistics, Tariq indicated that financial services were targeted with DoS attacks more than other institutions. Adebiaye, Alryalat, and Owusu (2016) examined financial damages from cyber-crime, using financial losses as a dependent variable and cybercrime

as an independent variable. This study adds to the existing research by examining differences of rates, duration, and financial damages of DoS attacks over a 19-year period among the business sectors.

Correlation

Correlation analysis distinguishes which variables impact the dependent variable of interest and examines how well a model predicts a dependent variable. It is used to identify the relationship between a dependent and one or more independent variables and explore the forms of these relationships (Singleton & Straits, 2017). The study analyzed the hypotheses for Research Questions 4 and 5 using correlation analysis (Spearman's correlational coefficient). Spearman's correlational analysis measures the degree of relationship between variables.

I tested these relationships for each business sector: educational, financial, informational, and retail. Insurance was included in the overall correlations, but a separate correlation for insurance could not be calculated because there were only two cases of DoS attacks on insurance companies. Testing the strength and direction of the relationship took place at an $\alpha < .05$ level of significance. A p value of $p < .05$ indicates that the researcher can reject the null hypothesis.

Research Questions 4 and 5 consider whether a target's financial value was a factor in making companies suitable and attractive targets for motivated attackers. In other words, did having high values of assets and high-generated revenues make certain companies more attractive to attackers and, therefore, more likely to be targeted with long attacks that result in financial damages?

Tajalizadehkhoob et al. (2014) used RAT to examine four aspects that drive target selection attacks: value, portability, visibility, and accessibility. Their research questions included whether the high values (richness) of the sector attracted more companies to be targeted by attack. They employed regression analysis and Spearman's correlational test to determine metrics for per week attacks; also, they calculated the average of the attacks from a ranked database to evaluate how the intensity of attacks related to size.

The right type of correlation depends upon the quantity of data. While Pearson's correlation is used for parametric tests, Spearman correlation is used for nonparametric tests. Spearman correlation tests measure continuous variables that have failed the assumption of the Pearson correlations. I used Spearman rank correlation statistically to measure the strength and directions of nonparametric relationships among data. The r_s and significance (p) values indicate the effect of a variable.

Threat to Validity

While qualitative researchers ensure the integrity of their research by implementing measures to ensure study credibility and transferability, quantitative researchers focus on a study's internal and external validity as key measures of research quality (Nowell, Norris, White, & Moules, 2017; Singleton & Straits, 2017). Employing quantitative measures of validity is a significant factor for researchers as their engagements help to make certain academic value, meaningful, precise, and properly constructed studies. Although scholars may use various definitions to assess the validity of their research, essentially, validity relates to the overall accuracy and creditability of a

study (Singleton & Straits, 2017). In this study, validity serves to ensure the rigor of procedures and processes to ensure and minimize errors or discrepancies in this work.

To help achieve reliability in this work, I explained and described every essential detail of the inquiry. Issues related to validity might affect the outcome of research results or quality of a study. Research results may have internal, external, and/or construct validity. Internal validity refers to the researcher's ability to form inferences (Sikorskii & Noble, 2013) or to legitimately, effectively, and accurately measure what they intend to measure. On the other hand, external validity rerefers to my ability to generalize or apply findings and results to larger populations, groups, or other settings (Singleton & Straits, 2017).

In this research, the greatest threat to validity in utilizing and transferring data from one database to another was human entry errors. While there is nothing that could be done to validate original reports' correctness by the companies, validity of transferring this data into an Excel spreadsheet and later an SPSS database for analysis was ensured through a repeated data collection and comparison process. The primary drawback is that the previous research data may not have been collected to the researcher's standard; this researcher has no control over how the data were reposted and collected when using archived information. The data may be inaccurate or may possibly fail to address certain issues. Further, publicly available datasets were used to identify the amount of financial damage and the likely duration of attacks. The archival data might not generalize to other industries or business sectors in other countries.

The issue of validity could affect the result of the research. According to Lakshmi and Mohideen (2013), the study upshots may encompass one of the validities (internal or external). Through the association of validity and reliability, the researcher reduced biases and enhanced the research accuracy by using Singleton and Strait's (2017) and Neuman's (2011) methods and by double checking the archival data and evaluation techniques. Additional analysis of the data sampling frames and methods and research dealing with the accuracy of the statistics appears in Chapter 4.

External Validity

In a quantitative study, threats to external validity are any elements within the research that lessens the generalizability. As the external validity is the extent to which the outcome of a research can be generalized (Avellar et al., 2016), it is important to state that all obtainable data were gathered to address the research questions. To protect their confidentiality, some companies targeted by attacks may have been unwilling to report all types of cyber-attacks. Unreported incident variable might be significant for analysis. Targeted attacked data is limited only to United States companies, which limits the generalizability of the data. The validation procedure included collecting and analyzing data to evaluate the correctness of a method. Achieving external validity for outcomes that may not be generalizable to other situations with various company levels is challenging. Balancing conflicting and dynamic occurrences within the data set is also difficult. Thus, using multiple types of analyses to examine the same data and eliminate all threats to external validity that intermingle with independent valuables may have strengthened the study.

Internal Validity

An internal threat to validity is the process of archival data collection methods and ensuring its validity. This study was designed to remove the possibility that variables other than any independent variables alter dependent variables. As internal validity is a means to evaluate if research is complete, an appropriate measure was taken to avoid confounding variables (Avellar et al., 2016).

The goal of this study was to systematically analyze the data and correctly move from measurements to conclusions. Internal validity refers to a researcher's ability to effectively and precisely measure what they anticipated to measure. Internal validity associates to the congruency of research results (Singleton & Straits, 2017). Use of archival data sets can provide some significant benefits to reduce threats to internal validity. In this study, the researcher managed threats to internal validity by relying on a governmental database for data collection that was appropriate for evaluating and examining DoS attacks. Due to varying U.S. states' reporting and disclosure laws, there is no single repository that includes comprehensive information about all DoS attacks, damages, and durations. I employed ex post facto research, which is a type of nonexperimental research in which there is no ability to control for extraneous variables as the research happens after the fact. I determined whether the duration of DoS attacks is strongly correlated with higher business values (assets and revenues) and whether the financial damages from attacks is strongly correlated with higher business values (assets and revenues). I addressed the limitations of ex post facto and correlational research in terms of the inability to measure or infer causality from

statistical association or differences and the inability to control for extraneous variables that may contribute to the relationships or comparisons of interest. Greater effort was given to double checking to exclude extraneous variables such as selection, history, and selection-maturation in this study.

Construct Validity

Threat to construct validity can occur from the selection of independent variables and the choice of dependent variables. As construct validity is the most multifaceted and complex, statistical data analysis techniques were designed to measure the data in relation to the research questions as they were intended to be measured (Singleton & Straits, 2017). Construct validity has been the center of theoretical and empirical consideration in several fields of studies (Singleton & Straits, 2017). Researchers use construct validity to examine correlations between an intended measure of a construct and other measures that must be theoretically aligned. To simplify the account construct validity ascertained by using delineations and measurement processes for selected variables, ensuring internal validity requires extraneous variables to need be controlled and confound variable be excluded.

Ethical Procedures

Ethical research requires the pursuit of the overall principles of scientific research (Singleton & Straits, 2017); as such, this research project adhered to Walden University's Institutional Review Board (IRB) parameters. Accessing the existing data online does not require consent from the owner of the selected data. All secondary data from CSI, Privacyrights.org, FBI Incident/Crime Reports, and other databases are public domain.

The compiled data on targeted business sectors with DoS attack are from the public domain. This research does not include personal identifiers to identify individuals. An online available dataset does not require preexisting arrangement with the data originator to provide secure mechanism for data usage. Resource interpretation is bounded by the study. I conducted a comprehensive literature review to show that the archival data that are publicly accessible have not already been analyzed.

Summary

This chapter included a discussion of the components of compiling and analyzing the data for this DoS attack study. This chapter included information on the quantitative design and research convention. I demonstrated that a quantitative approach produced the best and most accurate data for a study on DoS attacks. The focus of this section was on describing the procedural phases that took place in the study. Using multiple analysis methods resolved the issues of validity and reliability and helped maintain the quality of research. The chapter included a discussion on the collection and analysis methods of archival data on DoS attacks and an arrangement for selecting companies. The aim of using companies as the unit of analysis was to present findings that are valuable to organizational leaders in comparing, measuring, and evaluating their targeted values and strengthening their defense systems. Chapter 4 presents the result of this study.

Chapter 4: Results

Introduction

The purpose of this quantitative study was to examine differences in rates and severity (in terms of duration of attacks and financial damages resulting from attacks) of DoS attacks across business sectors (RQ1, RQ2, RQ3) and to determine the relationship between a company's assets and/or revenues and duration of the attack (RQ4) and the relationship between a company's assets and/or revenues and the financial damages from an attack (RQ5). I implemented a quantitative, nonexperimental research design using archival data from 100 companies to answer the guiding research questions. To examine the first three research questions, I studied the overall differences across sectors in the attack rates, attack duration, and financial damages resulting from DoS attacks. To examine the remaining two research questions for this study, I studied the relationship between company assets/revenues and the duration of attacks as well as the relationship between company assets/revenues and the financial damages resulting from DoS attacks. I used an ex post facto data search to develop the dataset. To perform the analysis, I compiled the data on DoS attacks from websites, journals, and books in the form of an Excel text file and imported the Excel text file into SPSS.

I applied two analytical techniques for this study to test the hypotheses. To test the first three hypotheses, I examined the differences among sectors (independent variable) in the rate of, duration of, and financial loss from DoS attacks (dependent variables). The proposal called for using 1-way ANOVAs to answer these research questions. As part of ANOVA testing, it was found that the data violated the assumption

of normality; therefore, Kruskal-Wallis tests, a nonparametric alternative to ANOVA, were substituted. To test the other hypotheses, I examined the relationship between the dependent variables and company assets and/or revenues using correlation analysis. Because these questions also employed data that violated the assumption of normality, Spearman rank-order correlation was substituted for Pearson product-moment correlation.

For this study, I examined five research questions and hypotheses. For the first and the second research questions, I examined the differences in the rate and duration of DoS attacks among five business sectors, in the aggregate from the period 2000–2019. For the third research question, I examined the differences in the financial damage resulting from DoS attacks across the five business sectors from the period 2000–2019. For the fourth and fifth research questions, I examined the relationships between the duration of DOS attacks and financial damages resulting from DoS attacks from the period 2000–2019 and the value of assets held and revenues generated by the business. In this chapter, I describe the data collection process, discusses discrepancies in this process compared to what was described in Chapter 3, and includes a discussion of the research findings for each of the research questions. Chapter 4 concludes with a summary of the results.

Data Collection

According to Irwin (2013), there is an increasing trend towards the use of secondary analysis. This study follows suit in that it is based on analyzing existing archival data, collection methods, and analysis techniques. I compiled the existing data

from archival datasets that included a total of 100 business/organization sectors that were attacked between 2000 and 2019, a period of 19 years. As shown in Table 3, the attacked companies were from the following sectors: educational (9%), financial (38%), informational (37%), insurance (2%), and retail (14%). Of the total 100 businesses, the majority were from the financial and informational sectors, and the fewest were from the insurance sector. All organizations were from the United States and were among the 100 firms from each sector. There were some necessary discrepancies in data collection compared to the plan presented in Chapter 3, specifically in the process of data collection it became apparent that some business sectors did not report/publish their data. Additionally, some resources had conflicting data and sporadic website outages reports. I recognize that too much missing data is problematic and can lead to bias; in order to minimize the loss of cases due to missing data, I utilized pair-wise rather than list-wise deletion. To reduce the missing data on financial loss, I calculated a few companies' revenues based on their yearly generated revenues.

Table 3
Number of Attacks on the 100 Companies in Each Sector

Sector	Attacks
Educational	9
Financial	38
Informational	37
Insurance	2
Retail	14
Total	100

Study Results

I utilized secondary data for both the independent and dependent variables. For this study, I used G*Power analysis. I examined 500 companies—100 from each sector, resulting in a dataset of 100 attacked companies and 400 companies that were not attacked. Finally, I applied convenience sampling to choose companies from each sector.

Descriptive Data

Table 4 presents the descriptive data for the five dependent variables. The most important values in this table are the skew and kurtosis numbers. For all five variables, the skew and kurtosis values are well outside the normal range, indicating that the variables are not normally distributed. As a result, I used the Kruskal-Wallis test, which is the non-parametric equivalent of ANOVA, and Spearman correlations, the non-parametric equivalent of Pearson correlations, throughout the analyses

Table 4
Descriptive Statistics for the Dependent Variables

	Mean	*Std. Error*	*Median*	*Mode*	*Std. Dev.*
Cases	0.2	0.02	0	0	0.45
Duration	284.78	38.67	180	60	376.87
Assets	284.78	38.67	180	60	376.87
Revenues	15.21	4.59	2.29	0.08	45.67
Fin. Damage	$9,964,454	$3,403,268	$614,386	$100,000	$32,995,912

	Kurtosis	*Skewness*	*Range*	*Min.*	*Max.*
Cases	5.68	2.33	3	0	3
Duration	9.3	2.82	2,155.00	5	2,160.00
Assets	9.3	2.82	2,155.00	5	2,160.00
Revenues	54.69	6.76	404.25	0	404.25
Fin. Damage	31	5	$240,000,000	0	$240,000,000

Kruskal-Wallis Analysis: RQs 1, 2, and 3

I examined companies with one or more attacks in comparison to companies with no attacks. I used Kruskal-Wallis to test the null hypothesis for RQ1. Because there were only two insurance companies attacked, I conducted the analysis without the insurance sector.

Based on the work of Levene (1960) and Derrick et al. (2018), I rejected the null when the *p*-value was smaller than the alpha level. Kruskal-Wallis uses a two-tailed test to determine whether or not the means or counts are significantly different across sectors (Snedecor & Cochran, 1983). I used an alpha level of .05 for the tests.

RQ1: Between 2000–2019, were there significant differences among business sectors in the rate of DoS attacks?

To examine Research Question 1, I conducted a Kruskal-Wallis test to assess if there was a significant difference among business sectors in the rate of attacks between 2000 and 2019. Kruskal-Wallis requires at least five observations in each cell and so the insurance sector could not be included. There is a statistically significant difference in the mean rank of attacks among business sectors.

With insurance excluded, the overall differences among sectors were significant ($H(3,400) = 39.22$, $p < .001$). The Dunn post hoc comparisons indicated that the financial and informational sectors are significantly higher in the rate of attacks than the educational sector and retail sector. The significance levels for each pairwise comparison

appear in Table 6. The null hypothesis is rejected with 95% confidence that the differences among the various sectors is not due to random chance.

Table 5
The Rate of Attacks

SUMMARY			
	Count	*Sum*	*Average*
Educational	100	9	0.09
Financial	100	38	0.38
Informational	100	37	0.37
Retail	100	14	0.14

H (3,400) =39.22, p<.001

Table 6
Kruskal-Wallis Rate of Attacks (Dunn Contrasts, Pairwise p Values.)

	Educational	Financial	Information
Financial	p<.001		
Informational	p<.001	p=.768	
Retail	p=.768	p<.001	p<.001

RQ2: Between 2000–2019, were there significant differences among business sectors in the duration of DoS attacks?

To analyze Research Question 2, I performed a Kruskal-Wallis test to assess if there were differences among business sectors in the duration of attacks (Table 7). Kruskal-Wallis requires at least five observations in each cell; therefore, I could not include the insurance. Excluding the insurance sector, there is a statistically significant difference among business sectors in duration of attacks ($H(3,98)=10.69$, $p = 0.014$). Dunn post hoc contrasts *p* values for pairwise comparisons appear as Table 8 and indicate that the duration of attacks was significantly higher for the educational and informational

sectors than for the retail sector or financial sector. The other differences were not significant due to the small sample size. The average duration for the educational sector was 621 minutes while the average duration for the financial sector was 175.42 minutes, and the informational sector and the retail sector had averages of 357.54 minutes and 286.43 minutes respectively. The null hypothesis is rejected with 95% confidence that the variance between the various sectors is not due to random chance. It would be justifiable to conclude that durations are significantly longer for educational and informational companies than for financial and retail companies.

Table 7
Duration

Groups	*Count*	*Sum*	*Average*
Educational	9	5589	621.00
Financial	38	6666	175.42
Informational	37	13229	357.54
Retail	14	4010	286.43

H(3,98)=10.69, $p = 0.014$

Table 8
Kruskal-Wallis Duration of Attacks (Dunn Contrasts, Pairwise p Values.)

	Educational	Financial	Informational
Financial	p=.171		
Informational	p=1	p=.027	
Retail	p=1	p<.001	p=1

RQ3: Between 2000–2019, were there significant differences among business sectors in the financial damage per DoS attack?

To analyze RQ3, I performed a Kruskal-Wallis test to assess if there were differences among business sectors in financial loss resulting from attacks (Table 9).

Kruskal-Wallis requires at least five observations in each cell; therefore, I omitted the insurance sector. There is a statistically significant difference among business sectors, as determined by Kruskal-Wallis tests ($H(3,92)=20.34$, $p = .00014$). The average financial loss for each sector was as follows: the educational sector average loss was $379,828.9; the financial sector average loss was $2,183,218; the informational sector average loss was $12,046,218, and the retail sector average loss was $28,530,387. I rejected the null hypothesis with 95% confidence that the various sectors' differences are not due to random chance. Financial damages for informational and retail companies were higher than for educational and financial companies. Dunn post hoc contrasts *p* values for pairwise comparisons appear in Table 10 and indicate that the educational sector's financial loss was significantly lower than the financial sector, informational sector, or retail sector. In addition, the loss for the retail sector was higher than the loss for the financial sector.

Table 9
Financial Loss

Groups	*Count*	*Sum*	*Average*
Educational	8	3038631.2	379828.9
Financial	37	80779073.75	2183218.209
Informational	34	409571428.8	12046218.49
Retail	13	370895025.3	28530386.56

$H(3,92)=20.34$, $p = .00014$

Table 10
Kruskal-Wallis Financial Loss (Dunn Contrasts, Pairwise p Values.)

	Educational	Financial	Informational
Financial	p=.029		
Informational	p=<.001	p=.082	
Retail	P<.001	p<.006	p=.163

Correlational Analyses: RQs 4 and 5

I used Correlation analysis for RQs 4 and 5 to measure the degree of a relationship between independent and dependent variables and predict the value of the variable and how one variable affects another (Ciaburro, 2018). I used Spearman Rank-order correlation analysis rather than Pearson product-moment correlation to identify the relationship's strength or the absence of a relationship between independent and dependent variables (Ciaburro, 2018) as the variables displayed a non-normal distribution. To consider the relationship between asset/revenue and duration (RQ4) and asset/revenue and financial damage (RQ5), I first ran Spearman correlations to determine if the sector's asset/revenue correlated to its duration of the attack. Based on this test, I

found that asset/revenue correlates to the sector's financial damage because of DoS attacks. I tested relationships for each of four business sectors: educational, financial, informational, and retail (excluding insurance because there were only two cases). Testing the strength and direction of the relationship took place at an $\alpha < .05$ level of significance. A p-value of $p < .05$ indicated that I can reject the null hypothesis.

RQ4: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and duration of DoS attacks?

Due to missing data on assets for five businesses (specifically one from educational and four from the informational sector), the dataset for Research Question 4 included a total of 95 businesses that had been attacked.

To answer Research Question 4, I had to decide if there was a relationship between the assets/revenues and duration of attack. Table 11 shows the results of the correlation for the duration by assets. The negative coefficient (-.247) means that higher assets correspond to lower duration. The correlation across all sectors is significant as p=.016, meaning that the relationship between assets and duration is significant across sectors. Spearman Correlation Analysis was used to measure the degree of a relationship between assets and duration of attacks. The Coefficient ranges from +1 to -1, with +1 representing a positive correlation and -1 representing a negative correlation. One company from the educational sector had missing data in financial damage and four companies from the informational sector had missing data in the asset and revenue variables. Across all sectors, there is a significant negative correlation between duration and assets. (r_s=-.247, p=.016). Within sectors, there is a significant positive correlation

between duration and assets for financial companies (r_s=.424, p=.008). The higher the assets within the financial sector, the longer the duration of attacks.

Table 11
Spearman Correlations: Duration by Assets

Source	*N*	Correlation	Significance
Financial	38	.424	.008
Informational	32	.245	.176
Retail	14	-.024	.933
Educational	9	.427	.252
All Companies	95	-.247	.016

Note: No analysis was done for Insurance (N=2).

The relation between duration and revenue is negative, meaning that when the revenue is higher, the duration of attacks tends to decrease (r_s=-.162, p=.108) (Table 12). This relationship is not significant; therefore, the null hypothesis cannot be rejected. H_0: There wasn't a significant relationship between company revenues and the duration of DoS attacks.

For duration by revenue, Spearman Correlation Analysis was used to measure the degree of a relationship. There was not a significant relationship between duration and revenue. Retail is highest in correlation (r_s-.438), but not significant (p=.072) due to the small N. The N is low for retail and so even a quite high r_s is not significant.

Table 12
Spearman Correlations: Duration by Revenue

Source	*N*	Correlation	Significance
Financial	37	-.293	.074
Informational	32	.288	.110
Retail	13	-.438	.072
Educational	8	.240	.535
All Companies	99	-.162	.108

Note: No analysis was done for Insurance (*N*=2).

RQ5: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and the financial damage resulting from DoS attacks?

The relationship between the financial damage and assets is negative, meaning that higher assets lead to lower financial damage (Table 13). In addition, the relationship is not statistically significant (p=.164), indicating that the null hypothesis cannot be rejected.

Table 13
Correlations: Financial Damage by Assets

Source	*N*	Correlation	Significance
Financial	35	-.070	.673
Informational	32	.423	.016
Retail	13	.269	.374
Educational	9	.237	.538
All Companies	94	.145	.164

Note: No analysis was done for Insurance (*N*=2).

The relationship between financial damages and revenues is positive, meaning that higher revenues indicate higher financial damages (r_s=.158). However, the results are

statistically insignificant (p=.121). The null hypothesis could be accepted. H_0: There were no significant relationships between company revenues and the financial damage of DoS attacks.

I conducted a Spearman Correlation Analysis of the relationship between financial damage by revenue of business sectors (Table 12). There was not a significant correlation between financial damage and revenues.

Table 14
Correlations: Financial Damages by Revenue

Source	*N*	Correlation	Significance
Financial	37	.072	.668
Informational	31	.200	.273
Retail	12	.114	.623
Educational	7	.110	.777
All Companies	98	.158	.121

Note: No analysis was done for Insurance (N=2).

Summary

The purpose of this chapter was to present the results of the quantitative analyses used to test each of the research questions and hypotheses generated for this study. Three of the research questions were analyzed using Kruskal-Wallis analyses to find significant differences. Spearman correlational analysis was used to examine two of the research questions. Four research questions denoted statistically significant results. Specifically, for Research Question 1, the outcome indicated that there is a significant difference in the rate of attacks between business sectors. The financial and informational sectors are significantly higher in the rate of attacks than the educational sector and retail sectors. The alternative hypothesis was accepted and the conclusion to this question showed the

rate of attacks were different among business sectors. For Research Question 2, the results revealed that there is a significant difference in the duration of attacks among business sectors. The duration of attacks was significantly higher for the educational and informational sectors than for the retail sector or financial sector. For Research Question 3, the results revealed that there is a significant difference in the financial damage of attacks among business sectors. The educational sector's financial loss was significantly lower than the financial sector, informational sector, or retail sector. In addition, the loss for the retail sector was significantly higher than the loss for the financial sector.

In the first, second, and third research questions, the null hypotheses were rejected. This indicates there are statistically significant differences in the severity of the DoS attacks regarding rate, duration, and financial damage for educational, financial, informational, and retail sectors.

The fourth research question involved looking at the correlations of assets and revenues with duration of attacks. The correlation between assets and duration across all sectors is negative and significant (r_S=-.247, p=.016), meaning lower assets correspond to greater duration of attacks. Within sectors, there is a significant positive correlation between duration and assets of financial companies (r_s=.424, p=.008). As such, greater assets correspond to greater duration of DOS attacks for financial companies. There was not a significant relationship between duration and revenue.

The fifth research question involved examining the correlations of assets and revenues with financial damages resulting from attacks. There were no significant relationships between assets or revenues and financial damages.

In Chapter 4, I included an introduction, description of data collection, report of data analysis and findings of the study, and the summary of the chapter. Chapter 5 provides an interpretation of the findings presented in this chapter. Chapter 5 also includes discussion, an elucidation of the limitations of the study, implications, and recommendations for further research and includes implications for positive social change. Finally, Chapter 5 includes conclusions of the study.

Chapter 5: Discussion, Conclusions, and Recommendations

In this chapter, I discuss the research findings and offer conclusion and recommendations based on these findings. As described in Chapter 1, this study contributes to the theoretical understanding of targeted business sector attacks with DoS, as existing studies remain limited. At the same time, the advances in Internet technology over the last several decades have resulted in ever more cyber-security attacks (Harris & Maymi, 2016; Lee, 2013). Targeted DoS attacks have become more sophisticated and more challenging to defend against. Existing research has recorded increases in annual recurring attacks; however, little research has examined the different rates at which business sectors are targeted with DoS attacks, and, at the time of this study, there are few or no published research articles on the relationship between the values held and generated by the business sectors and DoS attacks. The purpose of the study was to fill the gap in literature by exploring DoS attacks in the U.S. from 2000 to 2019, to identify significant differences among business sectors in the rate, duration, and financial damages/loss resulting from DoS attacks, and to examine the relationships between business sectors' assets/revenues and attack duration as well as financial damages resulting from DoS attacks.

My objective was to answer the five research questions. In addition to conducting quantitative analysis to answer these questions, I used Cohen and Felson's (1979) RAT and Cornish and Clarke's (1987) RCT as theoretical frames for examining the data in relation to the research questions. These theoretical models have been valuable in

analyzing the attractiveness of particular business sector types and business values, which could make them more likely to be targeted.

The results of the study indicated there is a significant difference among business sectors in the rate of DoS attacks, in the duration of attacks, and in financial damages, as determined by Kruskal-Wallis tests. The Dunn post hoc comparisons indicated that the financial sector and informational sector are significantly higher in rate of attacks than the educational sector and retail sector. In addition, the Dunn post hoc comparisons indicated that the duration of attacks was significantly higher for the educational sector and informational sector than for the retail sector or financial sector. Financial damages were significantly higher for the informational and retail sectors than for the educational or financial sectors. Spearman correlation analysis was used to measure the degree of a relationship between duration of attacks and financial damages and asset/revenues. Across all sectors, there is a significant negative correlation between duration of attacks and company assets. (r_s=-.247, p=.016), and within sectors, there is a significant positive correlation between duration of attacks and assets for financial companies (r_s=.424, p=.008). However, the result indicated no evidence of relationships between revenues and duration of attacks or asset/revenue and financial damage resulting from attacks.

Interpretation of Findings

I employed quantitative analysis techniques to determine whether there were significant differences in rate, duration, and damage of attacks among business sectors and to determine whether there was a relationship between assets/revenues and attack durations and financial damage resulting from DoS attacks. I designed the quantitative,

ex post facto study to answer five research questions. This section is organized to present the findings of each of the research questions in relation to existing literature on DoS attacks and in relation to the RAT and RCT theoretical foundations that were derived from prior criminological studies in order to better understand the motivation of attackers.

Research Question 1

RQ1: Between 2000–2019, were there significant differences among business sectors in the rate of DoS attacks?

$H_0$1: Between 2000–2019, there were no significant differences among business sectors in the rate of DoS attacks.

H_a1: Between 2000–2019, there were significant differences among business sectors in the rate of DoS attacks.

The results of the Kruskal-Wallis test indicated the overall differences among sectors were significant (H (3,400) =39.22, p<.001)). The number of cases was highest in the financial sector at 38 followed by the informational sector at 37 while retail recorded only 14 cases. The null hypothesis is rejected with 95% confidence that the differences among the various sectors is not due to random chance.

With the exception of a few studies (e.g. Bendovschi et al. (2016), Leukfeldt and Yar (2016), and O'Leary et al. (2017)), there is a gap in the research literature whether attackers target some business sectors with DoS more than they target others. In this study, I found that there are statistically significant differences in attack rates among five business sectors. The results revealed that the financial sector is the preferred choice

among the five sectors for targeting attackers. This could be attributed to Romanosky (2016)'s finding that organizations in the financial sector were the most vulnerable to attacks. Further, Leukfeldt and Yar (2016) found that online financial business sectors' high visibility plays a role in cyber-crime victimization. The results from this study add evidence to the existing literature that suggests financial companies are targeted in DoS attacks.

I interpreted the results from this study according to RAT and RCT theoretical frameworks, which indicate that because attacks are not distributed equally, attackers are more inclined to attack specific targets. Specifically, the results suggest there is a higher motivation for attacks within the financial sector and the informational sector. According to Décary-Hetú and Dupont (2012), attackers target companies' defense weaknesses in software. In other words, an attacker uses Internet opportunity (its remoteness of the victim) and a lack of cyber security defense in order to target companies. The findings from this study could be interpreted as evidence that frequent attacks indicate a lack of security defense, allowing for opportunities for attack, which influence attackers' decisions and motivations.

Research Question 2

RQ2: Between 2000–2019, were there significant differences among business sectors in the duration of DoS attacks?

$H_0$2: Between 2000–2019, there were no significant differences among business sectors in the duration of DoS attacks.

H_a2: Between 2000–2019, there were significant differences among business sectors in the duration of DoS attacks.

The results of the Kruskal-Wallis test indicated that there is a statistically significant difference among business sectors in duration of attacks *(*H(3,98)=10.69), p = 0.014). The duration for the informational and educational sectors were significantly higher than the duration for financial or retail sectors; however, the other differences were not significant due to small sample size. The null hypothesis is rejected with 95% confidence that the variance between the various sectors is not due to random chance.

There is no existing published research on the duration of attacks among business sectors. As such, the findings from this study work to fill the gap in the research literature about whether some business sectors are more vulnerable to longer DoS attacks. This study found that there are statistically significant differences in attack durations. The two theoretical frames for this study, RAT and RCT, emphasize the role of attackers' choices and opportunities when making decisions about whether to attack targets. One interpretation of the statistically significant differences in duration of attacks among business sectors is that offenders chose to attack the educational and informational targets for longer periods. In the case of this finding, the theories might be extended to indicate that the lack of a capable guardian might lead to longer attacks.

Research Question 3

RQ3: Between 2000–2019, were there significant differences among business sectors in the financial damage per DoS attack?

$H_0$3: Between 2000–2019, there were no significant differences among business sectors in the financial damage per DoS attack.

H_a3: Between 2000–2019, there were significant differences among business sectors in the financial damage per DoS attack.

The results of the Kruskal-Wallis test indicated that there is a statistically significant difference among business sectors ($H(3,100)=18.73$, $p = .0003$). The average financial loss for the retail sector and informational sector was higher than the average financial loss for other sectors, and the average financial loss for the educational sector was significantly lower, likely because educational institutions are not dependent on online (Internet) business for their revenues (tuition). The null hypothesis is rejected with 95% confidence that the differences among the various sectors are not due to random chance.

There were an alarming number of DoS attacks aimed at major U.S. business sectors between 2000-2019. These attacks resulted in financial damages for all types of businesses, but for specific business sectors the damages were greater. Financial damage refers to a negative effect on the asset values by denying services through the DoS attack. As companies are highly dependent on an Internet connection, service interruptions can interfere with business activities (revenue) and can be devastating to the business. According to Arora, Dumar, and Sachdeva (2011), the financial impact of attacks can be devastating to a business, and a few hours of network service interruption can be costly to a company. Financial damages include tangible losses, lost revenue, and other types of

damages (Palekiene et al., 2014). For this study, damages were the monetary value of losses caused by DoS online business interruption.

The results from this study indicated that the retail sector and informational sector experienced greater financial damages than other sectors. Because retail sectors are often dependent on online sales, service interruptions are likely to result in significant losses. The high financial damages caused by attacks could be a motivating factor for attackers. The findings could also be interpreted as evidence that certain sectors are vulnerable to financial damage.

Research Question 4

RQ4: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and duration of DoS attacks?

$H_0$4: Between 2000–2019, within sectors, there were no significant relationships between company assets and/or revenues and the duration of DoS attacks.

H_a4: Between 2000–2019, within sectors, there was a significant relationship between company assets and the duration of DoS attacks.

H_b4: Between 2000–2019, within sectors, there was a significant relationship between company revenues and the duration of DoS attacks

The results of the Spearman's correlation analysis indicated there was a significant relationship between duration of attacks and assets. The negative coefficient (-.247) means that higher assets correspond to lower duration. The correlation across all sectors is significant as p=.016, meaning that the relationship between assets and duration is significant across sectors. Within sectors, there is a significant positive correlation

between duration and assets for financial companies (r_s=.424, p=.008); the higher the assets within the financial sector, the longer the duration of attacks.

The relation between duration and revenue is negative, meaning that when the revenue is higher the duration of attacks tends to decrease (r_s=-.162, p=.108) (Table 9). This relationship is not significant and the null hypothesis can be accepted.

As businesses or industries are categorized according to the type of their economic activities, assets and revenues are fundamental elements of business sectors. Assets are resources with economic value that the business owns and that are recorded in companies' balance sheets (Siegel, Dauber, & Shim, 2005). In relation to this study, Leukfeldt and Yar (2016) noticed that value has a financial character and cyber-attackers are interested in assigned value. The concept of a suitable target in RAT is a combination of value and opportunity

According to Cohen and Felson (1979) and Cornish and Clarke (1986), (the founders of the research theories RAT and RCT), attackers make a choice to commit a crime based on opportunity, a lack of guardian, motivation, and attractiveness of the targets. Within the financial sector, there is a significant positive correlation between duration of attacks and company assets. The relation indicates that businesses with higher assets in the financial sector were the target of longer attacks, which is likely based on the attractiveness of the target and the opportunity to attack. In other words, the higher the value of the company within the financial sector, the higher the motivation of attackers.

Research Questions 5

RQ5: Between 2000–2019, within sectors, were there significant relationships between company assets and/or revenues and the financial damage resulting from DoS attacks?

$H_0$5: Between 2000–2019, within sectors, there were no significant relationships between company assets and/or revenues and the financial damage of DoS attacks.

H_a5: Between 2000–2019, within sectors, there was a significant relationship between company assets and the financial damage resulting from DoS attacks.

H_b5: Between 2000–2019, within sectors, there was a significant relationship between company revenues and the financial damage resulting from DoS attacks.

The results of the Spearman's correlational analysis indicated that the relationship between financial damages and company assets is negative, meaning that higher assets indicate lower financial damages (Table 13). However, the relationship is not statistically significant (p=.164); therefore, the null hypothesis cannot be rejected.

The relationship between financial damages and company revenues is positive, meaning that higher revenues indicate higher financial damages (r_s=.158). However, the results are statistically insignificant (p=.121). The null hypothesis can be accepted.

Previous published research has not focused on revenues and assets aside from confirming that DoS attacks lead to a loss of profits (Anderson et al., 2013). Researchers have not investigated the role of financial metrics in determining business sectors and target candidates for cyber-attack. Tajalizadehkhoob et al. (2014) drew upon RAT to

describe why criminals go after a certain target and examined DoS attacks through the lens of the economics of crime, but they did not categorize targets by assets or revenues.

Based on the findings from this study, I could not reject the null hypotheses in relation to assets/revenue and financial damage. However, research that focuses on business sector attractiveness and targets, damages, and sector types are valuable to creating financial metrics that can help predict the likelihood for attacks.

According to RAT and RCT, attackers make choices to attack based on target attractiveness and opportunity, and they rationally consider the positive or negative valuation of potential attack results. Taken together, the results from this study suggest that DoS attack rates are higher in the financial sector and that financial companies with higher assets experience attacks of a longer duration. The financial sector is likely seen as a suitable target that offers opportunities for attacks and positive results for attackers. Similarly, the informational sector experienced significantly more attacks of a longer duration and resulting in higher financial damages. Again, these findings suggest that companies in this sector are seen as suitable targets, offering both attractiveness and opportunity to attackers. The educational sector experiences longer durations of attacks but the financial damages are lower in comparison to other sectors. Because educational sectors are not dependent on online (Internet) business for their revenues (tuition), as retail and other sectors are, the financial damage effect is lower, suggesting that the motivation for attacks is not purely about (financial) gains but also includes considerations of lower risks (weaker defenses). Finally, the retail sector suffered the highest financial damages but had lower rates and durations of attacks. These results

show that some sectors are more vulnerable to high financial damages but may not be as attractive to attackers.

Limitations of the Study

The most significant limitation of this study was use of nonparametric tests. The proposal called for using 1-way ANOVAs and Pearson correlational analysis to answer the research questions, but the data violated the assumption of normality. Kruskal-Wallis tests were substituted for ANOVAs, and Spearman rank-order correlation was substituted for Pearson product-moment correlation. Nonparametric tests are less robust; as a result, null hypotheses should be rejected with caution.

In addition to sample size of the business sector groups, a limitation of nonexperimental quantitative research is lack of ability of the researchers to control the atmosphere in which the data were gathered from the archival database. These limitations were introduced in Chapter 1, and they allow for recommendations for further studies, which will be discussed later in this chapter.

There is no national database recording information on the rate of attack, duration of attack, and financial loss caused by DoS attacks. Collecting complete information about targeted business sectors with DoS attacks is not straightforward; some institutions, businesses, organizations, and agencies did not make these data publicly available. The lack of precise and definite incident reports makes precise equilibrium calculations difficult. Finding asset and revenue data, specifically from information companies was a challenge. There was the possibility of missing important data (variables). The process of

determining the precise rate of attacks, duration of attacks, and financial losses arising from DoS can be difficult.

Collecting all possible data on every attempt of DoS attack from all organizations is impractical. As such, the data in this study are limited to five business sectors in the U.S. Additionally, the study was limited to U.S. companies that had data on DoS attacks analytics and company incident reports for the years 2000-2019 and The data that have not been reported and collected limits the study. Due to the shortcoming of resources and inconsistent information, this research used various websites. Specifically, the findings of this study cannot be generalized outside of the U.S. or outside of the five business sectors included in the study design.

Despite the difficulties of obtaining data and precise reports, this research method has more depth of information but less generalization proficiency. Despite the challenging process of collecting data, and the resultant limitations, this research may be significant to security practitioners and business leaders and contribute new ideas in the young cyber security research field.

Recommendations

Cyber security attacks have become more problematic and are often bewildering because of their increased complexity. It has been difficult to find precise theory and protective systems that address the complexity of these attacks. The interconnected nature of IT systems has limited the possibility of controlling attacks. Previous research on the method and technique of DoS attacks has not yet resulted in a theory of the motivations of targeted attacks. Further research is needed that incorporates multiple disciplines, such

as sociology, psychology, information systems, and economics in order to comprehend the motivations of attackers and targeting metrics and to design appropriate approaches to protect businesses and groups against these attacks.

Due to the difficulty of obtaining reliable data, this study was limited to five business sectors, and one of those sectors could not be included in all of the statistical tests due to low population size. Further research could include more business sectors and more businesses or organizations in the U.S. to ensure the accuracy of the study. Such studies might require different data collection procedures. Because DoS attacks are but one type of cyber-security threat, it would be worthwhile to replicate this study with malware breach attacks and to potentially expand it to include more companies and possibly various countries.

Finally, there are no consistent, unified, and broadly accepted theories in the literature about why cyber security attackers attack businesses and there are no clear and applicable approaches to protecting business sectors from DoS attacks. Future research could employ additional theoretical frames, in addition to RAT and RCT, to study and understand the relationship between attackers and defenders.

This research disclosed several findings resulting in possible professional recommendations that security practitioners and business managers may find pertinent. The study showed that the financial sector and informational sectors were the most targeted business sectors with DoS attacks. Moreover, the retail sector and informational sector suffered the largest financial damages. Finally, informational and educational sectors experienced the longest duration of attacks. Identifying targeted sectors allows

professional to take appropriate countermeasures and to erect extra layers of protection to safeguard businesses.

To overcome the limited use of reported archival public data, researchers need to combined research techniques to and aim for a more in-depth inquiry. For example, data could be collected from security defenders as well as from attackers to ensure that only professionals who met the study's criteria provided data. Designing and using theory by obtaining data on attackers' tactics and strategies and business' defensive tactics and strategy (between attacker and defender) can be suitable for framing the recursive relationship. Accordingly, recommendations for future comprehensive research are as follows: examine the larger samples, collect data from attackers, and defenders, include all businesses in the study, and consider longitudinal studies.

Implications

For two decades, the growth of complex DoS attacks on business sectors has corresponded directly with the growth of the Internet and its use within diverse services. DoS attacks targeted the availability of services, disrupted online access, disabled computer functions, and controlled computing systems remotely (Harris & Maymi, 2016). Though protecting companies from targeted DoS attacks is a challenging task that requires diligence and ingenuity, businesses, organizations, and cyber security professionals have the legal obligation to protect network communications and defend against financial losses from attackers. Crucial to tackling DoS attacks is not only technical know-how but also the ability to identify the most targeted business sectors and the metrics of attacks.

This study serves as a common starting point for further discussion and investigation, while informing a basic and an effective cyber security approach. Leaders of cyber security defenders not only need to trace technological advancement of attack tools to bridge the gap between attacks and defense but also need to identify which business sectors are more targeted (victims) and understand thoroughly the persistent motivation for targeted attack metrics. This study offers positive social change that impacts business sectors with DoS attacks and the population in general by increasing understanding of the motivation behind targeted attacks and improving the protection system (countermeasures) of businesses. The information from this research affects social change by presenting business leaders with information crucial to decision-making in relation to cyber security.

The nature of the research questions called for a quantitative method of research to investigate the problem. Selecting quantitative inquiry for data collection and analysis for cyber- security attacks with DoS, targeting companies, and rate of attacks research was indispensable as it facilitated the understanding of relationships and associations among the variables (Neuman, 2006). The financial metrics that explains how attackers collectively target companies with DoS attacks was statistically evaluated. This study shows there is a significant difference in the financial damage of attacks among business sectors. The implications of financial damage could potentially impact investors and cause customer fear.

In this dissertation, I conducted an analysis of targeted attacks using DoS and a cyber security related literature review used combined theories (RAT and RCT) to

examine cybercrime as an outcome of a continual interaction between a criminal's desires and target preferences (Cornish & Clarke, 2008). These theories may assist researchers and security professionals in considering and identifying the metrics of sectors targeted with DoS attacks.

This research is intended to address the gap in literature through its research design, analytical methods, and results. The outcomes of this research are beneficiary to business administration and to diverse fields. The findings of this research contribute information to agencies and organizations and could trigger scholars to further research the issues raised in the study. The findings of the study, that there are significant differences in the rate, duration, and financial damages of attacks between business sectors and that there is a significant relationship between the duration of attacks and assets, have the potential for positive social change on students, researchers, agencies, and organizations, which in turn can be utilized to design techniques and program mechanism towards understanding the targeting metrics and motivation of security attackers. The results from my research analysis have numerous implications for measuring and constructing standards for non-traditional forms of research for advancements in the cyber security field of study.

Conclusion

The exponential growth of Internet technology that enables businesses and organizations connectivity across the globe has led to an increase in DoS attacks. DoS attacks are formidable techniques that deplete the availability of the targeted companies' networking systems. Since 2000, in the U.S., business sectors were targeted with DoS

attacks at an increasing rate of occurrence and cost. Combating cyber-attacks costs organizations billions annually. In the U.S. businesses/organizations have experienced the burden of DoS attacks. DoS attack threats pose a serious risk to business activities. It was important to find and understand differences among business sectors in attack rates, duration of attacks, and financial damages as well as the relationship between company assets and revenues and the duration of attacks and the financial damages resulting from attacks.

This research was conducted in order to determine whether there were differences among business sectors in the rate and duration of attacks and in financial loss/damages as a result of DoS attacks. The second aim was to determine whether there were relationships between business sector's assets/revenues and the duration of attacks and financial damages as a result of DoS attacks. The analyses resulted in the identification of the differences of the rate, duration, and financial damage at which companies in each sector are targeted with DoS attacks. Findings from the Kruskal-Wallis test analyses indicated statistically significant differences among business sectors in the rate of attacks and duration of attacks as well as financial damage caused by DoS attacks. The correlation between assets and duration across all sectors is negative and significant (r_s=.247, p=.016,) except within the financial sector in which there is a significant positive correlation between duration of attacks and assets (r_s=.424, p=.008). In other words, greater assets correspond to a greater duration of DoS attacks. The Spearman's correlation indicated that there was not a significant relationship between duration and revenue or assets/revenue and financial damage.

While no one measure can entirely prevent all possible attacks, in order to efficiently manage network (online service) accessibility and reduce the rate of attack, duration, and financial damages resulting from DoS attack, business managers and cyber security professionals should continuously evaluate targeted metrics and implement appropriate preemptive measures that reduce the impact of coordinated DoS attacks on the system and other business information activity.

References

Adebiaye, R., Alryalat, H., & Owusu, T. (2016). Perspectives for cyber-deterrence: A quantitative analysis of cyber threats and attacks on consumers. *International Journal of Innovative Research in Science, Engineering and Technology, 5*(7). doi:10.15680/IJIRSET.2016.0507157 12946

Adomi, E. E. (2011*). Handbook of research on information communication technology policy: Trends, issues and advancements* (vol. 1). Hershey, PA: IGI Global.

Agbogun, J. B., & Ejiga, F. A. (2013). Network security management: Solution to network intrusion related problems. *International Journal of Computer and Information Technology*, *2*(4). Retrieved from http://www.ijcit.com/archives/volume2/issue4/Paper020412.pdf

Akamai (2015). *Faster forward to the latest global broadband trends*. Retrieved from https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/2015-q1-internet-security-report.pdf

Alomari, E., Manickam, S., Gupta, B. B., Karuppayah, S., & Alfaris, A. (2012). Botnet-based distributed denial of service (DDoS) attacks on web servers: Classification and art. *International Journal of Computer Applications, 49*(7), 24-32. doi:10.5120/7640-0724

Amro, S., & Alkhalifah, A. (2015). A comparative study of virus detection techniques. *International Journal of Computer, Electrical, Automation, Control and Information Engineering, 9*(6). Retrieved from

https://waset.org/publications/10002328/a-comparative-study-of-virus-detection-techniques

Amoroso, E. (2011*). Cyber attacks: Protecting national infrastructure.* Burlington, MA: Butterworth-Heinemann

Amoroso, E. (2013). *Cyber attacks: Protecting national infrastructure*. Waltham, MA: Elsevier.

Anderson, K. M., & Paterson, M. (2015). Overview of secondary data analysis with a description of heart failure hospitalizations from the national hospital discharge survey. *Clinical Scholars Review, 8*, 130-138. doi:10.1891/1939-2095.8.1.130

Anderson, R., Barton, C., Bohme, R., Clayton, R., Eeten, M. J., Levi, M., Moore, T., … Savage, S. (2013). Measuring the cost of cybercrime. In R. Bohme (Ed.), *Economics of information security and privacy* (pp. 265-300). Heidelberg, Berlin: Springer.

Andress, J. (2011). *The basics of information security: Understanding the fundamental of infoSec in theory and practice.* Waltham, MA: Elsevier.

Andress, J., & Winterfeld, S. (2014). *Cyber warfare: Techniques, tactics, and tools for security practitioners* (2nd ed.). Waltham, MA: Syngress.

Anstee, D. (2013). Q1 findings from Atlas. *Arbor Networks*. Retrieved from http://www.arbornetworks.com/corporate/blog/4855-q1-key-findings-from-atlas

Arora, K., Kumar, K., & Sachdeva, M. (2011). Impact analysis of recent DDoS attacks. *International Journal on Computer Science and Engineering, 3*(2), 877-884. Retrieved from http://www.enggjournals.com/ijcse/doc/IJCSE11-03-02-093.pdf

Ary, D., Jacobs, L. C., & Sorensen, C. K. (2010). Introduction to research in education (8th ed.). Belmont, CA: Wadsworth.

Avellar, S. A., Thomas, J., Kleinman, R., Samal-Miller, E., Woodruff, S., Coughlin, R., …Westbrook, R. T. (2016). External validity: The next step for systematic reviews? *Evaluation Review, 1*, 1-43. doi:10.1177/0193841X16665199

Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminology, 4*(1&2). Retrieved from https://pdfs.semanticscholar.org/bf09/3c90e7cba8c50b1244db02902973f3f5d89pdf

Ballora, M., Giacobe, N. A., McNeese, M., & Hall, D. L. (2012). Information data fusion and computer network defense. In C. Onwubiko & T. Owens (Eds.), *Situational awareness in computer network defense: Principles, methods and applications* (pp. 141-164). Hershey, PA: IGI Global.

Banerjee, U., Vashishtha, A., & Saxena, M. (2010). Evaluation of the capabilities of Wirehark as a tool for Intrusion detection. *International Journal of Computer Applications, 6*(7), 1-5. doi:10.5120/1092-1427a

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, *76*, 169-217. doi:10.1086/259394

Behal, S., & Kumar, K. (2017). Characterization and comparison of DDoS attack tools and traffic generators - a review. *International Journal of Network Security, 19*(3), 383-393. doi:10.6633/IJNS.201703.19(3).07

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance, 28,* 24-31. doi.org/10.1016/S2212-5671(15)01077-1

Bendovschi, A., Al-Nemrat, A., & Ionescu, B. S. (2016). Statistical investigation into the relationship between cyber-attacks and the type of business sectors. *International Journal of Business, Humanities and Technology, 6*(1), 49-61.

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices* (2nd ed.). Tampa, FL: Created Space Independent Publisher Platform.

Blau, P. M. (1964). *Exchange and power in social life*. New York, NY: John Wiley.

Bolden, M., & Nalla, M. (2014). *Theorizing cybercrime: Applying routine activities theory*. Retrieved from http://www.academia.edu/8897451/Theorizing_Cybercrime_Applying_Routine_Activities_Theory

Bondarenko, P. (2014). *Revenue economics*. Retrieved from https://www.britannica.com/topic/revenue-economics

Bonner, L. (2012). Cyber risk: How the 2011 Sony database breach and the need for cyber risk insurance policies should direct the federal response to rising data breaches. *Washington University Journal of Law & Policy*, *40*(257). Retrieved from http://digitalcommons.law.wustl.edu/cgi/viewcontent.cgi?article=1581&context=wujlp

Bosworth, S., & Kabay, M. (Eds.) (2002). *Computer Security Handbook* (4th ed.). New York, NY: John Wiley & Sons.

Bosworth, S., Kabay, E. M., & Whyne, E. (Eds). (2014). *Computer security handbook* (6th ed., vol. 1). Hoboken, NJ: John Wiley& Sons.

Bragg, S. (2017). *Fixed asset accounting* (4th ed.). Centennial, CO: Accounting Tools.

Brenner, B. (2015). Q4 2014 State of the Internet—Security Report: Numbers, *Acamai.com*. Retrieved from https://blogs.akamai.com/2015/01/q4-2014-state-of-the-internet---security-report-somenumbers.html

Bryman, A., & Bell, E. (2015). *Business research methods*. Oxford, United Kingdom: University Press

Buldas, A., Laud, P., Priisalu, J., Saarepera, M., & Willemson, J. (2006). *Rational choice of security measures via multi-parameter attack trees*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.4560&rep=rep1&type=pdf

Burns, T. R., & Roszkowska, E. (2016). Rational choice theory: Toward a psychological, social, and material contextualization of human choice behavior. *Theoretical Economics Letters*, *6*(2), 195-207. doi:10.4236/tel.2016.62022

Cameron, & Kornhauser, L. (2015). Rational choice attitudinalism? European Journal of Law and Economics,, 43(3).doi: 10.1007/s10657-015-9512-1

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy, 2*(1).

Chabinsky, S. R. (2010). Cyber security strategy: A primer for policy makers and those on the front. *Journal of National Security Law &Policy*, *4*(1), 27-40. Retrieved

from http://jnslp.com/2010/08/13/cybersecurity-strategy-a-primer-for-policy-makers-and-those-on-the-front-line/

Chapple, M., & Seidl, D. (2015*). Cyberwarfare: Information operations in a connected world.* Burlington, MA: Jones & Bartlett Learning.

Carcello, J. (2008). *Financial & managerial accounting.* New York, NY: McGraw-Hill Irwin.

Carter, R., & Lubinsky, J. (2016*). Rehabilitation research: Principles and applications* (5th ed.). St. Louis, MO: Elsevier

Cayubit, R., Rebolledo, K., Kintanar, R., Pastores, A., Santiago, A., & Valles, P. (2017). *Psychological Studies*, 62 (4), 386-384. Doi:10.1007/s12646-017-0423-9.

CFI. (2018). *Types of assets*. Retrieved fromhttps://corporatefinanceinstitute.com/resources/knowledge/accounting/types-of-assets

Chu, B., & Holt, T. J. (2015). *Examining the creation, distribution, and function of malware on-line*. Washington, DC: Scholar's Choice.

Chu, B., Holt, T. J., & Ahn, G. J. (2010). *Examining the creation, distribution, and function of malware on-line* (NIJGrant No. 2007-IJ-CX-0018). Washington, DC: National Institute of Justice. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/230111.pdf

Ciaburro, G. (2018). Regression Analysis with R: Design and Develop Statistical Nodes to Identify Unique Relationships Within Data at Scale. Liberty Place Birmingham, UK: Packt Publishing Ltd.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice, 6*, 147-185. doi:10.1086/686041

Clarke, R. V., & Cornish, D. B. (2001). Rational choice. In R. Paternoster & R. Bach man (Eds.), *Explaining criminals and crime: Essays in contemporary criminological theory* (pp. 23-42). Los Angeles, CA: Roxbury.

Clarke, R. A., & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it.* New York, NY: HarperCollins.

Clifford, R. D. (2011). *Cybercrime: The investigation, prosecution and defense of a computer-related crime* (3rd ed.). Durham, NC: Carolina Academic Press.

Claude, A., & Siponen, M. (2014). *Toward a rational choice process theory of internet scamming: The offender's perspective*. Thirty Fifth International Conference on Information Systems, Auckland: New Zealand, 2014. Retrieved from https://pdfs.semanticscholar.org/9b8a/d31d762a64f944a780c13ff2d41b9b4f3ab3.pdf

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

Coleman, E. G. (2013). *Coding freedom: The and the ethics and aesthetics of hacking*. Princeton, NJ: Princeton University Press.

Coleman, J. (1973). *The mathematics of collective action*. London, England: Hienemann.

Conrad, E., Misenar, S., & Feldman, J. (2015). *CSSI study guide* (3rd ed.). Waltham, MA: Syngress.

Cook, K. S. (1977). Exchange and power in networks of interorganizational relations. *Sociological Quarterly*, *18*, 62-82. doi:10.1111/j.1533-8525.1977.tb02162.x

Cornish, D., & Clarke, R. (1986). *The reasoning criminal: Rational choice perspectives on offending*. New York, NY: Springer-Verlag.

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, *25*(4), 933–947. doi:org/10.1111/j.1745-9125.1987.tb00826.x

Cornish, D. B., & Clarke, R. V. (2008). *The rational choice perspective: Environmental criminology and crime analysis*. Portland, OR: Willan Publishing.

Cyber Security Enhancement Act. (2005). Congressional Bills 109th Congress H.R. 285 Introduced in House (IH). Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS-109hr285ih/html/BILLS-109hr285ih.htm

D'Arcy, J., & Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics, 89*, 59-71.

Décary-Hetú, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160-175. doi:org/10.1080/17440572.2012.702523

DePoy, E., & Gitlin, L. (2011). *Introduction to research understanding and applying multiple strategies* (4th ed.). St. Louis, MO: Elsevier.

Derrick, B., Ruck, A., Toher, D., & White, P. (2018). Tests for equality of variances between two samples which contain both paired observations and independent observations. *Journal of Applied Quantitative Methods, 1*(2), 36–47.

Dietrich, S., Long, N., & Dittrich, D. (2000, December). *Analyzing distributed denial of service tools: The Shaft case*. USENIX Association, Proceedings of the 14th Systems Administration Conference (LISA 2000). New Orleans, Louisiana, Retrieved from https://www.usenix.org/legacy/events/lisa00/full_papers/dietrich/dietrich_html/

Downess, D., Rock, P., & McLaughlin, E. (2016). *Understanding deviance: A guide to the sociology of crime and rule-breaking* (7th ed.). New York, NY: Oxford University Press.

Dzurenda, P. (2015). Network protection against DDoS attacks. *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems, 4*(1). doi:org/10.11601/ijates.v4i1.103

Edmonds, W., & Kennedy, T. D. (2013). *An applied reference guide to research designs: Quantitative, qualitative, and mixed methods*. Thousand Oaks, CA: Sage.

Exum, L. M., & Layana, C. M. (2016). A test of the predictive validity of hypothetical intentions to offend. *Journal of Crime and Justice, 41*(2). doi:org/10.1080/0735648X.2016.1244486

Felson, M. (1986). Routine Activities, Social Controls, Rational Decisions, and Criminal Outcomes. In D. Cornish and R.V.G. Clarke (Eds.), *The reasoning criminal,* (pp. 119-128). New York, NY: Springer-Verlag.

Felson, M. (1987). Routine activities and crime prevention in the developing metropolis. *Criminology, 25*, 911-93.

Felson, M., & Boba, R. (2010). *Crime and everyday life* (4th ed.). Thousand Oaks, CA: Sage.

Forbes. (2018). *America's largest public companies*. Retrieved from https://www.forbes.com/top-public-companies/list/#tab:overall

Freilich, J. D. (2015). Beccaria and situational crime prevention. *Criminal Justice Review, 40*(2). doi:10.1177/0734016814550815

Frohlich, T., & Comen, E. (October 8, 2016). America's fastest growing companies. *USA Today*. Retrieved from https://www.usatoday.com/story/money/business/2016/10/08/americas-fastest-growing-companies/91728104/

Fuchs, C. (2010). Labor in informational capitalism and on the Internet. *Information Society, 26,*179-196. doi:org/10.1080/01972241003712215

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers and Security, 24*(1) 31-43. doi:org/10.1016/j.cose.2004.06.011

Harris, S., & Maymi, F. (2016). *CISSP all-in-one exam guide* (7th ed.). New York, NY: McGraw Hill & Osborne.

Harrison, A. (2000). Cyberassaults hit Buy.com, eBay, CNN and Amazon. *Computerworld.* Retrieved from https://www.computerworld.com/article/2593369/cyberassaults-hit-buy-com--ebay--cnn-and-amazon.html

Hassan, M. H., Reza, M. D., & Farkhad, A. M. (2015). An experimental study of influential elements on cyberloafing from general deterrence theory perspective

case study: Tehran subway organization. *International Business Research, 8*(3). doi:10.5539/ibr.v8n3p91

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., … Spiegel, J. (2012). Law of cyber-attack. *California Law Review*, *100*, 817-886. Retrieved from http://www.californialawreview.org/

Hill, B. J., & Marion, E. N. (2016). *Introduction to cyber crime: Computer crimes, laws, and policing in the 21st century*. Santa Barbara, CA: Praeger. https://www.youtube.com/watch?v=_FuLMEenUmU

Hinton, P., McMurray, I., & Brownlow, C. (2014). *SPSS Explained* (2nd ed.). New York, NY: Routledge.

Hoffer, J. A., & Straub, D. W. (1989*).* The 9 to 5 underground: Are you policing computer crimes? *Sloan Management Review*, *30*(4), 35-44. Retrieved from https://mit-sloan-management-review.com-sub.biz/?gclid=COm5-82_xdMCFUMdaQodDXsP7A &gclsrc=aw.ds

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety, 15*, 69-79. doi:10.1057/cpcs.2012.14

Holosko, M. J., Jolivette, K., & Houchins, D. E. (2014). Reporting guidelines for intervention and evaluation research conducted in juvenile and adult corrections: A guide for better quality and uniform standardization. *Journal of Correctional Education*, *65*(3), 66-89. Retrieved from

https://www.ashland.edu/founders/programs/correctional-education/journalcorrectional-education

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31*(2), 165-177. doi:10.1177/0894439312452998

Holt, T. J. (2017). (Ed.). *Cybercrime through an interdisciplinary lens*. New York, NY: Routledge.

Holt, T. J., & Bosler, M. A. (2013). Examining the relationship between routine activities infection indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420-436. doi:10.1177/1043986213507401

Holt, T. J., & Bossler, M. A. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior 35*(1). doi:10.1080/01639625.2013.822209

Homans, C. G. (1961). *Social behavior: Its elementary forms*. New York, NY: Harcourt, Brace and World.

Hoque, N., Bhuyan, H. M., Baishya, C. R., Bhattacharyya, K. D., & Kalita, K. J. (2014). Network attacks: Taxonomy, tools and systems. *International Journal of Network and Computer Applications*, *40*(1), 307-324.

Hostettler, J. (2011). *Cesare Beccaria; The genius of 'on crime and punishments.'* London: Waterside Press

Hughes, J., & Cybenko, G. (2013). Quantitative metrics and risk assessment: The three tenets model of cybersecurity. *Technology Innovation Management Review,3*(8), 15-24. Retrieved from http://timereview.ca/article/712

Hunter, N. B. (2016). *The power of KM harnessing the extraordinary value of knowledge management*. San Francisco, CA: Spirit Rising Productions.

Hutchings, A. (2014). Crime from the keyboard: Organized cybercrime, co-offending, initiation and knowledge transmission. *Crime, Law & Social Change, 62*(1), 1-20. http://dx.doi.org/10.1007/s10611-014-9520-z

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimization: Who gets caught in the net? *Current Issues in Criminal Justice, 20*(3). Retrieved from http://www.austlii.edu.au/au/journals/CICrimJust/2009/6.html

Identity Theft Resource Center. (2014). *Identity theft resource center breach report hits record high in 2014*. Retrieved from fhttp://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html

Imenda, S. (2014). Is there a conceptual difference between theoretical and conceptual frameworks? *Journal of Social Sciences*, *38*(2), 185-195. Retrieved from http://www.krepublishers.com/journalofsocialsciences.html

Imperva. (2012). Hacker intelligence initiative, monthly trend report. Retrieved from https://www.imperva.com/docs/HII_Monitoring_Hacker_Forums_2012.pdf

Irwin, S. (2013). Qualitative secondary data analysis: Ethics, epistemology and context. *Progress in Development Studies*, *13*, 295–306. doi:10.1177/1464993413490479

Jaafar, G., Abdullah, S., & Ismail, S. (2019). Review of recent detection methods for http DDoS attack. *Journal of Computer Networks and Communications*, 2019. https://doi.org/10.1155/2019/1283472

Jarvis, K. (2014). *Cryptolocker ransomware*. Retrieved from http://www.secureworks.com/cyber-threat-intelligence/threats/ cryptolocker-ransomware

Jasiul, B., Szpyrka, M., & Sliwa, J. (2014). Detection and modeling of cyber attacks with Petri Nets. *Entropy, 16*(12), 6602-6623. doi:10.3390/e16126602

Jennings, W. G., & Beaudry-Cyr, M. (2014). Rational choice. In J. M. Miller (Ed.), *Encyclopedia of theoretical criminology*. Malden, MA: Wiley-Blackwell.

Jyothsna, V., Prasad, V. V., & Prasad, K. M. (2011). A review of anomaly based intrusion detection systems. *International Journal of Computer Applications, 28*(7), 26-35.

Kansagra, D., Kumhar, M., & Jha, D. (2016). Ransomware: A threat to cyber security. *International Journal of Computer Science & Communication, 7*(1), 224-227. doi:10.090592/IJCSC.2016.035

Kashyap, B., & Jena, S. K. (2012). DDoS attacks detection and attacker identification. *International Journal of Computer Applications*, *42*(1), 28-33. doi:org/10.5120/5657-7549

Kaspersky. (2013). *Heuristic analysis in anti-virus*. Retrieved from http://support.kaspersky.com/8641.

Kaspersky report. (2019). *DDoS attacks in Q1 2019*. Retrieved from https://securelist.com/ddos-report-q1-2019/90792/

Kaur, P., Kumar, M., & Bhandari, B. (2017). A review of detection approaches for distributed denial of service attacks. *System Science and Control Engineering*, 5(1), 301-320. doi.org/10.1080/21642583.2017.1331768

Kelty, C. (2008). *Two bits: The natural significance of free software*. Durham, IA: Duke University Press.

Kende, M. (2014, June). Global Internet report. *Internet Society*. Retrieved from http://www.internetsociety.org/doc/globalinternetreport?gclid=CKuiiPvFysMCFdcWgQduRgArw

Kesan, J. P., & Hayes, C. H. (2012). Mitigative counterstriking: Self-defense and deterrence in cyberspace. *Harvard Journal of Law & Technology, 24*(2), 431-462. Retrieved from http://jolt.law.harvard.edu/

Kjaerland, M. (2005). A classification of computer security incident based on reporterd attack data. *Journal of Investigave Psychology and Offender Profiling, 2*, 105-120. doi:wiley.com/10.1002/jip.31

Langton, J. T., & Baker, A. (2013, June). *Information visualization metrics and methods for cyber security evaluation.* Paper presented at 2013 IEEE International Conference on Information Visualization Metrics and Methods for Cyber Security Evaluation. In Intelligence and Security Informatics (ISI), 292-294). Seattle, WA. dio: 10.1109/ISI.2013.6578846

Lapan, S. D., Quartaroli, M., & Riemer, J. F. (Eds.). (2012). Q*ualitative research: An introduction to methods and designs*. San Francisco, CA: Jossey-Bass.

Lakshmi, S., & Mohideen, M. A. (2013). Issues in reliability and validity of research.

International Journal of Management Research and Reviews, *3*, 2752–2758. Retrieved from http://ijmrr.com/

Langager, C. (2019). Industry vs. sector: What's the difference? *Investopedia*. Retrieved from https://www.investopedia.com/ask/answers/05/industrysector.asp

Lawrence, D., Townsend, F., Murphy, T., Castelli, J., Garrie, D., Squires, J., … Lawrence, M. (2017). It's the cybercrime and its sponsors (not my cybersecurity), stupid. *Journal of Law and Cyber Warfare,* 5(2), 1-56.

Lee, R. B. (2013). Improving cyber security. In Hsu, & Marinucci (Eds.), *Advances in cyber security: Technology, operation, and experiences* (pp. 37-59). New York, NY: Fordham University Press.

Lemos, R. (2000). Script kiddies: The net's cybergrands. *ZDNet*. Retrieved from http://www.zdnet.com/script-kiddies-the-nets-cybergangs-3002080125/

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands. Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking, 17*(8), 551–555.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280. doi:org/10.1080/01639625.2015.1012409

Levene, H. (1960). Robust tests for equality of variances. In I. Olkin et al. (Eds.), Contributions to probability and statistics: Essays in honor of Harold Hotelling (pp. 278-292). Stanford, CA: Stanford University Press.

Levy, S. (1984). *Hackers: Heroes of the computer revolution*. New York, NY: Doubleday.

Liu, S., & Cheng, B. (2009, May). Cyber attacks: Why, what, and how. *IT Professional Magazine*, *11*(3), 14-21. doi:http://dx.doi.org/10.1109/MITP.2009.46

Long, H. (2014). An empirical review of research methodologies and methods in creativity studies (2003–2012). *Creativity Research Journal*, 26, 427–438. doi:10.1080/10400419.2014.961781

Madarie, R. (2017). Hackers' motivations: Testing Schwartz's theory of motivational types of values in a sample of hackers. *International Journal of Cyber Criminology, 11*(1), 78-97. doi:10.5281/zenodo.495773

Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks, 13*(12). doi:10.1177/155014771774146

Malik, M. (2016). DDoS prevention technique. *Expression Journal*. Retrieved from http://expressionjournal.com/downloads/3.-madhu-malik1.pdf

Mancuso, V., Strang, A., Funke, G., & Finomore, V. (2014). *Human factors of cyber attacks: A framework for human-centered research.* Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting–2014. doi:10.1177/1541931214581091

Mandelcorn, S., Modarres, M., & Mosle, A. (2013). An explanatory model of cyber-attacks drawn from rational choice theory. *Transactions of the American Nuclear Society,* 109. Retrieved from

https://www.researchgate.net/publication/266137255_An_Explanatory_Model_of_Cyber-Attacks_Drawn_from_Rational_Choice_Theory

Mandelcorn, S., Modarres, M., & Mosleh, A. (2016). An explanatory model of cyber-attacks drawn from rational choice theory. Retrieved from https://www.researchgate.net/publication/266137255

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., … Frye, J. (2012, March). *Cyber threat metrics* (Report No. SAND2012-2427). Albuquerque, NM: Sandia National Laboratories.

McAfee. (2009). *New zombies*. Retrieved from https://www.wired.com/images_blogs/threatlevel /2009/07/mcafeeq2.pdf

McAfee. (2017). *The Mirai botnet exploited poorly secured IoT devices to perform the largest ever distributed denial-of-service attack*. Retrieved from https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

McDonald. J. H. (2014). *Handbook of biological statistics*. Baltimore, MD: Sparky House.

McGee, M. K. (2014, July). Why hackers are targeting health data CIO: Today it's a totally different kind of attack. *Data Breach: Prevention, Response, Notification Today*. Retrieved from http://www.databreachtoday.co.uk/hackers-are-targeting-health-data-a-7024

McMillan, R. (2010). Maripoza botnet ran under the radar but was not one of the biggest ever. *Techworld.com*. Retrieved from

http://news.techworld.com/security/3214049/spanish-police-shut-down-worlds-largest-botnet/?olo=rss

Middleton, B. (2017). *A history of cyber security attacks 1980 to present*. Boca Raton, FL: Taylor & Francis Group.

Mishra, B., & Saini, H. (2013). *Cyber attack classification using game theoretic weighted metrics approach*. Retrieved from https://www.semanticscholar.org/paper/Cyber-Attack-Classification -using-Game-Theoretic-Mishra-Saini/4f137a39e0528ea92c0156a963c4ca 705bd35ebf

Mohiuddin, A., Uddin, A. M., & Someswar, M. G. (2014). Design and development of an effective DDoS Shield to implement a well secured Defense System against vulnerable attacks. *International Journal of Advancements in Research & Technology, 3*(3). Retrieved from http://www.ijoart.org/docs/Design-and-Development-of-an-effective-DDoS-Shield-to-implement.pdf

Moore, N., Salter, A., Stanley, L., & Tamboukou, M. (2017). *The archival project: Archival research in social sciences.* New York, NY: Routledge.

Moore, R. (2015). *Cybercrime: Investigating high-technology computer crime* (2nd ed.). New York, NY: Routledge.

Morgan, D. L. (2015). From themes to hypotheses: Following up with quantitative methods. *Qualitative Health Research*, *25*, 789-793. doi:10.1177/1049732315580110

Mulligan, D. K., & Schneider, F. B. (2011). *Doctrine for cybersecurity*. Retrieved from www.cs.cornell.edu/fbs/.../publicCYbersecDaed.pdf

Nakashima, E. (2014). U.S. notified 3,000 companies in 2013 about cyberattacks. *Washington Post*. Retrieved from http://www.cyber-sec.info/?p=3434

National Cyber Security Center. (2016, January). *Common cyber attacks: Reducing the impact cyber attacks*. Retrieved from https://www.ncsc.gov.uk/ content/files/protected files/guidance_files/common_cyber_attacks_ncsc.pdf

National Institute of Standards and Technology. (2011). *Management information security risk organization, mission, and information systems view*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

National Research Council. (2009). *NRC technology, policy, law, and ethics regarding U.S. acquisition and use of cyber security capabilities.* Washington, DC: The National Academies Press, 2009.

Navarro, J. N., & Jasinski, J. L. (2012). Going cyber: Using routine activities theory to predict cyberbullying experiences. *Sociological Spectrum*, *32*, 81-94. doi:org/10.1080/02732 173.2012.628560

Newman, I., & Covrig, D. M. (2013). Building consistency between title, problem statement, purpose, & research questions to improve the quality of research plans 150 and reports. *New Horizons in Adult Education & Human Resource Development, 25*(1), 70-79. doi:10.1002/nha.20009

Neuman, W. L. (2011). *Social research methods: Qualitative and quantitative approaches* (7th ed.). Boston, MA: Allyn & Bacon.

Nowell, L., Norris, J., White, D., & Moules, N. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*, 1-13. doi:10.1177/1609406917733847 journals.sagepub.com/home/

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational-level factors. *International Journal of Cyber Criminology*, *5*, 773-793. doi:10.19107/IJISC

O'Leary, D., Grahn, A., & Poarch, D. (2017, June). How to successfully combat targeted cyber attacks. *Forsythe Focus.* Retrieved from http://focus.forsythe.com/articles/268/ Combating-Advanced-Persistent-Threats

Orebaugh, A., Burke, J., Perce, L., Wright, J., & Morris, G. (2007). *Wireshark & ethereal network protocol analyzer toolkit*. Rockland, MA: Syngress.

Palekiene, O., Bruneckiene, J., & Simanaviciene, Z. (2014). Critical Analysis of Loss and Damage Concepts under Process of Economic Assessment. Procedia - Social and Behavioral Sciences, 156, 304-309. doi.org/10.1016/j.sbspro.2014.11.193

Patel, C. M., & Borisagar, V. (2012). Survey on taxonomy of DDoS Attacks with impact and mitigation techniques. *International Journal of Engineering Research & Technology)*, *1*(9). www.ijert.org

Paternoster, R., Jaynes, C., & Wilson, T. (2017). Rational choice theory and interest in the "fortune of others." *Journal of Research in Crime and Delinquency*. doi:10.1177/0022427817707240 journals.sagepub.com/home/

Pathak, B. P. (2016). A dangerous trend of cybercrime: Ransomware growing challenge. *International Journal of Advanced Research in Computer Engineering & Technology*, *5*(2). doi:10.1126/science.1065467

Patil, M., & Kulkarni, U. L. (2011). Mitigating APP DDoS attacks on Web server. *International Journal of Computer Science and Telecommunications, 2*(5), 13-18. Retrieved from http://ijcst.com/

Patil, P. (2017). Ransomware-the evolution of malwares. *International Journal of Innovative Research in Science, Engineering and Technology, 6*(2). doI:10.15680/IJIRSET.2017.0602027 1614

Pau, L. (2013). Business and social evaluation of denial of service attacks of communications networks in view of scaling economic counter-measures. *IOS Press*. doi:10.1109/NOMSW.2010.5486591

Perugini, M., Gallucci, M., & Costantini, G. (2018). A practical primer to power analysis for simple experimental designs. *International Review of Social Psychology*, *31*(1), 20. doi: http://doi.org/10.5334/irsp.181

Pinguelo, F. M., & Muller, B. W. (2011). Virtual crime, real damages: A primer on cybercrimes in the United States and efforts combat cyber criminals. *Virginia Journal of Law & Technology, 16*(1). Retrieved from http://ellblog.com/wpcontent/uploads /2012/04/Pinguelo-UVA%20JoLT%20Spring%202011.pdf

Prasad, M. K., Reddy, R. A., & Rao, V. K. (2014). DoS and DDoS attacks: Defense, detection and traceback mMechanisms - A survey. *Global Journal of Computer*

Science and Technology, 14(7). Retrieved from https://computerresearch.org/index.php /computer/article/view/1081

Prasad, S. T. (2014). Ethical hacking and types of hackers. *International Journal of Emerging Technology in Computer Science & Electronics, 11*(2), 24-27. Retrieved from http://www.ijetcse.com/wp-content/plugins/ijetcse/file/upload/docx/524Ethical-Hacking-and-Types-of-Hackers-pdf.pdf

Pratt, T., Holtfreter, K., & Reisig, M. (2010). Routine online activity and Internet fraud targeting: Extending the generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Radware. (2013). *Pre-attack planning causes successful DDoS attack*. Retrieved from http://security.radware.com/uploadedFiles/Resources_and_Content/Attack_Tools/Attack_Planning_ERT_Research_Brief.pdf

Radware. (2017). *History of DDoS attacks*. Retrieved from ttps://security.radware.com/ddos-knowledge-center/ddos-chronicles/ddos-attacks-history/

Raj Kumar, P. A., & Selvakumar, S. (2011). Distributed denial of service attack detection using an ensemble of neural classifier. *Computer Communications*, *34*(11), 1328-1341. doi:10.1016/j.comcom.2011.01.012

Rajab, M. A., Zarfoss, J., Monrose, F., & Terzis, A. (2006). *A multifaceted approach to understanding the botnet phenomenon*. Retrieved from http://conferences.sigcomm.org/imc/2006/papers/p4-rajab.pdf

Rajesh, S. (2013). Protection from application layer DDoS attacks for popular websites. *International Journal of Computer & Electrical Engineering, 5*(6), 555-558. https://doi.org/10.7763/ijcee.2013.v5.771

Ramesh, S. (2013). Layer model for reducing malware jamming attacks. *International Journal of Computer Trends and Technology, 4*(10), 3450-3456. Retrieved from http://www.ijcttjournal.org/

Ransbotham, S., & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139.

Raymond, E. S. (1996). *A new hacker dictionary* (3rd ed.). Cambridge, MA: The MIT Press.

Reilly, R., & Schweihs, R. (2014). *Guide to intangible asset valuation*. New York, NY: Linda Prentice Cohen

Reyns, B. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

Reyns, B. (2016). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency, 50*(2), 216-238. doi:10.1177/0022427811425539

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*, 1149-1169. Retrieved from http://journals.sagepub.com/home/cjb

Rittinghouse, J. W., & Hancock, M. W. (2003). *Cyber security operations handbook.* Burlington, MA: Digital Press.

Rivalhost Managed Web Hosting. (2013, August). Industries most affected by DDoS attacks. Retrieved from https://www.rivalhost.com/industries-most-affected-by-ddos-attacks

Rogers, M. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study* (Doctoral dissertation). Retrieved from https://www.cerias.purdue.edu/assets/pdf/bibtexarchive/rogers_01.pdf

Romanosky, S. (2016*).* Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121-135. https://doi.org/10.1093/cybsec/tyw001

Sales, N. A. (2013). Regulating cyber-security. *Northwestern University Law Review*, *107*(4), 1503-1568.

Salim, M. (2014). Cyber safety: A systems thinking and systems theory approach to managing cyber security risks. Retrieved from http://web.mit.edu/smadnick/www/wp/2014-07.pdf

Sampson, J. P., Hou, P.-C., Kronholz, J. F., Dozier, V. C., McClain, M.-C., Buzzetta, M., … Kennelly, E. L. (2014). A content analysis of career development theory, research, and practice-2013. *The Career Development Quarterly*, *62*, 290-326. doi:10.1002/j.2161-0045.2014.00085.x

Sanghvi, H. P., & Dahiya, M. S. (2013). Cyber reconnaissance: An alarm before cyber attack. *International Journal of Computer Applications, 63*(6), 36-38. doi:10.5120/10472-5202

Savola, R. M. (2009). A security metrics taxonomization model for software-intensive systems. *Journal of Information Processing Systems, 5*(4). doi:10.3745/JIPS.2009.5.4.197

Schell, B. H., & Melnychuk, J. (2011). Female and male hacker conference attendees: Their austism-spectrum quotient (AQ) scores and self-reported adulthood experiences. In T. J. Holt & B. H. Schell (Eds.), *Corporate hacking technology drive in crime: Social dynamic and implications* (pp. 144-169). Hershey, PA: IGI Global.

Schwartz, M. J. (2011, May). Lockheed Martin Suffers massive cyber attack. *Information Week.* Retrieved from http://www.informationweek.com/news/government/security/229700151

Schwartz, M. J. (2013, April). DDoS attack bandwidth jumps 718%. *Information Week.* Retrieved from http://www.informationweek.com/attacks/ddos-attackbandwidthjumps-718-/d/d-id/1109576

Siegel, J. G., Dauber, N., & Shim, J. K. (2005). *The Vest Pocket CPA*. Hoboken, NJ: John Wiley & Sons.

Semantic. (2015). *Banks likely to remain top cybercrime targets*. Retrieved from https://www.symantec.com/content/en/us/enterprise/other_resources/b_Financial_Attacks_Exec_Report.pdf

Shakarian, P., Shakarian, J., & Ruef, A. (2013). *Introduction to cyber-warfare: A multidisciplinary approach.* Waltham, MA: Elsevier.

Shearer, J. (2010). W32. Stuxnet. Retrieved from www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99

Sheldon, T. F., & McDonald, J. T. (2012). Introduction to the special issue on cyber security and management. *Information Systems and e-Business Management, 10*(4). doi:10.1007/s10257-012-0204-

Silnov, D. (2013). Feature of virus detection mechanism in Microsoft security essentials (Microsoft forefront endpoint protection). *Journal of Information Security, 4*(2), 124-127. doi:10.4236/jis.2013.4201

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know.* New York, NY: Oxford University Press.

Singleton, R. A., & Straits, B. (2017). *Approaches to social research* (6th ed.). New York, NY: Oxford University Press.

Skoudis, E., & Zeltser, L. (2006). *Counter hack reloaded: A step-by-step guide to computer attacks and effective defenses* (2nd ed.). Upper Saddle River, NJ: Prentice-Hall.

Somal, K. L., & Virk, S. K. (2014). Classification of distributed denial of service attacks –architecture, taxonomy and tools. *International Journal of Advanced Research in Computer Science & Technology, 2*(2). Retrieved from http://www.ijarcst.com/doc/vol2-issue2/l_k_somal.pdf

Sood, A., & Enbody, R. (2014). *Targeted cyber attacks: Multi-staged attacks driven by exploits*. Waltham: MA, Syngress.

Statista. (2017). *Largest life insurance companies in the United States in 2017, by assets (in billion U.S. dollars)*. Retrieved from https://www.statista.com/

Steele, R. (2016). How Offenders Make Decisions: Evidence of Rationality. *British Journal of Community Justice*, 13(3), 7-20.

Stewart, M. J. (2011). *Network security, firewalls, and VPNS*. Sudbury, MA: Jones and Bartlett.

Stewart, M. J., Chapple, M., & Gibson, D. (2015). *CISSP (ISC)2 certified information systems security professional official study guide* (7th ed.). Indianapolis, IN: John Wiley & Son.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *Management Information Systems Quarterly, 14*(1), 45-62. https://doi.org/10.2307/249307

Symantec. (2014). *Symantec intelligence report, 19*. Retrieved from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

Symantec. (2015). Internet security threat report: Attackers are bigger, bolder, and faster. Retrived from https://www.symantec.com/connect/blogs/2015-internet-security-threat-report-attackers-are-bigger-bolder-and-faster

Tajalizadehkhoob, S., Asghari, H., Ganan, C., & van Eeten, M. (2014). Why them? Extracting intelligence about target selection from Zeus financial malware. *In*

Proceedings of the 13th Annual Workshop on the Economics of Information Security (WEIS), State College, PA, WEIS, June 23-24, 2014. Retrieved from https://www.econinfosec.org/archive/ weis2014/papers/Tajalizadehkhoob-WEIS2014.pdf

Tariq, N. (2018). Impact of cyberattacks on financial institutions. J*ournal of Internet Banking and Commerce, 23*(2). Retrieved from http://www.icommercecentral.com/open-access/ impact-of-cyberattacks-on-financial-institutions.pdf

Thakkar, S. (2014). Ransomware-exploring the electronic form of extortion. *International Journal for Scientific Research & Development, 2*(10), 2321-0613. Retrieved from https://www.researchgate.net/profile/Samir_Thakkar/publication/308802806_Ransomware_Exploring_the_Electronic_form_of_Extortion/links/581ae2f908aed2439386d642.pdf

The Economist. (2014, August). *Hacking the banks: Who lies behind the latest cyber-attacks on JPMorgan Chase*? Retrieved from http://www.economist.com/news/business-and-finance/21614181-who-lies-behind-latest-cyber-attacks-jp-morgan-chase-hacking-banks

TrendLabs. (2017, February). Trend *micro security news. A record year for enterprise threats*. Retrieved from https://www.trend micro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup

Trend Micro (2015). Understanding Targeted Attacks: What is a Targeted Attack? https://www.trendmicro.com/vinfo/us/security/news/cyber - attacks/understanding-targeted-attacks-what-is-a-targeted-attack

Trend Micro (2019). Banks Under Attack: Tactics and Techniques Used to Target Financial Organizations. Retrieved from https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/banks-under-attack-tactics-and-techniques-used-to-target-financial-organizations

Tripathi, S., Gupta, B., Almomani, A., Mishra, A., & Veluru, S. (2013). Hadoop based defense solution to handle distributed denial of service (DDoS) attacks. *Journal of Information Security, 4*, 150-164. doi:10.4236/jis.2013.43018

Trost, R. (2010). *Practical intrusion analysis: Prevention and detection for the twenty-first century*. Upper Saddle River, NJ: Addison-Wesley.

Turakira, R. (2016). *Use Spearman's Rank Correlation to increase your business profits.: An application of Rank Correlation Coefficient*. Scotts Valley, CA: CreateSpace

Turner, T. L., Balmer, D. F., & Coverdale, J. H. (2013). Methodologies and study designs relevant to medical education research. *International Review of Psychiatry*, *25*, 301–310. doi:10.3109/09540261.2013.790310

Uma, M., & Padmavathi, G. (2013). A survey on various cyber attacks and their classification. *International Journal of Network Security, 15*(5), 390-396.

Vacca, J., & Rudolph, K. (2011). *System forensics, investigation, and response*. Sudbury, MA: Jones and Bartlett.

Van Beveren, J., & Falkinder, S. (2005). *Understanding the motives of malware creators*. San Francisco, CA: International Academy of E-Business (IAEB).

Vance, A., & Siponen, M. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing*, *24*, 21-41. doi:10.4018/joeuc.2012010102

Verendel, V. (2009). Quantified security is a weak hypothesis: A critical survey of results and assumptions. *In ACM New Security Paradigms Workshop.* Proc. NSPW'09. 37-50.

Verisign. (2014). Verisign distributed denial of service trends report issue 2–2nd quarter 2014. *Verisign.* Retrieved from http://www.verisign.com/assets/report-ddos-trends-Q22014.pdf?inc=www.verisigninc.com

Vijayan, J. (2011, April). FAQ: Epsilon e-mail breach. *Computer World*. Retrieved from http://www.computerworld.com/s/article/9215527/FAQ_Epsilon_e-mail_breach

Villeneuve, N. (2011, October). Trends in targeted attacks. *Trend Micro.com.* Retrieved from www.trendmicro.com/.../wp_trends-in-targeted-attacks.pdf

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

Wark, M. (2004). *A hacker manifesto*. Cambridge, MA: Harvard University Press.

Whalen, K. (2017). DDoS attacks in 2017: No days off. *Arbor Networks. Retrieved from* https://www.arbornetworks.com/blog/insight/ddos-attacks-2017-no-days-off/

White, L. (2016). UK banks reluctant to report extent of relentless cyber attacks. *Insurance Journal*. Retrieved from www.insurancejournal.com/news/international/2016/10/ 14/429327.htm

Whitman, M., & Mattord, H. (2016). *Management of information security* (5th ed.) Boston, MA: Cengage/Course Technology.

Wiles, J., Gudaitis, T., Jabbusch, J., Rogers, R., & Lowther, S. (2012). *Low tech hacking: Street smarts for security professional*. Waltham: MA: Syngress.

Williman, N. (2011). *Research methods: The basics*. New York, NY: Routledge.

Wilson, J. Q., & Herrnstein, R. (1985). Crime and human nature, Simon and Schuster. *Criminology*, 23 (2).

Wueest, C. (2014). The continued rise of DDoS attacks. *Symantec.* Retrieved from http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-continued-rise-of-ddos-attacks.pdf

Xuan, Y., Shin, I., Thai, M., & Znati, T. (2010). Detecting application denial-of-service attacks: A group-testing-based approach. *IEEE Transactions on Parallel and Distributed Systems. 21*(8), 1203-1216. doi:10.1109/TPDS.2009.147

Yadav, H., & Gour, S. (2014). Cyber attacks: An impact on economy to an organization. *International Journal of Information & Computation Technology, 4*(9), 937-940. Retrieved from https://www.ripublication.com/irph/ijict_spl/ijictv4n9spl_11.pdf

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? The *Howard Journal of Crime and Justice*, 387-399.

Yar, M. (2006). The novelty of cybercrime. *European Journal of Criminology*, *2*, 407-427. doi:10.1177/147737080556056

Yar, M. (2013). *Cyber crime and society* (2nd ed.). Thousand Oaks, CA: Sage.

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.

York, K. (2017). Dyn statement on 10/21/2016 DDoS attack. Retrieved from http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/

Yu, S. (2014). *Distributed denial of service attack and defense.* New York, NY: Springer.

Yucedal, B. (2010). Victimization in cyberspace: An application of routine activity and lifestyle exposure theories (Doctoral dissertation, Kent State University). Retrieved from http://etd.ohiolink.edu/send-pdf.cgi/YUCEDAL%20BEHZAT.pdf?kent1279290984