Scientific Research Publishing

Journal of Information Security, 2020, 11, 261-291
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Using Linear Regression Analysis and Defense in Depth to Protect Networks during the Global Corona Pandemic

Rodney Alexander

Hutchinson Community College, Hutchinson, Kansas, USA
Email: rdnyalex@aol.com

How to cite this paper: Alexander, R. (2020) Using Linear Regression Analysis and Defense in Depth to Protect Networks during the Global Corona Pandemic. *Journal of Information Security*, **11**, 261-291.
https://doi.org/10.4236/jis.2020.114017

Received: September 13, 2020
Accepted: October 18, 2020
Published: October 21, 2020

Abstract

The purpose of this research was to determine whether the Linear Regression Analysis can be effectively applied to the prioritization of defense-in-depth security tools and procedures to reduce cyber threats during the Global Corona Virus Pandemic. The way this was determined or methods used in this study consisted of scanning 20 peer reviewed Cybersecurity Articles from prominent Cybersecurity Journals for a list of defense in depth measures (tools and procedures) and the threats that those measures were designed to reduce. The methods further involved using the Likert Scale Model to create an ordinal ranking of the measures and threats. The defense in depth tools and procedures were then compared to see whether the Likert scale and Linear Regression Analysis could be effectively applied to prioritize and combine the measures to reduce pandemic related cyber threats. The results of this research reject the H_0 null hypothesis that Linear Regression Analysis does not affect the relationship between the prioritization and combining of defense in depth tools and procedures (independent variables) and pandemic related cyber threats (dependent variables).

Keywords

Information Assurance, Defense in Depth, Information Technology, Network Security, Cybersecurity, Linear Regression Analysis, Pandemic

1. Introduction

The research background in cyber security defense-in-depth (DID) prioritization included a literary review of recent cyber security breaches and how organizational network security managers prioritize their network defenses to prevent those breaches. An analysis of former cyber security prioritization research

disclosed that organizational network security managers need to use additional systematic decision-making approaches when prioritizing their network defenses. To summarize the problem involving former research; network security managers need additional decision theories when deciding how to deploy their defenses. This research introduced using Linear Regression and the Likert scale to give network security managers an additional systematic way to prioritize their network defenses.

The dependent variables of cyber threats were determined to see whether they could be influenced by the independent variables (prioritized defense in depth tools and procedures) to reduce organizational cyber breaches. The independent variables of defense in depth tools and procedures were determined to be effective means used by security managers to counter cyber threats. The independent variable weights were determined by calculating the effects of combining or layering the independent variables.

During the Global Corona Virus Pandemic, the number of mobile subscribers has reached 6.8 billion worldwide and almost 40% of the world's population is now using the Internet [1]. Cyber-attacks that occur during the pandemic due to working and learning from home caused by social distancing requirements can be reduced by deploying security tools and procedures. Corona Virus test results and vaccine laboratories will require enhancing security attention during the pandemic.

Cybersecurity should be applied commensurately with the risk and the value of the asset requiring protection [2]. Critical infrastructure requires the highest security priority. In the field of cyber security, threats have evolved such that they are usually complex interactions between an assailant (the "threat actor") and the target system [3]. During the Global Corona Virus Pandemic hackers will try to use elaborate means to intrude into systems.

Although implementation of technological solutions is the usual response to security threats and vulnerabilities, wireless security is primarily a management issue [4]. How the network security manager designs and implements a network will influence how well the network is protected during the Global Corona Virus Pandemic. Defense in depth (DiD) prevents network intrusions by deploying tools and procedures such as firewalls, access control and detection. Most of the systems use robust architectures to enhance business and reduce costs by increasing the integration of external, business, and control system networks [5].

During the Global Corona Virus Pandemic large organizations, laboratories and networks are necessary to process test results and produce vaccines. The DID strategy recommends a balance between the protection capability and cost, performance, and operational considerations [6]. Social networks are extremely popular in today's world [7]. During the Global Corona Virus Pandemic with its social distancing requirements, social networks have become an important part of organizational operations.

Millions of people use various forms of social networks as they allow individ-

uals to connect with friends and family and share private information [7]. Social networks have become an effective way to manage social distancing during the Global Corona Virus Pandemic. Concept of defense in depth is adopted from military defense where different obstacles are deployed to eventually expend the resources of attacker [8]. A hacker's time, skills and funding can be exhausted by deploying defensive barriers centered on loss of privacy prevention for example.

During this process, one or more intermediate target devices (e.g., DNS servers, routers, etc.) may be used to gain progressively deeper access to the target network to approach the target system [3]. While working from home, remote access to the organizational network can also offer hackers a way into the network. The overall security objectives remain the same: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems [4].

Linear regression analysis is the study of dependence [9]. The reduction of security threats to organizational networks is dependent on the network security tools and procedures designed to reduce those threats. By deploying the same defenses on the internal network as on the external edge, the network can secure itself and other networks [10]. During the Global Corona Virus Pandemic, for example firewalls can be combined to secure different segments of the network.

At a high level, the threat actor can use several techniques to breach the target network, bypassing the defensive devices and either installing malicious code on a target system or directly accessing the target system [3]. There are many tools available on the Internet which will allow hackers to breach systems, access networks and steal data. When considering the most logical route an attacker will take in compromising a control network, it is easy to visualize an attack path that pries deeper and deeper into the architecture [5]. An attacker will try to access the core of a system to steal or manipulate privacy data.

A Social Network Service (SNS) is a kind of web service for establishing a virtual connection between people with similar interests, backgrounds, and activities [7]. People with the same hobbies and work environments need to keep network security in mind when using social media networks. Effective management of the threats associated with technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats [4]. Threats to a network despite the Global Corona Virus Pandemic must be assessed and a plan to mitigate those threats must be developed.

Identifying critical assets based on a risk assessment is a good starting point, but security must not end there [2]. Once critical assets are identified; a security blanket must be developed around the organizational critical assets. Once the target system is compromised, the threat actor can then act upon target data and/or target systems or intermediate systems in some way that achieves a malicious goal [3]. A hacker gains access to sensitive data by compromising vulnerable systems.

The main thrust of the research is to indicate an approximate linear mapping between a nonfrontal face image and its frontal counterpart [11]. The physical network security tool *i.e.* a network intrusion detection system (NIDS) is mapped against the hidden process of intrusion reduction in this research. The linear regression analysis can be deployed in the information assurance planning process. The logic of the theory can easily be extended to decisions about selecting goals or managerial strategy [12].

Can we predict the time of the next eruption of Old Faithful Geyser from the length of the most recent eruption [9]? The number of organizational security breaches can be predicted based on the type of layered defenses used to secure those organizational networks.

Instead of a focusing on feature-centric network defense requirements, the defense in depth (DiD) model should be redesigned to be a functional or capability focused model [10].

Defense in depth priorities and focus should align with current threats, for example DDOS and DOS attacks. Exemplary actions on the target data can include but are not limited to theft of data exfiltration), destruction of data, modification of data, or some combination thereof [3]. While on the Internet because of social distancing requirements, user passwords can be stolen as well as bank information and medical records.

In the case of measuring the linear relationship between a predictor and an outcome variable, simple linear regression analysis is conducted [13]. Linear regression can be used to predict Network security outcomes based on the deployment of certain defense in depth security tools. Decision theory provides a normative framework for representing and reasoning about decision problems under uncertainty [14]. The ambiguity of deciding which defense in depth measures to use to reduce network intrusions can be solved using this modeling principle.

As with most statistical analyses, the goal of regression is to summarize observed data as simply, usefully, and elegantly as possible [9]. The purpose of this statistical analysis is to give the organizational network security a clearer picture on how to manage the difficult multi-criteria decision making problem associated with network security. Symmetry in the DiD model allows for the network defense system to recognize the insider threat, preventing data exfiltration and allowing attacks to be stopped at the originating network instead of being defended by the attacked network [10].

This research proposes a simple but efficient linear regression-based classification (LRC) for the problem of face identification [11]. The reduction of security threats to an organizational network can be shown by using linear regression. The idea behind the defense in depth approach is to defend a system against any attack using several independent methods [15]. Defense in depth measures should be arrayed against threats to attack them from several different directions.

Wireless Networks present a host of issues for network managers [4]. Network security managers because of the pandemic face varying threats when it comes to wireless networks. In today's rapidly changing world, networks change daily, software is updated weekly, and threats may change by the hour [3]. Computer networks during the corona virus pandemic are fluid environments which require the constant attention of network security managers.

Statistical methods are important for exploring the relationships between variables and can be applied to many studies [13]. Linear regression can be significant in exploring the relationship between network security threat variables and defense in depth security tool variables. Dynamic defenses must also be enabled, which change attack surfaces to proactively defend a network [10]. Defense in depth intrusion detection systems can adjust to the changing nature of attacks.

Unauthorized access points, broadcasted SSIDs, unknown stations, and spoofed MAC addresses are just a few of the problems addressed in WLAN [4]. Most of these threats are specific to wireless networks especially during times when people are working from home and learning from home. This research study explores whether the Linear Regression Analysis can be effectively applied to the array of information assurance defense-in-depth measures to mitigate network security threats.

1.1. Network Security Threats

A "peel-the-onion" analysis shows that an attacker trying to affect a critical infrastructure system would most likely be after the core control domain [5]. In a corona virus vaccine lab for example an attacker is most likely will try to disrupt or steal data from the labs vaccine producing systems. This study uses the Likert Scale to rank network security threats (**Table 1**) and their corresponding defense in depth security measures which will assist network security managers in prioritizing their network resources. Rank correlations also work well with ordinal rating data, and continuous data are reduced to their ranks [13]. The weights represent the value added of layering the defense in depth measures.

Table 1. Top ten network security threat prioritization.

Priority	Threat	Weights
1	Network Intrusions	16
2	Privacy Loss	12
3	Hacking	12
4	Trojans	7
5	Stolen Passwords	7
6	Phishing attacks	6
7	Data Theft	5
8	MitM Attacks	5
9	DOS Attacks	5
10	Sniffing Attacks	3

These attacks attempt to deliberately modify information shared within the smart grid to corrupt critical data exchange in the smart grid [16]. Trojans can destroy data and functions designed to operate and control the smart grid. An increasing number of wireless devices are abused for illicit cybercriminal activities, including malicious attacks, computer hacking, data forging, financial information theft, online bullying/stalking [1]. Users should be extremely careful while social distancing and using wireless networks.

The target of the attacks is either customer's information (e.g., pricing information and customer account balance) or network operation information (e.g., voltage readings, device running status) [16]. Because of social distancing requirements smart grid operators may be forced to work remotely. Network intruders may attempt to disrupt this smart grid data traveling over the Internet.

Malicious attacks targeting network availability can be considered as denial-of-service (DoS) attacks [16]. If networks become unavailable, then working from home or distance learning will come to a screeching halt. This causes the direct loss of about 83 billion euros with an estimated 556 million users worldwide impacted by cybercrime each year, according to the 2012 Norton cyber-crime report [1]. Cybercrime is responsible for large financial losses to the global economy; this is something to keep in mind while working from home.

Ad-hoc networks can pose a security threat [4]. A Bluetooth connection for example has fewer security controls than a managed wireless network. Differing from attacks targeting network availability, attacks targeting data integrity can be regarded as less brute force yet more sophisticated attacks [16]. Integrity attacks can try to discredit the integrity and data privacy of Corona Virus test results.

The new paradigm of global availability in networks offered by IPv6, must also be accounted for [10]. Because of social distancing requirements and remote computing, global cloud security must be included in an organization's security structure. Threat actors can gain access to credentials for normal or privileged access to the target network [3]. During the Global Corona Virus Pandemic thieves may pay inside workers for compromising information.

An unauthorized node in a wireless network is capable of inflicting intentional interferences with the objective of disrupting data communications between legitimate users [1]. Denial of service attackers can cause havoc for Internet users. Since network availability is the top priority in the security objectives for the smart grid, we use experiments to quantitatively evaluate the impact of denial-of-service (DoS) attacks on a power substation network [16]. A denial of service (DOS) attack could potentially plunge entire regions into darkness.

An attacker must then not only compromise security controls at the perimeter but must be able to compromise each layer behind the perimeter to reach the critical asset [2]. While we are learning from home an attack is less likely to be successful if an attacker must breach multiple obstacles. A major difference between the smart grid and the Internet is that the smart grid is more concerned

with the message delay than the data throughput due to the timing constraint of messages transmitted over the power networks [16]. Denial of service attacks can prevent critical smart grid messages from reaching their final destinations.

Due to the broadcast nature of radio propagation, the wireless air interface is open and accessible to both authorized and illegitimate users [1]. It is important to keep in mind while social distancing that both friend and enemies have access to wireless networks because wireless networks transmit over the airways.

1.2. Defense in Depth Security Strategy

The first defense approach is prevention [17]. The first defense in depth measure that a network security manager should take is to protect the network and the data that crosses the network. The network should especially be protected in way that allows users to safely work and learn from home. Next defense approach is detection. Detective measures are taken to reveal the presence of attacks and intrusions that have compromised or circumvented preventive mechanisms [17]. It is important to deploy defense in depth tools such as NIDS that can identify potential attacks such as Trojans.

Though firewalls, IDSs, and IPSs are ineffective network security systems when deployed by themselves, layering them provides additional protection [10]. Deploying defense measures as a unit increases their effectiveness. In the event there is a security-related incident in the controls system domain, activities to recognize, respond, mitigate, and resume need to be established [5]. Security planning and operations should take place before, during and after a security breach. For example, install up to date antivirus is critical before breach operation.

Incident response consists of policies, procedures, and technical measures that enable the identification of potential cyber intrusions and the structure to react to and remediate the event [2]. During the pandemic response teams may be forced to work from home via virtual meetings. Tactically, security is incomplete without proper assessment of assets, risks associated with them and policies to control these risks; the outermost layer of the model covers all these aspects [8]. Organizations must consider the risk to organizational assets before establishing remote connections due to social distancing requirements.

Each of these defensive devices has been created to act upon specific types of threats and when used in combination can theoretically help prevent, limit, or detect the attack of a threat actor, resulting in better safety for target data and target systems [2]. If a hacker can bypass one defensive tool they can be stopped by another defensive tool and user data can remain safe while they remotely access the network to social distance. Defensive strategies that secure each of the core zones can create a defensive strategy with depth [5].

A layered defense approach is the best way to protect communications while users work from home.

In information security terms, administrator or organization deploy layers of

defensive measures to minimize risk of unauthorized access or information attacks [8]. The defensive layer of an UpToDate antivirus for example can help reduce the risk of identity theft. Deflection is a means of diverting attackers from the valuable assets to a faux environment where their techniques and methods can be studied [17]. Honey pots can be used to deflect users away from sensitive areas where Corona Virus test results may be stored.

Security issues do not solve magically but administrators must evaluate different methodologies to consider as best practice for their organization [8]. Network security managers should develop the best defense in depth strategy that fits their organization. For example, if Trojans are a concern they should focus on firewalls and Network Intrusion Detection Systems (NIDS). Information assurance (IA) mechanisms may be subdivided into three categories: preventive, corrective and detective [18]. Corona virus vaccine labs can remain safe from attacks by using the defense in depth measures of protection, identifying potential attacks, and removing them.

Target organizations typically take action to prepare and assess their security posture to locate holes in their security systems [3]. Network security managers are constantly looking for areas in their networks that can be breached by hackers while employees are remotely working because of social distancing requirements. Overlapped layers can cover shortcomings of one layer by other [8]. During the Global Corona Virus Pandemic encryption can be overlapped within the network to cover firewall shortcomings.

The strategy recommends a balance between the protection capability and cost, performance, and operational considerations [19]. During the Global Corona Virus Pandemic defense in depth requires strategic planning. Development of a defense-in-depth strategy starts with mapping the control systems architecture [5]. Network security managers must have intimate knowledge of the network to understand how to effectively deploy a defense in depth strategy.

The DiD model uses layers of different network protection devices to create a secure network [10]. UpToDate antivirus is one example of a measure that can be deployed in the defense in depth model. Layer 1 focuses on perimeter security and the controls surrounding the protection of the ingress/egress point of the substation electronic security perimeter [2]. The first level of protection is entry into the network. While working from home this involves a remote connection or VPN.

Layer 2 focuses on the security controls for communication and devices that perform data aggregation [2]. The second level are the areas where critical data is stored, databases containing Corona Virus test results for example. Layer 3 focuses on host-based cybersecurity controls used to provide security at the device level [2]. The final protection level involves protecting individual devices for example, laptops used for home offices while social distancing.

No single security solution will keep a determined thief from the goal of compromising the hardware or software given enough time and resources [19]. Loss

of privacy can be reduced by deploying to defensive tools in the path of the attacker. A single strategy to defense information and its associated components may not be sufficient [8].

Multiple layered defense measures are required to protect organizational systems while employees work from home.

Historically, a military defender would build a series of defensive positions and fall back as the attacker advanced, eventually defeating the attacker [10]. Confidentiality of corona virus vaccine labs should be built on the onion approach with the most sensitive data being in the middle and hardest for an attacker to reach. Instead of attempting to prevent inbound attacks and blocking specific forms of outbound traffic, a functional DiD model should look to deploy defenses that are symmetric [10]. During online learning sessions, defense in depth can be designed to prevent both internal and external data theft.

The DoD Defense-In-Depth model is extended to logical, layered, and virtual "boundaries" beyond more traditional physical and geographic boundaries [18]. Cloud or logical boundaries have enhanced the capabilities of traditional defense in depth strategies. Having multiple DMZs protects the information resources from attacks using Virtual-LAN (VLAN) hopping and trust exploitation [5]. Corona Virus test results can be processed in secure zones which are harder for hackers to reach.

Dynamic defenses can be enabled both through dynamic computing platforms and dynamic network addressing [10]. Demilitarized zones (DMZ) can be dynamically established using DHCP to segment and block traffic. A tool such as encryption can be combined with firewalls, NIDS and authentication to create repeated barriers to defeat attackers [3]. These systems, when layered together, create a system of defense known as Defense-in-Depth, where each layered defensive device prevents a deeper level of attack.

Each layer in defense in depth architecture has heterogeneous implementation of security controls which results in administration overhead [8]. Each defensive player must be configured separately by a security manager or an administrator. Multilayer security puts the critical assets at the most reliable and secure layer [2]. A corona virus vaccine lab for example should be placed in the most critical level of the defense in depth strategy.

A DMZ is an exceptionally good way to enhance the security posture and add another layer to the defense-in-depth strategy [5]. Systems used by employees working from home can be placed in a secure zone (DMZ) which protects their communications. With multiple layers, each layer can have unique yet complementary security controls [2]. Trojans attacks can be reduced with specific but supportive defensive layers.

Defense in depth base on layered architecture, every layer has its own implementation [8]. Although defense measures may cover vulnerabilities that others miss. Each requires its individual configuration. Because of social distancing requirements this will involve Internet protection.

1.3. Defense in Depth Security Tools and Procedures

Effective security policies and procedures are the first step to a secure control systems network [5]. During the Global Corona Virus Pandemic, it is important for organizations to outline in detail how they will protect their data from network intrusions. The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic [4]. During times when people are working from home or learning from home using authentication and encryption is the most effective way to secure wireless networks.

A well-defined and well implemented defense in depth strategy prevents a wide variety of attacks and generates real-time intrusion alarms to the administrators [8]. Network Intrusion Detection Systems NIDS can tell network security managers when their network is being attacked and steps necessary to prevent the attack. There are several common methods for monitoring a network for unusual or unauthorized activity, with one of the most effective being Intrusion Detection Systems (IDS) [5]. Illegal access to systems can be monitored and blocked by several devices before intruders could steal data.

Network Security Situation Awareness (NSSA) is a new notion deriving from Air Traffic Control (ATC) [20]. Knowing where the attacks are occurring is an important step in stopping an attack. Ensure that Software is up-to-date, systems are appropriately configured on its network, and access is appropriately controlled [3]. Software must be properly patched to prevent zero-day attacks.

Informing personnel of their responsibilities when it comes to cybersecurity is an important step in implementing and enforcing policies and procedures [2]. Employee training and an effective security awareness campaign are critical to a successful cybersecurity program for example security necessary to maintain confidentiality of corona virus vaccine labs. The next generation cyberspace intrusion detection systems will fuse data from heterogeneous distributed network sensors to create cyberspace situational awareness, and analogized cyberspace situational awareness with ATC [20]. Sensors can be deployed to spot phishing attacks occurring at confidentiality corona virus vaccine labs phishing attacks.

Over time, there have developed two key practices for this assessment: tabletop exercises and penetration tests [3]. Security managers should use these tools to assess their networks to ensure they are effective at preventing breaches such as phishing attacks which are designed to steal passwords. Specific tool fingerprinting and operating system detection can be used to profile attacker activities, skill level and motivations [21]. What an attacker is trying to achieve during social distancing remote sessions can be viewed in real time.

To maintain confidential transmission, existing systems typically employ cryptographic techniques for preventing eavesdroppers from intercepting data transmissions between legitimate users [1]. The defense in depth measure encryption can help stop man-in-the-middle attackers from disrupting and intercepting Internet communications. If the message is not encrypted, or encrypted

with a weak algorithm, the attacker can read it, thereby compromising confidentiality [4]. Authentication and encryption are critical to wireless network security especially while working from home and learning from home.

Situational awareness was defined by Endsley as "the perception of the elements in the environment with a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" [20]. Two factor authentication can be used to deter an attacker for a limited amount of time. At the point that the authentication expires the user should reauthenticate. This intelligence is vital for initiating appropriate responses and for law enforcement investigations [21]. Cybersecurity forensics can benefit by capturing this data.

Penetration tests are live fire exercises in which White Hat Hackers' perform as threat actors and are tasked with attempting to infiltrate the target network, access the target systems [3]. White hat hackers are hackers hired by the organization to identify system security weaknesses which might possibly disrupt social distancing remote access activities. Network situation elements consist of Internet/Intranet (environment), entities in the network including software and hardware, network security events including alerts, logs and files, correlation team and network intrusion behavior [20]. The status of the entire must be known to prevent intrusions such as DOS attacks.

Anomaly based intrusion detection systems, but care must be taken to avoid overwhelming the human operator [21]. Network intrusion detection systems must take the limitations of the security manager into consideration. White hat hackers can retrieve a sample of target data to prove that network defense is ineffective, thus locating a route that should be remediated [3]. Using this tool, network security managers can fix network security issues before they cause real security problems.

The long-term goal is to create a library of visual signatures that can be used by the expert or novice analysts to detect malicious activity [21]. Corona Virus test results can be protected when security managers share the collected attacker profiles. Due to the external nature of the penetration tests, they tend to be expensive to execute and are typically undertaken infrequently (usually once or twice a year) [3]. Unfortunately pen testing is too costly and disruptive and therefore not frequently conducted.

NSSA fuses data from tools of IDS, VDS (Virus Detection System), Firewall, Netflow etc., to find what happens in the network [20]. Data is collected from several points to see for example when a Man in the middle attack is attacking the network. There are a wide variety of potential visualizations that can be used to display network traffic data in a way that is meaningful for security analysis [21]. Network security managers can see Trojans that are placed on the network from several different views. In addition, they usually stop at the first successful breach, resulting in a single Successful breach log and one or more failed breach attempts [3]. Pen testing is unlikely to discover a vulnerability which can be ex-

ploited by an advanced persistent attack (APT) for example man in the middle attacks. These type attacks put working from home remote access at risk.

In the MAC layer, the MAC address of a user should be authenticated to prevent unauthorized access [1]. To prevent hackers from entering the network, security managers should use MAC authentication. Training is a core component of an overarching security awareness program [5]. Because of social distancing requirements network security training for administrators and users may have to be carried out remotely.

Vulnerability scanning is not a passive operation, and as such can produce real-world failures that can impact operations inside of the organization [3]. Scanning should be done during non or low operational maintenance periods so that it does not disrupt normal organizational network functions. Interception and alteration of wireless transmissions represent a form of "man-in-the-middle" attack [4]. Encryption can stop a man-in-the-middle attacker from viewing the content of the data that he has managed to steal especially during times when people are working from home and learning from home.

To secure networks, the DiD model must be viewed as a system of systems and updated with current network defense strategies [10]. Latest Encryption algorithms allow systems to securely communicate together with lower risk of privacy or data loss. The open communications environment makes wireless transmissions more vulnerable than wired communications to malicious attacks [1]. Using a wired network is safer than using a wireless one.

In the network layer, the WPA and theWPA2 are two commonly used network-layer authentication protocols [1]. Authentication is a critical part of defense in depth. Firewalls, for blocking access from or to unwanted locations to or from the defended networks; Intrusion Detection Systems (IDS), for detecting suspicious traffic on the defended networks [3]. During the Global Corona Virus Pandemic these devices are critical in protecting remote connections.

The control center receives security events from each element to preprocess and save them in a database before transferring to situation analysis [20]. Once security data is analyzed; it can be uploaded to create UpToDate antivirus files. Security measures such as Demilitarized Zones (DMZ), firewall, Intrusion Detection System (IDS), Malware Protection and Virtual Private Networks (VPNs) provide defense in depth strategy that deflect information security attacks aim to gain unauthorized access to an organization assets from the internet or public network [8]. Along with other measures such as antivirus these defensive measures are critical for stopping attacks from the Internet.

New advances in cloud computing allow for users to rapidly scale provisioned computing resources to consume DoS and DDoS attacks [10]. Network intrusion can be severely limited by placing resources in the cloud. Network segmentation has traditionally been accomplished by using multiple routers. Firewalls should be used to create DMZs to protect the control network [5]. To stop malware such as trojans, firewalls should be used to create protected zones within

the network.

One problem with tabletop exercises is that they test the theoretical function of the systems under test, not the actual function [3]. Penetration test (pentest) can be used in lieu of tabletop exercises to locate system vulnerabilities which hackers may try to exploit or sniff Corona Virus test results. Systems such as firewalls, IDSs and IPSs are still used, but layered with new devices that provide different new capabilities to the network defense system [10]. Corona Virus test results and privacy loss can be prevented with both traditional and new devices.

Each of these devices acts as obstacle to the attacker [8]. Trojans can be stopped by using successive defensive barriers. Defense to stop the threat actors at the earliest point in the attack, and to provide the earliest warning of the presence of threat actors attempting to access a defended network [3]. While learning from home network security managers try to stop an attacker as far away from user data as possible. Preferably before they gain access to the network.

Current network defenses are designed around the features of specific network defense tools, such as identifying malware, blocking packets, or analyzing network events [10]. Two-factor Authentication is designed to stop unauthorized network Intrusion. Malware is very prevalent in operating systems that typically run on laptops, desktops, and server hardware platforms [2]. Security managers should ensure that all device firmware updates are installed from a trusted source.

1.4. Network Security during the Global Corona Virus Pandemic

Defense in depth is an Information Assurance (IA) strategy developed by the National Security Agency (NSA) that involves multiple layers of defenses for networked electronic and systems security [10]. During the Global Corona Virus Pandemic hackers will have a large amount of time to try to break into systems. The layered approach is the best security strategy used to combat the hackers. The effectiveness of such a defense-in-depth is predicated upon the effectiveness of every layer of security [3]. Every barrier that can be thrown at the attacker must be deployed during the Pandemic.

Defense in depth can be considered a multilayer security approach that applies to existing substation environments and can be integrated into the planning and design phases of new substation projects [2]. Depth in depth should be a part of the planning process for infrastructure projects during the Global Corona Virus Pandemic. Security systems can also be misconfigured, unknowingly allowing an attacker access to sensitive systems or information [10]. Because of social distancing requirements security systems are more vulnerable to Internet attacks. Proper configuration of security devices becomes essential.

Currently, there is no uniform and general definition of network situation awareness [20]. During the Pandemic, situation awareness should be built to meet the needs of the organization. Network-centric operations are multidimen-

sional, layered and often virtual [18]. Network security managers can take advantage of the current virtual nature of network security during the Pandemic.

Based on a top-down analysis, we categorize the goals of potential attacks against the smart grid communication networks into three types: network availability, data integrity and information privacy [16]. If the electrical grid becomes unavailable during the Pandemic, this could cause significant disruption and potential loss of life. Applying defense-in-depth cybersecurity from the very beginning of the planning and design phases results in a robust and secure system that provides a reliable platform for future applications and improves the cybersecurity of existing implementations [2]. Cybersecurity defense in depth should be built into the initial network infrastructure to stop attacks during the Pandemic.

To adapt to the ever-changing threat profile of network attacks, the DiD model must be adapted to be symmetric and focus on new vectors for defense instead of authenticating, blocking, or analyzing all traffic [10]. The job of defense in depth is not only to serve as barrier but also to be responsive to different threats during the Global Corona Virus Pandemic. Classical intrusion detection systems working symbiotically with a visualization-enhanced human will outperform algorithmic systems operating alone [21]. During the Global Corona Virus Pandemic network security managers can use software to help them identify DOS attacks.

Online Vulnerability Scanning provides for testing of specific known vulnerabilities against equipment visible and accessible from the network [3]. Password sniffing attacks vulnerabilities can be closed through security scanning. Firewalls provide additional levels of defense that support the traditional routers, providing the capability to add much tighter and more complex rules for communication between the different network segments or zones [5].

Several zones to include remote access, can be created during the Global Corona Virus Pandemic. These zones can be separated and protected by firewalls. Strong authentication schemes are required for customers and electronic devices to ensure communications with full security [16]. The data transfer between smart grid components and users can be protected with the latest encryption combined with authentication.

1.5. Network Security for Online Learning

The importance of training and educating users about secure wireless behavior cannot be overstated [4]. During these times of working from home, distance learning and social distancing because of the Corona Virus, training users is critically important. Despite these practices, a steady stream of successful cyber-attacks still occurs, targeted toward organizations that spend millions of dollars pursuing each of these avenues [3]. Constant Network security tool improvement and employee training is needed to stem the steady flow of hackers. This training must continue from home during the pandemic.

While great progress has been made, there exists an unacceptable rate of false positives and false negatives in such systems [21]. There is still a lot of work to be done around intrusion detection, while we learn from home connections may not be completely safe. Dynamic defenses must also be enabled, which change attack surfaces to proactively defend a network [10]. While learning from home network defenses must be innovative enough so that they can prevent attacks before they start.

To be effective, user training and education needs to be repeated periodically [4]. The network security manager because of the Global Corona Virus Pandemic should ensure that users and administrators receive training periodically so that their security skills are not diminished. Due to the wide variety of mechanisms that can be used by a threat actor to attack a network, many defensive devices have been created to block or monitor these mechanisms [3]. School network security managers can deploy several tools, *i.e.* firewalls and NIDS while students are learning from home.

Network situation indicates the whole network current status and its changing trend according to some factors of running status of network facilities, network and user behavior, etc. [20]. Because of social distancing requirements the network security boundary must reach out to the location of the remote user. New dynamic resource tools, such as cloud computing, can also be used to absorb attacks, preventing standard Denial-of-Service (DoS) attacks from being effective [10]. Because of social distancing requirements remote meeting software such as Zoom or Cisco WebEx has moved parts of network security to the cloud.

If any layer has no holes, it can keep back the intrusion [3]. Attacks, for example spam can be stopped during social media sessions if tools function properly. Visual intrusion detection systems can effectively supplement traditional signature [21]. Normal attacker profiles can be enhanced to protect systems while learning from home.

Defense in depth offers the administrators more opportunities for information and resources control, as well as introducing cascading countermeasures that will not necessarily impede business functionality [5]. Learning from home will not be disrupted while the security manager has several tools to protect the system. If any of the defensive devices are ineffective or misconfigured, it can create an opening sufficient for the threat actor to successfully attack the target network, access the target system(s) and reach the target data [3]. Online learning connections can be disrupted if DOS attacks enter and are not stopped by network security tools such as a properly configured firewall.

1.6. Network Security for Working from Home

Multi-network integration strategies often lead to vulnerabilities that greatly reduce the security of an organization and can expose mission-critical control systems to cyber threats [5]. Current work from home requirements has introduced additional cyber threats into the networks caused by accessing the network from

different geographical locations. Intrusion Detection System (IDS) helps information systems to deal with attacks [22]. Because of social distancing requirements remote connections are vulnerable to man in the middle intrusion attacks.

Threat actors conspire with users who have legitimate access to the target network or target devices or systems [3]. Colleagues may give hackers personal information while social distancing which could be used during a phishing attack. Companies need to address the security challenges of datacenter using a comprehensive defense-in-depth strategy [19].

Because of social distancing requirements remote access to sensitive organizational data requires focused security.

To make the administrators understand the alerts and network situation and take appropriate actions, security situation analysis of network is needed [20]. Network security managers should interpret and translate social distancing security data so that it is understandable for other network personnel. Human analysts can visually identify network attacks even if they do not exactly match the precise signatures or statistical anomalies of past attacks [21]. Remote attacks may be identified by the security manager if they are missed my IDS when remote connections are used while employees are working from home.

The transport-layer authentication includes the SSL and its successor, namely the TLS protocols [1]. For users that use the Internet because of the need to social distance, transport layer authentication is a necessity. There are numerous combinations of these mechanisms which can be used to access, exfiltrate, modify, or destroy data on target systems [3]. While working from home always use VPNs and encryption to protect systems and data.

The smart grid, generally referred to as the next-generation power electric system, relies on robust communication networks to provide efficient, secure, and reliable information delivery between power generators, suppliers, and customers [16]. The power grid relies on a computer network that is generally owned and operated by utility companies. If they are disrupted, they could disrupt, working from home, distance learning and other social distancing requirements. Control networks have evolved from stand-alone islands to interconnected networks that co-exist with corporate IT environments, introducing security threats [5]. The need to social distance and to have corporate oversight has forced control systems from an environment of isolation into one of interconnectivity.

Defense in depth promotes the idea that a layered approach to datacenter security makes for a formidable challenge for attackers to circumvent and/or compromise networks and their systems [19]. While working from home extra security is necessary to protect organizational data. Much like the layers of an onion, if there is one opening in each layer, it can be permeated, and a liquid will locate any opening in a layer [3]. Network intrusions can occur if one tool in the defense in depth protection fails while we work from home.

To fully support a defense-in-depth strategy, a robust incident response capa-

bility is required [5]. Organizations should develop an emergency response team to quickly deal with security breaches for example Trojans. By refocusing the DiD model on capabilities important for network defense instead of features, network defense can be advanced and improved [10]. While working from home security should be focused on man in the middle attacks and refitted with encryption and two-factor authentication.

By having an internal security team walk through the threat Scenario(s), they attempt to locate holes in how the systems will work to defend them [3]. Vulnerability assessment software can be used to block attacks before they occur. Network managers can conduct these assessments while employees work from home. Denial-of-service (DoS) attacks attempt to delay, block or corrupt information transmission to make network resources unavailable to nodes that need information exchange in the smart grid [16]. Hackers can potentially sniff or phish passwords to gain access to the smart grid network. Working from home would cease to exist until the situation is rectified.

1.7. Network Security of Corona Virus Vaccine Labs

Classical algorithmic intrusion detection systems (IDS) rely upon machine-detected signatures and statistical anomalies to discover intrusions [21]. Confidentiality corona virus vaccine labs can be protected with algorithms that can detect SQL injection attacks. To maintain an adequate defense-in-depth, a target organization (also described as a target entity) should take measures to maintain each of its defensive devices in accordance with best practices [3]. Authentication and encryption tools can be properly sustained to ensure that corona virus vaccine labs are not compromised.

Potential networking intrusion caused by intentional attackers may lead to a variety of consequences, from customers' information leakage to a cascade of failures, such as massive power outage and destruction of infrastructures [16]. Corona virus vaccine labs could be delayed or disabled by trojans that invade the network. Exploits due to programming errors are not as common in security tools as in common applications, but still occur [10]. The proper configuration of defense measures is critical to corona virus vaccine labs confidentiality.

They are less likely to discover patterns or more general, pervasive security holes in a system [3]. Trojans exploit vulnerabilities may be discovered which could affect corona virus vaccine labs. In many cases, the individuals administering a control system network may not have adequate security training [5]. Network security managers in corona virus vaccine labs must be adequately trained in the latest security best practices.

It will be easy for gateway or firewall software to perform traffic control on information flows in smart grid to block undesired or even suspicious flows generated by malicious nodes [16]. Constant data flow is critical to smart grid networks that host Corona vaccine labs. To advance the current DiD model, a functional DiD model should be focused on the capabilities of symmetry and

dynamic defenses [10]. Confidentiality of corona virus vaccine labs can be protected against DOS attacks with coordinated and flexible defenses.

1.8. Network Security for Corona Virus Test Results

Threat actors can gain access to credentials for normal or privileged access to the target devices or systems on the target network [3]. Corona test results can be illegally accessed if a hacker steals the credentials on the server which stores the results. In many sectors the malicious attack on the control system will have real-world, physical results [5]. Lab results may be manipulated or stolen by hackers illegally accessing the network.

By bringing humans more directly into the intrusion detection loop, correct visualizations can tap into the high bandwidth visual recognition capabilities of the human cognitive system and help address the serious problem of false positives and false negatives that exists today [21]. A loss of privacy in Corona Virus test results can possibly be prevented when a network security manager inspects and analyzes IDS data for false results. Implementing the concept of symmetry into the DiD model allows for each network to provide inbound and outbound security, preventing unknowingly compromised systems from being used as attack relays [10]. The validity of Corona Virus test results should be protected from attacks coming into the network from the outside as well as inside attacks.

The attacks are usually caused by a failure to implement security policies and failure of using of security tools that are readily available [22]. A simple vulnerability that was overlooked should not be allowed to compromise Corona Virus test results. There are correlations in time and space between events occurring on each entity [20]. Corona Virus test results may be infiltrated in the lab or during the test result reporting phase.

In the modern IT environment, information and its associated technologies are exposed to a wide range of security risks, including data leakage, disruption and denial of services resulting in negative impact on business continuity [8]. The protection of Corona Virus test results could involve several defense measures including employee training and antivirus.

New vectors, such as dynamic network addressing, enterprise computing resources, and network architectures, must be used by the DiD model to prevent attacks from reaching network, consuming attackers often limited resources, and securing networks in their design and architecture [10]. Networks should be built on defense in depth when protecting Corona Virus test results.

2. Theoretical/Conceptual Framework

2.1. Linear Regression Theory

Regression analysis answers questions about the dependence of a response variable on one or more predictors [9]. The question of reducing the dependent variable (security threats) is dependent on the independent variable (network security tools). These statistical concepts are illustrated by using a data set from

published literature to assess a computed tomography– guided interventional technique [13]. The methods used in this study consisted of scanning 20 peer reviewed Cybersecurity Articles from prominent Cybersecurity Journals for a list of defense in depth measures (tools and procedures) and the threats that those measures were designed to reduce. The methods also involve using the Likert Scale Model to create an ordinal ranking of the measures and threats (see Table 2).

The values of the parameters were determined in the following manner. The weights were determined by how many times a threat was listed by a cyber security journal, for example network intrusions were listed 16 times for a weigh of 16 ($16 \times 16 = 256$) total. The prioritization was determined by how many times the independent variables (tools and procedures) were listed as reducing the dependent variable (threat) in the articles. This number was then multiplied by weight, for example network intrusion detection system (NIDS) was listed as reducing network intrusions 4 times ($4 \times 16 = 64$).

Table 2. Security measures and threats ordinal ranking.

	Network Security Threats Dependent Variables (multiplied by weight)									
Security Tools & Procedures Independent Variables	**Sniffing Attacks**	**DOS Attacks**	**MitM Attacks**	**Data Theft**	**Phishing Attacks**	**Trojans**	**Stolen Passwords**	**Hacking**	**Privacy Loss**	**Network Intrusions**
Weight	**3**	**5**	**5**	**5**	**6**	**7**	**7**	**12**	**12**	**16**
Averages	**3**	**6.25**	**6.25**	**6.25**	**7.2**	**8.17**	**9.8**	**14.4**	**18**	**32**
Use NIDS		5						12		64
Use Firewalls		5			6	7	14	12	12	64
Use NIPS										16
Use 2F Authentication		5	5	5	6	14		12	12	
Use Anti-DOS										
Use Digital Certificates					6	7	7	24	12	16
Use Hashing Algorithm	3		5	5				12		
Use Encryption	3	10	10	10	6	7		24	60	
Use SIEM								12		
Train Employees					6	7	14		12	32
Apply Patches							7	12		16
Use Whitelist	3		5							
Stenography									12	
Use Remote Access Server										16
Backup files				5				12		
Use Permission Controls									12	
Use Antivirus					6	7	7	12	12	32
Totals	**9**	**25**	**25**	**25**	**36**	**49**	**49**	**144**	**144**	**256**

The estimation of linear mapping is further formulated as a prediction problem with a regression-based solution [11]. Organizational network security managers can make security predictions based on the linear regression process. We can draw graphs that will generally allow us to see relationships between variables and decide whether the models we are using make any sense [9]. The relationship between reduced security threats and security tools can be drawn in a graph to make sure that the security tools can reduce the threats that they are designed to reduce.

The purpose of correlation analysis is to measure and interpret the strength of a linear or nonlinear (e.g., exponential, polynomial, and logistic) relationship between two continuous variables [13]. This research represents a linear relationship between defense in depth measures independent variables and associated network security threats dependent variables (see **Figure 1**).

Analyses between two variables may focus on 1) any association between the variables, 2) the value of one variable in predicting the other, and 3) the amount of agreement [13]. For example, firewalls show a strong association with network intrusions. The presence of a firewall can predict the reduction of the intrusion threat and to what extent that threat can be reduced.

In some problems, a theory may be available that specifies how the response varies as the values of the predictors change [9]. The network security tools will change in response to security threat changes as outlined in this Linear Regression Theory. It is a fair assumption that a systematic approach should be taken in the deployment of information assurance measures.

2.2. Linear Regression Multiple Criteria Decision Making (MCDM)

Since it normally involves more than one criterion, the task of algorithm selection can be modeled as multiple criteria decision making (MCDM) problems [23]. Securing networks normally involve more than one criterion, *i.e.* it can involve

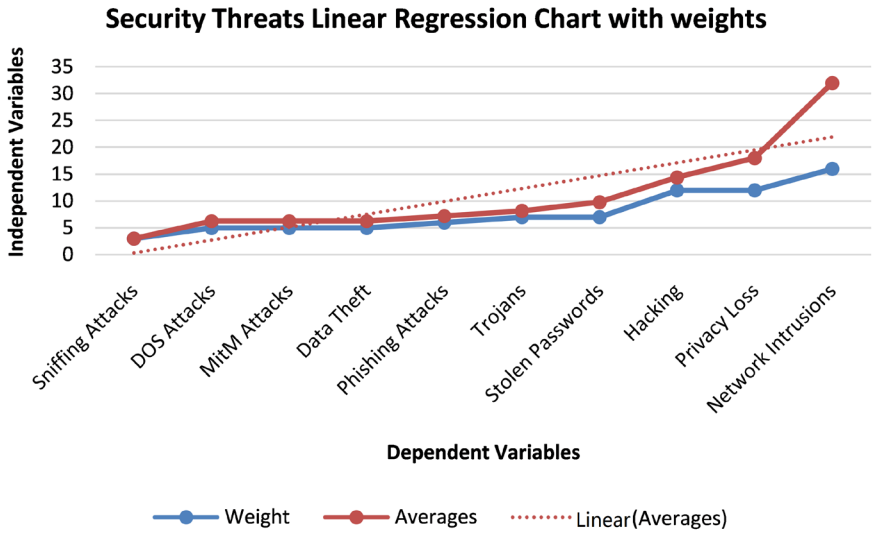

Figure 1. Security threats linear regression chart with weights.

preventing intrusions, data theft or sniffing. Network security issues are multiple criteria decision making (MCDM) problems. When conducting correlation analysis, we use the term association to mean "linear association" [13]. There is a linear association between protecting organizational networks and the deployment of defense in depth security measures.

2.3. Analytic Network Process (ANP) and other Current Analytical Methods

Problems are often characterized by interdependent criteria and dimensions and may even exhibit feedback-like effects [24]. Defense in the depth security tools IS layered together interdependently and adds weight to the network defense. Different MCDM methods evaluate classifiers from different aspects and thus they may produce divergent rankings of classifiers [23]. Different MCDM methods must be examined closely to ensure that they address the network security issues that the network security manager is trying to solve.

Relatively good solutions from the existing alternatives are replaced by aspiration levels to fit today's competitive markets [24]. The network security aspirations of the security manager can be met by tailoring and layering defense in depth security measures.

For example, when the value of the predictor is manipulated (increased or decreased) by a fixed amount, the outcome variable changes proportionally (linearly) [13]. When a network security manager is faced with a potentially increasing amount of MitM attacks (predictor) for example, the defense in depth variable of two-factor authentication can be deployed on the network to proportionally decrease the threat.

The evaluation criteria are seldom independent, and the relationships between them are frequently characterized by a degree of interactivity, interdependence, and feedback effects [24]. A feedback loop is created when network security linear regression criteria *i.e.* encryption and authentication interact together and form interdependencies. An approach to resolve disagreements among MCDM methods is based on Spearman's rank correlation coefficient [23]. Network security managers can use different ways to understand and choose different MCDM criteria.

Saaty (1996) proposed using the Analytic Network Process (ANP), which relaxes the hierarchical structure restriction [24]. Deploying the necessary security tool to meet network security aspirations adds flexibility to the tiered approach to network security. The purpose of simple regression analysis is to evaluate the relative impact of a predictor variable on a particular outcome [13]. The reduction of the data theft variable for example can be predicted based on the deployment of the encryption variable.

Five MCDM methods are examined using 17 classification algorithms and 10 performance criteria over 11 public-domain binary classification datasets in the experimental study [23]. Different MCDM methods can be chosen to meet the network security threats that the network security manager faces. Two questions

related to the ANP model warrant attention: how to generate the influential network relationship and how to evaluate the degree of influence [24]. The defense in depth model allows the network security manager to build relationships between security tools, having one or more tools influence the other tools.

Two major threats to wireless client devices are 1) loss or theft, and 2) compromise [4]. Encryption, two factor authentication and file backup are useful in preventing data loss and theft. The decision maker sets an aspiration level as the benchmark [24]. The network security manager and other organizations staff members should decide on the organizational network security goals, *i.e.* no network intrusions.

The experimental results prove that the proposed approach can resolve conflicting MCDM rankings and reach an agreement among different MCDM method [23]. The best solution becomes apparent once an in-depth analysis is made on the MCDM approaches.

The rankings of classifiers are quite different at first [23]. At the beginning of the MCDM analysis process it may not be clear which criteria is best suited to address the network security needs.

In a multivariate linear regression model, the output is modeled as a function of independent variables [25]. Network security tools *i.e.* encryption, two factor authentication and digital signatures make up the independent variables in this multivariate linear regression model. The data for 10 panels (out of a total of 12 collected panels) were applied to develop a linear regression model based on **Table 2** [25]. The null hypothesis states that the underlying linear correlation has a hypothesized value, 0 [13]. According to this study the chance that the linear regression of network security threats will not influence organizational network security is null.

After applying a decision approach, the differences among MCDM rankings are largely reduced [23]. The network security manager can make a defense in depth deployment decisions based on the results of the MCDM analysis. It is worth noting that even if two variables (e.g., cigarette smoking and lung cancer) are highly correlated, it is not sufficient proof of causation [13]. Although the firewall independent variable is highly correlated with the intrusion dependent variable; there is no guarantee that a firewall will always cause a reduction in intrusions. This study shows using linear regression analysis, that there is a combined relationship between security tools and measures variables and an inverse relationship with the variable—security threat.

3. Methodology

3.1. Research Design

This experimental survey research design was used to survey a simple random sample frame of 20 peer reviewed information security research articles. The peer reviewed information security research articles were scanned for a list of ten network security tools and procedures.

The ordinal ranking was done using a Likert scale instrument with a (1 - 10) prioritization of the tools and procedures listed most frequently in the peer reviewed articles. Below is a Flow chart of the Research Design.

Step 1. Find 20 peer review articles that deal with the subject of cyber security

Step 2. List those dependent variables (threats) and independent variables (tools and procedures designed to reduce those threats.

Step 3. Using the Likert Scale, prioritize the variables according to how many times they were listed together in the articles.

Step 4. Using linear regression analysis, determine if there is a pattern of how often threats are listed with tools and procedures.

3.2. Data Analysis

The data analysis was conducted using a Likert Scale, with a (1 - 10) prioritization of 10 network security tools and procedures and linear regression analysis to conduct a pair-wise comparison of each of the ten tools and procedures to their ability to reduce threats to network security. Decision-makers will understand the gaps between each alternative and the aspiration level [24]. Using linear regression based on aspirations, the network security manager can see how one defense in depth security measure can cover a gap that another measure fails to cover. The research methods used in the study provided the advantage of using statistics to make inferences about larger groups, using very small samples, referred to as generalizability [26]. The findings are presented in the results section. The process used to analyze the data involved listing how often the independent variables were reported as reducing the dependent variables. This could imply a correlation between the independent and dependent variables. The variables were then prioritized (ranked) and listed on a Linear Regression Scale to identify any possible correlations between the independent and dependent variables.

4. Results

The purpose of this chapter is to present the analysis which rejects the H_0 null hypothesis that linear regression analysis does not affect the relationship between the prioritization and combining of 20 Cybersecurity Article's defense in depth tools and procedures (independent variables) and cyber threats (dependent variables). Preferential independence can be described as the preferential outcome of one criterion over another that is not influenced by the remaining criteria [24]. Encryption can be seen in a network security linear regression analysis as the preferred security tool for preventing privacy loss.

Data collected before the analysis in this experiment shows a lack of combining security measures and tools to combat specific security threats. The data capture (recording) and coding methodology employed in this study was used to determine the best defense-in-depth choices from a list of decision alternatives (network security threats). Finally, a summary of the results is included in this

chapter.

5. Investigative Questions

The study design included one investigative question which provided foundation for the main research questions. This section lists the investigative question and includes the statistical analysis to explore the question.

Investigative Question 1

Of the ten network security tools and procedures, prioritize them according to their prioritization from 20 Network Security Articles. Linear regression analysis was then used to array network threats to defense in depth measures. Network security issues for example, viruses, spam and phishing attacks can be graphically displayed using linear regression diagrams.

They can depict the key elements, including decisions, uncertainties, and objectives as nodes of various shapes and colors. The effects of using security tools such as antivirus and procedures such as pen testing can be shown in a linear fashion.

6. Discussion

The current agenda of prioritizing and combining defense in depth measures can continue to evolve based on this investigation. Defense in depth is an effective method of mitigation and prevention of automatic attacks that an organization faces from public internet [8]. Two-factor Authentication can help to prevent Internet attacks password sniffing for example.

Two types of countermeasures can significantly reduce the risk of such attacks: strong encryption and strong authentication of both devices and users [4]. It is imperative that network security managers because of the Global Corona Virus Pandemic, to deploy strong encryption and authentication on their wireless network as a part of their defense in depth approach. Defense in depth takes a holistic approach to network security, protecting the network from several different perspectives with both tools and procedures.

It is of importance to increase the secrecy capacity by exploiting sophisticated signal processing techniques, such as the artificial-noise-aided security [1]. While working from home user communications must remain private to protect personal and organizational information. The new concept has decision makers setting an aspiration level, though it may not be reachable using current resources, or simply redesigning the decision space [24]. Defense in depth allows the security manager to be creative in security tool deployment so that he can successfully achieve his security goals.

Secure communications should satisfy the requirements of authenticity, confidentiality, integrity, and availability (CIA) [1]. The goal of defense in depth security is to protect CIA. Communications are also vulnerable to denial-of-service (DoS) attacks [4].

Firewalls and NIDS should also be included in the wireless network defense in depth deployment to prevent DOS attacks.

7. Conclusions

The research concluded that linear regression analysis can play a role in the organization's decision process to arraying and combining defense in depth measures against network threats. If an eavesdropper lies in the transmit coverage area of the source node, the wireless communications session can be overheard by the eavesdropper [1]. Like how spies operate, eavesdroppers (sniffers) can easily intercept wireless communications. A combination of both security procedures and security tools plays an important role in defense in depth.

An aspiration level could be attained by expanding employees' competence set (e.g., training) or adding or changing new resources (e.g., through strategy alliance, innovation, or creativity) to expand the original decision space [24]. Both administrator and user employee training are critical in achieving network security goals and objectives. To maintain confidential transmission, typically cryptographic techniques relying on secret keys are adopted for preventing eavesdropping attacks from intercepting the data transmission [1].

To help meet social distancing requirements, encryption should be used to prevent intruders from tapping into private communications.

Differing from the Internet, the smart grid has only two major directional information flows: bottom-up and top-down [16]. Because of the vertical nature of smart grid communications, redundant communication paths are required to enhance communications. Hackers collect data on different systems; the information collected is analyzed for possible security problems [22]. During the Global Corona Virus Pandemic stopping this reconnaissance is the first step in preventing an attack.

Organizations can take several steps to reduce the risk of such unintentional DoS attacks [4]. Encryption and authentication are two of the many measures that should be taken to prevent both intentional and unintentional DoS attacks. Building interrelationships (dependence and feedback) among criteria and improvement of criteria in general is used to achieve the aspiration level [24]. Deploying defense in depth analytically can help to build the synergy between security tools necessary to achieve organizational security goals.

Fructification of each layer of model presents a vast variety of implementation alternatives and adoptability according to the design and architecture of organization [8].

Each organization will deploy a different variation of defense in depth During the Global Corona Virus Pandemic. A malicious node in wireless networks can readily generate intentional interference for disrupting the data communications between legitimate users, which is referred to as a jamming attack (also known as DoS attack) [1]. Innocent conversations, both business and pleasure can be interrupted by interference.

The smart grid must have the ability to detect the attempt of an intruder to gain unauthorized access to computer systems [16]. Network intrusion detection systems can identify malware that has gained access to the smart grid. Insecure, poorly configured wireless access points can compromise confidentiality by allowing unauthorized access to the network [4]. Network administrators during the Global Corona Virus Pandemic should be professionally trained on wireless network security when implementing wireless networks.

The available published knowledge of linear regression analysis can be used to prioritize defense in depth measures against network threats. This is confirmed by the research conclusion.

Defense in depth decision making can be deployed using BNM to enhance organizational IT security. To make the security policy effective, it must be practical and enforceable, and it must be possible to comply with the policy [5]. Organizations must develop effective network security plans to protect corona virus test results. These plans should be strictly enforced.

Defense in depth and linear regression analysis can be an important asset to the organization. Further advances can be gained in the use of defense in depth by continuing linear regression analysis. The decision space may be modified to achieve aspiration level of the objective space in changeable space situations [24]. The security of portable devices is changing the network security decision space, and defense in depth tools must adapt to meet those changes.

To better understand the role that linear regression analysis can play in IT security this research proposed a linear regression analysis structural and measurement model of the relevant factors. The future of IT security should include additional exploratory models to advance understanding of why the current models are not substantially improving IT security. To understand the shortcoming of current IT security models, further exploratory studies should be conducted on additional models.

Declarations

1) Ethical Considerations

The potential benefits of research in organizations, especially public safety organizations, can be greatly beneficial, but there are risks that some employees or the organization could be unfairly stigmatized. This study was conducted with the informed consent of all the participants.

The participants were not subjected to risk. To avoid conflict of interest, the survey participants are in no way related to the researcher.

2) Consent for Publication

For specifically addressing autonomous agency, the design included an informed consent process to ensure that participation was voluntary, with adequate information provided to participants to make their decision of whether or not to participate [27]. Specifically addressing diminished autonomy, while ensuring extra protection is afforded to prevent harm from exclusion.

Availability of Data and Material

All datasets on which the conclusions of the manuscript rely will be deposited in publicly available repositories (where available and appropriate) supporting files, in machine-readable format (such as spreadsheets rather than PDFs).

Funding

There was no outside funding for this article

Authors' Contributions

Rodney Alexander is the sole author of this article

Acknowledgements

University of Phoenix Dissertation Mentor.

Conflicts of Interest

The author has no financial and non-financial competing interests.

References

[1] Zou, Y.L., Zhu, J., Wang, X.B. and Hanzo, L. (2016) A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, **104**, 1727-1765.

[2] Ewing, C. (2010) Engineering Defense-in-Depth Cybersecurity for the Modern Substation. *Proceedings of the* 12*th Annual Western Power Delivery Automation Conference*, Spokane.

[3] Carey, M.J. and Paulsen, G.B. (2017) System and Method for Simulating Network Security Threats and Assessing Network Security. US Patent Application No. 14/837,033.

[4] Choi, M.K., Robles, R.J., Hong, C.H. and Kim, T.H. (2008) Wireless network security: Vulnerabilities, Threats and Countermeasures. *International Journal of Multimedia and Ubiquitous Engineering*, **3**, 77-86.

[5] Fabro, M. (2007) Control Systems Cyber Security: Defense-in-Depth Strategies (No. INL/CON-07-12804). Idaho National Laboratory (INL), Idaho Falls.

[6] Cleghorn, L. (2013) Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth. *Journal of Information Security*, **4**, 144-149. https://doi.org/10.4236/jis.2013.43017

[7] Rathore, S., Sharma, P.K., Loia, V., Jeong, Y.S. and Park, J.H. (2017) Social Network Security: Issues, Challenges, Threats, and Solutions. *Information Sciences*, **421**, 43-69. https://doi.org/10.1016/j.ins.2017.08.063

[8] Goztepe, K., Kilic, R. and Kayaalp, A. (2014) Cyber Defense in Depth: Designing Cyber Security Agency Organization for Turkey. *Journal of Naval Science and Engineering*, **10**, 1-24.

[9] Weisberg, S. (2005) Applied Linear Regression. John Wiley & Sons, Hoboken. https://doi.org/10.1002/0471704091

[10] Groat, S., Tront, J. and Marchany, R. (2012) Advancing the Defense in Depth Model. 2012 7*th International Conference on System of Systems Engineering* (*SoSE*),

Genova, 16-19 July 2012, 285-290. https://doi.org/10.1109/SYSoSE.2012.6384127

[11] Naseem, I., Togneri, R. and Bennamoun, M. (2010) Linear Regression for Face Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, **32**, 2106-2112. https://doi.org/10.1109/TPAMI.2010.128

[12] Meier, K.J., Favero, N. and Zhu, L. (2015) Performance Gaps and Managerial Decisions: A Bayesian Decision Theory of Managerial Action. *Journal of Public Administration Research and Theory*, **25**, 1221-1246. https://doi.org/10.1093/jopart/muu054

[13] Zou, K.H., Tuncali, K. and Silverman, S.G. (2003) Correlation and Simple Linear Regression. *Radiology*, **227**, 617-628. https://doi.org/10.1148/radiol.2273011499

[14] Haddawy, P. (1999) An Overview of Some Recent Developments in Bayesian Problem-Solving Techniques. *AI Magazine*, **20**, 11.

[15] Schneier, B. (2006) Security in the Cloud. *Blog Post.* http://www.schneier.com/blog/archives/2006/02/security_in_the.html

[16] Lu, Z., Lu, X., Wang, W.Y. and Wang, C. (2010) Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid. 2010—*Milcom* 2010 *Military Communications Conference*, San Jose, 31 October-3 November 2010, 1830-1835. https://doi.org/10.4304/jnw.4.7.552-564

[17] Nilsson, D.K. and Larson, U. (2009) A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure. *Journal of Networks*, **4**, 552-564.

[18] Bass, T. and Robichaux, R. (2001) Defense-in-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations. 2001 *MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force* (Cat. No. 01*CH*37277), **1**, 64-70.

[19] El-Khameesy, N. and Mohamed, H.A.R. (2013) A Proposed Model for Datacenter in Depth Defense to Enhance Continual Security. *International Journal of Information Technology and Computer Science*, **5**, 55-67. https://doi.org/10.5815/ijitcs.2013.04.07

[20] Mixia, L., Qiuyu, Z., Hong, Z. and Dongmei, Y. (2008) Network Security Situation Assessment Based on Data Fusion. 1*st International Workshop on Knowledge Discovery and Data Mining* (*WKDD* 2008), Adelaide, 23-24 January 2008, 542-545. https://doi.org/10.1109/WKDD.2008.35

[21] Conti, G. and Abdullah, K. (2004) Passive Visual Fingerprinting of Network Attack Tools. *Proceedings of the* 2004 *ACM Workshop on Visualization and data mining for Computer Security*, Washington DC, October 2004, 45-54. https://doi.org/10.1145/1029208.1029216

[22] Kaur, T., Malhotra, V. and Singh, D. (2014) Comparison of Network Security Tools-Firewall, Intrusion Detection System and Honeypot. *International Journal of Enhanced Research in Science Technology and Engineering*, **3**, 200-204.

[23] Kou, G., Lu, Y., Peng, Y. and Shi, Y. (2012) Evaluation of Classification Algorithms Using MCDM and Rank Correlation. *International Journal of Information Technology & Decision Making*, **11**, 197-225. https://doi.org/10.1142/S0219622012500095

[24] Liou, J.J. and Tzeng, G.H. (2012) Comments on "Multiple Criteria Decision Making (MCDM) Methods in Economics: An Overview". *Technological and Economic Development of Economy*, **18**, 672-695. https://doi.org/10.3846/20294913.2012.753489

[25] Mohammadi, S., Ataei, M., Khaloo Kakaie, R. and Mirzaghorbanali, A. (2018) Prediction of the Main Caving Span in Longwall Mining Using Fuzzy MCDM Tech-

nique and Statistical Method. *Journal of Mining and Environment*, **9**, 717-726.

[26] Cooper, C.R. and Schindler, P.S. (2008) Business Research Methods. 10th Edition, McGraw-Hill, Boston.

[27] National Commission for the Protection of Human Subjects (1979) Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research. Department of Health and Welfare, Washington DC.

[28] Chen, P., Desmet, L. and Huygens, C. (2014) A Study on Advanced Persistent Threats. In: De Decker, B. and Zúquete, A., Eds., *Communications and Multimedia Security*, *CMS* 2014, *Lecture Notes in Computer Science*, Springer, Berlin, 63-72.

[29] Dictionary, M.W. (2015) An Encyclopedia Britannica Company. http://www.merriam-webster.com/dictionary

[30] Singh, A. and Bora, M.S. (2013) Cyber Threats and Security for Wireless Devices. *JECET*, **2**, 277-284. https://doi.org/10.2139/ssrn.3419703

[31] Rouse, M. (2007) Defense in Depth. http://searchsecurity.techtarget.com/definition/defense-in-depth

[32] Cobb, M. (2014) Firewall. http://searchsecurity.techtarget.com/definition/firewall

[33] Cole, B. (2014) Intrusion Detection System. http://searchcompliance.techtarget.com/definition/intrusion-detection-systems-IDS

[34] Mallik, A., Ahsan, A., Shahadat, M. and Tsou, J. (2019) Man-in-the-Middle-Attack: Understanding in Simple Words. *International Journal of Data and Network Science*, **3**, 77-92. https://doi.org/10.5267/j.ijdns.2019.1.001

[35] Merriam-Webster. (n.d.) Public-Key. In Merriam-Webster.com Dictionary. https://www.merriam-webster.com/dictionary/public-key

[36] Pavlyushchik, M.A. (2014) System and Method for Detecting Malicious Code Executed by Virtual Machine. US Patent No. 8713631. U.S. Patent and Trademark Office, Washington DC.

List of Abbreviations

***Advanced Persistent Threat* (*APT*).** "An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)" [28].

***Biometrics*.** "The measurement and analysis of unique physical or behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity" [29].

***Botnets*.** "A botnet is a group of compromised computers under the control of an attacker" [30].

***Defense in-depth*.** "Defense in-depth is the coordinated use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier" [31].

***Denial of service* (*DOS*).** "A denial of service attack is an attempt by multiple attackers to make a service unavailable to its users" [32].

***Firewall*.** "A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules" [32].

***Hash Algorithm* (*Hash*).** "An encryption algorithm *set* of rules by which information or messages are encoded so that unauthorized persons cannot read them" [29].

***Intrusion detection system*.** Host intrusion detection systems and network intrusion detection systems are methods of security management for computers and networks [33].

***Man-in-the-middle attack* (*MitM*).** "A kind of cyberattack where an unapproved outsider enters into an online correspondence between two users, remains escaped the two parties. The malware that is in the middle-attack often monitors and changes individual/classified information that was just realized by the two users" [34].

***Password*.** "A password is an un-spaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user" [30].

***Public Key Infrastructure* (*PKI*).** "A cryptographic element that is the publicly shared half of an encryption code and that can be used only to encode messages" [35].

***Phishing*.** "Phishing is the combined use of fraudulent e-mails and legitimate looking websites by cyber criminals in order to gain user credentials" [30].

***Social Engineering*.** "Social engineering refers to psychological manipulation of people into accomplishing goals that may or may not be in the target's best interest. In cyber-attacks, it is often used for obtaining sensitive information, or getting the target to take certain action (e.g. executing malware)" [28].

Spam. "Spam is the use of e-mail technology to flood mailboxes with unsolicited messages" [30].

SQL injection attacks. "These consist of attacks against web applications with the aim of extracting data or stealing credentials or taking control of the targeted web server" [30].

Watering Hole Attacks. "The concept of a watering hole attack is similar to a predator waiting at a watering hole in a desert, as the predator knows that the victims will have to come to the watering hole. Similarly, rather than actively sending malicious emails, the attackers can identify 3rd party websites that are frequently visited by the targeted persons, and then try to infect one or more of these websites with malware" [28].

Worms/Trojans. "Worms and malicious programs have the ability to replicate and redistribute themselves by exploiting the vulnerabilities of their target systems" [30].

Zero-day Attacks. "*Z*ero-day vulnerabilities, *i.e.*, threats that use an error or a vulnerability in the application or the operating system and arise immediately after the vulnerability is found, but before the relevant upgrade is issued" [36].