Scientific Research Publishing

Journal of Information Security, 2020, 11, 92-102
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Using the Latin Square Design Model in the Prioritzation of Network Security Threats: A Quantitative Study

Rodney Alexander

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

How to cite this paper: Alexander, R. (2020) Using the Latin Square Design Model in the Prioritzation of Network Security Threats: A Quantitative Study. *Journal of Information Security*, **11**, 92-102.
https://doi.org/10.4236/jis.2020.112006

Received: March 16, 2020
Accepted: April 19, 2020
Published: April 22, 2020

Abstract

Society is becoming increasingly dependent on cyberspace for both business and pleasure. Cyber attackers continue to attack organizational computer networks, as those same computer networks become increasing critical to organizational business process. Strategic planning and managing IT security risks play an important role in the business and government planning process. Deploying defense in depth security measures can ensure that organizations continue to function in times of crisis. This quantitative study explores whether the Latin Square Design (LSD) model can be effectively applied to the prioritization of cybersecurity threats and to the linking of information assurance defense in-depth measures to those threats. The methods used in this study consisted of scanning 10 Cybersecurity Websites such as the Department of Homeland Security US CERT (United States-Computer Emergency Readiness Team [1]) and the SANS Institute (SysAdmin, Audit, Network and Security [2]) using the Likert Scale Model for the Website's top ten list of cyber threats facing organizations and the network defense in depth measures to fight those threats. A comparison of each cybersecurity threats was then made using LSD to determine whether the Likert scale and the LSD model could be effectively applied to prioritize information assurance measures to protect organizational computing devices. The findings of the research reject the H_0 null hypothesis that LSD does not affect the relationship between the ranking of 10 Cybersecurity websites top ten cybersecurity threats dependent variables and the independent variables of defense in depth measures used in protecting organizational devices against cyber-attacks.

Keywords

Information Assurance, Latin Square Design Model, Defense in Depth, Information Technology, Network Security, Cybersecurity

1. Introduction

Organizational computing devices such as desktops, notebooks, and smart phones continue to become targets of cyber-attacks. The threat of attack by computer viruses is in reality a very small part of a much more general threat, specifically threats aimed at subverting computer security [3]. The computer networks security can be undermined by malicious threats if they can enter the network.

Defense in Depth is an information security practice adapted from a military defense strategy where an attacker is forced to overcome a great many obstacles that eventually expend the attacker's resources [4]. A network attacker can be forced to exhaust his or her tools and energy on a labyrinth of threat mitigation measures. Developed countries have begun to accept cyber space as a fifth operational domain after land, sea, air and space [5]. The importance of cyberspace has increased significantly.

Information technology (IT) has evolved into its own industry with global networks of interconnectivity, such as the Internet. Layers of defense often overlap in order to ensure that traffic is processed multiple times by heterogeneous security technologies in hopes that the shortcomings of one security control are covered by another [4]. One layered network security measure covers the weaknesses of another layered measure.

New threats appear on the Internet daily, which presents a constant security challenge for organizations. Cyber security experts claim that cyber warfare takes place all around us with [5]. The omnipresence of cyber criminals cannot be avoided when using the Internet today.

The defense in depth architecture is adapting lethargically to this new category of threats [5]. These new types of threats can be mitigated using defense in depth. Defense in depth is a tried and proven method of preventing automated attacks and many attacks with an active attacker participating in the intrusion [4].

The purpose of defense in depth approach is to maintain a system against any particular attack using several independent methods [5]. Several cyber security measures can be layered together to form a defense in depth to prevent cyber-attacks. Security measures such as firewalls, intrusion detection systems (IDS) and password policies continue to evolve.

Defense in depth is a tool which is only as useful as the administrators using it [5]. The person using defense in depth measures must be trained in how to effectively use them. Attacks can be performed by: countries, political, adversaries, terrorists, industrial spies, hacktivists, hackers, resentful and unconscious users [5].

There are many malicious individuals and groups whose purpose is to disrupt legitimate Internet traffic. In a scenario where an attacker is actively attempting to gain access from the internet, a defense in depth strategy will deflect the attack, assuming that security measures like Network Address Translation (NAT), a firewall, a Demilitarized Zone (DMZ), and gateway Intrusion Detection System (IDS) are in place [4]. Risks which come with Internet connectivity can be

mitigated by layering these devices.

This research study explores whether the Latin Square Design (LSD) Model can be effectively applied to the array of information assurance defense in-depth measures to mitigate network security threats. Here, computer viruses are examined as a malicious logic in a research and development environment [3]. This research experiment focuses on prioritizing network threats and the mitigation of those threats. Scholar-practitioners may be interested in this research because, according to [6], cyber threats pose a significant risk to economic and national security.

Cybersecurity experts, and both government and business leaders have recognized that cyber threats pose a threat to national security. A well-tuned defense in depth architecture will prevent a vast majority of attacks and alert an administrator to intrusions that pass through [4].

The organization will be alerted if a network attack is able to navigate the defense labyrinth in a well-organized defense in depth structure.

The key differences between this work and existing related studies are that this research aligns security threats with mitigation tools to defeat those threats as well as prioritization. Other related studies focused only on threat prioritization. This study also concentrated on using the Latin Square Design Model in the defense in-depth decision-making process. While other related studies considered alternative models.

Theoretical/Conceptual Framework

A relation is drawn between the viruses and various models of security and integrity [3].

Threat prioritization from 10 well-known security websites and mitigation measures are investigated using the Likert Scale and the Latin Square Design (LSD) experimental model. **Table 1** lists the prioritization of threats to computer networks.

Table 1. Top ten threat prioritization.

Priority	Threat
1	Trojan Horse
2	Computer Virus
3	Worms
4	Malware
5	Adware
6	DOS Attacks
7	SQL Injection
8	Spyware
9	Phishing Attacks
10	Ransomware

Current research techniques aimed at controlling the threats posed to computer systems by threatening viruses in particular and malicious logic in general are examined [3]. This research investigates the prioritization of computer threats and specifically tools to stop or reduce those threats. A brief examination of the vulnerabilities of research and development systems that malicious logic and computer viruses may exploit is undertaken [3]. Organizations should study weaknesses in their networks to understand where the attackers are most likely to strike.

Latin Square Design Model

The name "Latin square" was inspired by mathematical papers by Leonhard Euler (1707-1783), who used Latin characters as symbols [7]. A Latin square is a table filled with n different symbols in such a way that each symbol occurs exactly once in each row and exactly once in each column [7]. The n value in each column remains the same regardless of how the table is arranged.

Orthogonal Array Representation

If each entry of an Latin square is written as a triple (r, c, s), where r is the row, c is the column, and s is the symbol, we obtain a set of triples called the n $n \times 2$ n orthogonal array representation of the square [7]. The threat ranking and mitigation tools are listed in rows and columns. How often those tools are listed to mitigate those threats are listed as symbols in the squares.

Equivalence Classes of Latin Squares

A Latin square design is a method of placing treatments so that they appear in a balanced fashion within a square block or field. Treatments appear once in each row and column [7]. Each threat mitigation appears in a square aligned with a network threat. Replicates are also included in this design [7].

The Latin Square Design model also allows for duplicate treatments of a square, a null or 0 treatment for example. In the case of this experiment, the examined website did not list a specific mitigation to counter a specific threat. A Latin square is called diagonal if all elements in both its main diagonal and main antidiagonal are distinct [8].

A set of Latin squares is called mutually orthogonal or pairwise orthogonal if each Latin square in the set is pairwise orthogonal to all other Latin squares of the set [9]. The threat and mitigation elements in the main and antidiagonal square are different. Experiments are considered for main effects plans where we use 2 and 3 factors [10]. The two factors of computer network threats and mitigation tools designed to lessen their impact are used in this experiment.

Latin squares are elementary combinatorial objects that have been studied for a long time [11]. Experiment design techniques have included Latin Squares for several years. Informally, a Latin square is an $n \times n$ grid, where each cell is filled with a number in $\{1, \ldots, n\}$ and each number occurs exactly once in every row and every column [11].

In this design the computer network threats and the number of mitigations

that appeared in the investigated websites are listed in each row and column. The outstanding problem has been (and still is) the determination of the maximum number $N(t)$ of pairwise orthogonal Latin squares of order t [12]. How to prioritize network threats and how to link mitigations to reduce those threats is an ongoing concern for organizations.

In the design of experiments, Latin squares are a special case of row-column designs for two blocking factors: [13]. The best method to describe the theoretical/conceptual framework is to picture the variable interaction using visualization. The framework for this study is the Latin Square Design (LSD) model (Table 2).

Many operations on a Latin square produce another Latin square (for example, turning it upside down) [7]. Table 3 presents the interaction between LSD theory, information assurance, and resource inputs and outcomes. In Table 3 threats are listed in rows and their associated mitigations are listed in columns.

If we permute the rows, permute the columns, and permute the names of the symbols of a Latin square, we obtain a new Latin square said to be isotopic to the first [7]. The two figures should match exactly. Table 4 is an isotopic (exact match) of Table 3 although the rows and columns are reversed. In Table 4, the mitigations are listed in rows and the threats are listed in columns.

The study's theoretical/conceptual framework, shown in Table 3 and Table 4,

Table 2. 3 × 3 Latin square design model example.

	Example		
	Factor 1 (Columns)		
	1	2	3
Factor 2 (Rows)	2	3	1
	3	1	2

Table 3. 10 × 10 Information assurance Latin square table.

Threats	Mitigation Tools									
	Anti-virus	Anti-spyware	Spam Filters	Firewalls	IDS	Password Policy	Educate Employees	Anti-DOS	Load Balancers	Web Filters
1. Trojan Horse	1	1	0	1	1	1	0	0	0	0
2. Virus	4	0	0	3	2	2	0	0	0	0
3. Worms	1	1	0	0	0	0	0	0	0	0
4. Malware	1	0	0	0	0	0	0	0	0	0
5. Adware	2	1	0	0	0	0	0	0	0	0
6. DOS Attacks	0	0	0	0	0	0	0	1	1	0
7. SQL Injection	0	0	0	0	0	0	0	0	0	1
8. Spyware	0	2	1	0	0	0	0	0	0	0
9. Phishing Attacks	0	0	1	0	0	0	2	0	0	0
10. Ransomware	0	0	1	0	0	0	0	0	0	0

Table 4. 10 × 10 Latin square isotopic table.

Mitigation Tools	Threats									
	Trojan Horse	Virus	Worms	Malware	Adware	DOS Attacks	SQL Injection	Spyware	Phishing Attacks	Ransomware
Anti-virus	1	4	1	1	2	0	0	0	0	0
Anti-spyware	1	0	1	0	1	0	0	2	0	0
Spam Filters	0	0	0	0	0	0	0	1	1	1
Firewalls	1	3	0	0	0	0	0	0	0	0
IDS	1	2	0	0	0	0	0	0	0	0
Password Policy	1	2	0	0	0	0	0	0	0	0
Educate Employees	0	0	0	0	0	0	0	0	2	0
Anti-DOS	0	0	0	0	0	1	0	0	0	0
Load Balancers	0	0	0	0	0	1	0	0	0	0
Web Filters	0	0	0	0	0	0	1	0	0	0

Note. $p = (n \times n)$.

identifies how information assurance variables can be matched with security threats. One of the most thoroughly investigated branches of combinatorics is the theory of Latin squares [8]. The Latin Square Design model is commonly used to investigate the combination of two or more factors.

When people use the term "defense in depth" to discuss the proper implementation of information security, they are not referring to the use of four firewalls in a row [14]. Defense in depth does not mean using the same protective measures repeatedly. A Latin square is an n x n table filled with n different symbols in such a way that each symbol occurs exactly once in each row and exactly once in each column. Here are two examples.

2. Results

The purpose of this chapter is to present the analysis which rejects the H_0 null hypothesis that LSD does not affect the relationship between the prioritization of ten defense in-depth dependent variables and the ten independent threat variables. 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.

Investigative Question

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

Of the ten network security threats, prioritize them according to their prioritiza-

tion on ten well-known network security websites. A Latin square was then used to array network threats to defense in depth measures. Table 3 and Table 4 is a square table $N\,x\,N$ in which all elements are distinct.

A Latin square of order N is a square table $N \times N$ filled with elements from some finite set of size N in such a way, that all elements within a single row or single column are distinct [8].

Specific mitigation elements are arrayed to counter specific threat elements in this Latin Square Design. The results in the information assurance table (Table 3) and the isotopic table (Table 4) show that each threat square is pairwise orthogonal to a defense in depth security measure.

3. Discussion

The knowledge gained from this investigation can help in the prioritization of information assurance defense in-depth and in the evolution of the existing frameworks. Effective (best) practices exist but are underused at organizational, sector, national, and international levels [15]. Organizations can improve the deployment of their network security measures by using a defense in depth strategy.

Qualitative and quantitative metrics inform decisions, test hypotheses, and forecast future states [15]. Quantitative analysis such as the Latin Squares Design model can assist organizational decision-makers in effectively deploying network security measures. Defense in depth is a superb method of minimizing and preventing automated attacks, considering automated attacks seek out the most vulnerable assets facing the public Internet [5].

Attackers use scripts and BOTS to look for the weakest links that they can find on the Internet. Defense in Depth can help to defeat those scripts and BOTS. Trojan horses were listed as the most serious threat to networks and anti-virus, anti-spyware, IDS and organizational password policy can be arrayed against these types of network attacks. Additionally, computer virus was listed as second most serious, with anti-virus, firewalls, IDS and password policy arrayed to stop this threat.

4. Conclusions

The research concluded that the LSD model process can play a role in the organization's decision process to array defense in depth measures against network threats. The Internet threats are malicious software programs like spyware, adware, trojan horse, bots, viruses and worms, etc. which are set up on the system devoid of our information or we can say without any authorization [16]. These threats function on computer networks without permission or approval.

Organization network decision making process can be further advanced by additional network security research. With the increase of mobile devices and the implementation of the concept of "internet of things", human beings began to live entirely in a cyber-world besides physical world [7]. Today, the Internet plays a major role in our everyday lives. Defense in depth concept has emerged

as a model to isolate key resources with protective layers [5].

A layered security blanket can be placed around critical information infrastructure to protect them from cyber criminals. The available published knowledge of LSD 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 LSD to enhance organizational IT security. Defense in depth and LSD can be an important asset to the organization. Further advances can be gained in the use of defense in depth by continuing LSD research.

To better understand the role that LSD can play in IT security, this research proposed an LSD 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.

5. Methodology

5.1. Research Design

This non-experimental survey research design was used to survey a simple random sample frame of ten well-known network security websites. The well-known network security websites were scanned for a list of ten network security threats. The prioritization was done using a Likert scale instrument with a (1 - 10) prioritization of the threats listed most frequently on the well-known sites.

5.2. Data Analysis

The data analysis was conducted using a Likert Scale, with a (1 - 10) prioritization of 10 network security threats and the LSD model to conduct a pair-wise combination of each of the ten threats to 10 defense in depth measures. 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 [17]. The findings are presented in the results section.

6. Declarations

6.1. Ethical Considerations

The potential benefits of research in organizations, especially public safety organizations, can be very 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.

6.2. 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 [18]. Specifically addressing diminished autonomy, while ensuring extra protection is afforded to prevent harm from exclusion, the design used a web-based online survey methodology with potential participants included from a compiled database of IT security professionals.

6.3. List of Abbreviations

Botnets. "A botnet is a group of compromised computers under the control of an attacker" [19].

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" [20].

Denial of service (DOS). "A denial of service attack is an attempt by multiple attackers to make a service unavailable to its users" [19].

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" [21].

Intrusion detection system. Host intrusion detection systems and network intrusion detection systems are methods of security management for computers and networks [22].

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" [23].

Phishing. "Phishing is the combined use of fraudulent e-mails and legitimate looking websites by cyber criminals in order to gain user credentials" [19].

Rogueware/scareware. "Rogueware deliberately imitates the graphical user interface and branding of established legitimate antivirus or anti Spyware programs (in some cases even copying the designs or logos)" [19].

Spam. "Spam is the use of e-mail technology to flood mailboxes with unsolicited messages" [19].

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" [19].

Worms/Trojans. "Worms and malicious programs have the ability to replicate and redistribute themselves by exploiting the vulnerabilities of their target systems" [19].

7. 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).

Acknowledgements

Capella University Dissertation Committee.

Funding

There was no outside funding for this article.

Authors' Contributions

Rodney Alexander is the sole author of this article.

Authors' Information

Hello, my name is Rodney Alexander (Rod). Previously, Computer Network Analyst-Trainer at Hutchinson Community College. I have been a DoD Civilian Employee for the last 21 Years, completing the vast majority of my service with the Army in Germany. My last assignment was as a system analyst for the Dept. of Defense (DoD) Joint Interoperability Test Command (JITC) at Ft Huachuca, AZ.

Recently I taught online for Anthem College. I received both my Doctorate and Masters in Information Systems/Management from the University of Phoenix. I received my Bachelors Degree, 20 years ago in Criminal Justice from the University of Washington in Seattle. After completing my degree, I became an Army Officer in the Military Police Corps, where I served for nine years.

My hobbies are listening to Jazz Music and taking long quiet walks. I am single (never married). I currently live in Tucson AZ and work at the Army Base Ft Huachuca, AZ. My goals for attending the PhD program are to significantly improve my knowledge of information system organizations and increase my analytical skills.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Department of Homeland Security US CERT. https://www.us-cert.gov/sites/default/files/publications/RisksOfPortableDevices.pdf

[2] SANS Institute. https://www.sans.org/blog/wasc-web-hacking-incident-database-semi-annual-report/

[3] Bishop, M. (1991) An Overview of Computer Viruses in a Research Environment.

[4] 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

[5] 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.

[6] Biesecker, C. (2010) DHS IG Finds Adequate Cybersecurity Controls but More Needed. *Defense Daily*, **247**, 8.

[7] Gaio, L. (2005) Latin Squares in Experimental Design. Michigan State University, East Lansing.

[8] Vatutin, E., Zaikin, O., Kochemazov, S. and Valyaev, S. (2017) Using Volunteer Computing to Study Some Features of Diagonal Latin Squares. *Open Engineering*, **7**, 453-460. https://doi.org/10.1515/eng-2017-0052

[9] Raghavarao, D. (1988) Constructions and Combinatorial Problems in Design of Experiments. Corrected Reprint of the 1971 Wiley ed., Dover, New York.

[10] Pasles, E.B. (2004) Mutually Nearly Orthogonal Latin Squares and Their Applications. Doctoral Dissertation, Temple University, Philadelphia.

[11] Hajirasouliha, I., Jowhari, H., Kumar, R. and Sundaram, R. (2007) On Completing Latin Squares. In: *Annual Symposium on Theoretical Aspects of Computer Science*, Springer, Berlin, Heidelberg, 524-535. https://doi.org/10.1007/978-3-540-70918-3_45

[12] Jungnickel, D. (1980) On Difference Matrices and Regular Latin Squares. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, **50**, 219-231. https://doi.org/10.1007/BF02941430

[13] Bailey, R.A. (2008) 6 Row-Column Designs and 9 More about Latin Squares. In: *Design of Comparative Experiments*, Cambridge University Press, Cambridge.

[14] Riggs, C. (2004) Network Perimeter Security: Building Defense In-Depth. Auerbach Publications, New York. https://doi.org/10.1201/9780203508046

[15] Hathaway, M. (2014) Best Practices in Computer Network Defense: Incident Detection and Response. https://ebookcentral-proquest-com.library.capella.edu

[16] Bhola, S., Kaur, S. and Kumar, G. (2015) Internet Threats and Prevention—A Brief Review. *IJCA Proceedings on International Conference on Advancements in Engineering and Technology*, August 2015, No. 10, 13-17.

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

[18] 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.

[19] 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

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

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

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

[23] Rouse, M. (2007) Password. http://searchsecurity.techtarget.com/definition/password